

Từ điển AN TOÀN THÔNG TIN

ANH - VIỆT VÀ VIỆT - ANH

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT



ENGLISH - VIETNAMESE AND VIETNAMESE - ENGLISH DICTIONARY OF

INFORMATION SECURITY

TỪ ĐIỂN
AN TOÀN THÔNG TIN
ANH - VIỆT và VIỆT- ANH

English - Vietnamese and Vietnamese - English dictionary of INFORMATION SECURITY

(about 5000 terms, with explanations and illustrations)

6T1–6T1.3
KHKT–2001 123-348, 16/5/2001

SCIENCE AND TECHNICS PUBLISHING HOUSE
HANOI - 2001

BAN TỪ ĐIỂN
NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

TỪ ĐIỂN AN TOÀN THÔNG TIN ANH - VIỆT VÀ VIỆT- ANH

(Khoảng 5000 thuật ngữ, có giải thích và minh họa)

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT
HÀ NỘI - 2001

Biên soạn

Nguyễn Nam Hải

Nguyễn Phương Mai

Ninh Ngọc Nghĩa

Nguyễn Ngọc

Trịnh Văn Quyết

Đặng Văn Sử

Biên tập

Trần Hòa

Đặng Văn Sử

Vũ Trung Thành

LỜI NÓI ĐẦU

Cuốn "TỪ ĐIỂN AN TOÀN THÔNG TIN ANH - VIỆT VÀ VIỆT- ANH" này do Ban từ điển của Nhà xuất bản Khoa học và Kỹ thuật tổ chức biên soạn dựa trên những từ điển giải thích tiếng Anh mới nhất và những từ điển chuyên ngành và đa ngành gần đây của Nhà xuất bản Khoa học và Kỹ thuật.

Từ điển gồm khoảng 5000 thuật ngữ đề cập tới những chủ đề chủ yếu: phân tích rủi ro, các chuẩn, an toàn dữ liệu, an toàn mạng, máy tính cá nhân, quản lý khóa, virut, hệ tin cậy, vấn đề xác thực, kiểm soát truy nhập và một số chủ đề có liên quan khác phản ánh tình hình phát triển hiện thời trong lĩnh vực này.

Mỗi thuật ngữ tiếng Anh ngoài phần đối chiếu tiếng Việt còn kèm theo phần giải thích bằng tiếng Việt. Ở một số mục từ có hình để minh họa thêm cho chính văn. Thuật ngữ đối chiếu tiếng Việt được biên soạn theo nguyên tắc ngắn gọn, rõ nghĩa, cố gắng Việt hóa tới mức tối đa. Những thuật ngữ phiên chuyển được phiên vừa gần dạng tiếng Anh vừa đọc được theo chính tả tiếng Việt. Phần Việt - Anh chỉ có thuật ngữ đối chiếu để bạn đọc tham khảo khi dịch tài liệu từ tiếng Việt sang tiếng Anh.

Cuốn từ điển này dành cho các cán bộ giảng dạy, nghiên cứu, sinh viên và tất cả những ai quan tâm tới lĩnh vực này.

Mặc dù đã rất cố gắng nhưng do thông tin trong lĩnh vực còn mới mẻ này khá lớn nên không tránh khỏi sai sót. Chúng tôi trân trọng mọi ý kiến đóng góp của bạn đọc để giúp cho lần tái bản sau tốt hơn. Thư từ góp ý xin gửi về: Ban từ điển, Nhà xuất bản Khoa học và Kỹ thuật, 70 Trần Hưng Đạo, Hà Nội.

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

CÁCH SỬ DỤNG

1. Cách sắp xếp phần Anh - Việt

Các mục từ tiếng Anh được in đậm, xếp theo bảng chữ cái tiếng Anh. Các gián cách từ, dấu gạch nối, dấu phẩy, dấu chéo xuôi (/), dấu chỉ sở hữu (') không tính đến trong sắp xếp.

2. Tham khảo chéo

Tham khảo chéo trong từ điển này thể hiện bằng các từ "*xem*", "*so sánh với*" và "*đồng nghĩa với*". Các chữ viết tắt và ký hiệu cũng được tham khảo chéo tới mục từ chính.

3. Phần đối chiếu tiếng Việt

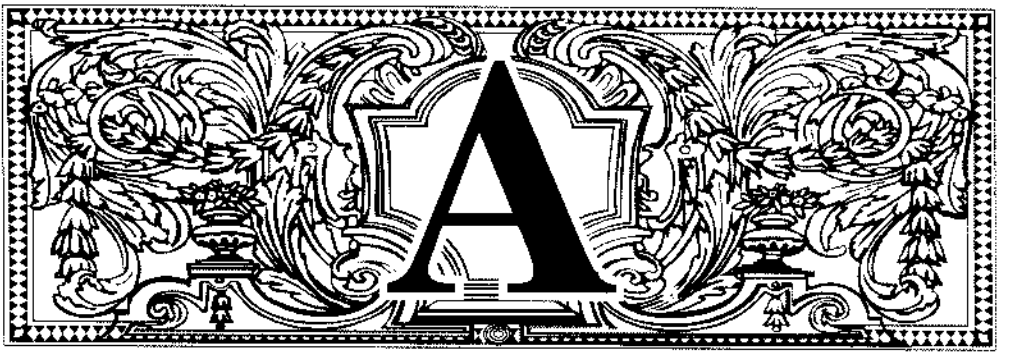
Các thuật ngữ đối chiếu tiếng Việt được in đậm nghiêng, đồng nghĩa cách nhau bằng dấu phẩy (,), khác nghĩa cách nhau bằng dấu chấm phẩy (;). Các thuật ngữ có phạm trù ngữ pháp khác nhau được tách ra bằng dấu chéo song song (//).

4. Phần tiếng Việt giải thích

Thuật ngữ có các định nghĩa khác nhau ở các lĩnh vực khác nhau được đánh số thứ tự như mục con.

5. Phần Việt - Anh

Các mục từ tiếng Việt xếp theo thứ tự chữ cái tiếng Việt thông thường, có thêm f, j, w, z và theo thứ tự dấu giọng: không dấu, huyền, hỏi, ngã, sắc, nặng. Đơn vị để xếp là từng khối viết liền, đơn tiết hoặc đa tiết.



A1 *Xem* Division A.

A & A *Xem* advice and assessment.

aborted connection ***hủy nối kết*** Trong an toàn truyền thông, sự ngắt mạch không tuân theo những quy trình đã thiết lập. Điều đó có thể ngẫu nhiên xảy ra do nối điện thoại kém, nhưng thường là do khi người sử dụng "ngừng" mà không cố phát ra các lệnh ngắt.

absolute rate ***suất tin tuyệt đối*** Trong lý thuyết thông tin, số cực đại các bit thông tin có thể được mã hóa trong mỗi ký tự với giả thiết tất cả các dãy khả dĩ đều hợp lệ như nhau. Nếu một ngôn ngữ bao gồm C ký tự và mỗi ký tự có xác suất xuất hiện như nhau trong một dãy thông báo bất kỳ thì suất tin tuyệt đối của ngôn ngữ có thể là $\lg_2 C$. Trong các ngôn ngữ tự nhiên như tiếng Anh, suất tin thực của ngôn ngữ thấp hơn nhiều so với suất tin tuyệt đối bởi vì những ngôn ngữ như thế có mức độ dư thừa cao. *Xem* rate.

abstract data type ***kiểu dữ liệu trừu tượng*** Trong các cấu trúc dữ liệu, kiểu dữ liệu được định nghĩa duy nhất theo các phép toán vốn có thể được thực hiện trên các đối tượng thuộc kiểu đó và khoảng các giá trị mà nó có thể nhận, bất kể phương pháp biểu diễn giá trị là như thế nào. *Xem* type.

abstract syntax notation 1 ***ký pháp cú pháp trừu tượng 1*** Trong truyền thông dữ liệu, ký pháp do ISO đưa ra, có thể dùng để mô tả rất nhiều loại cấu trúc dữ liệu. Khi một hệ máy tính truyền một thông báo tới một hệ máy tính khác thì rất có thể là hai hệ sẽ có các biểu diễn đạt các bit tạo thành những trường khác nhau của thông báo theo cách riêng. Ký pháp dữ liệu trừu tượng chuẩn bị một định nghĩa chung về cấu trúc dữ liệu của thông báo. Máy tính gửi sẽ biến đổi cấu trúc dữ liệu

của nó thành dạng xác định bởi ký pháp cú pháp trừu tượng. Tương tự, máy tính nhận sẽ giải mã thông báo tới từ biểu diễn ký pháp dữ liệu trừu tượng thành khuôn cục bộ của nó. Quy trình này khiến cho các hệ không cần phải lưu giữ một sơ đồ mã hóa riêng cho mỗi hệ mà nó giao tiếp. *Xem* ISO.

AC *AC* Viết tắt của Authentication Code (mã xác thực). *Đồng nghĩa với* MAC.

acceptability principle ***nguyên lý khả chấp*** Trong an toàn dữ liệu, các biện pháp an toàn phải không được gây cản trở quá mức cho công việc của người sử dụng, nhưng tất nhiên cũng phải tuân thủ mọi ràng buộc cần thiết về an toàn. *Xem* principles of secure systems.

acceptable level of risk ***mức rủi ro chấp nhận được*** Trong quản lý rủi ro, mức đánh giá đúng đắn và được xem xét thận trọng bởi một Cơ quan phê duyệt được chỉ định (DAA) thích hợp theo đó, hoạt động hoặc mạng xử lý dữ liệu tự động (ADP) đáp ứng được những yêu cầu tối thiểu của các chỉ thị hướng dẫn an toàn có thể áp dụng. Đánh giá phải tính đến giá trị các tài sản ADP; các hiểm hoạ và những điểm dễ bị tổn thương; các biện pháp đối phó và hiệu quả của chúng trong việc bù lại những chỗ dễ bị tổn thương; và các yêu cầu vận hành. *Xem* ADP, DAA, risk, threat, vulnerability. *Đồng nghĩa với* acceptable risk.

acceptable risk ***rủi ro chấp nhận được*** Đồng nghĩa với acceptable level of risk.

acceptance ***nghiệm thu, chấp nhận*** Trong an toàn máy tính, chỉ một phương tiện hoặc hệ thống nói chung đáp ứng các tiêu chuẩn kỹ thuật và tính năng nhưng có thể có những ngoại lệ nhỏ khiến cho phương tiện không đáp ứng những yêu cầu về vận hành và an toàn.

acceptance inspection ***kiểm tra nghiệm thu*** Trong an toàn máy tính, sự kiểm tra cuối cùng để xác định xem một phương tiện hoặc hệ thống có đáp ứng những tiêu chuẩn xác định về kỹ thuật và tính năng hay không. Kiểm tra được tiến hành ngay sau khi thử phương tiện và phần mềm và là cơ sở để đặt mua hoặc chấp nhận một hệ thông tin. *Xem* acceptance.

acceptance testing ***thử nghiệm thu, thử chấp nhận*** Quy trình để đảm bảo rằng một hệ đáp ứng được các yêu cầu của người dùng. *Xem* acceptance.

access ***truy nhập, truy cập*** (1) Trong kiểm soát truy nhập, một kiểu tương tác riêng giữa chủ thể và đối tượng dẫn tới luồn thông tin chạy từ thực thể này sang thực thể khác. *Xem* object, subject. (2) Trong kiểm soát truy nhập, khả năng và phương tiện cần để tiếp cận, lưu giữ hoặc truy lục dữ liệu, để liên lạc với, hoặc sử dụng bất kỳ tài nguyên nào của một hệ ADP. *Xem* ADP, resource. (3) Trong tin học, phương cách để máy tính tham chiếu các tệp hoặc các tập dữ liệu. *Xem* data set, dicrect access, random access, sequential access. (4) Trong kiểm soát truy nhập, một kiểu tương tác riêng giữa một chủ thể (tức là người, quá trình hoặc thiết bị nhập) và một đối tượng (tức là một tài nguyên AIS như bản ghi, tệp, chương

trình, thiết bị xuất) dẫn tới luồng thông tin từ thực thể này tới thực thể kia. *Xem* AIS. (5) Trong an toàn vật lý, một chế độ hoặc một điều kiện ở thiết bị kiểm soát truy nhập cho phép nhập vào một vùng hạn chế; ở chế độ này không nhất thiết phải khử kích hoạt các bộ cảm biến và không có cảnh báo nào được kích hoạt.

access authorization ***(sự) cấp quyền truy nhập*** Trong kiểm soát truy nhập, sự được phép cấp cho một chủ thể, ví dụ như người, đầu cuối, chương trình thực hiện một tập hợp các thao tác trong hệ thống.

Những sự cấp quyền như thế thường được biểu thị trong một ma trận đặc quyền truy nhập cho biết những chi tiết về các chủ thể, các kiểu truy nhập, ví dụ như đọc, ghi và các thời khoảng được phép truy nhập. *Xem* access matrix model, subject.

access barred ***có chắn truy nhập*** Trong truyền thông dữ liệu, phương tiện dữ liệu cho phép một thiết bị đầu cuối tiến hành các cuộc gọi đi hoặc nhận các cuộc gọi tới chứ không phải cả hai.

access card ***thẻ truy nhập*** *Đồng nghĩa với* card key.

access category ***hạng truy nhập*** Trong kiểm soát truy nhập, một trong các lớp gán cho một người sử dụng, một chương trình hoặc một quá trình trong một hệ ADP trên cơ sở các tài nguyên hoặc nhóm tài nguyên mà mỗi người sử dụng chương trình hoặc quá trình được phép sử dụng. *Xem* ADP, resource.

access control ***kiểm soát truy nhập, kiểm truy*** (1) Trong an toàn máy tính và truyền thông, việc ngăn ngừa sự sử dụng trái phép một tài nguyên, kể cả ngăn ngừa sử dụng tài nguyên theo cách không được phép. (2) Ở các mạng máy tính, việc kiểm soát sử dụng hệ thống thông qua các điều khiển phần cứng, phần mềm và quản trị. Những sự kiểm soát như thế bao gồm giám sát hệ thống, nhận dạng người sử dụng, đảm bảo toàn vẹn dữ liệu, ghi lại sự truy nhập hệ thống, và những thay đổi và những phương pháp cấp quyền truy nhập cho người sử dụng. *Xem* hardware, software. (3) Trong an toàn cơ sở dữ liệu, việc kiểm soát sử dụng thông tin của cơ sở dữ liệu. Việc truy nhập của một người sử dụng riêng có thể bị hạn chế về cả các mục dữ liệu có sẵn lẫn theo các thao tác có thể thực hiện trên nó, ví dụ như đọc, cập nhật v.v.. (4) trong an toàn dữ liệu, việc giới hạn các quyền hoặc các khả năng của một chủ thể khi giao tiếp với những chủ thể khác, hoặc khi sử dụng các chức năng hoặc các dịch vụ trong một hệ hoặc mạng máy tính. (5) Trong an toàn dữ liệu, các hạn chế chi phối truy nhập của một chủ thể vào một đối tượng. *Xem* object, subject. (6) Trong an toàn thông tin, các chức năng kiểm soát luồng thông tin qua lại giữa những người sử dụng, các quá trình và các đối tượng và việc sử dụng các tài nguyên của chúng kể cả việc quản trị và xác minh các quyền truy nhập. *Xem* information technology security evaluation criteria. (7) Phương pháp truyền thống bảo vệ tài sản là giữ cho chúng khỏi bị những kẻ phạm pháp

tiềm tàng tấn công, nói cách khác là đảm bảo rằng, chỉ những người thực sự được phép mới có quyền truy nhập những tài sản đó.

Theo truyền thống thì kiểm soát truy nhập bao gồm kiểm soát truy nhập vật lý mà có thể được định nghĩa như "việc sử dụng các khóa, những người bảo vệ, những thẻ và những biện pháp hành chính tương tự để kiểm soát truy nhập vào máy tính và thiết bị liên quan."

Trong an toàn máy tính, nơi nào thường có thể truy nhập dữ liệu được lưu trữ từ một đầu cuối ở xa, hoặc qua các mạng truyền thông, thì sự kiểm soát truy nhập vật lý như vậy có thể không bảo vệ được dữ liệu lưu trữ. Kiểm soát truy nhập logic định nghĩa như "việc sử dụng các thủ tục liên quan tới thông tin và tri thức" thường hay được sử dụng hơn.

Các quá trình liên quan tới kiểm soát truy nhập

Các quá trình kiểm soát truy nhập có thể được liệt kê như sau:

- cấp phát các đặc quyền;
- quản lý các đặc quyền;
- định dạng và xác thực người sử dụng;
- giám sát truy nhập;
- giới hạn kiểu truy nhập;
- ngăn ngừa truy nhập không được phép;
- thu hồi đặc quyền truy nhập.

Cấp phát các đặc quyền

Quyết định quan trọng nhất là ai sẽ được cấp phép tiếp cận tài sản? Trong trường hợp an toàn máy tính, có thể có một tập hợp lớn những người sử dụng và vô số tài sản dữ liệu. Làm sao có thể ra quyết định là người sử dụng *A* có thể truy nhập tệp *C* và phải cấp dạng ưu tiên truy nhập nào, ví dụ như đọc, ghi, thực hiện?

Có hai cách tiếp cận, thứ nhất là gán một thuộc tính nào đó cho mỗi người sử dụng và mỗi tài sản dữ liệu, và sau đó xác định một tập hợp các quy tắc hệ thống rộng rãi liên quan tới kiểu truy nhập cấp cho thuộc tính người dùng đã cho: cặp tài sản dữ liệu - thuộc tính. Cách tiếp cận thứ hai đơn giản cho phép một người thực sự có uy tín nào đó ra quyết định rằng người sử dụng *A* được phép truy nhập kiểu *B* tới tài sản *C*.

Cách tiếp cận thứ nhất được gọi là kiểm soát truy nhập bắt buộc; nó tuân theo một tuyến đặc tả các thuộc tính người sử dụng và tài sản dữ liệu, gọi là các cấp an toàn. Sau đó đặt ra một tập hợp các quy tắc hệ thống rộng rãi, chúng quy định có hay không thể cấp một kiểu truy nhập cho một cặp (cấp an toàn sử dụng, cấp an toàn tài sản dữ liệu), rồi sau đó hệ thống kiểm soát truy nhập phải bắt buộc thi hành những quy tắc đó. Với dạng kiểm soát truy nhập này một thực thể thẩm quyền trung tâm có vai trò cấp phát các mức an toàn cho người sử dụng và tài sản dữ liệu.

Mặt khác, kiểm soát truy nhập tùy ý không có những quy tắc truy nhập phổ biến như thế; một quyết định tùy ý do một nhân vật có thẩm quyền nào đó đưa ra, cho phép hoặc từ chối một dạng truy nhập tới một tài sản cho một người sử dụng nào đó. Với một tập hợp lớn người sử dụng và tài sản, các

quyền cấp phép thường được ủy thác cho các chủ tài sản dữ liệu. Trong một số trường hợp, chủ tài sản dữ liệu cũng có thể dành các quyền cấp phép cho những người sử dụng khác, mặc dù trong những trường hợp đó không người sử dụng nào có thể trao quyền nhiều hơn quyền của bản thân họ.

Kiểm soát truy nhập bắt buộc nói chung được xem như quá thô sơ nên không thể sử dụng một mình nó và thường chỉ được sử dụng để lọc lựa các yêu cầu. Nếu truy nhập được cho phép theo các quy tắc kiểm soát truy nhập bắt buộc, thì cần gọi tới hệ truy nhập tùy ý. Sự kết hợp kiểm soát truy nhập bắt buộc và tùy ý như thế đảm bảo rằng, không chủ tài sản dữ liệu nào có thể tùy tiện quyết định giao những dữ liệu khá nhạy cảm cho một người nào đó được xem là không thích hợp đối với dữ liệu đó. Đồng thời, một người sử dụng với một cấp an toàn cao không được phép tự động truy nhập những tài liệu có cấp an toàn thấp hơn; người sử dụng phải chứng minh "nhu cầu cần biết" cho một người quản trị an toàn.

Quản lý các đặc quyền

Phải có những sự sắp đặt để thông báo cho người sử dụng biết những đặc quyền của họ và chuyển giao cho họ những phương tiện để thực hiện những đặc quyền đó. Phải đảm bảo rằng các đặc quyền được chuyển giao cho đúng người và không một người không được phép nào có cơ hội nhận được quyền tiếp cận những đặc quyền đó trong khi sắp xếp chuyển giao. Có thể cũng hợp lý nếu đảm bảo rằng những nơi nhận được phép biết được những trách nhiệm về an toàn của họ.

Định dạng và xác thực người sử dụng

Khi một người sử dụng bắt tay vào truy nhập một tài sản, sẽ có một cơ chế nhờ đó người sử dụng chứng minh quyền truy nhập đó. Trong các hệ thống an toàn máy tính thường có một quá trình hai giai đoạn; đầu tiên người sử dụng khai danh tính với tư cách cá nhân, thường là bằng cách gõ ký hiệu nhận dạng người dùng vào, hoặc đưa ra một thẻ chứa ký hiệu nhận dạng (id) người dùng, và sau đó chứng minh rằng cá nhân có quyền yêu cầu các đặc quyền tương ứng với ký hiệu nhận dạng người dùng đó. Một ví dụ tốt về quá trình này là gài thẻ sọc từ tính vào một ATM, sau đó gõ PIN.

Chứng minh danh tính là một quá trình quan trọng trong kiểm soát truy nhập máy tính và mạng. Nếu một kẻ xâm nhập có thể cung cấp bằng chứng mà hệ thống yêu cầu về một người sử dụng hợp pháp thì từ đó hệ thống an toàn bị bỏ qua hoàn toàn. Bằng chứng nhận dạng có thể có một trong ba dạng, hoặc riêng rẽ hoặc kết hợp, tức là:

- một cái gì đó người sử dụng biết;
- một cái gì đó người sử dụng có;
- một cái gì đó chứng tỏ là người sử dụng.

Khi một người sử dụng khởi nhập một hệ máy tính thì có thể tin rằng đối thoại đó có thể thực sự rơi vào máy chủ của kẻ xâm nhập. Khi đó người sử dụng có thể bị lừa và tiết lộ thông tin bí mật, ví dụ như mật khẩu hoặc PIN, và thậm chí nhập dữ liệu bí mật vào máy đó.

Giám sát truy nhập

Một hệ thống giám sát có hiệu quả có

thể lập nên một tính năng thiết yếu của hệ thống kiểm soát truy nhập. Yêu cầu giám sát các truy nhập hệ thống này sinh do:

- hệ thống có thể bất tiện đối với người sử dụng tới mức nó ảnh hưởng tới hiệu quả làm việc và những người sử dụng hợp pháp có thể bị cám dỗ chấp nhận những cách làm có thể vô hiệu hóa các biện pháp an toàn kiểm soát truy nhập;
- có thể không ngăn ngừa được một kẻ tấn công thiết lập một cuộc đối thoại mở đầu với hệ thống;
- các quá trình nhận dạng và xác thực vẫn có khả năng bị tấn công;
- một người sử dụng có một tập hợp hạn chế các đặc quyền truy nhập có thể tìm cách mở rộng bất hợp pháp những đặc quyền đó;
- nếu xảy ra một sự cố an toàn thì điều thiết yếu là phải thu thập được đủ bằng chứng về sự cố cho những cải tiến an toàn sau này hoặc cho bằng chứng vào những biên bản kỷ luật;
- các cải tiến về thủ tục an toàn hoặc sự phát hiện những kịch bản tấn công có thể dựa trên một mô hình nào đó chứa hành vi bình thường của hệ thống.

Giới hạn kiểu truy nhập

Với dữ liệu trữ trong máy tính thì có thể thực hiện mức kiểm soát đáng kể đối với các tác động của người sử dụng. Ví dụ, trong một hệ thống cơ sở dữ liệu, đa số người sử dụng được phép đọc dữ liệu, tuy nhiên, hoàn toàn không được phép sửa đổi dữ liệu đã nhớ. Trong môi trường tài chính, sẽ phải áp dụng những sự kiểm soát nghiêm ngặt đối với kiểu giao dịch do những số lớp người dùng nhất định tiến hành. Do đó các hệ thống kiểm soát truy nhập logic thường chỉ ra hoạt động nào người sử dụng có thể thực hiện trên một tệp: đọc, ghi, thực hiện, nối thêm. Truy nhập "nối thêm" cho phép một người sử dụng bổ sung thêm dữ liệu vào một tệp nhưng không đọc hoặc sửa đổi dữ liệu hiện thời.

Ngăn ngừa truy nhập không được phép

Việc duy trì tính an toàn của hệ thống kiểm soát truy nhập vật lý hoặc logic có liên quan tới nhiều vấn đề hơn chỉ là đơn giản phân biệt người sử dụng được phép với người sử dụng không được phép. Một khi truy nhập đã bị từ chối thì điều quan trọng là đảm bảo rằng sự từ chối phải được tuân thủ.

Trong trường hợp kiểm soát truy nhập vật lý, sự từ chối truy nhập liên quan tới việc đảm bảo rằng, những cửa có thể khóa thì không được để ngỏ, không có cách nào để phá cửa sổ mà vào v.v.

Với kiểm soát truy nhập logic, kẻ tấn công có thể có khả năng sử dụng những phương pháp cực kỳ phức tạp để khắc phục các kiểm soát an toàn. Các kỹ thuật sửa đổi phần mềm như các cửa bẫy, ngựa thành Toroa v.v. có thể phá được những hệ điều hành được thiết kế thận trọng nhất.

Thu hồi đặc quyền truy nhập

Việc xóa một khẩu khỏi tập mật khẩu không cần sự phối hợp từ phía người sử dụng và không ảnh hưởng tới những người sử dụng khác. Tuy nhiên, trong các hệ có một tập hợp lớn người sử dụng và một số tài sản được bảo vệ, có thể gặp khó khăn trong việc quản trị



những thay đổi các quyền truy nhập. Một ma trận liệt kê mỗi người sử dụng theo hàng, mỗi tài sản dữ liệu theo cột và một mục nhập đối với mỗi đặc quyền người sử dụng/tài sản, có thể là cực kỳ thưa thớt; những người sử dụng nói chung chỉ truy nhập vào một tỷ lệ nhỏ trong tổng tài sản. Một ma trận như thế có thể khó lưu giữ, duy trì và bảo vệ.

Có thể gắn vào mỗi tài sản một danh sách cho biết những người sử dụng nào có các đặc quyền truy nhập. Tuy nhiên, nếu các đặc quyền của một người sử dụng bị thu hồi thì cần phải xem xét danh sách truy nhập của mỗi tài sản đơn lẻ, tìm kiếm tên của người sử dụng. Phương pháp thay thế lưu giữ một danh sách các tài sản được phép mỗi người sử dụng cũng có những vấn đề tương tự (nếu cần phải xem lại số người sử dụng có các đặc quyền truy nhập hiện thời đối với một tài sản riêng).

Việc không thu hồi được các đặc quyền truy nhập của những người sử dụng đã rời công ty cũng thường xảy ra, hậu quả của điều đó có thể nghiêm trọng khi người sử dụng không còn trung thành với tổ chức nữa. *Xem* access matrix model, ATM, biometrics, discretionary access control, logical access control, magnetic stripe card, mandatory access control, password, PIN, user id. *Đồng nghĩa với* controlled accessibility.

access control list ***danh sách kiểm soát truy nhập*** (1) Trong kiểm soát truy nhập, danh sách các thực thể, cùng với những quyền truy nhập của họ, được phép truy nhập vào một tài nguyên. (2) Trong kiểm soát truy nhập, danh sách các chủ thể được phép truy nhập vào một đối tượng nào đó. *So sánh với* capability list. *Xem* access matrix model, object, subject. *Đồng nghĩa với* access list.

access control measures ***(các) biện pháp kiểm soát truy nhập*** Trong kiểm soát truy nhập, các đặc trưng phần cứng và phần mềm, các kiểm soát vật lý, các thủ tục điều hành, các thủ tục quản lý và những tổ hợp khác nhau của những biện pháp đó được thiết kế để phát hiện hoặc ngăn ngừa sự truy nhập trái phép vào một hệ ADP và để tăng cường kiểm soát truy nhập.

access control mechanisms ***(các) cơ cấu kiểm soát truy nhập*** Trong kiểm soát truy nhập, các đặc trưng phần cứng hoặc phần mềm, các thủ tục điều hành, các thủ tục quản lý và những tổ hợp khác nhau của những cơ cấu đó được thiết kế để phát hiện và ngăn ngừa sự truy nhập không được phép, và cho phép sự truy nhập được phép vào một hệ ADP. *Xem* access, ADP.

access control roster ***bản phân định kiểm soát truy nhập*** Trong kiểm soát truy nhập, danh sách nhân viên, người sử dụng v. v.. nêu mức độ truy nhập và kiểm soát đối với mỗi người.

access group ***nhóm truy nhập*** Trong kiểm soát truy nhập, một lớp gán vào một người sử dụng hoặc một quá trình; lớp có những đặc quyền truy nhập xác định đối với các đối tượng. *Xem* object.

access label ***nhãn truy nhập*** *Xem* label.

access level ***mức truy nhập*** Trong kiểm soát truy nhập, mức gắn liền với một chủ thể (ví dụ như mức truy nhập) hoặc với một đối tượng (ví dụ như mức phân loại). *Xem* category, classification level, clearance level, object, security level, sensitivity label, subject.

access line ***đường truy nhập*** Trong truyền thông dữ liệu, đường viễn thông liên tục nối một trạm ở xa với một DSE. Một số điện thoại gắn với những đường như thế. *Xem* DSE.

access list ***danh sách truy nhập*** Trong kiểm soát truy nhập, catalô tên những người sử dụng, các chương trình hoặc các quá trình và các đặc tả của các dạng truy nhập mà mỗi thực thể được gán vào. *Xem* access category. *Đồng nghĩa với* access control list.

access matrix model ***mô hình ma trận truy nhập*** Trong kiểm soát truy nhập, mô hình liên hệ các chủ thể, các đối tượng và các kiểu truy nhập. Chủ thể là một thực thể hoạt động có khả năng truy nhập các đối tượng, ví dụ như một chương trình đang thực hiện, một người sử dụng trong một hệ phân thời. Đối tượng là một thực thể mà việc truy nhập vào đó bị kiểm soát, ví dụ như một tệp, một đoạn bộ nhớ, một chương trình. Một kiểu truy nhập chỉ là một loại truy nhập vào một đối tượng, ví dụ kiểu truy nhập vào một chương trình có thể là: thi hành, đọc danh sách nguồn; truy nhập tới một tệp có thể là: đọc, ghi, gắn thêm (nối thêm).

Ma trận kiểm soát truy nhập là một mảng hai chiều với các đối tượng liệt kê theo hàng, các chủ thể liệt kê theo cột và mỗi ô chứa kiểu truy nhập của chủ thể đã cho đối với đối tượng tương ứng. Trong thực tiễn mảng như thế sẽ thưa thớt và lãng phí không gian nhớ. Do đó, khi thực hiện có thể biểu diễn nó theo danh sách kiểm soát truy nhập hoặc danh sách khả năng.

Danh sách kiểm soát truy nhập cung cấp các chi tiết về các chủ thể và các đặc quyền truy nhập của chúng đối với mỗi đối tượng. Mặt khác, danh sách khả năng liệt kê các đối tượng và các kiểu truy nhập tương ứng. *Xem* access control list, access type, capability list, object, sparse array, subject.

access mode ***chế độ truy nhập*** (1) Trong kiểm soát truy nhập, một hoạt động phân biệt rõ được các cơ chế bảo vệ thừa nhận như hoạt động khả dĩ trên một đối tượng. Đọc, ghi và nối thêm là những chế độ truy nhập khả dĩ đối với một tệp, trong khi đó thi hành là một chế độ truy nhập bổ sung đối với một chương trình. *Xem* object. *Đồng nghĩa với* permission. (2) Trong kiểm soát truy nhập, một chế độ của thiết bị kiểm soát truy nhập. *Xem* access.

access password ***mật khẩu truy nhập*** Trong kiểm soát truy nhập, mật khẩu dùng để được phép truy nhập dữ liệu và được phân phối cho tất cả những ai được phép truy nhập tương tự vào dữ liệu đó. *Xem* password.

access period ***chu kỳ truy nhập*** Trong kiểm soát truy nhập, khoảng thời gian nói chung tính bằng ngày hoặc tuần, trong đó các quyền truy nhập chiếm ưu thế. *Xem* access right.

access permission *(sự) cho phép truy nhập* Trong kiểm soát truy nhập, sự xác định rõ những chủ thể nào có khả năng thay đổi các chế độ truy nhập và/hoặc khả năng chuyển khả năng cho một chủ thể khác. *Xem* subject.

access port *cổng truy nhập* Trong an toàn máy tính, một thiết bị nhận diện logic hay vật lý mà máy tính dùng để phân biệt các dòng dữ liệu vào/ra từ thiết bị đầu cuối khác nhau.

access right *quyền truy nhập* Trong kiểm soát truy nhập, sự cấp phép truy nhập cụ thể (tức là đọc, ghi, nối thêm, thi hành, xoá, tạo ra, sửa đổi) cho một chủ thể đối với một đối tượng. *Xem* access permission, object, subject.

access to information *truy nhập thông tin* Trong lập pháp, chức năng cung cấp cho các thành viên trong công chúng, theo yêu cầu của họ, thông tin của chính phủ mà họ có quyền được đòi hỏi theo luật định. *Xem* data protection, freedom of information.

access type *kiểu truy nhập* Trong kiểm soát truy nhập, bản chất của một quyền truy nhập đối với một thiết bị, chương trình, hoặc tệp cụ thể; ví dụ, đọc, ghi, thi hành, nối thêm, sửa đổi, xoá, tạo ra. *Xem* access mode.

accidental destruction *hủy vô tình dữ liệu* Trong an toàn dữ liệu, sự ghi đè hoặc xóa vô tình dữ liệu, ví dụ như do phần cứng hoặc phần mềm hỏng. Cần có bản sao dự phòng để khôi phục lại. *Xem* backup/restore.

accidental threat *đe dọa ngẫu nhiên, hiểm họa tình cờ* Trong an toàn vật lý, mối đe dọa gây hư hại không cố ý đối với hệ thống do sử dụng không đúng hoặc do các hiện tượng tự nhiên, ví dụ như lũ lụt, hỏa hoạn v.v.. *So sánh với* active threat, deliberate threat, logical threat, passive threat, physical threat. *Xem* threat.

accountability *tính phân định trách nhiệm, tính khả quy trách nhiệm* (1) Trong an toàn dữ liệu, tính chất đảm bảo rằng các tác động của một thực thể sẽ để lại dấu vết duy nhất đến thực thể đó. (2) Trong an toàn thông tin, các chức năng ghi lại sự thi hành các quyền thực hiện các tác động liên quan tới an toàn. *Xem* information technology security evaluation criteria. (3) Trong an toàn thông tin, tính chất hoặc trạng thái cho phép chỉ ra dấu vết các vi phạm hoặc dự định vi phạm an toàn hệ thống ADP, dẫn tới có thể quy trách nhiệm tới các cá nhân. *Xem* ADP.

accountability information *thông tin khả quy trách nhiệm* Trong an toàn máy tính, tập hợp các bản ghi thường tham chiếu như một vết kiểm toán, cung cấp bằng chứng có dẫn liệu về quá trình hay những tác động khác liên quan tới an toàn của một hệ ADP. *Xem* audit trail.

account balance *số dư tài khoản* Trong hoạt động ngân hàng, tổng tất cả những khoản có trừ tất cả những khoản nợ thành một con số sử dụng hiện thời đối với một sản phẩm bất kỳ nào đó. *Xem* current utilization, product.

account freezing *phong tỏa tài khoản* Trong hoạt động ngân hàng, kỹ thuật tạm thời từ chối tiến hành các giao dịch của một tài khoản nếu PIN không đúng

được đưa vào nhiều hơn một số lần xác định. *Xem* PIN.

account identification ***nhận dạng tài khoản*** Trong hoạt động ngân hàng, thủ tục nhận dạng do ngân hàng phục vụ tài khoản quy định để nhận biết tài khoản của chủ sở hữu tài khoản. *Xem* account servicing bank, primary account number.

account owner bank ***ngân hàng sở hữu tài khoản*** Trong hoạt động ngân hàng, ngân hàng mà một tài khoản của nó được phục vụ ở một ngân hàng khác. *Xem* account servicing bank.

account servicing bank ***ngân hàng phục vụ tài khoản*** Trong hoạt động ngân hàng, ngân hàng nhận giữ một tài khoản. *So sánh với* account owner bank.

accreditation ***công nhận*** (1) Trong an toàn máy tính, sự cấp phép và phê chuẩn cho một hệ hoặc mạng ADP xử lý những dữ liệu nhạy cảm trong một môi trường vận hành. Sự cấp phép và phê chuẩn đó đưa ra trên cơ sở xác nhận của ban kỹ thuật được chỉ định về mức độ đáp ứng các yêu cầu kỹ thuật định trước theo thiết kế và lắp đặt công cụ hệ thống, nhằm đạt được an toàn dữ liệu thích hợp. *Xem* approval/accreditation, certification, data security. (2) Trong an toàn máy tính, sự cấp phép chính thức của DAA thích hợp để đưa một hệ thống tự động vào ứng dụng vận hành. Sự cấp phép này là một báo cáo nói rằng, mức rủi ro còn lại trong vận hành hệ thống đủ thấp để cho phép một ứng dụng xác định. Sự công nhận có tính đặc thù vị trí và phụ thuộc vào việc đáp ứng các biện pháp và các thủ tục an toàn cục bộ. (3) Trong an toàn máy tính, sự cấp quyền chính thức cho một hệ thông tin xử lý thông tin nhạy cảm trong môi trường vận hành của nó, dựa trên sự đánh giá an toàn toàn diện về thiết kế an toàn phần cứng, phần sụn và phần mềm của hệ thống, về cấu hình và cài đặt của hệ thống, và về các kiểm soát an toàn thủ tục, hành chính, vật lý, Tempest, nhân sự và truyền thông khác của hệ thống. *Xem* Tempest.

accreditation authority ***quan chức công nhận*** Trong an toàn máy tính, một quan chức được chỉ định để ủy quyền đưa các hệ thống vào xử lý, sử dụng, lưu giữ và tạo ra tư liệu phòng thủ nhạy cảm. *Xem* accreditation, DAA.

accreditation range ***phạm vi công nhận*** Trong an toàn truyền thông, chỉ một phạm vi đối với một mạng riêng, là một tập hợp các mức kiểm soát truy nhập bắt buộc đối với việc lưu giữ, xử lý và truyền dữ liệu. Phạm vi công nhận chung sẽ phản ánh các mức độ nhạy cảm của dữ liệu mà quan chức công nhận tin hệ chủ có thể giữ tách biệt một cách tin cậy với một mức độ rủi ro chấp nhận được trong khung cảnh của một mạng riêng mà đối với nó phạm vi công nhận được quy định. Như vậy, mặc dù hệ chủ có thể được công nhận để sử dụng các mức kiểm soát truy nhập MẬT, TUYỆT MẬT và TỐI MẬT trong vận hành một mình, nó có thể có phạm vi công nhận gồm giá trị đơn TỐI MẬT để kết nối với một mạng nào đó. *Xem* accreditation, mandatory access control.

accumulator circuit ***mạch tích lũy*** Trong an toàn vật lý, mạch kích hoạt

tín hiệu báo động do kết quả của sự tích lũy các dữ liệu từ các bộ cảm biến.

accuracy ***tính chính xác*** Trong an toàn thông tin, các chức năng đảm bảo tính đúng đắn và nhất quán của thông tin liên quan tới an toàn. *Xem* information technology security evaluation criteria.

ACF2 ***bộ chương trình ACF2*** Trong an toàn máy tính, bộ chương trình an toàn dữ liệu. *Xem* data security package.

ACH *Xem* Automated Clearing House.

ACIA *Xem* asynchronous communications interface adapter.

ACK *Xem* acknowledge character.

ACK0 *Xem* affirmative acknowledgement.

ACK1 *Xem* affirmative acknowledgement.

acknowledge character ***ký tự báo nhận*** Trong truyền thông dữ liệu, ký tự do một trạm truyền đi như một lời đáp xác nhận cho trạm mà nó đã thiết lập nối. *So sánh với* negative acknowledgement. *Xem* acknowledgement, station.

acknowledgement ***báo nhận*** Trong truyền thông dữ liệu, việc máy thu truyền các ký tự báo nhận để đáp lại máy gửi. *Xem* affirmative acknowledgement, negative ackonowledgement.

acknowledgement frame ***khung báo nhận*** Trong truyền thông dữ liệu, gói tin gửi từ một máy thu để báo đã nhận đúng một khung dữ liệu truyền qua mạng. *Xem* data link layer, frame. *So sánh với* data frame.

ACM *Xem* Association for Computing Machinery.

acoustic coupler ***bộ ghép âm*** Trong truyền thông dữ liệu, thiết bị để ghép nối một hạng mục thiết bị, tạo ra các tín hiệu số vào một mạng điện thoại. Những bộ chuyển đổi âm thanh trong bộ ghép âm tạo ra các âm ứng với các tín hiệu số; ống điện thoại được đặt tiếp xúc với các bộ chuyển đổi âm thanh để các âm đó có thể truyền tới mạng điện thoại. *Xem* MODEM, transducer.

acoustic eavesdropping ***nghe lén âm thanh*** Trong an toàn truyền thông, sự nghe lén các sóng âm do tiếng nói con người, tiếng động máy in, tiếng động máy đục bìa hay thiết bị truyền gây ra. *So sánh với* electronic eavesdropping. *Xem* eavesdropping.

acoustic emission ***phát xạ âm thanh*** Trong kiểm soát truy nhập, phương pháp xác minh chữ ký động dùng giám sát âm thanh do bút viết phát ra trong khi ký chữ ký. *Xem* dynamic signature verification.

acquired data ***dữ liệu thu nhận*** Trong an toàn vật lý, dữ liệu truy nhập hoặc cảnh báo thu thập trong thời gian thực và truyền tới hệ cảnh báo trung tâm để xử lý. *Xem* central station.

acquirer ***cơ sở nhận*** (1) Trong hoạt động ngân hàng, một cơ sở bên trong mạng trao đổi giao dịch nhận thông tin nhận dạng và xác thực từ một đầu cuối. Cơ sở nhận chịu trách nhiệm thu nhận thanh toán cho bên nhận thẻ từ bên phát thẻ. *Xem* card acceptor, card inssuer interchange. (2) Trong hoạt động ngân hàng, cơ sở hoặc đại lý của nó, nhận các dữ liệu tài chính liên quan tới

giao dịch từ bên nhận thẻ và chuyển dữ liệu đó vào một hệ thống giao dịch. Mọi cơ quan chuyển thông báo mà không tính đến dữ liệu tài chính thì không phải là một cơ sở nhận. *Xem* card acceptor, interchange. (3) Trong hoạt động ngân hàng, cơ sở trong mạng trao đổi giao dịch nhận thông tin nhận dạng và xác thực từ một khách hàng.

activation ***kích hoạt*** Trong các mạng máy tính, quá trình đưa một bộ phận trong một nút mạng vào thế sẵn sàng thực hiện các chức năng mà nó được chỉ định. *Xem* node.

active attack ***tấn công chủ động*** Trong an toàn truyền thông, sự tấn công trong đó đối phương sửa đổi thông tin đã truyền hoặc đưa lén thông tin vào đường truyền thông. Các cuộc tấn công chủ động có thể được chia thành ba loại:

- sửa đổi luồng thông báo;
- từ chối dịch vụ thông báo;
- phát lại và giả dạng.

Sửa đổi luồng thông báo có thể nhằm mục đích thay đổi địa chỉ gốc, nội dung thông báo, địa chỉ nơi nhận hoặc trình tự truyền của các thông báo. Từ chối dịch vụ thông báo liên quan tới xóa, làm trễ thông báo hoặc làm tràn mạng bằng những thông báo giả.

Các cuộc tấn công phát lại thông báo dựa trên việc ghi và sau đó phát lại các thông báo hợp pháp. Giả dạng nhằm cố gắng thiết lập liên lạc giữa người sử dụng đích thực và kẻ tấn công. *So sánh với* passive attack. *Xem* active wiretapping, authentication, delay/denial of service, masquerading, message authentication, replay.

active sensor ***(bộ) cảm biến chủ động*** Trong an toàn vật lý, bộ cảm biến có thể sinh ra một trường bức xạ cho mục đích phát hiện. *So sánh với* passive sensor.

acvite threat ***hiểm họa chủ động*** (1) Trong quản lý rủi ro, hiểm họa thay đổi cố ý bất hợp pháp đối với trạng thái của một hệ thống. *So sánh với* passive threat. (2) Trong quản lý rủi ro, sự vi phạm an toàn tiềm ẩn mà nếu xuất hiện, nó sẽ có thể gây hư hỏng hoặc thay đổi thực sự đối với máy tính: phần cứng, phần mềm hoặc dữ liệu. *So sánh với* accidental threat, deliberate threat, logical threat, passive threat, physical threat. *Xem* active attack, denial of service, masquerading, replay, threat, traffic padding.

active wire concentrator ***bộ tập trung dây chủ động*** Trong các mạng máy tính, các tủ với cách nối hình sao tới những nút riêng lẻ. Ở các mạng cục bộ, chúng được nối thành vòng, do đó tạo ra cấu hình vòng/sao kết hợp. *Xem* local area network, node, ring, star.

active wiretapping ***nối lén chủ động*** (1) Trong an toàn máy tính, việc nối một thiết bị không được phép, như đầu cuối máy tính, vào một mạch truyền thông nhằm mục đích truy nhập vào dữ liệu thông qua việc tạo ra các thông báo hoặc các tín hiệu điều khiển giả hoặc bằng cách thay đổi các cuộc liên lạc của những người sử dụng hợp pháp. *Xem* masquerading, telephone intrusion, wiretapping. (2) Trong an toàn truyền thông, nối lén nhằm mục đích truy nhập dữ liệu bằng cách tạo ra các thông báo hoặc tín hiệu giả, thay đổi truyền thông



của những người sử dụng hợp pháp. *So sánh với* passive wiretapping. *Xem* denial of service, wiretapping.

activity ***hoạt động*** Trong an toàn máy tính, quy tắc mô hình hóa an toàn phát biểu rằng, khi một đối tượng không được hoạt động thì sẽ không thể truy nhập tới nó cho tới khi làm cho nó hoạt động trở lại. *Xem* object.

actual data transfer rate ***tốc độ chuyển dữ liệu thực*** Trong truyền thông dữ liệu, số trung bình các bit, các ký tự hoặc các khối được truyền đi trong đơn vị thời gian từ một nguồn dữ liệu và được một bộ phận gom dữ liệu tiếp nhận. *Xem* source sink.

ACU *Xem* automatic calling unit.

ADAC *Xem* administratively directed control access.

adaptive channel allocation ***cấp phát kênh thích ứng*** Trong truyền thông, phương pháp dồn kênh trong đó các kênh được cấp phát theo nhu cầu chứ không phải theo kế hoạch cố định từ trước. *Xem* multiplexing, frequency division multiple access, time division multiple access.

adaptive routing ***định tuyến thích ứng, chọn đường thích ứng*** Sơ đồ định tuyến đối với các bó tin hoặc thông báo trong đó động thái của các bó tin hoặc thông báo thích ứng với các thay đổi trên mạng như các sự cố đường truyền hay với sự thay đổi mô hình lưu lượng. *So sánh với* delta routing, directory routing, fixed routing, hot potato routing. *Xem* centralized adaptive routing, message switching, packet switching, routing.

ADCCP *Xem* advanced data communications control procedure.

add-in ***phần bổ sung*** Ở phần cứng, các mở rộng cắm vào khe máy tính để cung cấp những phương tiện bổ sung. *Xem* MODEM.

additive cipher ***mã cộng*** *Đồng nghĩa với* translation cipher.

add-on security ***an toàn tăng cường, hỗ trợ an toàn*** Trong an toàn máy tính, hỗ trợ các cơ chế bảo vệ do phần cứng hoặc phần mềm thực hiện sau khi đã vận hành hệ ADP. *Xem* ADP.

address ***địa chỉ // lập địa chỉ*** (1) Trong tin học, địa chỉ là ký tự hoặc nhóm ký tự định danh một thanh ghi, một phần cụ thể của bộ nhớ, hoặc một nguồn hoặc nơi nhận dữ liệu khác nào đó. (2) Trong tin học, lập địa chỉ là chỉ tới một thiết bị hoặc một mục dữ liệu bằng địa chỉ của nó. (3) Trong truyền thông, địa chỉ là phần tín hiệu chọn lọc cho biết nơi nhận cuộc gọi.

addressing ***(sự) lập địa chỉ, (sự) gán địa chỉ*** (1) Trong tin học, sự gán các địa chỉ cho các lệnh của một chương trình. *Xem* address. (2) Trong truyền thông, cách trạm gửi hoặc trạm điều khiển chọn thiết bị để gửi một thông báo tới. *Xem* station.

address space ***vùng địa chỉ*** Trong kiến trúc mạng, bộ nhớ ảo mà một quá trình có thể lập được địa chỉ. Kích thước tối đa của vùng địa chỉ của quá trình thường phụ thuộc vào phần cứng cơ sở. *Xem* virtual memory.

ad hoc enquiry ***hỏi riêng, vấn tin đặc biệt, vấn tin không theo thể thức*** Trong các cơ sở dữ liệu, phương

pháp cho phép người sử dụng trong một môi trường cơ sở dữ liệu tạo động khung nhìn dữ liệu riêng của mình và phương pháp truy lục thông tin mà không có sự can thiệp.

adjacent channel ***kênh lân cận*** Trong truyền thông, kênh tiếp theo hoặc một kênh bên cạnh về mặt vật lý hoặc về mặt điện với một kênh hiện đang sử dụng. *Xem* channel.

ADLC *Xem* advanced data link control.

administratively directed access control ***kiểm soát truy nhập theo hành chính*** Trong kiểm soát truy nhập, chỉ một hệ thống trong đó các nhà quản trị kiểm soát xem ai có thể truy nhập những đối tượng nào. *So sánh với* user directed access control. *Xem* mandatory access control.

administrative security ***an toàn hành chính*** Trong an toàn dữ liệu, các ràng buộc quản lý, các thủ tục điều hành, các thủ tục phân định trách nhiệm và các điều khoản bổ sung được thiết lập để tạo ra mức bảo vệ có thể chấp nhận được đối với dữ liệu nhạy cảm. *Xem* accountability. *Đồng nghĩa với* procedural security.

ADP ***ADP*** Viết tắt của Automatic Data Processing (xử lý dữ liệu tự động). *Xem* automatic data processing system.

ADP availability ***(tính) sẵn sàng ADP*** Trong an toàn máy tính, trạng thái tồn tại khi có thể nhận được các dịch vụ ADP trong khoảng thời gian chấp nhận được. *So sánh với* application confidentiality, application integrity, data integrity. *Xem* ADP, data confidentiality.

ADP security ***an toàn ADP*** Trong an toàn máy tính, các biện pháp cần thiết chống lại sự tiết lộ, sự sửa đổi hoặc sự phá hủy trái phép (ngẫu nhiên hoặc cố ý) đối với các hệ ADP và dữ liệu, và từ chối dịch vụ xử lý dữ liệu. An toàn ADP bao gồm việc xem xét tất cả các chức năng, đặc trưng và/hoặc đặc điểm của phần cứng/phần mềm; các thủ tục điều hành, các thủ tục phân định trách nhiệm và các kiểm soát truy nhập tại phương tiện máy tính trung tâm, máy tính ở xa và các phương tiện đầu cuối; các ràng buộc về quản lý; các cấu trúc và thiết bị vật lý; và những kiểm soát về nhân sự và truyền thông cần thiết để có mức rủi ro chấp nhận được đối với hệ ADP và đối với dữ liệu hoặc thông tin chứa trong hệ. *Xem* automatic data processing system, ADP security.

ADP security staff ***nhân viên an toàn ADP*** Trong an toàn máy tính, các cá nhân được chỉ định và hoạt động như các quan chức có ảnh hưởng đối với an toàn ADP trong tổ chức tương ứng của họ. *Xem* ADP, ADP security.

ADP system security ***an toàn hệ thống ADP*** Trong an toàn máy tính, tất cả các biện pháp an toàn công nghệ và các thủ tục quản lý được thiết lập và áp dụng cho phần cứng, phần mềm và dữ liệu của máy tính để đảm bảo bảo bệ tài sản của tổ chức và bí mật cá nhân. *Xem* ADP, ADP security.

advanced data communications control procedure ***thủ tục kiểm soát truyền dữ liệu nâng cao*** Trong thuyền thông dữ liệu, chỉ hoạt động của một liên kết dữ liệu có sử dụng một



giao thức tiên tiến (SDLC, HDLC). *Xem* HDLC, protocol, SDLC.

advanced data link control ***điều khiển liên kết dữ liệu nâng cao*** Trong truyền thông dữ liệu, giao thức liên kết dùng trong các hệ HDLC và SDLC. *Xem* HDLC, SDLC.

advice ***(thư) thông báo*** Trong hoạt động ngân hàng, sự khẳng định rằng một hoạt động đã được tiến hành.

advice and assessment ***thông báo và đánh giá*** Trong an toàn máy tính, sự phân tích về mặt kỹ thuật tình thế an toàn máy tính của một hệ riêng và thông báo cho khách hàng về những điểm dễ bị tổn thương của hệ thống. *Xem* vulnerability.

AFCEA ***hiệp hội AFCEA*** Viết tắt của Armed Forces Communications and Electronics Association (Hiệp hội điện tử và truyền thông quân đội).

Affirm ***phương pháp luận Affirm*** Trong tin học, phương pháp luận hình thức phát triển ở Đại học Khoa học thông tin Nam California (USC-ISI) về đặc tả và xác minh các kiểu dữ liệu trừu tượng, kết hợp chặt chẽ các kỹ thuật đặc tả đại số và sự phát triển phân cấp. *Xem* HDM.

affirmative acknowledgement ***khẳng định nhận*** Trong truyền thông dữ liệu, các tín hiệu đáp ACK0 và ACK1 trong truyền nhị phân đồng bộ cho biết rằng, máy thu đã nhận được khối truyền trước đó và đang sẵn sàng để nhận khối tiếp theo. ACK0 và ACK1 được gửi xen kẽ tạo ra sự kiểm tra tuần tự chuỗi các tín hiệu đáp. ACK0 cũng được dùng như tín hiệu đáp (xác nhận) cho một tín hiệu chọn trạm trong mạch nhiều điểm, hoặc đáp lại dãy tín hiệu khởi động trong vận hành điểm tới điểm. *So sánh với* negative acknowledgement. *Xem* binary synchronous communications, multidrop circuit, point to point.

AFIPS ***liên hiệp AFIPS*** Viết tắt của American Federation of Information Processing Societies Inc (Liên hiệp các hội xử lý thông tin Hoa Kỳ). Liên đoàn được thành lập năm 1961 bao gồm Hội Khoa học thông tin Hoa Kỳ, Hiệp hội thống kê Hoa Kỳ, Hiệp hội máy tính, Hiệp hội hệ dữ liệu giáo dục, Hiệp hội quản lý xử lý dữ liệu, Hội máy tính IEEE, Hội chế tạo công cụ Hoa Kỳ, Hội mô phỏng máy tính, Hội toán học công nghiệp và ứng dụng, Hội hiển thị thông tin. Nó là thành viên của Hoa Kỳ trong IFIP. *Xem* IFIP.

AFNOR ***hội AFNOR*** Hiệp hội tiêu chuẩn hóa Pháp (Association Française de NORmalisation).

AFR ***AFR*** Viết tắt của Air Force Regulation (điều lệ không lực).

agency activity ***hoạt động đại lý*** Trong hoạt động ngân hàng, hoạt động mà ngân hàng tham gia nhân danh khách hàng và không phải chịu rủi ro trực tiếp.

aggregation ***phần gộp, phần ghép; phép gộp*** (1) Trong an toàn dữ liệu, phần gộp là các hệ dữ liệu và các phần tử dữ liệu riêng lẻ có thể không phải là mật và thuộc một nhóm nhạy cảm riêng. Khi những dữ liệu đó được kết hợp với những dữ liệu khác thì toàn bộ thông tin có thể được coi là mật

hoặc thuộc nhóm nhạy cảm cao hơn, với những yêu cầu bảo vệ cao hơn. *Xem* multilevel database security. (2) Trong toán học, phép gộp là một phép trừu tượng hóa nhờ đó quan hệ giữa các đối tượng được coi như một đối tượng mức cao hơn.

AGI ***virut AGI*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới vận hành trong thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

aging ***(sự) lập ngày tháng sử dụng, (sự) phân loại theo thời hạn sử dụng*** Trong xử lý dữ liệu, sự nhận dạng các mục liên quan hoặc chưa xử lý trong các tệp theo ngày tháng của chúng, thường là ngày tháng chuyển tác. Sự phân loại thời hạn sử dụng xếp các mục theo những khoảng ngày tháng khác nhau.

AGI-Plan ***virut AGI-Plan*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới vận hành trong thời gian chạy, làm sai lệch các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

Aids ***virut Aids*** Trong an toàn máy tính, virut lây nhiễm các tệp COM. *Xem* virus names.

AIM ***AIM*** Viết tắt của Automatic Identification Manufacturers (nhận dạng tự động các nhà sản xuất).

AirCop ***virut AirCop*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động đĩa mềm, làm sai lạc cung khởi động và ảnh hưởng tới vận hành trong thời gian thực. *Xem* virus names.

AIS ***AIS*** Viết tắt của Automated Information System (hệ thống tin tự động hóa).

AMAIS security ***an toàn AMAIS*** Trong an toàn máy tính, toàn bộ các biện pháp an toàn cần thiết để có mức bảo vệ chấp nhận được đối với một AIS và dữ liệu xử lý bởi AIS. *Xem* AIS.

Alabama ***virut Alabama*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp EXE, ảnh hưởng tới vận hành thời gian thực, làm sai lạc các tệp chương trình, OVL và liên kết tệp. *Xem* virus names.

Alameda ***virut Alameda*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động đĩa mềm và làm sai lạc cung khởi động. *Xem* virus names.

alarm assessment system ***hệ đánh giá cảnh báo*** Trong an toàn vật lý, hệ cho phép người thao tác đánh giá một cảnh báo đã báo cáo trước đó, ví dụ như CCTV cung cấp các hình ảnh để người thao tác phân tích. *Xem* CCTV.

alarm discriminator ***bộ phân biệt cảnh báo*** Trong an toàn vật lý, thiết bị hoặc máy phát hiện bổ sung vào một hệ thống để giảm xác suất các cảnh báo giả này sinh từ những rung động hoặc tạp nhiễu từ bên ngoài.

alarm indicating device ***thiết bị chỉ thị cảnh báo*** Trong an toàn vật lý, tín hiệu nhìn thấy hoặc nghe thấy cho biết phạm vi tác động của một vụ cháy.

alarm line ***tuyến báo động*** Trong an



toàn vật lý, mạch hữu tuyến giám sát bằng điện, giữa một vùng được bảo vệ và máy thu tín hiệu báo động, dùng để truyền các tín hiệu báo động. *Xem* alarm signal.

alarm receiver ***máy thu báo động*** Trong an toàn vật lý, bảng báo hiệu dùng dự phòng để giám sát một tuyến báo động. Nó có thể có hoặc không có dụng cụ phát tiếng báo động. *Xem* alarm line, annunciator, audible alarm device.

alarm screen ***màn báo động, màn cảnh báo*** Trong an toàn vật lý, màn chắn có cửa sổ được trang bị điện, nó phát báo động khi đi ngang qua.

alarm signal ***tín hiệu báo động*** Trong an toàn vật lý, tín hiệu quan sát trực quan hoặc âm thanh cho biết trường hợp khẩn cấp đòi hỏi tác động ngay lập tức (ví dụ như sự cố thiết bị, nước, khói, lửa, thâm nhập, giả mạo đường dây hoặc sự cố đường dây, điều kiện thiết bị không an toàn).

alarm station ***đài báo động*** Trong an toàn vật lý, chuyển mạch hoặc thiết bị vận hành thủ công kích hoạt tín hiệu báo động.

ALE *Xem* annual loss expectancy.

algorithm ***thuật toán, giải thuật*** Trong tin học, tập hợp hữu hạn các quy tắc xác định rõ ràng để giải quyết một vấn đề trong một số bước hữu hạn, ví dụ như sự mô tả chính xác các bước liên quan tới việc xác định bản ghi với giá trị cao nhất của một thuộc tính bằng số xác định.

Aloha ***mạng Aloha*** Trong truyền thông dữ liệu, mạng truyền thông của các hệ vô tuyến có căn cứ trên mặt đất vốn sử dụng một giao thức tránh xung đột để phân phối kênh phát rộng cho người sử dụng. Những người sử dụng truyền bất kỳ lúc nào họ có dữ liệu để gửi đi. Nếu hai người sử dụng có kênh phát rộng phủ nhau thì các gói dữ liệu sẽ bị sai lạc. Những người gửi giám sát kênh phát rộng, nếu họ phát hiện thấy gói tin họ vừa truyền bị sai lạc thì họ chờ một khoảng thời gian ngẫu nhiên và truyền lại gói tin. *Xem* broadcast, carrier sense protocol, carrier sense multiple access-collision detection.

alphabetic character set ***bộ ký tự chữ cái*** Bộ ký tự chứa các chữ cái nhưng không có các chữ số. Nó có thể chứa các ký tự điều khiển, các ký tự đặc biệt và ký tự dấu cách. *So sánh với* alphanumeric. *Xem* control character.

alphanumeric ***chữ - số*** Chỉ bộ ký tự gồm các chữ cái, chữ số và thường có cả những ký tự khác, ví dụ như các dấu câu. *So sánh với* alphabetic character set.

alternate route ***tuyến thay thế, đường thay thế*** Trong truyền thông, tuyến thứ hai hoặc dự phòng được sử dụng khi tuyến bình thường không khả dụng.

AM *Xem* amplitude modulation.

ambush code ***mã nằm chờ*** Trong an toàn vật lý, mã đặc biệt đối với hệ kiểm soát truy nhập, hoặc mục nhập vùng phím số, nó tạo ra tín hiệu báo động cưỡng bức từ xa khi được đưa vào hệ kiểm soát truy nhập. *Xem* access control, digital keypad, duress alarm.

amend ***sửa đổi, cải tiến*** Trong hoạt động ngân hàng, sửa đổi các chi tiết ở máy tính cho một khách hàng, phương tiện hoặc dịch vụ.

American National Standards Institute ***Viện tiêu chuẩn quốc gia Hoa Kỳ*** Trong công tác tiêu chuẩn hóa, cơ quan tổ chức các ủy ban hình thành từ những người sử dụng máy tính, những nhà sản xuất v.v., để phát triển và công bố các tiêu chuẩn công nghiệp, ví dụ như ANSI FORTRAN, ANSI Standard Code for Periodical Identification. ANSI X3 liên quan tới các tiêu chuẩn máy tính và xử lý dữ liệu, ANSI X9 liên quan tới các tiêu chuẩn ngân hàng.

amplitude modulation ***điều biên, điều biến biên độ*** Trong truyền thông, một dạng điều biến trong đó biên độ của tín hiệu sóng mang thay đổi phù hợp với biên độ của tín hiệu điều biến. *So sánh với* frequency modulation, phase modulation. *Xem* carrier, modulation.

Amstrad ***virut Amstrad*** Trong an toàn máy tính, virut lây nhiễm các tệp COM và làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

analog ***tương tự, analog*** Trong tin học và truyền thông, chỉ dạng các đại lượng vật lý biến thiên liên tục. *So sánh với* digital. *Xem* analog signal.

analog channel ***kênh tương tự, kênh analog*** Trong truyền thông, kênh dữ liệu trong đó biên độ của tín hiệu truyền đi có thể có giá trị bất kỳ giữa các giới hạn xác định cho kênh. Các kênh cấp tiếng nói là các kênh tương tự. *Xem* analog.

analog signal ***tín hiệu tương tự, tín hiệu analog*** Tín hiệu thay đổi liên tục theo thông tin khi truyền, ví dụ như sóng âm. *So sánh với* digital signal. *Xem* analog.

analog transmission ***truyền tương tự, truyền analog*** Trong truyền thông, sự truyền thông tin bằng tín hiệu tương tự. *Xem* analog.

analysis ***phân tích*** *Xem* cost-risk analysis, cryptanalysis, risk analysis.

analytical attack ***tấn công phân tích*** Trong mã thám, sự tấn công trong đó tập hợp các phương trình toán học thu được từ các định nghĩa của thuật toán mật mã được giải để tìm một biến hoặc các biến biểu diễn bản rõ (văn bản gốc) hoặc khóa mật mã chưa biết. *So sánh với* exhaustive attack. *Xem* cryptographic key.

ancillary equipment ***thiết bị phụ*** Trong truyền thông, thiết bị nằm ở chỗ thuê bao, ví dụ như thiết bị đáp, bộ quay số tự động, để tạo ra tiện ích lớn hơn cho một kênh truyền thông đối với các thuê bao riêng lẻ.

anisochronous signal ***tín hiệu dị thời*** Trong điện tử học, tín hiệu không liên quan tới bất kỳ đồng hồ nào và trong đó các quá trình chuyển tiếp có thể xảy ra ở bất kỳ thời điểm nào. *Xem* anisochronous transmission

anisochronous transmission ***truyền dị thời*** Trong truyền thông dữ liệu, một dạng truyền dữ liệu tương tự với truyền không đồng bộ nhưng ở đó có thể có các thời khoảng biến thiên giữa các bit bên trong một ký tự cũng như giữa bản thân các ký tự. *So sánh với*

asynchronous transmission, isochronous transmission. *Xem* bit.

annual loss expectancy ***dự kiến tổn thất hằng năm*** Trong quản lý rủi ro, số đo chi phí tiềm tàng hằng năm của một mối đe dọa đối với sự an toàn hệ thống. *Xem* risk analysis, threat.

annunciator ***hệ chỉ báo*** Trong an toàn vật lý, hệ hiển thị hoặc âm thanh chỉ báo sự thay đổi trạng thái vùng bảo vệ trong một hệ an toàn. *Xem* protection pattern.

anonymous refunder ***người trả tiền nặc danh*** Trong hoạt động ngân hàng, một người chuyển tiền từ tài khoản này sang tài khoản khác không theo phương pháp thông thường.

ANSI *Xem* American National Standard Institute.

ANSI X.12 ***chuẩn ANSI X.12*** Trong hoạt động tiêu chuẩn hóa, tiêu chuẩn ANSI cho EDI. Không giống như EDIFACT, tiêu chuẩn này giải quyết cả hai cơ chế đinh khuôn dạng và vận chuyển các thông báo. Các tài liệu gửi cho cùng nơi nhận hoặc người nhận được nhóm lại trong một bao gói (phong bì) trao đổi, các nhóm cùng kiểu tài liệu bên trong bao gói trao đổi lại nằm trong bao gói nhóm hoạt động và các tài liệu riêng lẻ lại chứa trong một bao gói tập hợp giao dịch. Sự an toàn của các thông báo được thảo luận trong X12.58, các dịch vụ an toàn trao đổi dữ liệu điện tử và sự an toàn nhằm đảm bảo tính toàn vẹn, tính kín đáo và sự xác minh người gửi, nhưng chỉ sử dụng các mật mã đối xứng, ví dụ như DES. Phép lọc bản mã được sử dụng để đảm bảo bản mã chỉ chứa các ký tự từ tập ký tự được phép truyền. Việc quản lý khóa được mô tả ở X.12.42. *So sánh với* EDIFACT. *Xem* DES, filtering, key management, symmetric cipher.

ANSI X3.T1 ***Ủy ban ANSI X3.T1*** Trong tiêu chuẩn hóa, ban kỹ thuật mã hóa của ANSI.

ANSI X3.92 - 1981 ***chuẩn ANSI X3.92 - 1981*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về thuật toán mã hóa dữ liệu. *Xem* data encryption algorithm.

ANSI X3.105 - 1983 ***chuẩn ANSI X3.105 - 1983*** Trong tiêu chuẩn hóa, tiêu chuẩn của ANSI về mã liên kết dữ liệu. *Xem* OSI security.

ANSI X3.106 - 1983 ***chuẩn ANSI X3.106 - 1983*** Trong tiêu chuẩn hóa, tiêu chuẩn của ANSI về các chế độ vận hành đối với thuật toán mã hóa dữ liệu. *Xem* ANSI X3.92 - 1981, data encryption algorithm.

ANSI X3.118 - 1984 ***chuẩn ANSI X3.118 - 1984*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về số hiệu nhận dạng cá nhân - bộ đệm PIN. *Xem* PIN pad.

ANSI X9.2 - 1980 ***chuẩn ANSI X9.2 - 1980*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả trao đổi thông tin đối với bên nợ và trao đổi thông báo thẻ tín dụng giữa các cơ sở tài chính.

ANSI X9.3 - 1981 ***chuẩn ANSI X9.3 - 1981*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI đối với đặc tả chứng thực đằng sau sức (ký hậu séc).

ANSI X9.5 - 1988 ***chuẩn ANSI X9.5 - 1988*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI đối với hệ thống đánh số tổ chức

tài chính (FINS).

ANSI X9.7 - 1988 ***chuẩn ANSI X9.7 - 1988*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI đối với cơ sở séc ngân hàng và lĩnh vực doanh số tiện lợi.

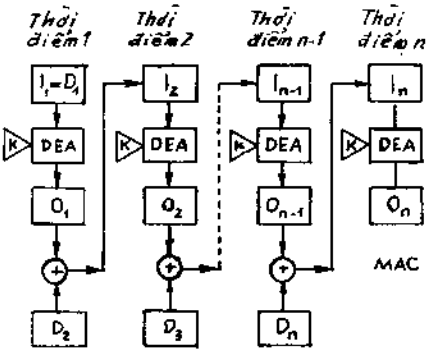
ANSI X9.8 - 1982 ***chuẩn ANSI X9.8 - 1982*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về quản lý và an toàn số hiệu nhận dạng cá nhân. *Xem* PIN management and security.

ANSI X9.9 - 1986 ***chuẩn ANSI X9.9 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI đối với xác thực thông báo tổ chức tài chính. Tiêu chuẩn xem xét các thông báo tài chính, bao gồm những sự chuyển khoản quỹ, thư tín dụng, những chuyển khoản chứng khóan, các hợp đồng cho vay và kiểm soát ngoại hối. Tiêu chuẩn định nghĩa một tập hợp tối thiểu các phần tử thông báo cần có trong quá trình xác thực. Tập hợp tối thiểu đó là:

- giá trị giao dịch và loại tiền tệ;
- nhận dạng tín dụng, các bên nợ và có;
- ngày tính giá trị;
- ngày xuất thông báo;
- ký tự nhận diện thông báo.

Tiêu chuẩn cũng cho phép xác thực toàn bộ văn bản của thông báo.

Việc xác thực đảm bảo rằng, bên nhận thông báo có thể kiểm tra xem nội dung



ANSI X9.9: *chuẩn ANSI X9.9.* Trong thuật toán xác thực, thông báo được ráp thành các khối dữ liệu 64 bit (T_n). Khối thứ nhất (D_1) đi qua DEA, DEA sử dụng khóa mật (K) để tạo ra 64 bit ở thanh ghi ra (O_1). Khối 64 bit dữ liệu thứ hai (D_2) cần xác thực được cộng theo phép "loại trừ-hoặc" (EXCLUSIVE-OR) từng bit một với 64 bit ở thanh ghi xuất, và kết quả được nạp vào thanh ghi nhập (I_2). Quá trình được tiếp tục cho tới khi 64 hoặc vài bit còn lại cần xác thực. 32 bit bên trái nhất của đầu ra cuối cùng (O_n) được lấy làm MAC. 32 bit còn lại là phần dư MAC, không tạo thành một phần của tiêu chuẩn, nhưng có thể dùng để xác thực người gửi thông báo bằng cách lập một yêu cầu mà người gửi phải đáp lại. *Các ký hiệu*: I, nhập; DEA, thuật toán mã hóa dữ liệu; O, xuất; K, khóa DEA; D, khối dữ liệu; +, hàm "EXCLUSIVE-OR".

thông báo có bị thay đổi ngẫu nhiên hay cố ý không. Một tổng kiểm tra đơn giản cho biết chắc về sự sai lạc ngẫu nhiên, song kẻ tấn công có thể tính toán lại tổng kiểm tra cho một thông báo đã bị sửa đổi. Một tổng kiểm tra đã mã hóa cho biết chắc về sự sửa đổi cố ý vì kẻ tấn công không có khả năng tính lại tổng kiểm tra đã mã hóa.

Việc thực hiện tiêu chuẩn đòi hỏi người gửi tạo ra mã xác thực thông báo (MAC) nhờ dùng thuật toàn mã hóa dữ liệu, MAC được gộp vào thông báo gửi tới bên nhận. Người nhận nhờ sử dụng cùng khóa DEA mật. Sau đó anh ta so sánh MAC được tạo ra với MAC gộp trong thông báo. Bất kỳ sự không khớp nào giữa hai MAC đều cho thấy rằng một hoặc nhiều phần tử thông báo gộp trong quá trình xác thực đã bị sửa đổi. Cả bên gửi lẫn bên nhận đều phải dùng chung khóa mật và thỏa thuận về các phần tử thông báo cần đưa vào quá trình xác thực. Khóa đó phải được tự động thay đổi đều đặn, ví dụ nhờ các thủ tục quy định ở ANSI X9.17.

Theo thỏa thuận giữa hai bên, thuật toán xác thực có thể được áp dụng cho toàn bộ thông báo hoặc cho những phần tử chọn lọc của thông báo. Nếu xác thực toàn bộ thông báo thì thân thông báo phải không được thay đổi giữa người gửi và người nhận; thông tin ở phần đầu và đuôi dùng cho mục đích truyền phải được bỏ đi.

Nếu chỉ có các phần tử thông báo riêng được xét tới trong quá trình xác thực thì tiêu chuẩn xác định chi tiết tập hợp tối thiểu các phần tử thông báo và cách chọn lọc chúng để đưa vào thuật toán xác thực. Thuật toán xác thực được áp dụng nhờ sử dụng các chế độ xích khối mã hoặc hồi tiếp mã trong thao tác DES. 64 bit dữ liệu đầu tiên được dùng làm biến khởi đầu còn dữ liệu còn lại đưa vào thường trình mã hóa cho tới khi xử lý khối dữ liệu cuối cùng. Khối này có thể bổ sung các số 0 tạo thành khối đủ 64 bit nếu cần. 32 bit bên trái nhất của khối dữ liệu cuối cùng được lấy làm MAC.

Xem ANSI X9.17 - 1985, authentication, cipher block chaining, cipher feedback, DEA, MAC, MAC residue, value date.

ANSI X9.12 - 1983 ***chuẩn ANSI X9.12 - 1983*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả các chứng khoán cấp thành phố đã đăng ký đầy đủ.

ANSI X9.13 - 1983 ***chuẩn ANSI X9.13 - 1983*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả xếp đặt và bố trí việc in bằng nhận dạng ký tự mực từ (MICR). *Xem* MICR.

ANSI X9.14 - 1983 ***chuẩn ANSI X9.14 - 1983*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả các mẫu điền trao đổi giao dịch chứng khoán.

ANSI X9.16 - 1984 ***chuẩn ANSI X9.16 - 1984*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về các khuôn dạng cho các kiểu thông báo, tiêu chuẩn.

ANSI X9.17 - 1985 ***chuẩn ANSI X9.17 - 1985*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về quản lý khóa của tổ chức tài chính (bán buôn).

Phạm vi của tiêu chuẩn bao gồm những vấn đề sau:

- Kiểm soát trong thời hạn tồn tại tư

liệu khóa mã để ngăn ngừa sự tiết lộ, sửa đổi hoặc thay thế không được phép.

- Phân phối tư liệu khóa mã để cho phép giữa thiết bị khóa mật mã hoặc các phương tiện sử dụng thuật toán DEA có khả năng liên vận hành.
- Đảm bảo tính toàn vẹn của tư liệu khóa mã trong tất cả các giai đoạn tồn tại của nó, bao gồm tạo ra, phân phối, lưu giữ, nhập vào, sử dụng và hủy bỏ.
- Khôi phục trong trường hợp quá trình quản lý khóa có sự cố hoặc khi tính toàn vẹn của tư liệu khóa mã có vấn đề.

Các chức năng của hệ quản lý khóa là cung cấp các khóa và các vectơ khởi đầu (IV) tới những nơi có yêu cầu và duy trì sự bí mật của các khóa. Các biện pháp phải ngăn ngừa được sự tiết lộ, sửa đổi, thay thế, chèn và xóa các khóa và các IV.

Các khóa có thể được phân phối thủ công hoặc tự động, tức là nhờ sự phân phối tự động hóa. Kiến trúc phân phối tự động hóa dựa trên giả thiết rằng, mạng dữ liệu sẽ có thể mở rộng được và một cặp bên liên lạc có một khóa mã hóa khóa chung, hoặc mỗi bên có một khóa mã hóa khóa chung với trung tâm.

Có thể sử dụng kiến trúc phân phối khóa hai hoặc ba lớp. Với kiến trúc hai lớp, khóa mã hóa khóa lớp trên cùng thường phân phối thủ công còn các khóa dữ liệu tương ứng với sự phân phối tự động sẽ được mã hóa bằng các khóa lớp trên cùng (cao nhất). Trong kiến trúc ba lớp, lớp cao nhất lại là khóa mã hóa khóa được phân phối thủ công, lớp thứ hai bao gồm các khóa mã hóa khóa được mã hóa bằng khóa lớp thứ nhất, và đến lượt mình nó lại được sử dụng để mã hóa các khóa dữ liệu lớp thứ ba. Kiến trúc được thiết kế để đáp ứng những yêu cầu nêu dưới đây.

- Các cặp liên lạc có ít nhất một khóa dữ liệu có thể thay đổi một cách tự động.
- Khóa dữ liệu có thể dùng để hoặc mã hóa, hoặc xác thực, nhưng không dùng được cho cả hai, trừ trong trường hợp các thông báo dịch vụ mật mã.
- Các khóa dữ liệu dùng chung bởi hai bên liên lạc phải đảm bảo không bị tiết lộ hoặc sử dụng bởi bên thứ ba ngoài trung tâm phân phối hoặc dịch khóa.
- Việc dàn xếp một khóa dùng chung bởi một cặp liên lạc không được tiết lộ cho bất kỳ bên thứ ba nào.
- Kiến trúc phải hỗ trợ các cặp truyền thông không có các khả năng tạo khóa và phải hỗ trợ nhóm bất kỳ nào muốn khởi đầu liên lạc an toàn với nhóm khác bất kỳ.
- Có thể gửi các khóa dữ liệu để sử dụng hiện tại hoặc trong tương lai và phải đảm bảo an toàn và toàn vẹn cho khóa.
- Khóa được một cặp truyền thông sử dụng sẽ không được cố ý để cho cặp bất kỳ nào khác hoặc cũng cặp đó dùng sau khi một bên trong cặp đó đã thôi không sử dụng nó nữa.
- Mỗi bên trong cặp liên lạc có thể ngừng sử dụng một khóa.
- Mỗi cặp liên lạc bất kỳ có thể sử



dụng nhiều hơn một khóa mã khóa.

- Kiến trúc cho phép hai, hoặc ba, lớp các khóa và trong kiến trúc ba lớp, các khóa mã khóa có thể được trao đổi tự động giữa các cặp truyền thông.

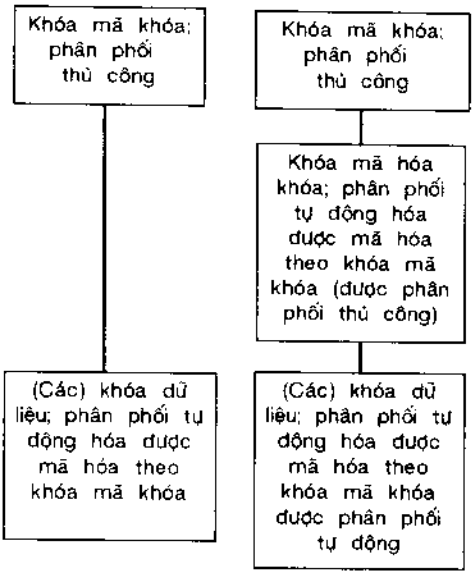
Quá trình tạo khóa và IV cho phân phối thủ công và tự động phải đảm bảo bảo vệ các tài nguyên phân phối và lưu giữ khỏi bị sử dụng, thay đổi, thay thế và phá hủy trái phép. Các quá trình sinh khóa đối với các khóa, các IV phân phối thủ công phải được kiểm soát kép.

Sự phân phối tự động các khóa có thể được tiến hành trong các môi trường điểm tới điểm, môi trường trung tâm phân phối khóa hoặc trung tâm dịch khóa. Trong môi trường điểm tới điểm, ít nhất một bên trong cặp truyền thông phải có khả năng tạo ra hoặc thu được các khóa và hai bên dùng chung khóa mã khóa. Trong môi trường trung tâm phân phối khóa, các bên riêng rẽ dùng chung các khóa mã khóa với trung tâm chứ không dùng chung khóa với nhau. Bên khởi đầu yêu cầu một hay nhiều khóa dữ liệu từ trung tâm sẽ cung cấp các chi tiết về danh tính người nhận đã định. Trung tâm tạo hoặc nhận các khóa dữ liệu. Khóa dữ liệu được mã hóa bằng khóa mã khóa dùng chung giữa người khởi đầu và trung tâm, khóa dữ liệu đó cũng được mã bằng khóa mã khóa dùng chung với người nhận. Sau đó cả hai tập khóa đã mã được chuyển tiếp tới người khởi đầu. Khi nhận được các tệp khóa dữ liệu đã mã, người khởi đầu gửi tập thứ hai cho người nhận đã định. Môi trường trung tâm dịch khóa hoạt động theo cách tương tự trừ một điều là người khởi đầu có khả năng tạo ra, hoặc thu được một khóa dữ liệu. Trong trường hợp này, người khởi đầu mã hóa khóa dữ liệu bằng khóa mã khóa dùng chung với trung tâm dịch khóa và gửi nó cho trung tâm cùng với danh tính của người nhận đã định. Trung tâm giải mã khóa đã mã nhận được, mã hóa lại nó bằng khóa mã khóa dùng chung giữa trung tâm và người nhận đã định và gửi trả kết quả lại cho người khởi đầu.

Các khóa dùng trong các quá trình nêu ở trên có thể là khóa đơn lẻ hoặc các cặp khóa. Một cặp khóa gồm hai khóa độc lập; quá trình mã hóa bằng một cặp khóa liên quan tới sự mã hóa bằng khóa này (của cặp), giải mã kết quả bằng khóa còn lại, tiếp theo lại mã hóa lại bằng khóa đầu. Sự giải mã là các quá trình ngược lại, tức là giải mã bởi khóa thứ nhất, mã hóa bởi khóa thứ hai, mã hóa bởi khóa thứ hai và sau đó giải mã bằng khóa thứ nhất. Mã hóa và giải mã các cặp khóa bằng các cặp khóa khác bao gồm những quá trình trên mỗi phần tử của cặp khóa nêu ở trên và nối ghép kết quả đầu ra của các quá trình.

Các bên liên lạc cũng sử dụng những bộ đếm để theo dõi các thông báo giữa các bên cụ thể. Người khởi đầu cập nhật bộ đếm với mỗi thông báo đã truyền thích hợp còn người nhận cập nhật "số đếm mong đợi" đối với người khởi đầu khi nhận một thông báo. Người nhận sẽ tiến hành tác động thích hợp nếu số đếm gộp trong thông báo không tương ứng với "số đếm mong đợi" đối với người khởi đầu, ví dụ nếu

số đếm nhỏ hơn số đếm mong đợi thì thông báo lỗi sẽ được trả lại cho người khởi đầu. Giá trị bộ đếm (dịch vị) cũng có thể được kết hợp với khóa mã khóa và kết quả được dùng để mã hóa khóa khác để truyền. Công chứng khóa là phương pháp chính thức công nhận các khóa có các mã nhận dạng các cặp truyền thông. Dòng ký tự 16 byte biểu diễn các mã nhận dạng của mỗi bên được tạo ra và kết hợp, qua các quá trình mã hóa bằng khóa mã khóa. Kết quả của những thao tác đó tạo ra một khóa công chứng dùng để mã hóa khóa mã hoặc khóa dữ liệu.



(a) Hai lớp (b) Ba lớp

ANSI X9.17 - 1985: *chuẩn ANSI X9.17 - 1985.* Kiến trúc phân phối khóa hai và ba lớp

Tiêu chuẩn xác định các thông báo được trao đổi giữa các bên truyền thông, các trung tâm phân phối khóa và dịch khóa. Những thông báo dịch vụ mật mã (CSM) đó bao gồm: khởi đầu dịch vụ yêu cầu (RSI), thông báo dịch vụ khóa (KSM), thông báo dịch vụ đáp (RSM), thông báo dịch vụ báo lỗi (ESM), thông báo dịch vụ ngắt (DSM), thông báo yêu cầu dịch vụ (EFS), thông báo trả lời dịch vụ yêu cầu (RTR) và thông báo của dịch vụ khôi phục lỗi (ERS).

Thông báo khởi đầu dịch vụ yêu cầu là một thông báo tùy chọn nhằm yêu cầu khởi đầu một quan hệ khóa mã mới. Thông báo dịch vụ khóa mã chuyển khóa từ một người gửi tới người nhận, còn thông báo dịch vụ đáp tạo ra lời đáp đã xác thực cho một KSM. Lỗi trong CSM trước đó được báo cáo trong thông báo dịch vụ báo lỗi và các khóa có thể được ngắt bởi một thông báo dịch vụ ngắt.

Các CSM sử dụng trong các môi trường trung tâm phân phối khóa hoặc dịch khóa là:

- thông báo yêu cầu dịch vụ gửi các khóa tới trung tâm dịch khóa để dịch nhằm dành cho người nhận cuối cùng;
- thông báo đáp lại dịch vụ yêu cầu trả lời cho RFS, ERS hoặc RSI;
- thông báo dịch vụ khôi phục lỗi báo cáo số đếm và các lỗi về khóa cho trung tâm, yêu cầu đồng bộ hóa lại các trường số đếm và khởi động lại dịch vụ.

Xem authentication, communicating pair, cryptographic equipment, crypto- graphic key, cryptographic service message, data key, DEA; dual control, initialization vector, interoperability, IV, key encrypting key, key distribution center, key generator, keying material, key management, key notarization, key pair,

key translation center, multiple DES encipherment, offset, originator, point to point, recipient, three layer architecture, two layer architecture.

ANSI X9.18 - 1986 ***chuẩn ANSI X9.18 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả giấy làm séc.

ANSI X9.19 - 1986 ***chuẩn ANSI X9.19 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về xác thực thông báo bán lẻ của tổ chức tài chính.

ANSI X9.20 - 1986 ***chuẩn ANSI X9.20 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về chứng khoán hệ giao hàng của tổ chức.

ANSI X9.21 - 1986 ***chuẩn ANSI X9.21 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về từ vựng và các phần tử dữ liệu cho chuyển quỹ bán buôn và các thông báo có liên quan.

ANSI X9.22 - 1986 ***chuẩn ANSI X9.22 - 1986*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về đặc tả các khuôn thức telex tiêu chuẩn cho các thông báo dịch vụ tài chính bán buôn.

ANSI X9.23 - 1988 ***chuẩn ANSI X9.23 - 1988*** Trong tiêu chuẩn hóa, tiêu chuẩn ANSI về mã hóa các thông báo tài chính bán buôn của tổ chức tài chính.

answer back ***tín hiệu hồi đáp*** Trong truyền thông dữ liệu, tín hiệu do thiết bị nhận gửi cho trạm gửi để định dạng hoặc để chỉ báo rằng nó đã sẵn sàng để truyền. *Xem* voice answer back.

answering ***đáp, trả lời*** Trong truyền thông dữ liệu, quá trình đáp lại trạm gọi để hoàn thành việc thiết lập nối giữa các trạm dữ liệu. *Xem* station.

Anthrax-Boot ***virut Anthrax-Boot*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm bảng phân chia đĩa cứng, ảnh hưởng tới thao tác trong thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

Anthrax-File ***virut Anthrax-File*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM và EXE, ảnh hưởng tới thao tác trong thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

anti-eavesdrop device ***thiết bị chống nghe lén*** Trong an toàn vật lý, thiết bị phát hiện sự có mặt các dụng cụ nghe lén bằng cách quét các tần số truyền RF. *Xem* electronic countermeasures sweeping, RF.

anti-fixed point ***điểm không cố định*** Trong mật mã học, khối văn bản rõ vốn được biến đổi thành phần bù của nó nhờ thuật toán mật mã. Trong DES, nếu sử dụng một khóa bán yếu tự đối ngẫu thì có 2^{32} điểm không cố định. *So sánh với* fixed point. *Xem* anti-palindromic key, complement, data encryption standard, plaintext, semiweak key.

anti-jam ***chống nghẽn*** Trong an toàn máy tính, chỉ các bộ quay số điện thoại đặc biệt được thiết kế để ngăn ngừa sự ngắt quay số bởi các cuộc gọi tới. *Xem* telephone intrusion, telephone dialer.

anti-palindromic key ***khóa tự đối ngẫu*** Trong mật mã học, khóa DES trong đó khóa con 1 là phần bù của khóa con 16, khóa con 2 là phần bù của

khóa con 15 v.v.. Bốn khóa ba yếu của DES có tính chất này. *So sánh với* palindromic key. *Xem* complement, cryptographic key, data encryption, standard, semiweak key, sub-key.

anti-passback ***chống chuyển ngược*** Trong an toàn vật lý, chỉ một hệ thống được thiết kế để ngăn ngừa "chuyền ngược" thẻ truy nhập từ một cá nhân đã truy nhập được. Biện pháp này đảm bảo rằng thẻ đã dùng để nhập vào một vùng cũng được sử dụng để thoát khỏi vùng đó trước khi nó được sử dụng lại để vào. *Xem* tailgating.

anti-surveillance ***chống theo dõi*** Trong an toàn vật lý, chỉ một hệ được thiết kế để ngăn ngừa hoặc phát hiện việc sử dụng thiết bị theo dõi. *Xem* anti-eavesdrop device.

anti-viral measures ***(các) biện pháp chống virut*** Trong an toàn máy tính, các biện pháp được áp dụng để ngăn ngừa sự tấn công của các virut máy tính và khôi phục sau sự tấn công như thế. Mặc dù có nhiều chương trình được coi là phòng và diệt được virut nhưng không có biện pháp bảo vệ hoàn hảo nào chống lại virut. Phải thừa nhận là không có thuộc tính đơn lẻ nào chắc có trong virut lại không có khả năng có ở một đoạn mã hợp pháp và không có một tác động đơn lẻ nào do virut thực hiện lại không có khả năng do một đoạn mã hợp pháp thực hiện.

Các sản phẩm chống virut có xu hướng rơi vào một trong ba nhóm như sau:

- *Nhóm 1*: ngăn ngừa lây nhiễm nhằm chấm dứt các quá trình sao chép virut và ngăn ngừa lây nhiễm ban đầu;
- *Nhóm 2*: phát hiện lây nhiễm, nhằm tìm ra những sự tấn công của virut ngay khi chúng vừa xảy ra, đánh dấu những bộ phận cụ thể bị nhiễm và cho phép tiến hành tác động chữa trị;
- *Nhóm 3*: nhận dạng lây nhiễm chỉ ra những kiểu đặc thù của dòng virut, nó sẽ nhận diện các virut trong các hệ thống và có thể loại bỏ chúng, nhưng chỉ có tác dụng đối với những virut đã biết.

Các sản phẩm ở nhóm thứ nhất chặn các tín hiệu có vẻ "khả nghi" và thông báo cho người sử dụng.

Việc phát hiện có hiệu quả có thể xảy ra sau khi chúng đã tấn công. Như vậy các sản phẩm nhóm hai có thể ít gặp khó khăn hơn trong việc phân biệt tác động hợp pháp và tác động ác ý. Mặt khác, sự lây nhiễm ảnh hưởng ít nhất tới một chương trình; mục đích của sản phẩm là cảnh báo cho người sử dụng khi bắt đầu có lây nhiễm để có thể ngăn ngừa sự lan truyền tiếp, giảm tối thiểu hư hại.

Một kỹ thuật chung của sản phẩm nhóm 2 là:

- tính toán tổng kiểm tra trên phần mềm "sạch" và lưu giữ kết quả;
- trước khi chạy phần mềm, tính toán lại tổng kiểm tra và so sánh kết quả với kết quả đã lưu;
- cho phép thi hành chương trình nếu hai tổng kiểm tra giống nhau, nếu không sẽ hủy bỏ việc thi hành và hiển thị thông báo cảnh báo.

Đây là sự bảo vệ có hiệu quả có thể được triển khai trong hoạt động bình thường. Nó sẽ phát hiện phần mềm bị nhiễm virut sắp gây lây nhiễm. Tuy

nhiên, giống như tất cả các biện pháp chống virut phải thừa nhận nó có các hạn chế:

- nó sẽ cho phép ít nhất một chương trình bị lây nhiễm;
- thường trình tổng kiểm tra phải phát hiện được những thay đổi rất nhỏ trong chương trình, việc lấy tổng kiểm tra như vậy tiêu tốn thời gian, gây ra sự chậm trễ phát bực đối với người sử dụng, một số thường trình tổng kiểm tra nhanh có nhanh hơn nhưng lại không phát hiện được những thay đổi nhỏ trong chương trình;
- thường trình chỉ cho một sự đảm bảo về tính toàn vẹn của chương trình vào thời điểm so sánh tổng kiểm tra, nếu chương trình bị nhiễm virut giữa thời điểm kiểm tra tổng kiểm tra và thực hiện chương trình thì tệp tiếp theo sẽ bị lây nhiễm, tức là tấn công TOCTTOU cổ điển (thời gian kiểm tra tới thời gian cập nhật);
- một số bộ chương trình phần mềm, ví dụ như Word Perfect, tự sửa đổi và do đó có thể gây ra các cảnh báo sai;
- đối với virut chắc là không có khả năng tính lại tổng kiểm tra đối với chương trình bị nhiễm và sau đó cập nhật tổng kiểm tra đã nhớ.

Điểm cuối cùng có thể đáp ứng được bằng cách sử dụng các thường trình tổng kiểm tra mật mã và sử dụng khóa mật mà virut không thể truy nhập được.

Việc sử dụng các hệ nhóm 3 kiểm tra dấu hiệu của các virut đã biết là phổ biến vì nó rất tiện cho người sử dụng. Dấu hiệu virut được sử dụng trong sản phẩm phải nhận dạng được virut. Nếu được sử dụng một cách khôn ngoan, các sản phẩm trong nhóm này có thể bổ sung hữu ích cho các thủ tục an toàn máy tính cá nhân tốt, nhưng chúng có một số nhược điểm rõ ràng:

- phải duy trì cập nhật được danh sách các dấu hiệu virut;
- các virut có thể thay đổi đột biến để thay đổi dấu hiệu của chúng và do đó tránh được sự phát hiện;
- chỉ phát hiện được những virut đã biết.

Trong trường hợp của tất cả các sản phẩm chống virut, điều quan trọng là đảm bảo để virut không thể nắm quyền kiểm soát ở giai đoạn đầu tiên và bỏ qua hoặc sửa đổi có hiệu quả tác động của sản phẩm chống virut.

Ngoài việc phát hiện virut, một số sản phẩm tự cho là diệt được virut, tức là loại bỏ được mã virut khỏi đĩa. Tác dụng đó có một sức hấp dẫn nào đó đối với người sử dụng, nhưng không cần thiết và nó chứa đựng những mối nguy cố hữu đối với phần mềm và dữ liệu của người sử dụng.

Nếu một thường trình dự phòng nhạy cảm được bảo trì cho phần mềm và dữ liệu, thì phương tiện diệt một virut chắc chắn nhất là khởi động theo cách đảm bảo cho virut không thể nắm quyền kiểm soát, định dạng lại đĩa đã bị lây nhiễm, ghi đè tất cả các tệp và tải phần mềm và dữ liệu vào từ tệp dự phòng không bị nhiễm. Các cố gắng diệt virut có thể là không hoàn hảo; các tấn công của virut thường trở lại sau những cố gắng loại bỏ rõ ràng thành công các đoạn mã bị nhiễm. Các sản phẩm diệt

virut cũng có thể dẫn tới phá hỏng dữ liệu của người sử dụng, nhất là nếu tác động của virut với dấu hiệu nào đó đột biến gây ra sự thay đổi trong bản chất của mã virut. Người ta đã khuyến nghị rất nhiều rằng các thủ tục an toàn đối với các máy tính cá nhân, nhất là những thủ tục trong các tổ chức có nhiều người còn chưa hiểu biết về tin học, cần có sự bảo vệ theo chiều sâu, tránh các virut, những biến cố và an toàn dữ liệu khác. Những khía cạnh quan trọng nhất của một chính sách như vậy là:

- kiểm soát chặt chẽ việc nhập khẩu phần mềm;
- nhóm trung tâm kiểm tra và chứng thực mọi phần mềm mới trước khi chuyển nó cho người sử dụng;
- thông tin và dịch vụ trợ giúp trực tuyến cho người sử dụng, cảnh báo các triệu chứng virut, khuyên người sử dụng báo cáo lại hành vi bất thường của phần mềm;
- áp dụng chặt chẽ các chương trình dự phòng;
- các thủ tục khôi phục cần được tiến hành bởi một ban có thẩm quyền về mặt kỹ thuật;
- hạn chế nhân viên sử dụng máy tính, ví dụ cấm sử dụng máy tính để chơi trò chơi, ấn định cho những sinh viên làm một phần thời gian ở đại học v.v., một số tổ chức dành một máy tính cho việc sử dụng không chính thức như thế và cấm xử lý dữ liệu của tổ chức trên máy chuyên dụng.

Bảng mạch chứa bộ mã hóa cho phép bảo vệ các máy tính cá nhân khỏi việc sử dụng trái phép, kéo theo rủi ro nhiễm virut. Mọi phần mềm trên đĩa cứng đều được mã hóa và cần trình mật khẩu trước khi có thể đưa dữ liệu hoặc chương trình từ đĩa mềm vào. Người sử dụng hợp pháp dùng máy có cắm tấm mạch thiết bị mã được đảm bảo rằng không người sử dụng không được phép nào có cơ hội đưa phần mềm nhiễm virut vào. *Xem* encryptor board, TOCTTOU problems, virus.

AOSS ***hệ AOSS*** Trong tin học, viết tắt của Automated Office Support Systems (hệ hỗ trợ văn phòng tự động hóa), bao gồm các bộ vi xử lý độc lập, các bộ xử lý văn bản và các thiết bị đầu cuối nối với các máy chính.

API ***API*** *Xem* application program interface, automatic personal identification. *Đồng nghĩa với* biometrics.

application confidentiality ***độ bí mật ứng dụng*** Trong an toàn máy tính, trạng thái tồn tại khi mã nguồn và mã đối tượng ứng dụng và bộ hồ sơ được lưu giữ một cách tin cậy và được bảo vệ khỏi sự tiết lộ không được phép. *So sánh với* ADP availability, application integrity. *Xem* confidentality, data confidentality, object code, source code.

application disaster recovery plan ***kế hoạch khôi phục thảm họa ứng dụng*** Trong quản lý rủi ro, kế hoạch phục hồi lại hoạt động của một chương trình ứng dụng sau khi nó đã bị ngừng một khoảng thời gian. *Xem* disaster recovery.

application integrity ***toàn vẹn ứng dụng*** (1) Trong an toàn máy tính, những quá trình nhằm đảm bảo rằng một ứng dụng, được xem như một hệ,

tiếp tục hoạt động theo các đặc tả của nó và duy trì khả năng sử dụng. *So sánh với* denial of service. (2) Trong an toàn máy tính, trạng thái tồn tại khi mã nguồn và mã đối tượng giống như lúc được phát triển, được chứng thực/chính thức công nhận ban đầu hoặc chúng đã sửa đổi, được thử phù hợp với những chuẩn và thủ tục đã thiết lập và được chứng thực/chính thức công nhận lại và không bị những thay đổi hoặc hủy hoại vô tình hay cố ý. *So sánh với* ADP availability, application confidentiality. *Xem* data integrity, object code, source code.

application layer ***tầng ứng dụng*** Trong truyền thông dữ liệu, tầng trên cùng trong mô hình kết nối các hệ thống mở của ISO. Tầng này có thể cung cấp rất nhiều dịch vụ cho người sử dụng, ví dụ như giải quyết vấn đề các thiết bị đầu cuối không tương thích trên mạng, các giao thức chuyển tệp, thư điện tử v.v.. *So sánh với* data link layer, network layer, physical layer, presentation layer, session layer, transport layer. *Xem* electronic mail, network virtual terminal, open systems interconnection, X.400.

application process ***quá trình ứng dụng*** (1) Trong an toàn máy tính, quá trình không tin cậy thực hiện tính toán ở phía người sử dụng. *Xem* trusted process. (2) Trong truyền thông dữ liệu, một phần bên trong một hệ mở vốn xử lý thông tin và sử dụng các dịch vụ truyền thông kết nối hệ thống mở để giao tiếp với những quá trình ứng dụng khác trong các hệ thống mở khác. *Xem* open systems interconnection.

application program ***chương trình ứng dụng*** Trong tin học, chương trình thường viết tại cơ sở cho một ứng dụng riêng của người sử dụng, ví dụ như bảng lương.

application program interface ***giao diện chương trình ứng dụng*** Trong tin học, tập hợp các lệnh mà một ứng dụng có thể thực hiện đối với một modun phần mềm cung cấp một dịch vụ xác định, ví dụ như dịch vụ mật mã.

application software ***phần mềm ứng dụng*** Trong tin học, các đoạn chương trình và các chương trình được thiết kế bởi, hoặc cho những người sử dụng hệ thống hoặc khách hàng. Thông qua việc sử dụng thiết bị hệ thống tự động hóa có sẵn và phần mềm cơ bản, phần mềm ứng dụng hoàn thành những nhiệm vụ, công việc hoặc chức năng định hướng công tác cụ thể. Nó có thể là những bộ chương trình đa năng, như kế toán nhu cầu quỹ, bảng lương, điều khiển máy công cụ v.v., hoặc những chương trình ứng dụng riêng được thay đổi để hoàn thành một hay một số hạn chế các chức năng của người sử dụng, ví dụ như nhân sự ở mức cơ bản, bảo quản kho, theo dõi tên lửa hoặc vệ tinh v.v.. Trừ những bộ chương trình đa dụng nhận trực tiếp từ những người bán phần mềm hoặc những nhà sản xuất thiết bị từ gốc (OEM), còn thì loại phần mềm này nói chung được người sử dụng phát triển với các tài nguyên tại cơ sở hoặc thông qua các dịch vụ ký kết. *Đồng nghĩa với* application program.

approval/accreditation ***phê chuẩn/chứng nhận*** Trong an toàn máy tính, sự cấp quyền chính thức cho một hệ

ADP để xử lý thông tin nhạy cảm trong môi trường hoạt động của nó, dựa trên sự đánh giá an toàn toàn diện về thiết kế an toàn phần cứng, phần sụn và phần mềm, cấu hình và cài đặt của hệ thống và về những sự kiểm soát an toàn thủ tục, hành chính, vật lý, Tempest, nhân sự và truyền thông khác của hệ thống. *Xem* accreditation, Tempest.

approval to operate ***phê chuẩn cho hoạt động*** Trong an toàn máy tính, sự chấp nhận của DAA cho rằng đã dự phòng một mức an toàn thỏa đáng (các yêu cầu tối thiểu đã được đáp ứng và có một mức rủi ro chấp nhận được). Nó cấp quyền hoạt động cho một hệ thống tự động hóa hoặc mạng ở một phương tiện máy tính. Sự chấp nhận xuất phát từ việc DAA phân tích các xác nhận về phương tiện máy tính, hệ tự động hóa và hệ thống dữ liệu tự động và môi trường hoạt động của thực thể trong hệ tự động hóa. *Xem* accreditation, DAA.

approved circuit ***mạch được chấp nhận*** *Đồng nghĩa với* protected wireline distribution system.

a priori control ***kiểm soát tiên nghiệm*** Trong an toàn cơ sở dữ liệu, một dạng kiểm soát suy luận quyết định trước xem có thể phát hành một tập các số liệu thống kê mà không gây tiết lộ bí mật cá nhân hay không. *So sánh với* audit based control, memoryless control. *Xem* inference control, personal disclosure.

AR ***AR*** Viết tắt của Army Regulation (điều lệ quân đội).

Arab Virus ***virut Arab*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động trong thời gian chạy và làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

arbiter ***trọng tài*** Trong quá trình xác thực, một bên giữ dữ liệu công cộng do người sử dụng tạo ra và được người nhận sử dụng để phê chuẩn các chữ ký. *Xem* arbitrated signature.

arbitrated signature ***chữ ký đã qua trọng tài*** Trong quá trình xác thực, chữ ký số liên quan tới bên thứ ba, trọng tài. Thông báo đã ký được người gửi chuẩn bị và chuyển tới trọng tài. Trọng tài kiểm tra danh tính của người gửi, ký vào thông báo và sau đó phê chuẩn nó cho người nhận. *So sánh với* universal signature. *Xem* digital signature.

arc-breakdown protector ***bộ bảo vệ chống hồ quang đánh thủng*** Trong an toàn vật lý, thiết bị để bảo vệ thiết bị điện chống điện áp tăng quá mức, như những điện áp do sét gây ra ở các đường dây tải điện. *Xem* arrester.

architecture ***kiến trúc*** (1) *Xem* security architecture. (2) Trong tin học, đặc tả các quan hệ giữa các bộ phận của một hệ máy tính. *Xem* von Neumann.

archive ***lưu trữ // kho lưu*** (1) Trong các quá trình hoạt động, lưu trữ là giữ lại các bản ghi hoặc các tệp ngoại tuyến. (2) Trong các quá trình hoạt động, kho lưu là nơi giữ các bản ghi hoặc tệp đã lưu giữ.

area mat ***thảm báo động*** Trong an toàn vật lý, tấm thảm cao su hoặc nhựa vinyl mỏng có các bộ cảm biến áp suất

dùng để phát hiện các cuộc đột nhập. *Xem* intrusion detector. *Đồng nghĩa với* floor sensor.

area protection ***bảo vệ khu vực*** Trong an toàn vật lý, việc sử dụng các bộ cảm biến siêu âm, vi ba, hồng ngoại hoặc quang điện để bảo vệ một khu vực xác định. *Xem* intrusion detector. *Đồng nghĩa với* space protection.

Armageddon ***virut Armageddon*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động trong thời gian chạy và làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

arming station ***trạm vận hành báo động*** Trong an toàn vật lý, bảng phím điều khiển hoặc chuyển mạch phím dùng để đưa một hệ báo động vào chế độ phát hiện báo động.

ARPA ***ARPA*** *Xem* DARPA.

ARPANET ***mạng ARPA, mạng Arpanet*** Trong truyền thông dữ liệu, viết tắt của ARPA NETwork (mạng ARPA), mạng máy tính ban đầu được thành lập dưới sự đỡ đầu của Cơ quan các dự án nghiên cứu cao cấp để nghiên cứu các mạng máy tính và sử dụng chung các tài nguyên máy tính. Trách nhiệm về mạng được chuyển cho Cơ quan truyền thông quốc phòng năm 1975. Mạng Arpanet sau này được tách thành mạng nghiên cứu và phát triển, vẫn mang tên gọi Arpanet và mạng dữ liệu quốc phòng (DDN). *Xem* DDN, Internet, Milnet.

ARQ *Xem* automatic retransmisstion request.

array ***mảng*** Trong tin học, cấu trúc hoặc mẫu hình có trật tự của các mục tin hoặc các số, ví dụ như bảng các con số. *Xem* loop, vector.

array processor ***bộ xử lý mảng*** Trong kiến trúc, hệ máy tính được thiết kế để thực hiện các thao tác giống nhau đối với các phần tử của một mảng một cách song song. Nó có thể là thiết bị độc lập hoặc gắn kèm với một máy tính chính thông qua một bus trong hoặc cổng vào/ra. *Xem* parallel processing.

arrest ***ngăn chặn*** Trong an toàn máy tính, việc phát hiện hoạt động của người sử dụng không cần thiết cho xử lý dữ liệu bình thường có thể dẫn tới vi phạm tính an toàn hệ thống và buộc phải ngừng xử lý.

arrester ***bộ ngăn chặn*** Trong an toàn vật lý, thiết bị phi tuyến để triệt các chuyển tiếp điện áp do sét đánh, quá áp đường dây tải điện hoặc nhiễu. *Xem* arc breakdown protector.

artificial intelligence ***trí tuệ nhân tạo*** Sự tái tạo hoạt động trí óc bằng tính toán. Trong thực tế, trí tuệ nhân tạo là một bộ môn được định nghĩa hơi không rõ ràng liên quan tới nhiều khía cạnh mô phỏng trí tuệ của con người và sự tư duy của các hệ thống logic được thể hiện trong các chương trình máy tính. Những định nghĩa chính xác hơn thường khó hiểu bởi vì chủ đề này vẫn còn phôi thai, còn những sự bất đồng lớn về ranh giới riêng của nó giữa chính những người nghiên cứu nó. Động cơ cho nghiên cứu trí tuệ nhân tạo có hai phần. Một mặt, nó được theo đuổi với hy vọng rằng, việc áp dụng các

phương pháp tính toán chặt chẽ và logic kèm theo chúng có thể hé mở hoạt động tinh thần của con người. Nói nôm na hơn, động cơ chiếm ưu thế đằng sau nghiên cứu trí tuệ nhân tạo là ước muốn phú cho máy móc khả năng hoạt động linh hoạt hơn và truyền cảm hơn, cho phép sao chép một cách dễ dàng một số lĩnh vực chuyên môn của con người và có thể giải phóng cho công nhân những nhiệm vụ nguy hiểm và đơn điệu. *Xem* expert systems.

ARU ***ARU*** Viết tắt của Audio Response Unit (thiết bị đáp âm thanh). *Xem* audio response terminal.

AS 2805 ***chuẩn AS 2805*** Trong tiêu chuẩn hóa, tập hợp các tiêu chuẩn của Ôxtrâylia về chuyển qũy điện tử:

- Phần 1: Giao diện truyền thông và biểu diễn dữ liệu;
- Phần 2: Cấu trúc thông báo, khuôn thức và nội dung;
- Phần 3: Quản lý và an toàn PIN;
- Phần 4: Xác thực thông báo;
- Phần 5: Thuật toán mã hóa dữ liệu;
- Phần 6.1: Các nguyên tắc quản lý khóa
- Phần 6.2: Quản lý khóa - các khóa giao dịch;
- Phần 6.3: Quản lý khóa - các khóa phiên - nút tới nút;
- Phần 6.4: Quản lý khóa - các khóa phiên - đầu cuối tới cơ sở nhận;
- Phần 7: Nội dung thông báo POS;
- Phần 8: Nội dung thông báo tài chính;
- Phần 9: Bí mật truyền thông.

Xem ANSI X9.17 - 1985, data encryption standard, key management, message authentication, transaction key system.

AS 3801 - 1989 ***chuẩn AS 3801 - 1989*** Trong tiêu chuẩn hóa, tiêu chuẩn của Ôxtrâylia về trao đổi dữ liệu điện tử cho quản trị, thương mại và vận tải (EDIFACT) - các quy tắc cú pháp mức ứng dụng. *So sánh với* AS 3802 - 1991, AS 3803 - 1991, AS 3804 - 1991, AS 3805 - 1991. *Xem* EDIFACT, electronic data interchange.

AS 3802 - 1989 ***chuẩn AS 3802 - 1989*** Trong tiêu chuẩn hóa, tiêu chuẩn của Ôxtrâylia về các phần tử dữ liệu và khuôn thức trao đổi thông tin - biểu diễn trao đổi thông tin về ngày tháng và thời gian. *So sánh với* AS 3801 - 1991, AS 3803 - 1991, AS 3804 - 1991, AS 3805 - 1991.

AS 3803 - 1989 ***chuẩn AS 3803 - 1989*** Trong tiêu chuẩn hóa, tiêu chuẩn của Ôxtrâylia về trao đổi dữ liệu điện tử cho quản trị, thương mại và vận tải (EDIFACT) - hướng dẫn trao đổi thương mại. *So sánh với* AS 3804 - 1991, AS 3802 - 1991, AS 3804 - 1991, AS 3905 - 1991. *Xem* EDIFACT, electronic data interchange.

AS 3804 - 1989 ***chuẩn AS 3804 - 1989*** Trong tiêu chuẩn hóa, tiêu chuẩn của Ôxtrâylia về trao đổi dữ liệu điện tử đối với quản trị, thương mại và vận tải (EDIFACT) - bộ mã cồng Ôxtrâylia. *So sánh với* AS 3801 - 1991, AS 3802 - 1991, AS 3803 - 1991, AS 3804 - 1991. *Xem* EDIFACT, electronic data interchange.

ASA ***hiệp hội ASA*** Trong tiêu chuẩn hóa, viết tắt của American Standards Association (Hiệp hội tiêu chuẩn Hoa Kỳ), cơ quan với các nhóm chịu trách

nhiệm thiết lập các tiêu chuẩn xử lý dữ liệu.

ASCII ***mã ASCII*** Trong mã hóa, viết tắt của American Standard Code for Information Interchange (mã trao đổi thông tin tiêu chuẩn của Hoa Kỳ), đọc là ASKEE. Mã truyền dữ liệu tiêu chuẩn được đưa ra để đạt được tính tương thích giữa các thiết bị dữ liệu. Nó gồm 7 bit thông tin và 1 bit chẵn lẻ để kiểm tra lỗi, như vậy sẽ có 128 tổ hợp mã. Trong đó 32 tổ hợp dùng cho ký tự hoa và một số dấu câu, nhóm 32 tổ hợp khác dùng cho các chữ số, dấu cách và các ký hiệu dấu câu bổ sung, nhóm 32 tổ hợp mã thứ ba được gán cho các ký tự thường và một số dấu ít dùng. Tập 32 tổ hợp cuối cùng dành cho các lệnh máy và điều khiển, ví dụ như xuống dòng, trở lại đầu dòng. *Xem* International Alphabet Number 5, parity checking. *Đồng nghĩa với* USASCII.

ASET ***viện ASET*** Trong an toàn máy tính, viết tắt của Academy of Security Educators and Trainers (Học viện giáo dục và đào tạo về an toàn).

ASIS ***ASIS*** (1) Trong an toàn máy tính, viết tắt của American Society for Industrial Security (Hội an toàn công nghiệp Hoa Kỳ). (2) Viết tắt của American Society for Information Science (Hội khoa học thông tin Hoa Kỳ).

ASN.1 *Xem* abstract syntax notation 1.

assembler ***bộ hợp dịch*** Trong tin học, chương trình dịch chương trình nguồn viết bằng ngôn ngữ bậc thấp sang ngôn ngữ máy. *Xem* low level language, machine code instruction, source program, translator.

assembly language ***hợp ngữ*** Trong tin học, ngôn ngữ cho phép người lập trình phát triển chương trình mã máy có sử dụng các ký hiệu và quy ước dễ nhớ cho các vị trí nhớ và các thao tác. *So sánh với* high level language. *Xem* low level language, manchine code instruction, translator.

asset ***tài sản*** Trong an toàn thông tin, thông tin hoặc các tài nguyên cần phải bảo vệ bằng các biện pháp kỹ thuật và phi kỹ thuật của một mục tiêu đánh giá. *Xem* information technology security evaluation criteria, target of evaluation.

Association for Computing Machinery ***Hiệp hội máy tính*** Tổ chức khoa học máy tính chuyên nghiệp của Hoa Kỳ. Mục tiêu của nó là đẩy mạnh mọi khía cạnh của xử lý thông tin và khuyến khích trao đổi các kỹ thuật như thế giữa các chuyên gia và những người sử dụng máy tính.

associative law ***định luật kết hợp*** Trong toán học, một phép toán nhị nguyên, tức là phép toán liên quan tới hai biến, thỏa mãn định luật kết hợp nếu

$$x * (y * z) = (x * y) * z$$

trong đó x, y và z là các biến và * biểu thị phép toán nhị nguyên. *So sánh với* commutative law, distributed law. *Xem* Galois field.

assurance ***độ bảo đảm*** Trong an toàn máy tính, số đo độ tin cậy mà các đặc điểm an toàn và kiến trúc của một AIS dàn xếp chính xác và bắt tuân thủ chính sách an toàn. Nếu dựa vào các đặc điểm an toàn của một AIS để xử lý thông tin nhạy cảm và hạn chế truy

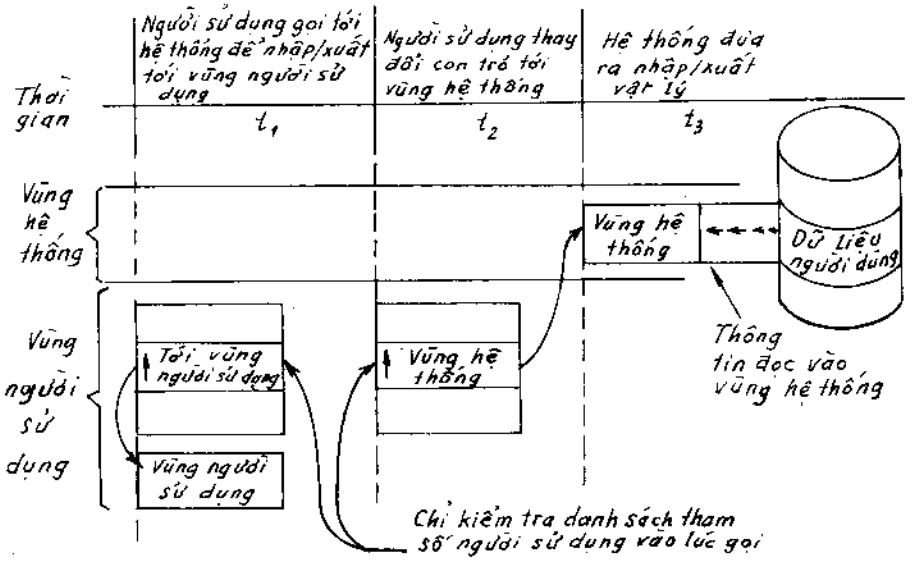
nhập của người dùng thì thử nghiệm chúng để đảm bảo rằng, chính sách an toàn được tuân thủ chắc chắn trong hoạt động của AIS. *Xem* AIS.

asymmetric algorithm ***thuật toán không đối xứng*** Trong mật mã học, thuật toán mật mã sử dụng một khóa công khai để mã hóa và một khóa mật để giải mã. Hai khóa đó gộp chung tạo thành một bộ khóa không đối xứng. *Xem* asymmetric cryptosystem, public key, secret key.

asymmetric cipher ***mật mã không đối xứng*** *So sánh với* symmetric cipher. *Đồng nghĩa với* asymmetric cryptosystem.

asymmetric cryptosystem ***hệ mật mã không đối xứng*** Trong mật mã học, một hệ trong đó không thể bằng tính toán suy ra được khóa mật mã từ khóa giải mã và/hoặc ngược lại. *So sánh với* symmetric cryptosystem. *Xem* computationally infeasible, public key cryptography. *Đồng nghĩa với* two key cryptosystem.

asymmetric key system ***hệ mã khóa không đối xứng*** Trong mật mã học, hệ thống mật mã sử dụng một thuật toán hoặc khóa mã để mã hóa và thuật toán hoặc khóa thứ hai để giải mã. Ví dụ về việc sử dụng hệ mã khóa không đối xứng là mã khóa công khai. Điều này cho phép các thông báo mật được



asynchronous attacks: *tấn công không đồng bộ.* Cuộc tấn công này đôi khi được gọi là bài toán thời gian kiểm tra và thời gian sử dụng. Lúc đầu khi các tham số được chương trình giám sát kiểm tra thì chúng đúng. Nhưng sau khi kiểm tra và trước khi sử dụng chúng, kẻ tấn công mới thay đổi chúng để lừa một đặc tính bảo vệ nào đó. Cuộc tấn công này có thể xảy ra vì máy tính có khả năng xử lý I/O và trả điều khiển về cho người sử dụng cho xử lý tương tranh.

gửi công khai tới người giữ khóa hoặc thuật toán riêng. Trong một số hệ thống (đặc biệt là các chữ ký số) thuật toán mã hoặc khóa mã là riêng còn khóa hoặc thuật toán giải mã là công khai. Khóa công khai và khóa riêng đôi khi được coi là cặp khóa. *So sánh với* symmetric key system. *Xem* asymmetric cryptosystem, digital signature, public key cryptography.

async ***TTKĐB*** Trong truyền thông dữ liệu, viết tắt của asynchronous communication (truyền thông không đồng bộ). *Xem* asynchronous transmission.

asynchronous ***không đồng bộ*** Chỉ các tác động và biến cố không liên quan tới một chuẩn thời gian nào đó.

asynchronous attacks ***tấn công không đồng bộ*** (1) Trong an toàn máy tính, phương pháp cố thực hiện hai hoặc nhiều cuộc tấn công đồng thời với hy vọng rằng ít nhất một cuộc sẽ thành công trong khi những cuộc khác đang bị đối phó. *xem* computer fraud control. (2) Trong an toàn máy tính, các cuộc tấn công TOCTTOU. *Xem* TOCTTOU problems.

asynchronous communications interface adaptor ***bộ thích ứng giao diện truyền thông không đồng bộ*** Ở phần cứng, một thiết bị để thực hiện chức năng tương tự với UART. *Xem* UART.

asynchronous transmission ***truyền không đồng bộ*** Trong truyền thông dữ liệu, một dạng truyền dữ liệu trong đó các khoảng thời gian giữa các ký tự có thể thay đổi song các bit trong một ký tự được gửi đi theo các khoảng thời gian cố định. Các bit khởi và dừng được dùng để chỉ điểm bắt đầu và kết thúc của các ký tự. *So sánh với* anisochronous transmission, synchronous transmission.

ATM *Xem* automated teller machine.

attack ***tấn công*** Trong quản lý rủi ro, sự thực hiện một cuộc đe dọa. Một mối đe dọa được thực hiện thường xuyên đến mức nào còn phụ thuộc vào những yếu tố như vị trí, loại hình và giá trị của thông tin được xử lý. Như vậy, trừ phi di chuyển hệ thống hoặc thiết bị hoặc thay đổi tận gốc nhiệm vụ của nó, còn thì thường không có cách nào để một cấp bảo vệ có thể tác động tới tần suất tấn công. Các ngoại lệ là những đe doạ từ phía con người ở những nơi các biện pháp an toàn có hiệu quả có tác dụng ngăn chặn. Sự kiện một cuộc tấn công được thực hiện không nhất thiết có nghĩa là nó sẽ thành công. Mức độ thành công phụ thuộc vào tính dễ bị thương tổn của một hệ thống hoặc vào sự hoạt động và tính hiệu quả của các biện pháp đối phó hiện hành. *Xem* attacker, threat, vulnerability.

attacker ***kẻ tấn công*** Trong an toàn máy tính và dữ liệu, kẻ có ý đồ vượt qua các biện pháp an toàn máy tính hoặc dữ liệu. *Xem* attack, intruder.

attack path ***tuyến tấn công*** Trong an toàn thông tin, dãy các biện pháp đối phó mà một kẻ tấn công phải vượt qua để phá vỡ mục tiêu an toàn của một đích đánh giá. *Xem* information technology security evaluation criteria, target of evaluation.

attack signalling ***báo hiệu tấn công*** Trong an toàn máy tính, đặc điểm của

một PDD nào đó đưa ra một dạng tín hiệu cảnh báo nào đó và một bản ghi về các cuộc tấn công quay số. *Xem* port protection device, telephone intrusion.

attention character ***ký tự nhắc chú ý*** Trong an toàn máy tính, một ký tự mà khi được đưa vào thiết bị đầu cuối sẽ báo cho TCB (cơ sở tính toán tin cậy) rằng, người sử dụng muốn một đường truyền thông an toàn từ đầu cuối tới một mã tin cậy nào đó, để cung cấp một dịch vụ an toàn cho người sử dụng, ví dụ đăng nhập hoặc rời hệ thống. *Xem* TCB.

attenuation ***(sự) suy giảm*** Trong điện tử học và truyền thông, sự giảm cường độ của một tín hiệu điện khi nó đi qua mạch, hoặc của một sóng điện từ khi truyền qua một phương tiện truyền thông.

attribute ***thuộc tính*** Trong các cơ sở dữ liệu, một trường chứa thông tin về một thực thể, ví dụ trong một cơ sở dữ liệu nhân sự, "địa chỉ nhà" có thể là một thuộc tính của thực thể nhân viên. *So sánh với* entity, relationship. *Xem* field.

AT&T ***hãng AT&T*** Viết tắt của American Telephone and Telegraph (hãng điện thoại và điện báo Mỹ).

AU ***AU*** Viết tắt của authorized user (người sử dụng hợp pháp).

audible alarm device ***thiết bị báo động bằng âm thanh*** Trong an toàn vật lý, thiết bị phát ra âm thanh để chỉ báo một trạng thái báo động hoặc chỉ sự thay đổi trong chế độ hoạt động của một hệ thống an toàn.

audio detection ***dò tìm âm thanh, phát hiện âm thanh*** Trong an toàn vật lý, kỹ thuật sử dụng một micrô, bộ khuếch đại và rơle kích hoạt bằng âm thanh để phát hiện các tiếng ồn do một kẻ thâm nhập gây ra trong vùng được bảo vệ và để truyền một tín hiệu báo động tương ứng. *Xem* alarm signal, intrusion detector, audio listen in.

audio listen in ***nghe âm thanh*** Trong an toàn vật lý, hệ thống giám sát báo động sử dụng các tần số âm thanh để phát hiện sự xâm nhập. Thông tin âm thanh được hồi tiếp lại cho người vận hành tại vị trí giám sát trung tâm. *Xem* audio detection, intrusion detector.

audio response terminal ***đầu cuối đáp âm thanh*** Trong các thiết bị ngoại vi, thiết bị đầu cuối nhận thông tin nói từ một máy tính. Tiếng nói số hóa dưới dạng các từ/câu hoặc âm vị được chương trình truy nhập tới và được chuyển từ dạng số sang dạng tương tự để truyền đi. Nếu thiết bị nhận là một máy điện thoại bấm phím với các âm đa tần, thì người sử dụng có thể gửi các câu hỏi thông qua phím bấm. *Xem* speech synthesizer, voice answer back.

audio response unit ***thiết bị đáp âm thanh*** *Xem* voice answer back.

audit ***kiểm toán, kiểm tra*** (1) Trong an toàn thông tin, các chức năng phát hiện và nghiên cứu các biến cố mà có thể là một mối đe doạ đối với an toàn. *Xem* information technology security evaluation criteria. (2) Trong an toàn máy tính, tiến hành duyệt lại và xem xét độc lập các bản ghi và các hoạt



động của hệ thống nhằm kiểm tra tính thích hợp của các kiểm soát hệ thống, để đảm bảo sự phù hợp với chính sách đã thiết lập và các thủ tục điều hành và để khuyến nghị những thay đổi đã chỉ ra trong các điều khiển, trong chính sách hay thủ tục. *Xem* audit trail, external security audit, internal security audit, security audit.

audit based control ***kiểm soát dựa trên kiểm toán*** Trong an toàn cơ sở dữ liệu, dạng kiểm soát bằng suy luận trong đó, vết kiểm toán được duy trì để có thể kiểm tra xem một truy vấn, khi so sánh tương quan với thống kê đã phát ra trước đó, có khả năng gây một tiết lộ cá nhân hay không. *So sánh với* a priori control, memoryless control. *Xem* audit expert, audit trail, inference control, overlap control, personal disclosure.

audit data ***dữ liệu kiểm toán*** Trong an toàn máy tính, dữ liệu kiểm toán tiêu biểu được tạo ra trong một hệ phân thời bao gồm thông tin cần thiết để lập hóa đơn cho người sử dụng và các nhật ký an toàn cung cấp các danh sách các ý đồ sử dụng các lệnh đặc quyền. *Xem* audit trail.

audit expert ***chuyên viên kiểm toán*** Trong an toàn cơ sở dữ liệu, kỹ thuật hạn chế theo ô sử dụng vết kiểm toán để xác định xem một câu hỏi đã đề xuất, khi so sánh tương quan với dữ liệu phát ra bởi các câu hỏi trước đó, có thể được dùng để tìm ra thông tin cá nhân hay không. Một ma trận nhị phân được tạo ra với một cột dành cho mỗi cá nhân trong cơ sở dữ liệu, mỗi hàng biểu thị cơ sở cho một tập hợp các câu hỏi có thể suy từ các câu hỏi trước đó. Câu hỏi mới sẽ cập nhật ma trận và nếu một hàng chứa các số không trong mọi cột trừ một cột, thì thông tin liên quan tới cá nhân tương ứng với cột đó có thể được suy ra từ các câu hỏi đã đề xuất và câu hỏi trước đó. *So sánh với* cell suppression, grouping, implied queries control, overlap control, query set size control. *Xem* audit based control, cell restriction.

auditing ***(sự) kiểm toán*** Trong kiểm soát truy nhập, quá trình tạo ra và duy trì các bản ghi cần để hỗ trợ cho khả năng phân định trách nhiệm. *Xem* audit, audit trail.

audit trail ***vết kiểm toán*** (1) Tập hợp các bản ghi cùng cung cấp bằng chứng hồ sơ về quá trình xử lý được dùng để lần ra dấu vết từ các giao tác ban đầu tới các bản ghi và báo cáo có liên quan, và/hoặc lần ngược trở lại từ các bản ghi và báo cáo tới các giao tác nguồn thành phần của chúng. (2) Trong an toàn máy tính, bản ghi theo trình tự thời gian về các hoạt động hệ thống. Tập hợp thông tin đó đủ để cho phép tái lập, xem xét lại và nghiên cứu dãy các môi trường và các hoạt động xung quanh, hoặc dẫn tới từng biến cố trên đường chuyển tác từ lúc khởi đầu tới lúc ra kết quả cuối cùng. (3) Trong tin học, các dữ liệu được tạo ra như kết quả của phương pháp biên chép hay tự động hóa để tìm ra dấu vết các giao tác ảnh hưởng tới nội dung của một bản ghi. *Xem* audit, audit trail analysis, record. (4) Trong hoạt động ngân hàng, khả năng xem được cái mà hệ thống đã hoàn thành trong quá khứ.

audit trail analysis ***phân tích vết kiểm toán*** Trong kiểm soát truy nhập, việc xem xét một vết kiểm toán, theo cách thủ công hay tự động hóa, có thể chấp nhận được trong thời gian thực. *Xem* audit trail.

authenticate ***xác thực*** Thiết lập tính hợp lệ của một danh tính được khai báo. *Xem* authentication.

authentication ***(sự) xác thực*** (1) Trong an toàn dữ liệu, hành động xác định rằng, một thông báo không bị thay đổi từ khi nó rời vị trí ban đầu. Danh tính của người gửi được xác minh hoàn toàn. (2) Trong an toàn dữ liệu, quá trình được sử dụng giữa bên gửi và bên nhận để đảm bảo sự toàn vẹn của dữ liệu và đưa ra sự xác thực nguồn gốc dữ liệu. *Xem* data integrity, data origin authentication. (3) Trong an toàn dữ liệu, xác minh tính hợp lệ của một mã nhận dạng (danh tính) được khai báo. (4) Trong an toàn máy tính, hành động nhận diện hoặc xác minh tư cách của một trạm, người gửi hoặc cá nhân để truy nhập vào những hạng mục thông tin đặc thù. *Xem* access. (5) Trong an toàn dữ liệu, biện pháp chống sự truyền gian lận bằng cách xác minh tính hợp lệ của cuộc truyền, của thông báo, trạm hoặc bên gửi đi. (6) Trong an toàn dữ liệu, các quá trình đảm bảo mọi thứ liên quan đến một giao tác xử lý từ xa là xác thực, và thông báo không bị thay đổi hoặc sai lạc khi truyền. Các bên tham gia chuyển tác phải nhận dạng lẫn nhau một cách tin cậy, phải biết được mỗi thông báo họ nhận đến từ phía bên kia không bị sửa đổi, hoặc bị lưu giữ trước đó rồi phát lại bởi một bên thứ ba. Trường kiểm tra có thể được bổ sung vào nội dung của toàn thông báo và việc tính toán liên quan tới một khóa mật. Thông tin bổ sung cần có trong thông báo để bảo vệ tránh phát lại các thông báo trước đó; các trường thời gian/ngày tháng đôi khi được dùng cho mục đích này. Quá trình xác thực sử dụng khóa mật, dùng chung giữa bên gửi và bên nhận, không thể tham gia giải quyết các tranh chấp trong đó, bên nhận khiếu nại rằng bên gửi đã truyền đi một thông báo giả mạo, hoặc bên gửi không thừa nhận đã gửi thông báo đi, cho là nó bị bên nhận làm giả mạo. *Xem* ANSI X9.9 - 1986, cryptography, digital signature, MAC, message authentication, replay, wiretap. (7) Trong an toàn máy tính, quá trình xác minh danh tính của một cá nhân khi được xác minh bởi một quá trình nhận dạng. (8) Trong an toàn dữ liệu và truyền thông dữ liệu, thuật ngữ này dùng vừa với nghĩa ngăn ngừa sự sửa đổi không phát hiện được đối với dữ liệu, vừa với nghĩa xác thực thực thể ngang hàng. Xác thực thực thể ngang hàng thường được dùng trong liên lạc, nơi các bên truyền thông đều tìm cách xác minh danh tính của nhau. Thuật ngữ tính toàn vẹn (integrity) hiện nay thường hay dùng để chỉ quá trình ngăn ngừa sự sửa đổi không phát hiện được đối với dữ liệu. *Xem* integrity, peer entity authentication.

authentication algorithm ***thuật toán xác thực*** Trong xác thực, hoạt động xác định rằng, một thông báo tới từ một nguồn được phép gửi các thông báo loại đó và thông báo là được phép.

Xem message authentication.

authentication element ***phần tử xác thực*** Trong xác thực, nhóm các ký tự kề nhau cần được bảo vệ nhờ xử lý bằng thuật toán xác thực. *Xem* authentication algorithm.

authentication equipment ***thiết bị xác thực*** Trong kiểm soát truy nhập, thiết bị dùng để kiểm tra tính xác thực của một thông báo đã truyền của người gửi, hệ thống gửi hoặc hệ viễn thông, hoặc để bảo vệ chống sự truyền gian lận hoặc những hệ giả mạo.

authentication exchange ***trao đổi xác thực*** Trong xác thực, cơ chế nhằm đảm bảo định danh một thực thể nhờ sự trao đổi thông tin. *Xem* access control, dynamic password.

authentication information ***thông tin xác thực*** Trong xác thực, thông tin dùng để xác minh tính hợp lệ của một danh tính được khai báo. *Xem* authentication.

authentication key ***khóa xác thực*** Trong xác thực, khóa mật mã được thiết kế mà chỉ các bên tương ứng biết được. Khi khóa đó và văn bản của thông báo được áp dụng với thuật toán xác thực thì kết quả sẽ là MAC. *Xem* ANSI X9.9 - 1986, authentication algorithm, authentication key, MAC.

authentication of users ***xác thực người sử dụng*** Trong truyền thông dữ liệu, việc xác minh rằng người sử dụng ở đầu cuối tương ứng với danh tính mà anh ta khai báo. *Xem* access control, dynamic password, password.

authentication period ***chu kỳ xác thực*** Trong xác thực, chu kỳ tối đa chấp nhận được giữa một quá trình xác thực ban đầu bất kỳ và những qua trình tái xác thực sau đó trong một phiên làm việc đơn lẻ của đầu cuối hoặc trong khoảng thời gian dữ liệu được truy nhập.

authentication process ***quá trình xác thực*** Trong xác thực, các hành động bao gồm: (*a*) nhận một ký tự nhận dạng và một mật khẩu cá nhân từ một người dùng hệ thống ADP; (*b*) so sánh mật khẩu nhập vào với mật khẩu hợp lệ đã lưu sẵn. Mật khẩu này do cá nhân gắn với mã nhận dạng đó phát ra hoặc lựa chọn; (*c*) xác thực danh tính nếu mật khẩu nhập vào và mật khẩu được lưu giống nhau. (Chú ý: Nếu mật khẩu lưu được mã hóa thì mật khẩu nhập vào phải được mã hóa và được so sánh với bản mã đã lưu, hoặc bản mã phải được giải mã rồi so sánh với mật khẩu đã nhập). *Xem* password.

authentication sequence ***trình tự xác thực*** Trong xác thực, trình tự dùng để xác thực danh tính của một chủ thể hoặc đối tượng. *Xem* object, subject.

authentication server ***máy chủ xác thực, secvơ xác thực*** Trong xác thực, phương tiện tin cậy để phân xử các chữ ký số. Secvơ xác thực ký một thông báo từ người gửi, bằng cách mã hóa khối dữ liệu chứa phần dấu xác thực thông báo và danh tính người gửi, bằng khóa mật của trọng tài. Người nhận cũng phải trình chữ ký cho secvơ xác thực; secvơ giải mã chữ ký và cung cấp cho người gửi dấu xác thực và danh tính của người gửi. Sự liên lạc giữa những người sử dụng và secvơ xác thực được mã hóa theo các cặp khóa dùng chung

với những người sử dụng riêng lẻ. *Xem* arbitrated signature, authenticator, digital signature, trusted.

authenticator ***dấu xác thực*** (1) Trong xác thực, phương tiện để định dạng hoặc xác minh tính hợp lệ của một trạm, bên gửi hoặc cá nhân truy nhập tới những loại thông tin riêng. *Xem* access control. (2) Trong xác thực, ký hiệu, dãy các ký hiệu, hoặc dãy các bit được sắp xếp theo quy định và thường được chèn vào một điểm xác định trước bên trong thông báo hoặc cuộc truyền nhằm xác thực thông báo hoặc cuộc truyền. Dấu xác thực thường là hàm của thông báo đầy đủ, hay ít nhất, những phần nhạy an toàn của nó, và của khóa mật. Sự thay đổi bất kỳ đối với thông báo, mà không có những thay đổi tương ứng ở dấu xác thực, thì đều có thể được bên nhận phát hiện ra. *Xem* message authentication. (3) Trong xác thực, mã nằm trong một thông báo giữa người gửi và người nhận được dùng để xác nhận tính hợp lệ nguồn và toàn bộ hoặc một phần văn bản của thông báo, dựa trên sự nhất trí của hai bên về phương pháp tính toán. *Xem* MAC, test key.

authenticator key ***khóa dấu xác thực*** Trong xác thực, khóa mật mã chỉ các bên tương ứng biết được. Khi khóa này và văn bản của thông báo được áp dụng cho một thuật toán nhất trí chung thì kết quả sẽ là dấu xác thực. *Xem* authentication key, banking networks, SWIFT.

authorization ***(sự) cấp phép, (sự) cấp quyền; quyền ủy thác*** (1) Trong kiểm soát truy nhập, sự cấp phép hay sự cấp quyền truy nhập cho một người sử dụng, một chương trình hay một quá trình. *Xem* access. (2) Trong các hoạt động, quyền ủy thác là quyền được cấp cho một người sử dụng để liên lạc với hoặc để sử dụng một hệ máy tính hay dữ liệu lưu giữ. (3) Quyền ủy thác còn là đặc quyền mà một quan chức được chỉ định cấp cho một cá nhân để truy nhập thông tin dựa trên mức truy nhập và nhu cầu cần biết của cá nhân đó.

authorization code ***mã hợp pháp, mã ủy quyền*** Trong tin học, mã dùng để bảo vệ chống lại sự truy nhập trái phép đối với dữ liệu và các phương tiện hệ thống. Mẫy này thường gồm mã nhận dạng (id) của người sử dụng và mật khẩu. *Xem* user, id, password.

authorization level ***mức ủy quyền, mức cấp quyền*** (1) Trong kiểm soát truy nhập, cấp có mức truy nhập an toàn. (2) Trong an toàn máy tính, điểm hoặc vị trí nhập với một định mức an toàn xác định.

authorization parameter ***tham số ủy quyền*** Trong hoạt động ngân hàng, một giá trị được tạo ra như hàm của khóa thẻ bởi cơ sở phát hành thẻ và chuyển sang cho cơ sở nhận. Nó được thiết bị đầu cuối dùng để xác thực cơ sở phát hành thẻ và được thiết bị đầu cuối và cơ sở nhận dùng như một thành phần trong quản lý khóa. Nó không được truyền giữa các nơi đó. *Xem* acquirer, card issuer, card key, key management.

authorization process ***quá trình cấp phép*** Trong kiểm soát truy nhập, các hoạt động bao gồm: (*a*) mật khẩu truy

nhập từ một người sử dụng hệ thống ADP (danh tính của anh ta đã được xác thực có thể bằng mật khẩu cá nhân), (*b*) so sánh mật khẩu truy nhập với mật khẩu đi theo dữ liệu được bảo vệ và (*c*) xác thực sự truy nhập tới dữ liệu nếu mật khẩu nhập đưa vào và mật khẩu lưu giống nhau. *Xem* authorization, password.

authorized access control switch ***chuyển mạch kiểm soát truy nhập được phép*** Trong an toàn vật lý, cơ cấu, thường là phím bấm, dùng để đóng - ngắt hệ thống phát hiện. *Đồng nghĩa với* Day-Night switch, subscriber's unit.

auto-alarming switcher ***bộ chuyển mạch tự báo động*** Trong an toàn vật lý, bộ chuyển mạch hình ảnh với một phương tiện tự động đưa hình ảnh camera CCTV về một vùng phát tín hiệu báo động thông qua hệ thống CCTV. *Xem* CCTV, video switcher.

auto answer ***(hộ) đáp tự động*** *Đồng nghĩa với* automatic answering.

autoclave ***mã tự phụ thuộc, autoclap*** Trong mật mã học, sự hồi tiếp trong mật mã dòng khiến cho dòng bit mã hóa phụ thuộc vào dòng dữ liệu. *Xem* cryptographic bit stream, data stream, stream cipher.

auto dial ***quay số tự động*** *Đồng nghĩa với* automatic calling.

auto dial modem ***modem quay số tự động*** Trong truyền thông dữ liệu, modem đáp lại các lệnh thiết lập cuộc gọi từ một PC. Nó nghe âm đáp và tự tổ chức để nhận dữ liệu. Để so sánh, với modem thủ công người sử dụng phải quay số nhờ sử dụng một máy điện thoại, nghe lời đáp, sau đó ấn núm dữ liệu. *Xem* Hayes, MODEM, PC.

autoidentifier ***bộ tự động định danh*** Trong tin học, thiết bị dùng để một đầu cuối tự động tự định danh với một máy tính.

automated audit ***kiểm toán tự động hóa*** Trong hoạt động kiểm toán, một tính năng kiểm toán trong đó, việc xem xét các bước đã tiến hành trước đó hoặc các kết quả đã chuẩn bị trước đó, được tự động kích hoạt ở một số giai đoạn nhất định trong một chương trình hoặc thủ tục.

Automated Clearing House ***phòng thanh toán bù trừ tự động hóa*** Trong hoạt động ngân hàng, tập hợp các quá trình thực hiện việc thanh toán bù trừ các khoản trả liên ngân hàng dưới dạng các khoản trả tiêu chuẩn hóa và chúng có thể được xử lý bằng máy tính.

automated error correction ***sửa lỗi tự động hóa*** Trong xử lý dữ liệu, sự sửa tự động các lỗi trong một chuyển tác hoặc bản ghi mà vi phạm một tác động đò tìm nào đó.

Automated Information System ***Hệ thống tin tự động hóa*** (1) Tổ hợp phần cứng, phần mềm và phần sụn của máy tính được cấu hình để thu thập, truyền thông, tính toán, phổ biến và/hoặc điều khiển dữ liệu. (2) Các hệ tạo ra, chuẩn bị hoặc thao tác thông tin dưới dạng điện tử cho các mục đích ngoại trừ viễn thông và bao gồm các máy tính, các hệ xử lý văn bản, các hệ xử lý thông tin điện tử khác và thiết bị có liên quan. *Xem* NSDD-145.

automated security monitoring ***giám sát an toàn tự động hóa*** Trong an toàn máy tính, việc sử dụng các thủ tục tự động hóa để đảm bảo cho các cơ cấu kiểm soát an toàn tự động hóa không bị làm hỏng.

automated system security ***an toàn hệ thống tự động hóa*** Trong an toàn máy tính, tất cả các đặc tính an toàn cần để đưa ra một mức bảo vệ chấp nhận được đối với phần cứng, phần mềm và dữ liệu đã phân loại, chưa phân loại nhạy cảm hoặc quan trọng, tư liệu hoặc các quá trình trong hệ thống. Nó bao gồm: (*a*) Toàn bộ các chức năng, các đặc trưng và các đặc điểm phần cứng và phần mềm. (*b*) Các thủ tục vận hành. (*c*) Các thủ tục phân định trách nhiệm. (*d*) Các kiểm soát truy nhập ở mọi phương tiện máy tính (bao gồm cả các máy lớn, các thiết bị đầu cuối, các máy tính mini hoặc máy vi tính. (*e*) Các ràng buộc quản lý. (*f*) Bảo vệ vật lý. (*g*) Kiểm soát sự phát xạ gây tác hại (Tempest). (*h*) An toàn nhân sự và truyền thông (COMSEC). (*i*) Những lĩnh vực an toàn khác. *Xem* access control, COMSEC, physical security, Tempest.

automated teller machine ***máy trả nhận tiền tự động*** Trong các thiết bị ngoại vi, thiết bị dùng để rút tiền mặt, thanh toán các hóa đơn, hỏi số dư tài khoản, gửi và chuyển tiền giữa các tài khoản. *Xem* banking networks, cash dispenser, PIN management and security, self banking. *Đồng nghĩa với* automatic teller machine.

automatic alarm initiating device ***thiết bị khởi phát báo động tự động*** Trong an toàn vật lý, thiết bị chuyển tiếp tự động một tín hiệu báo động khi có chỉ báo về lửa, khói hoặc nước. *So sánh với* manual alarm initiating device.

automatic answering ***đáp tự động*** Trong truyền thông dữ liệu, hệ thống trong đó trạm được gọi tự động đáp lại tín hiệu gọi, cuộc gọi có thể được thiết lập cho dù trạm được gọi có nghe hay không. *Xem* call back. *Đồng nghĩa với* auto answer.

automatic calling ***gọi tự động*** Trong truyền thông, đặc tính của máy cho phép một trạm khởi đầu một cuộc gọi tự động qua một đường chuyển mạch. *Xem* automatic calling unit, station. *Đồng nghĩa với* auto dial.

automatic calling unit ***thiết bị gọi tự động*** Trong truyền thông dữ liệu, thiết bị cho phép một máy giao dịch tự động quay số các cuộc gọi qua một mạng. *Xem* automatic calling, automatic dialer.

automatic capture ***thu thập tự động*** Trong hoạt động ngân hàng, sự thu thập dữ liệu trực tiếp từ các hệ máy tính mà không có sự can thiệp thủ công.

Automatic Data Processing System ***hệ xử lý dữ liệu tự động*** Tổ hợp phần cứng, phần sụn và phần mềm của máy tính được cấu hình nhằm mục đích phân loại, sắp xếp, tính toán, xử lý, tóm tắt, truyền và nhận, lưu giữ và tìm kiếm dữ liệu với sự can thiệp ít nhất của con người.

automatic message switching center ***trung tâm chuyển mạch thông báo tự động*** Trong truyền thông dữ liệu, địa điểm tại đó các thông báo được tự động định tuyến theo thông tin mà chúng

chứa. *Xem* message switching.

automatic personal identification ***nhận dạng cá nhân tự động*** *Đồng nghĩa với* biometrics.

automatic polling ***hỏi vòng tự động*** Trong tin học và truyền thông dữ liệu, đặc tính của thiết bị điều khiển truyền cho phép nó xử lý các đáp ứng âm đối với sự hỏi vòng mà không cần ngắt CPU. *Xem* CPU, polling.

automatic renewal clause ***điều khoản đổi mới tự động*** Trong quản lý rủi ro, điều khoản trong hợp đồng tự động đổi mới hợp đồng đang tiếp tục, ví dụ như đối với một điểm nóng hoặc điểm nguội. *Xem* cold site, hot site.

automatic retransmission request ***yêu cầu truyền lại tự động*** Trong truyền thông dữ liệu, kỹ thuật để đảm bảo truyền chính xác dữ liệu. Dữ liệu cần truyền được lưu giữ trong bộ đệm cho tới khi liên kết truyền thông sẵn sàng giải quyết nó. Sau đó, dữ liệu được gửi đi và đồng thời sao lại một bản. Bản sao được giữ trong bộ đệm và được xóa đi khi thiết bị gửi nhận được tín hiệu báo xác nhận rằng, đã nhận được bản thu đúng như khi được xác minh bằng kiểm tra CRC. Nếu thiết bị nhận phát hiện có lỗi trong dữ liệu, nó thông báo cho thiết bị gửi để truyền lại bản sao trong bộ đệm. *Xem* CRC.

automatic teller machine ***máy trả nhận tiền tự động*** *Đồng nghĩa với* automated teller machine.

automation security ***an toàn tự động hóa*** Trong an toàn dữ liệu, các biện pháp dùng để bảo vệ sự tự động hóa và thông tin để xử lý khỏi những mối hiểm họa thù địch lẫn ôn hòa, và chống lại việc khai thác trái phép thông qua hoạt động tình báo, phá hoại, trộm cắp, lừa đảo, biển thủ hoặc lạm dụng. An toàn tự động hóa áp dụng cho tất cả các hệ ADP và áp dụng theo các khía cạnh tổng thể của bài toán an toàn. Bởi thế, nó bao gồm các khía cạnh an toàn của quản lý an toàn, phần cứng, phần mềm, thủ tục, truyền thông, nhân sự, vật lý và môi trường, và tất cả những khía cạnh an toàn khác nhằm bảo vệ các hệ thống tự động hóa (phần cứng và phần mềm), địa điểm, hoạt động, phương tiện hoặc sự vận hành như một mục tiêu tiềm tàng.

auto restore ***tự khôi phục*** Trong an toàn vật lý, chỉ sự thiết lập lại tự động một thiết bị báo động, trong một khoảng thời gian xác định, sau khi nhận được tín hiệu báo động.

auxiliary equipment ***thiết bị phụ*** Trong tin học, thiết bị không chịu sự điều khiển trực tiếp của bộ xử lý trung tâm. *Xem* central processing unit.

auxiliary fire alarm system ***hệ báo cháy bổ trợ*** Trong an toàn vật lý, hệ thống sử dụng các thiết bị khởi phát báo động, thiết bị này truyền một tín hiệu báo động qua hệ báo cháy thành phố tới trạm chữa cháy hoặc trực tiếp hoặc thông qua các sở chỉ huy phòng cháy chữa cháy. *Xem* automatic alarm initiating device, manual alarm initiating device.

availability ***tính sẵn sàng*** (1) Trong an toàn máy tính và truyền thông, tính chất có thể truy nhập được và có thể sử dụng được đối với một yêu cầu của

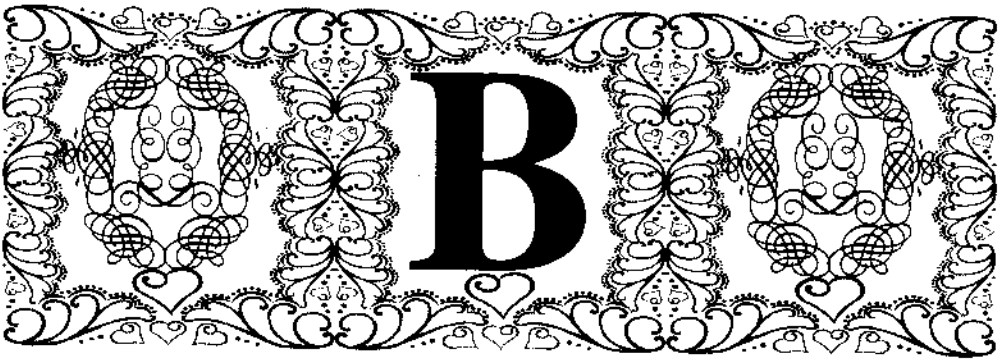
một thực thể được phép. *So sánh với* denial of service. (2) Trong an toàn máy tính, đặc trưng đảm bảo cho các tài nguyên máy tính sẽ sẵn sàng với những người sử dụng được phép khi họ cần chúng. Đặc trưng này nhằm chống sự từ chối phục vụ. *So sánh với* denial of service.

availability-automated security monitoring ***giám sát an toàn sẵn sàng tự động hóa*** Trong an toàn thông tin, chỉ việc sử dụng các thủ tục tự động hóa để bảo đảm chống việc phá vỡ các kiểm soát an toàn bên trong một hệ thông tin.

available funds ***quỹ có sẵn*** Trong hoạt động ngân hàng, quỹ có sẵn để rút ra. *Đồng nghĩa với* cleared funds.

available time ***thời gian sẵn sàng*** *Xem* up-time.

AVLOS ***cơ sở dữ liệu AVLOS*** Trong lập pháp, cơ sở dữ liệu của Hoa Kỳ lưu giữ dữ liệu cá nhân từ các chức vụ lãnh sự của Hoa Kỳ. *Xem* data protection - U.S.



B1 ***B1*** *Xem* Division B.

B2 ***B2*** *Xem* Division B.

B3 ***B3*** *Xem* Division B.

babble ***xuyên âm đa nguồn*** Trong truyền thông, xuyên âm tập hợp lại từ một số nguồn gây nhiễu. *Xem* cross-talk.

backdoor ***cửa sau*** *Xem* trapdoor.

background job ***công việc thứ cấp, công việc phụ*** Trong tin học, công việc (job) có mức ưu tiên tương đối thấp trong môi trường đa nhiệm; các tài nguyên máy tính chỉ được cấp cho nó khi những nhiệm vụ khẩn có mức ưu tiên cao hơn không yêu cầu chúng. *So sánh với* foreground program.

backing storage ***bộ nhớ dự phòng*** Trong tin học, phương tiện nhớ trung gian, ví dụ như băng từ, đĩa từ v.v. mà trên đó dữ liệu được nhận vào để máy tính trung tâm xử lý về sau. *Xem* magnetic disk, magnetic tape.

back office ***văn phòng gián tiếp, văn phòng hỗ trợ*** Trong hoạt động ngân hàng, nơi tiến hành sự hỗ trợ cho các hoạt động, bao gồm xử lý những tính toán làm khớp và thanh toán và tính toán ở chi nhánh. *So sánh với* front office.

backtracking ***dò tìm ngược, lần ngược*** Trong quản lý khóa, khả năng sử dụng giá trị khóa hiện thời cùng với thông tin đã truyền hoặc đã nhận trước đó để xác định các giá trị khóa trước đó. *Xem* cryptographic key, transaction key system.

backup plan ***kế hoạch dự phòng*** Trong quản lý rủi ro, kế hoạch dự phòng khả năng tiến hành bằng các phương tiện thay thế lượng công việc xử lý dữ liệu quan trọng. *Xem* contingency plans.

backup procedures ***(các) thủ tục dự phòng*** Trong quản lý rủi ro, những biện pháp dự phòng để khôi phục các tập dữ liệu và các thư viện chương

trình và để khởi động lại hoặc thay thế thiết bị ADP sau khi xảy ra sự cố hoặc thảm họa. *Xem* ADP, backup/restore.

backup/restore ***dự phòng/phục hồi*** Trong tin học, các hoạt động liên quan tới chuyển dữ liệu từ đĩa từ tới băng hoặc đĩa để lưu gián tiếp và hoạt động khôi phục dữ liệu vào đĩa. *Xem* magnetic disk, magnetic tape.

backward channel ***kênh ngược*** Trong truyền thông dữ liệu, kênh dùng cho các tín hiệu điều khiển hoặc kiểm soát lỗi nhưng với hướng truyền ngược với chiều mà thông tin của người sử dụng đang truyền đi. *So sánh với* forward channel.

backwards learning ***nghiên cứu ngược, học trở ngược, tập quen ngược*** Trong truyền thông dữ liệu, phương pháp định tuyến trong đó, các nút chuyển mạch có khả năng suy ra cách xử lý của mạng bằng cách quan sát các gói tin đi qua, có chú ý tới nguồn và số lượng các nối kết mà các gói tin đó đã truyền qua. *Xem* node, packet switching.

backward supervision ***giám sát ngược*** Trong truyền thông dữ liệu, việc sử dụng các giám sát gửi từ trạm thụ động tới trạm chủ. *Xem* station, supervisory signal.

BACS *Xem* banker's automated clearing services.

badge reader ***bộ đọc thẻ*** Trong an toàn vật lý, thiết bị để đọc thông tin được mã chứa trên thẻ nhận dạng cá nhân bằng chất dẻo. Thông tin có thể được mã hóa bằng sọc từ, chấm từ hoặc các mạch lân cận tần số vô tuyến. *So sánh với* dynamic password. *Xem* card reader.

balanced circuit ***mạch cân bằng*** Trong truyền thông, tuyến được kết thúc bằng một tải thích ứng.

balanced detection ***phát hiện có đối trọng*** Trong an toàn vật lý, phương pháp phát hiện báo động giả bằng cách yêu cầu để hai biến cố phát hiện phải xuất hiện trong một khoảng thời gian định trước.

balanced transmission ***truyền cân bằng*** Trong truyền thông dữ liệu, kỹ thuật để có tốc độ dữ liệu cao vốn đòi hỏi hai dây cho mỗi tín hiệu. *So sánh với* unbalanced transmission. *Xem* data rate.

balancing ***(làm) cân bằng, tự chỉnh*** (1) Trong kiểm toán, phương pháp phát hiện lỗi bằng cách thử tính cân bằng giữa các giá trị của hai khoản ghi tương đương hoặc giữa tổng điều khiển một tập hợp các mục. *Xem* batch balancing. (2) Trong tin học, phép thử sự bằng nhau giữa các giá trị của hai tập hợp mục tương đương hoặc một tập hợp mục và tổng điều khiển.

band ***dải tần; vùng*** (1) Trong truyền thông, dải tần là dải các tần số giữa hai giới hạn xác định, ví dụ dải tần tiếng nói trong điện thoại nằm trong khoảng 300 tới 3000 Hz. *Xem* Hz. (2) Trong các hệ thống nhớ, vùng là nhóm các vết trên trống từ hoặc trên một mặt của đĩa từ.

bandpass ***thông dải*** Trong điện tử học, chỉ bộ khuếch đại hoặc mạch có đáp tuyến tần số bằng phẳng trong

những giới hạn xác định trên một dải tần đã cho.

bandscrambler ***bộ xáo trộn dải tần*** *Đồng nghĩa với* bandsplitter.

band shift invertor ***bộ đảo dịch dải tần*** Trong an toàn truyền thông, một dạng bộ đảo tiếng nói trong đó một phần thành phần tần số cao của tín hiệu đảo được biến đổi tần số sao cho nó dịch chuyển tới dải tần ngay phía dưới tần số thấp nhất của tín hiệu đảo. Ví dụ, tín hiệu tiếng nói ban đầu sẽ chiếm dải tần từ 300 tới 3000 Hz. Nếu sử dụng tần số sóng mang 4000 Hz thì tín hiệu đảo sẽ nằm trong khoảng từ 1000 (4000 - 3000) Hz tới 3700 Hz. Dải tần ngoài dải thông điện thoại, tức là từ 3000 tới 3700 Hz, khi đó sẽ dịch xuống 300 - 1000 Hz. Tần số sóng mang có thể thay đổi sau 10 - 20 miligiây một lần, một cách bí mật theo thỏa thuận giữa máy phát và máy thu, như vậy khiến cho kẻ nghe lén khó thực hiện cùng chương trình giải xáo trộn như máy thu. Tuy nhiên, độ nghe rõ còn lại của tín hiệu phát có thể cao tới mức không chấp nhận được. *So sánh với* bandsplitter. *Xem* cyclical band shift invertor, residual intelligibility, speech invertor, voice scrambling.

bandsplitter ***bộ chặt dải, bộ tách dải*** Trong an toàn truyền thông, dạng bộ xáo trộn tiếng nói trong đó, khoảng tần số của thông báo tiếng nói được chia thành các dải, các dải sau đó được hoán vị với nhau. Các hoán vị các dải có thể thay đổi sau vài trăm giây một lần theo trình tự chỉ máy phát và máy thu biết được. Các dải riêng lẻ cũng có thể được đảo. *So sánh với* band shift invertor. *Xem* speech invertor, voice scrambling. *Đồng nghĩa với* bandscrambler.

bandwidth ***dải thông*** (1) Trong truyền thống, đặc trưng của một kênh truyền thông, là lượng thông tin có thể chuyển qua nó trong một khoảng thời gian nào đó, thường được biểu diễn theo đơn vị bit trên giây. (2) Trong truyền thông, hiệu số giữa các tần số giới hạn trong một dải. (3) Trong điện tử học, khoảng tần số mà một thiết bị có thể vận hành và đáp ứng một đặc trưng thực hiện xác định.

bank ***ngân hàng*** Tổ chức tài chính nhận tiền gửi, cho vay, thanh toán... các công việc liên quan tới tiền bạc.

bank camera ***camera ngân hàng*** Trong an toàn vật lý, camera giám sát dùng trong các ngân hàng sử dụng phim 16 mm hoặc 35 mm.

Bankers Automated Clearing Services ***hệ thống dịch vụ thanh toán bù trừ tự động hóa của các ngân hàng*** Trong hoạt động ngân hàng, hệ thống do Cty TNHH các dịch vụ thanh toán bù trừ của các ngân hàng thiết lập, công ty này được các ngân hàng thanh toán bù trừ chính thành lập với chức năng chính hoạt động như cơ sở thanh toán bù trừ tự động hóa các lệnh chi và các khoản ghi nợ trực tiếp.

banking cycle ***chu trình hoạt động ngân hàng, chu trình kinh doanh ngân hàng*** Trong hoạt động ngân hàng, chu trình thời gian trong đó một giao dịch được hoàn thành, bao gồm yêu cầu, sự xử lý và xác định các quỹ thanh toán đối với các sản phẩm thanh

toán. *Đồng nghĩa với* document cycle, payment cycle, trade cycle.

banking networks ***(các) mạng ngân hàng*** Trong hoạt động ngân hàng, các mạng được các ngân hàng quốc tế sử dụng để tiến hành các hoạt động kinh doanh hằng ngày của chúng.

Mở đầu

Các yêu cầu lập mạng của khu vực tài chính là khá đa dạng và thách thức. Một ngân hàng toàn cầu trước hết phải phục vụ các nhu cầu liên lạc nội bộ riêng của nó về thư điện tử, các hoạt động báo cáo quản lý và kho bạc. Thứ hai, các ngân hàng cần cung cấp cho các khách hàng của họ rất nhiều dịch vụ tài chính dựa trên mạng như các dịch vụ quản lý tiền mặt, EDI, quản lý kho bạc công ty và đầu tư. Thứ ba, và căn bản nhất, các ngân hàng phải cung cấp một loạt các dịch vụ thanh toán như các hệ ATM (máy trả nhận tiền tự động) cho nghiệp vụ ngân hàng bán lẻ, và EFT (chuyển tiền điện tử) cho các giao dịch ngân hàng bán buôn. Hơn nữa, các ngân hàng cũng như các ngân hàng cạnh tranh trong chúng cũng là các khách hàng của nhau, do đó họ phải hợp tác trong chuyển tiền và thanh toán tồn quỹ.

Để đạt được những mục tiêu đó, các ngân hàng quốc tế giao tác với nhiều nhà cung cấp dịch vụ mạng khác nhau, cũng như duy trì các mạng tư nhân riêng của họ trên cơ sở cả mạng cục bộ lẫn mạng toàn cầu. Các lĩnh vực quan tâm chính trong các mạng ngân hàng là:

- các mạng ngân hàng quốc tế;
- các mạng ngân hàng khu vực;
- các mạng ngân hàng tư nhân;
- quản lý kho bạc điện tử;
- BDI và các xu hướng trong tương lai.

Các mạng ngân hàng quốc tế

Một số ngân hàng lớn nhất có các mạng viễn thông sở hữu riêng của họ. Các ngân hàng cỡ lớn của Hoa Kỳ như Citibank, Chemical Bank và Chase Manhattan sử dụng các mạng nội bộ của họ để liên kết các văn phòng và các chi nhánh của họ trên toàn thế giới.

Các hãng chuyên về cung cấp các dịch vụ xử lý và truyền thông dữ liệu cũng cung cấp các đường nối quốc tế mà có thể cho các tổ chức tài chính và những cơ quan khác thuê. Những công ty như thế bao gồm McDonnell Douglas, các dịch vụ thông tin GE và ADP. Về cơ bản, những tổ chức dịch vụ đó cung cấp một văn phòng phân loại điện tử dành cho các thông báo máy tính của khách hàng. Công ty dịch vụ sáng tạo ra phần mềm và các khuôn thông báo tiêu chuẩn, (thường tuân theo các tiêu chuẩn SWIFT) và các máy tính trung tâm của công ty chuyển tiếp các cuộc liên lạc giữa các bên. Một số cơ quan có thẩm quyền về viễn thông công cộng cũng cung cấp các dịch vụ xử lý và truyền dữ liệu.

Hệ thống chuyển tiền quốc tế nổi tiếng nhất là SWIFT (Hội viễn thông tài chính liên ngân hàng thế giới). Nó là công ty hợp tác thành lập vào năm 1973 theo luật của Bỉ bởi 239 ngân hàng từ 15 quốc gia (các quốc gia Châu Âu, Hoa Kỳ, Canada). Mục tiêu của công ty là cung cấp "... việc nghiên cứu, sáng tạo, sử dụng và hoạt động của những phương tiện cần thiết cho viễn thông,

truyền và định tuyến các thông báo tài chính tư nhân, bí mật và sở hữu quốc tế vì lợi ích tập thể của các thành viên của Công ty".

SWIFT ngày nay có khoảng 2000 cổ đông (ngân hàng) và tổng cộng 3000 địa điểm trong khoảng 70 quốc gia. Những người sử dụng chủ yếu là các ngân hàng nhưng cũng bao gồm những người môi giới chứng khoán, những người môi giới tiền tệ, các phòng thanh toán bù trừ, các nhà phát hành séc du lịch. Họ trao đổi thông qua mạng SWIFT trên 1.000.000 thông báo mỗi ngày. Những nhà phát hành séc có thể trao đổi với nhau chín loại thông báo, khuôn thức của chúng được tiêu chuẩn hóa và được Tổ chức tiêu chuẩn hóa quốc tế (ISO) thừa nhận. Các loại thông báo gồm: các khoản thanh toán và các séc của khách hàng; tình trạng khách hàng; các khoản nhờ thu và thư tiền mặt; tín dụng và bảo lãnh có chứng từ; kinh doanh tài chính, chứng khoán; tổ chức nghiệp đoàn; séc du lịch.

Một hệ chuyển mạch thông báo như SWIFT cần tạo ra một mức tin cậy cao cho người sử dụng và nó phải giảm nguy cơ bị nghe lén chủ động hoặc thụ động. Việc bảo vệ tránh nguy cơ bị lộ kiểu này là một yêu cầu kinh doanh cơ bản, nhất là khi tổ chức SWIFT có trách nhiệm pháp lý về tài chính đối với các giao dịch từ điểm mà tại đó chúng được chấp nhận vào mạng SWIFT. Do đó, an toàn mức giao dịch là một đặc điểm rất quan trọng của thiết kế hệ thống và các thuật toán xác thực dùng để bảo toàn tính toàn vẹn của thông báo và tính chất bí mật của lưu thông.

Thiết kế mạng, quản lý mạng và kiểm soát mạng tốt là những đặc điểm chủ chốt đối với một mạng lớn như SWIFT và được tích hợp rất thận trọng để cung cấp khả năng phục hồi và khôi phục cần thiết. SWIFT cùng với nhiều ngân hàng thành viên của nó nhận thức được nhu cầu kế hoạch hóa bất ngờ, định tuyến mạng luân phiên và dư thừa thiết bị. Những biện pháp đó là cực kỳ quan trọng đối với mọi dịch vụ chuyển mạch thông báo quốc tế vốn thường xử lý có quy củ những khối lượng lớn lưu lượng tài chính.

Những người sử dụng nối mạng với các trung tâm xử lý khu vực (RPC) của SWIFT trong mỗi quốc gia qua các đường thuê bao hoặc các dịch vụ chuyển mạch công cộng. Các RPC tạo ra sự tập trung, quản lý khuôn thức và các giao thức truyền thông. Chúng được kết nối với một trong ba trung tâm điều hành có nhân lực (OPC) của SWIFT. Các trung tâm điều hành đó nằm ở Hoa Kỳ, Hà Lan và Bỉ (các trụ sở của SWIFT). Đến lượt mình các OPC lại có khả năng phê chuẩn các thông báo, lưu giữ các thông báo an toàn và cuối cùng phân phối các giao dịch đến địa chỉ cuối cùng của chúng.

Toàn bộ mạng được quản lý bởi ít nhất hai trung tâm điều khiển hệ thống có nhân lực thường xuyên. Chúng giám sát và điều khiển sự thi hành chung của mạng. Tuy nhiên, những tăng trưởng đều đặn về khối lượng kinh doanh đã khiến SWIFT chuyển sang thiết kế mạng có tính modun hơn. SWIFT II, vốn dựa trên cách tiếp cận xử lý chuyển tác phân tán hơn SWIFT II cho phép mạng

phản ứng dễ dàng hơn với sự tăng lưu lượng và với những nâng cấp về dung lượng xử lý của nó. Trong những năm gần đây SWIFT cũng đã xem xét lại các sắp xếp an toàn cho mạng để đảm bảo rằng, những tiến bộ công nghệ an toàn được khai thác một cách thích hợp. Mục tiêu chính là tăng tính thuận tiện trong vận hành của một số các thủ tục an toàn của các ngân hàng thành viên và tăng cường sự tự động hóa quản lý an toàn đối với lưu thông của ngân hàng thành viên.

Các mạng ngân hàng khu vực

Mặc dù SWIFT cực kỳ thành công, nhưng nhiều ngân hàng đã thấy được nhu cầu phát triển các mạng dùng chung giữa họ, trong cùng một quốc gia, để hỗ trợ những sự chuyển tiền nhanh bằng tiền địa phương. Sự khác nhau chính là ở chỗ, những mạng khu vực quốc gia như thế có thể thanh toán mau lẹ những khoản trả hoặc các giá trị khoản trả tổng cộng giữa các thành viên tương ứng.

Các cơ sở thanh toán bù trừ cho phép các hoạt động thanh toán nợ và có giữa các ngân hàng trên cơ sở số dư thực. Mỗi tổ chức thành viên đưa tất cả các khoản chuyển tiền của họ với những thành viên khác vào một khoản chung. Cơ sở thanh toán bù trừ thực hiện các phép cộng cần thiết và đi đến những tổng số tiền phải trả và được hưởng từ mỗi người tham gia vào cuối ngày. Thông thường, những sắp xếp như thế được thiết lập ở mức quốc gia hoặc địa phương. Không có một hệ thống quốc tế toàn diện cho những sự chuyển tiền thanh toán bù trừ. Hệ thống thanh toán tự động hóa của cơ sở bù trừ (CHAPS) đã hoạt động ở Anh từ năm 1984. Hệ thống đó có hiệu lực trên toàn quốc và truyền các khoản trả bằng bảng Anh qua hệ điện tử giữa các ngân hàng.

CHAPS hoạt động nhờ một số ngân hàng thanh toán (ngân hàng bù trừ Anh và Scôtlen). Chúng liên lạc trực tiếp với nhau thông qua dịch vụ luồng chuyển mạch gói tin Telcom của Anh nhờ sử dụng các máy tính và phần mềm tiêu chuẩn hóa. Do đó không có cài đặt trung tâm.

Các ngân hàng thanh toán gửi các thông báo cho nhau, cho các ngân hàng khác và cho các khách hàng. Các thanh toán gửi qua hệ thống được đảm bảo và không điều kiện và được thanh toán bù trừ trên cơ sở cùng ngày. Thanh toán liên ngân hàng được thực hiện bằng điện tử vào cuối mỗi ngày, qua các tài khoản của các ngân hàng thanh toán lưu ở Ngân hàng Anh.

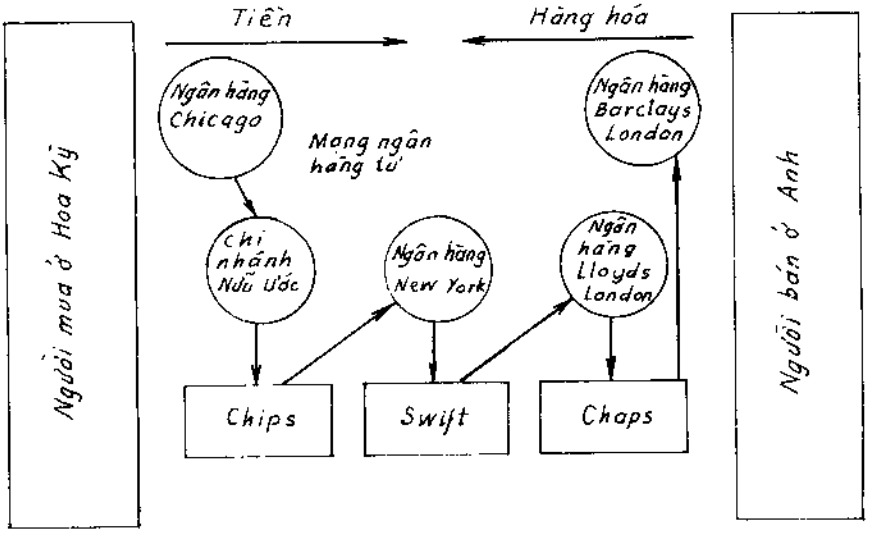
Các đặc tính toàn vẹn mạnh được thiết kế để bảo vệ khối lượng và giá trị lớn của các khoản tiền trả được gửi qua mạng CHAPS. Mọi giao dịch trả tiền đều được định danh duy nhất bởi tổ hợp dán tem thời gian và đánh số hiệu dãy. Dịch vụ sử dụng các kỹ thuật cả xác thực thông báo lẫn mã hóa, và các kỹ thuật đó được triển khai nhằm hạn chế mọi sự can thiệp trái phép đối với các giao dịch tài chính truyền giữa các ngân hàng.

Sự trao đổi các khóa xác thực thường xuyên giúp đảm bảo tính toàn vẹn của thiết kế an toàn. Các khóa tay đôi duy nhất đối với mỗi cặp người tham gia được sử dụng để tăng cường mức an

toàn cơ bản cho các mối quan hệ giao dịch kinh doanh giữa các cặp ngân hàng tham gia. Sự tin cậy của người sử dụng vào tính toàn vẹn của các khóa mã cao cấp được củng cố bằng việc đặt dưới sự kiểm soát của ủy ban các ngân hàng thanh toán bù trừ Luân Đôn (CLCB). Các khóa cao cấp được phân phối thủ công trong các mođun vận chuyển khóa chống giả mạo vốn được thu gom từ CLCB.

Nhu cầu về tính bí mật lưu thông giữa các thành viên được đáp ứng bằng mật mã liên kết. Nó sử dụng khóa mật mã giữa tất cả các ngân hàng. Điều này đạt được bằng thiết bị mã hóa liên kết X.25 vốn được phát triển chuyên cho mục đích này. Sử dụng các đặc tính bảo vệ nhóm người dùng khép kín (CUG) trong mạng nhằm hạn chế dịch vụ cho các thành viên có thiện chí và hạn chế mọi định tuyến sai lạc ngẫu nhiên đối với các giao dịch sẽ làm tăng thêm tính an toàn.

CHAPS hiện là dịch vụ thanh toán bù trừ tiền chủ yếu, nắm bắt các yêu cầu của các ngân hàng Anh về các vụ chuyển tiền giữa các ngân hàng. Tuy nhiên, bản thân mạng là một liên kết khác trong chuỗi các mạng tài chính quốc tế. Thông thường, các ngân hàng thành viên có các mạng truyền thông nội bộ và khách hàng riêng của họ. Đây là nơi phát ra các lệnh trả tiền chính. Mặc dù sự liên kết mạng này có vẻ như trong suốt đối với người sử dụng nội bộ hoặc khách hàng, song nhiều cơ cấu kiểm soát hệ thống cơ bản tập trung vẫn được dùng để tự động hóa các thủ tục kiểm soát hoạt động ngân hàng chắc chắn trước khi truyền tiếp. Sự can thiệp trong quá trình điểm tới điểm bởi các



banking networks: *(các) mạng ngân hàng.* Minh họa các hợp mạng các mạng ngân hàng tạo điều kiện cho các khoản trả tiền hàng hóa.

hệ thống ngân hàng tư nhân là yêu cầu kinh doanh cơ bản đối với sự ủy quyền tự động hóa và các áp dụng hạn chế tín dụng, cho cả khách hàng của những người sử dụng nội bộ lẫn cho các mục đích kế toán, xem hình minh họa.

Hệ trả tiền liên ngân hàng cơ sở thanh toán bù trừ (CHIPS) là mạng máy tính hóa ở Hoa Kỳ để chuyển các khoản trả quốc tế bằng đô la. Nó liên kết chừng 140 ngân hàng và các tổ chức nhận giữ tiền khác có các văn phòng hoặc các chi nhánh ở thành phố New York. Các thành viên của CHIPS được chia thành các ngân hàng tham gia thanh toán và không thanh toán. Mỗi ngân hàng tham gia không thanh toán có một tài khoản với một ngân hàng tham gia thanh toán sẽ thực hiện thanh toán nhân danh nó. CHIPS có các máy tính kép tại trụ sở ở New York của nó và một hệ giống hệt thứ ba ở một địa điểm tách riêng. Các thông báo được xác thực theo chuẩn ANSI X9.9. Mã hóa không được sử dụng. Các khuôn thức thông báo tiêu chuẩn được sử dụng và nhiều người tham gia có khả năng gửi các thông báo một cách tự động từ mạng này tới mạng khác mà không phải đánh tín hiệu lại. Ví dụ, hệ thu nhận các số hiệu nhận dạng SWIFT và tự động tham khảo chéo chúng với các số hiệu nhận dạng vạn năng của CHIPS.

FedWire là phương tiện chuyển tiền của Hoa Kỳ vận hành toàn quốc bởi Hệ dự trữ liên bang (Fed) ở Oasinton. Tất cả các giao dịch đều là chuyển tín dụng và khi khởi đầu đều được ghi nợ ngay vào tài khoản của người trả tiền. Mạng chuyển mạch gói nối mười hai ngân hàng dự trữ liên bang khu vực được kết nối với hệ thống.

Xấp xỉ 8000 tổ chức giận giữ tiền (các ngân hàng và các cơ quan nhận tiền gửi tương tự) sử dụng dịch vụ Fed. Cục kho bạc cũng là một thành viên tham gia trực tiếp. Nhiều trong số những tổ chức đó được nối trực tiếp với các máy tính của Cục dự trữ liên bang, như cục kho bạc Hoa Kỳ.

BankWire là một hệ truyền thông tư nhân phục vụ các ngân hàng thương mại ở các thành phố của Hoa Kỳ và Canada. Hệ thống này được sử dụng cho nhiều đường truyền thông liên ngân hàng liên quan tới chuyển tiền. Các vụ chuyển tiền có thể thực hiện trong cùng ngày nhờ ghi nợ và có vào các số dư tiền gửi theo nhu cầu liên ngân hàng, thông tin đã truyền có thể bao gồm các lệnh ghi nợ cho tài khoản của bên thứ ba. Dịch vụ bao gồm cả báo giá chuyên hóa gọi là CashWire. Dịch vụ này dự phòng thanh toán thực các vụ chuyển tiền trên sổ sách của Cục dự trữ liên bang.

Sagittaire là một hệ thống đặt tại Pari. Nó hoạt động phối hợp với nhóm người sử dụng SWIFT ở Pháp và các chuẩn thông báo được chấp nhận là tương thích với các khuôn thức SWIFT. Việc truy nhận hạn chế ở các ngân hàng nằm trong nước Pháp và hệ xử lý dành riêng cho các thanh toán bằng đồng frăng của Pháp nảy sinh từ những vụ chuyển tiền quốc tế.

Thủ tục thanh toán được Ngân hàng Pháp, ngân hàng trung ương Pháp quản lý, còn các phương tiện mạng được cung cấp bởi cơ quan viễn thông sở

hữu nhà nước - Cty bưu chính viễn thông, PTT.

Các mạng ngân hàng điện tử tư nhân

Nhiều ngân hàng quản lý các mạng ngân hàng điện tử tư nhân riêng của họ. Những mạng đó có khả năng cung cấp rất nhiều sản phẩm tài chính tự động hóa ngoài các lệnh trả tiền. Người sử dụng các mạng có thể là những khách hàng công ty chính, các khách hàng cá nhân hoặc nhân viên ngân hàng. Các dịch vụ mạng được xem như một phương tiện quan trọng đối với một ngân hàng để duy trì khả năng sắc bén trong cạnh tranh của nó.

Các khách hàng công ty lớn sử dụng các dịch vụ ngân hàng điện tử, thường cho những ứng dụng như quản lý tiền mặt, chuyển tiền và báo cáo số dư trên nhiều tài khoản công ty. Các khách hàng cá nhân sử dụng các mạng cho những dịch vụ như tự phục vụ (ATM), điểm trả tiền và những ứng dụng ngân hàng gia đình (hỏi tài khoản, sổ séc và ra lệnh báo cáo). Nhân viên ngân hàng sử dụng những ứng dụng nội bộ cho một loạt các sản phẩm tài chính nội bộ, để trả lời các yêu cầu bằng lời hoặc bằng giấy của khách hàng (mở tài khoản và yêu cầu đơn yêu cầu cho vay).

Các dịch vụ ngân hàng đưa ra được mở rộng liên tục bởi ngành công nghiệp để đáp ứng những nhu cầu thị trường mới, và để giành lấy những tài khoản mới. Các mạng truyền thông đóng một vai trò chủ chốt trong phân phối những sản phẩm điện tử đó cho giới mua bán, cho dù đó là từ gia đình, văn phòng, chi nhánh địa phương hoặc thậm chí "qua tường" chi nhánh ngân hàng địa phương. Nhiều ngân hàng sẽ sử dụng các mạng tư nhân mà họ trực tiếp quản lý và điều khiển.

Trong khi các mạng tư nhân là khác nhau, thì vẫn có những cách tiếp cận chuẩn hóa và giống nhau đối với các dịch vụ an toàn, mà quan trọng nhất trong đó là quản lý an toàn. Điều này cho phép ngân hàng kiểm soát của hệ quản lý khóa thủ công và tự động, các hệ xử lý giao dịch lớn và nhiều người sử dụng mạng. Việc mở rộng liên tục số lượng các dịch vụ và người sử dụng khiến cho yêu cầu này là một trong những xem xét quan trọng nhất trong việc lựa chọn thiết kế an toàn. Các đặc tính dễ quản lý sử dụng được công nhận là con đường thỏa đáng duy nhất để quản lý an toàn hệ thống đối với các mạng lớn có tài nguyên nhân lực hạn chế.

Mật mã liên kết thường được sử dụng bên trong các mạng ngân hàng công tác để tạo ra an toàn truyền dẫn, với các khóa được các ngân hàng quản lý. Điều này phản ứng các thực tiễn sử dụng ở những mạng tài chính quốc tế chính như SWIFT và CHAPS.

Các dịch vụ an toàn trung tâm có hiệu lực thông qua mã liên kết với các secvơ mật mã ứng dụng chủ cho các dịch vụ xác thực thông báo. Các kỹ thuật quản lý khóa thay đổi giữa các ngân hàng, nhưng RSA hiện đang được ưa chuộng vì phương pháp ưu tiên tự động hóa và phân phối khóa. Dịch vụ ứng dụng trung tâm thường kiểm soát các giới hạn giao dịch của khách hàng, nắm bắt các kiểm soát theo trình tự giao dịch quan trọng và quản lý việc tạo ra vết

kiểm toán. Thông thường có nhiều hơn một sản phẩm tài chính mà các khách hàng có thể sử dụng. Các ứng dụng trung tâm có thể xem xét chặt chẽ việc cấp các đặc quyền truy nhập cho người sử dụng.

Quản lý kho bạc điện tử

Các thủ quỹ công ty là những khách hàng quan trọng của ngân hàng, công việc của họ là thực hiện những công việc về tiền nong cho các công ty tương ứng của họ. Họ đầu tư tiền để có hiệu quả khả dĩ tốt nhất, cho vay với điều kiện hấp dẫn nhất, tuyên chiến với những vận chuyển tiền bạc không cần thiết và giảm chi phí chuyển khoản tới mức tối thiểu. Các bộ phận của kho bạc sống bằng thông tin và về nhiều mặt họ là hình ảnh phản chiếu của các chủ ngân hàng của họ.

Hoạt động ngân hàng điện tử không chỉ bao quát phân phối và thu nhận tự động hóa các giao dịch trả tiền. Thủ quỹ công ty ngày càng đòi hỏi nhiều hơn về "cửa sổ điện tử" quan sát thị trường tài chính để nhận và phân phối điện tử những dữ liệu tài chính như:

- truyền những khoản trả bằng tiền địa phương (CHAPS, SAGITTAIRE v.v.);
- truy nhập số dư tài khoản và dữ liệu giao dịch, ngay cả khi các tài khoản được bảo quản ở các ngân hàng ngoại quốc;
- kiểm soát và mô phỏng quản lý các rủi ro tổn thất tiền tệ của công ty.

EDI và các xu hướng tương lai

EDI là sự truyền các dữ liệu kinh doanh theo một khuôn thức có cấu trúc giữa các máy tính. Thông thường, dữ liệu kinh doanh liên quan tới các đơn mua hàng, các hóa đơn, thông báo gửi hàng và thông báo chuyển tiền. Với EDI, các tài liệu bằng giấy giảm đến tối thiểu và các thực tiễn thương mại truyền thống phải được đánh giá lại.

Trong môi trường thương mại, tiền tệ thường có thể được phân tích như thực trạng của số dư có trong một tài khoản ngân hàng và do đó là khoản nợ của khách hàng. Khoản trả tiền thường không phải là sự chuyển giao vật lý một tài sản hữu hình mà là sự truyền thông dữ liệu và lưu chuyển của các thông báo dữ liệu.

Một lệnh do khách hàng đưa ra cho ngân hàng và ngân hàng thực hiện trả tiền bằng cách liên lạc với ngân hàng nhận. Điều này đạt được hoặc nhờ giấy như ủy nhiệm chi của ngân hàng, telex, EFT hoặc một cơ chế tương tự nào đó. Sau đó là thanh toán liên ngân hàng, nhưng điều đó lệ thuộc vào cách thức trả tiền chủ yếu trong thương mại. Do đó việc trả tiền diễn ra hoàn toàn tự nhiên bên trong môi trường kinh doanh EDI.

Về cơ bản, không có sự khác nhau giữa giao dịch EDI và giao dịch chuyển tiền khi giao dịch chuyển tiền được truyền đi theo khuôn thức có cấu trúc giữa các máy tính. Theo nghĩa này, hệ SWIFT vốn có các kiểu thông báo theo khuôn thức có cấu trúc đối với dữ liệu tài chính, là một hệ EDI. Tuy nhiên, sự khác nhau là ở những người sử dụng hệ thống hoặc đúng hơn ở kiểu giao dịch được thuyền qua hệ thống. Trong khi ở hệ chuyển tiền quốc tế, người sử dụng là những tổ chức tài chính và các giao dịch chủ yếu liên quan tới các khoản

trả tiền thì ở hệ EDI, người sử dụng có thể là từ một loại hình công nghiệp bất kỳ và các giao dịch có thể gồm bất kỳ loại dữ liệu kinh doanh nào.

EDI đã phát triển chủ yếu trong các ngành công nghiệp dịch vụ, như bảo hiểm, vận tải hàng không, công nghiệp động cơ và hoạt động ngân hàng (SWIFT). Tiềm năng đối với các dịch vụ EDI là rất lớn và được hỗ trợ bởi nhiều nhà cung cấp mạng, như các dịch vụ thông tin GE, IBM, DEC cũng như được hỗ trợ bởi các PTT.

Liên kết cơ bản trong chuỗi kinh doanh EDI là chức năng trả tiền, xem hình minh họa. Các ngân hàng phải quan tâm tới EDI vì thế giới các khách hàng công tư đang thay đổi. Để có thể cạnh tranh, các ngân hàng sẽ cần phải làm cho các dịch vụ chuyển tiền của họ có hiệu lực bên trong khuôn khổ của các mạng EDI cộng tác.

SWIFT đã nhận thức được nhu cầu về một tập chặt chẽ các chuẩn kỹ thuật được quốc tế chấp nhận để hỗ trợ cho trao đổi các giao dịch thương mại. Ngoài các khuôn thức thông báo SWIFT hiện hành, các thông báo liên ngân hàng chuẩn dựa trên cú pháp EDIFACT đã được phát triển. Ngoài ra, các trao đổi lẫn nhau chuẩn hóa đang được phát triển mà hiện nay, có thể lập thành cơ sở của các hợp đồng EDI với bất kỳ sửa đổi nào mà người tham gia muốn thực hiện.

EFT là công cụ của các ngân hàng, nhưng bên trong môi trường mạng EDI, việc trả tiền EFT trở thành một phần không tách rời của chu trình kinh doanh EDI. Do đó, nó là một chức năng liên tục và tin cậy bên trong chu trình đó. Các ngân hàng tham gia EDI phải cung cấp cái gì khi dịch vụ giá trị gia tăng của họ là một yếu tố đảm bảo cho thông báo trả tiền.

EDI vừa là mối đe dọa vừa là cơ hội cho các ngân hàng. Là mối đe dọa bởi vì những người điều hành mạng độc lập, như các dịch vụ thông tin BT hoặc GE, có thể xâm phạm quan hệ truyền thống giữa các ngân hàng và các khách hàng cộng tác của họ và có khả năng cung cấp những dịch vụ thay thế. Tuy nhiên, EDI cũng là một cơ hội cho các ngân hàng bởi vì nó là một lĩnh vực kinh doanh mới mà trên đó, có thể phát triển thêm các dịch vụ giá trị gia tăng. Các ngân hàng được đặt vào vị trí tốt để cung cấp những dịch vụ đó bởi vì họ có sẵn hạ tầng cơ sở truyền thông mà EDI phụ thuộc vào để vận hành theo chuẩn X.400. Hơn nữa, họ có kinh nghiệm bảo trì các dịch vụ an toàn và rất đáng tin cậy. Khó khăn họ phải đương đầu là họ phải hợp tác trong những lĩnh vực mà trước đó đã có sự cạnh tranh mạnh mẽ. *Xem* ANSI X9.9 - 1986, ATM, BANKWIRE, EDI, EDIFACT, EPT, cashwire, CHAPS, CHIPS, closed user group, FEDWIRE, key, link encryption, message authentication, RSA, SAGITTAIRE, SPEED, SWIFT, tamper resistant module, X.25, X.400.

bank to bank information ***thông tin ngân hàng - ngân hàng*** Trong hoạt động ngân hàng, thông tin hỗn hợp liên quan tới sự chuyển khoản mà có thể bao gồm thông tin cho biết rõ thông tin dành cho ngân hàng hoặc các ngân hàng nào.

BankWire ***dịch vụ BankWire*** Trong hoạt động ngân hàng, dịch vụ viễn thông và thanh toán tư nhân cho các ngân hàng ở Hoa Kỳ. *Xem* banking networks.

base ***cơ sở, gốc; cơ số*** (1) Trong toán học, cơ sở là một giá trị chuẩn. (2) Trong toán học, cơ số là số dùng trong biểu diễn dấu phẩy động của các số. (3) Trong toán học, cơ số là giá trị qua đó một hệ thống số được thiết lập. Ví dụ, số học nhị phân sử dụng cơ số 2. *Xem* radix.

baseband ***dải gốc; truyền dải gốc*** (1) Trong truyền thông dữ liệu, dải gốc là khoảng tần số của thông tin mang các tín hiệu trước khi kết hợp với sóng mang bằng điều biến. (2) Trong truyền thông dữ liệu, truyền dải gốc là sự truyền các tín hiệu ở các tần số ban đầu của chúng, tức là chưa được điều biến. *Xem* carrier, modulation.

baseband modem ***modem dải gốc*** *Đồng nghĩa với* limited distance modem.

baseline ***đường cơ sở*** *Xem* baseline security controls.

baseline security controls ***(các) kiểm soát an toàn đường cơ sở*** Trong quản lý rủi ro, tập hợp các cơ cấu kiểm soát chung nhằm tạo ra mức an toàn cơ sở trong một lớp các hệ thống.

basic mode link control ***điều khiển liên kết chế độ cơ bản*** Trong truyền thông dữ liệu, sự điều khiển các liên kết dữ liệu bằng cách sử dụng các ký tự điều khiển của bộ ký tự 7 bit ISO/CCITT để trao đổi xử lý thông tin. *Xem* CCITT, ISO-7.

basic security theorem ***định lý an toàn cơ bản*** Trong an toàn máy tính, định lý phát biểu rằng, nếu một hệ bắt đầu ở một trạng thái an toàn và mọi sự chuyển tiếp đều tuân theo những quy tắc an toàn xác định thì trạng thái mới cũng sẽ an toàn. *Xem* Bell-La Padula model.

basic service ***dịch vụ cơ bản*** Trong truyền thông, dịch vụ của hãng truyền thông công cộng bị giới hạn đối với cung cấp dung lượng truyền cho vận chuyển thông tin. Các dịch vụ cơ bản được điều hành bởi FCC. *Xem* enhanced services, computer inquiry 1980, FCC.

batch balancing ***cân đối theo lô*** Trong kiểm toán, việc so sánh các hạng mục hoặc các tài liệu đã xử lý so với một tổng kiểm tra định trước. *Xem* balancing.

batched communication ***truyền thông theo lô*** Trong truyền thông dữ liệu, sự truyền một khối lớn dữ liệu từ trạm này đến trạm khác trong một mạng mà không có những đáp ứng can thiệp từ thiết bị nhận. *So sánh với* inquiry/response.

batch total ***tổng lô*** Trong tin học, tổng tính cho một thành phần chung nào đó của một lô dữ liệu vốn cho phép duy trì kiểm tra về tính hợp lệ của dữ liệu.

baud ***bốt, baud*** Trong truyền thông dữ liệu, số đo tốc độ truyền tín hiệu trong một mạch truyền thông số. Tốc độ tính theo bốt bằng số trạng thái rời rạc hoặc biến cố tín hiệu mỗi giây. Ví dụ, một bốt bằng một bit trên giây trong một chuỗi tín hiệu nhị phân. Vì bốt là

số đo của tất cả các phần tử tín hiệu đã truyền, kể cả những phần tử dùng để phối hợp sự truyền, cũng như thông báo thực dã truyền, nên nó không nhất thiết tương đương với tốc độ truyền tín hiệu dữ liệu. *Xem* data signalling rate.

Baudot code ***mã Baudot*** Trong truyền thông dữ liệu, mã để truyền dữ liệu trong đó năm bit độ dài bằng nhau biểu thị một ký tự.

BBS ***BBS*** (1) Viết tắt của Bulletin Board System (hệ bảng thông báo). (2) Viết tắt của Bulletin Board Software (phần mềm bảng thông báo). *Xem* bulletin board.

BCC *Xem* block character check.

BCD *Xem* binary coded decimal.

BCF *Xem* bromochlorodifluoromethane, byte cipher feedback.

BCP *Xem* byte control protocol.

BDN *Xem* Bell Data Network.

BDSG *Xem* Bundesdatenschutzgesetz.

beam break ***ngắt chùm*** Trong an toàn vật lý, kỹ thuật phát hiện kẻ xâm nhập dựa trên sự thay đổi cường độ chùm tia tạo ra khi một kẻ xâm nhập đi qua. Chùm tia có thể là chùm bức xạ điện từ phát ra từ một nguồn sáng, máy phát laze hoặc tần số vô tuyến. *So sánh với* break alarm.

bearer ***kênh thông cao*** Trong truyền thông dữ liệu, một kênh dải thông cao. *Xem* channel.

BeBe ***virut BeBe*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

Beeper ***virut Beeper*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

bel ***ben*** Trong điện tử học và truyền thông, đơn vị cơ bản của thang loga (cơ số 10) dùng để biểu thị tỷ số của các công suất. Hai công suất A và B liên quan với nhau bởi N ben khi $\lg(A/B)$ N. *Xem* decibel.

Bell 103 ***chuẩn Bell 103*** Trong truyền thông dữ liệu, tiêu chuẩn cho các modem tốc độ thấp sử dụng các kỹ thuật đánh tín hiệu dịch tần để tạo ra tốc độ truyền nằm trong khoảng giữa 0 và 300 bit mỗi giây. *So sánh với* Bell 212A. *Xem* bits per second, frequency shift keying.

Bell 212A ***chuẩn Bell 212A*** Trong truyền thông dữ liệu, tiêu chuẩn cho các modem sử dụng kỹ thuật đánh tín hiệu dịch pha để tạo ra tốc độ truyền dữ liệu 1200 bit mỗi giây. *So sánh với* V.22. *Xem* bits per second, phase shift keying.

Bell Data Network ***mạng dữ liệu Bell*** Trong truyền thông dữ liệu, hệ thống của hãng AT&T nhằm cung cấp cho các thuê bao với một khoảng rộng các phương tiện truy nhập truyền thông và cơ sở dữ liệu.

Bell-La Padula model ***mô hình Bell-La Padula*** (1) Trong an toàn máy tính, mô hình chuyển tiếp hình thức của chính sách an toàn máy tính

mô tả một tập hợp các quy tắc kiểm soát truy nhập. Ở mô hình hình thức này, các thực thể trong hệ máy tính được chia thành các tập hợp trừu tượng gồm các chủ thể và đối tượng. Khái niệm trạng thái an toàn được định nghĩa và người ta chứng minh rằng, mỗi chuyển tiếp trạng thái đều bảo toàn tính an toàn bằng cách chuyển từ trạng thái an toàn này sang trọng thái an toàn khác; như vậy, theo chứng minh quy nạp, hệ là an toàn. Trạng thái của hệ được xác định là "an toàn" nếu các chế độ truy nhập được phép duy nhất của các chủ thể tới các đối tượng là phù hợp với một chính sách an toàn đặc thù. Để quyết định xem một chế độ truy nhập riêng nào đó có được phép hay không, mức truy nhập của chủ thể được so sánh với mức phân loại của đối tượng và việc xác định được tiến hành xem chủ thể có được cấp phép với chế độ truy nhập riêng hay không. Sơ đồ mức truy nhập/cấp phân loại được biểu thị theo thuật ngữ giàn. *Xem* lattice, object, simple security property, star property, subject. (2) Trong an toàn máy tính, mô hình toán học xử lý các kiểu soát truy nhập bắt buộc và tùy ý; nó chủ yếu liên quan tới việc chống tiết lộ thông tin bất hợp pháp. Báo cáo thường được tóm tắt bằng hai tiên đề:

- quy tắc an toàn đơn giản phát biểu rằng, một chủ thể không thể đọc thông tin mà nó không được phép ("không đọc lên");
- tính chất sao (*) phát biểu rằng, một chủ thể không thể chuyển thông tin từ một đối tượng có cấp phân loại an toàn cao sang một đối tượng có cấp phân loại an toàn thấp hơn (không ghi xuống).

Mô hình có tầm quan trọng lớn, cung cấp một mô hình hình thức cho truy nhập an toàn tới các thực thể. Mô hình không tự hạn chế ở các hệ máy tính, nó có thể được áp dụng cho những dạng an toàn vật lý khác và cho an toàn thủ tục.

Mô hình cũng đưa ra khái niệm hệ tin cậy, tức là hệ được đảm bảo sự chuyển thông tin vi phạm tính an toàn không thực thi đầy đủ được ngay cả khi nó có thể.

Mô hình Bell-La Padula là nền tảng đối với các tiêu chuẩn cho các hệ thống (lớp) *A* và *B* trong Sách Vàng và đối với nhiều tiêu chuẩn đánh giá các hệ an toàn phát triển sau đó.

Mô tả mô hình

Mô hình có khả năng biểu diễn một cách trừu tượng các phần tử của các hệ máy tính và phần tử an toàn có liên quan tới việc xử lý thông tin mật lưu giữ trong một hệ máy tính. Vấn đề thiết yếu là kiểm soát truy nhập tới một tập hợp các thực thể thụ động được bảo vệ (gọi là đối tượng) của các thực thể chủ động (gọi là chủ thể) dựa trên một chính sách an toàn.

Trạng thái của một hệ được mô tả bởi một bộ (tập truy nhập hiện thời, ma trận được phép truy nhập, hàm mức và thứ bậc) hay (b, M, f, H). Mỗi một thành phần đó của trạng thái hệ thống được mô tả như dưới đây.

Tập truy nhập hiện thời (b)

Mục đích của một truy nhập trong mô hình là lấy thông tin ra từ một đối tượng hoặc chèn thông tin vào một đối

tượng. Bốn chế độ truy nhập: thi hành, đọc, nối thêm và ghi, được định nghĩa là:

- thi hành - không quan sát mà cũng không thay đổi;
- đọc - quan sát mà không thay đổi;
- nối thêm - thay đổi mà không quan sát;
- ghi - quan sát và thay đổi.

Chế độ nối thêm (hay gắn thêm) chẳng hạn có thể cho phép người sử dụng thêm một tập hợp các dữ liệu thống kê vào một tệp, mà không cung cấp phương tiện để đọc dữ liệu chứa trong tệp.

Truy nhập hiện thời của một chủ thể tới một đối tượng được biểu diễn bằng bộ (chủ thể, đối tượng, thuộc tính truy nhập). Toàn bộ tập hợp của tất cả các bộ như thế là tập hợp truy nhập hiện thời của mô hình, tức là "*b*" trong (*b*, *M*, *f*, *H*).

Thứ bậc (H)

Mô hình áp đặt một cấu trúc đối với các đối tượng vốn chỉ dành cho những cây có gốc hoặc những điểm tách riêng. Như vậy, thứ bậc của các đối tượng hoặc là của một đối tượng biệt lập, hoặc là thứ bậc trong đó, một đối tượng có thể có nhiều con nhưng một con chỉ có thể có một cha, tức là cấu trúc cây. Như vậy, thứ bậc riêng của các đối tượng trong hệ thống được biểu diễn bởi *H* trong trạng thái mô hình (*b*, *M*, *f*, *H*).

Cấp phép truy nhập (M)

Mô hình bao gồm sự dự phòng cho kiểm soát truy nhập tùy ý và sự cấp phép truy nhập được định nghĩa bởi ma trận *M* (xem hình 1).

Các cột của ma trận biểu thị các đối tượng của hệ thống, các hàng biểu thị các chủ thể còn ô ma trận biểu thị các thuộc tính truy nhập mà chủ thể có đối với đối tượng tương ứng. Như vậy ma trận truy nhập biểu diễn *M* trong mô hình (*b*, *M*, *f*, *H*).

Hàm mức (f)

Sự biểu hiện mức phân loại an toàn trong mô hình được cho bởi hàm mức *f*. Trong các lĩnh vực hoạt động của chính phủ, con người và tài liệu được gán một mức an toàn dưới dạng một cặp (cấp phân loại, tập hợp các loại hình).

Mức phân loại hay mức truy nhập là mức chỉ định phân cấp chặt chẽ, ví dụ.

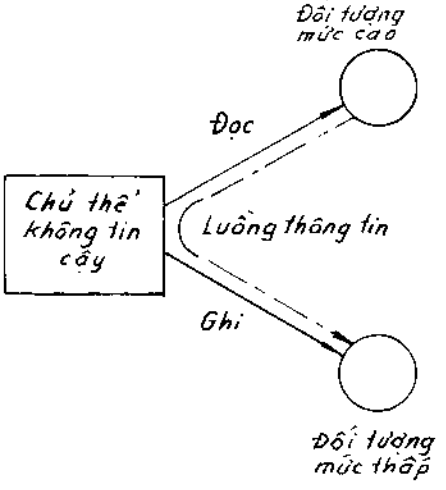
TỐI MẬT> TUYỆT MẬT>
MẬT> KHÔNG MẬT

	Chương trình 1	Đoạn A	Đoạn B
Quá trình 1	Đọc thi hành	Đọc Ghi	
Quá trình 1			Đọc

Bell-La Padula model : *mô hình Bell-La Padula*. Hình 1. Ma trận kiểm soát truy nhập.

Sự phân chia này, tuy vậy lại quá thô và nó cung cấp cho các cá nhân một quyền truy nhập dựa trên mức phân loại an toàn của họ mà không chú ý đến "nhu cầu cần biết" của họ. Thành phần thứ hai của chỉ định mức an toàn là tập hợp các loại hình, ví dụ như theo thuật ngữ quân sự, Hạt nhân, Nato, Crypto biểu thị các lĩnh vực quan tâm hợp pháp của cá nhân hoặc các chủ đề nêu trong một tài liệu (chẳng hạn). Như vậy một cá thể có thể có mức chỉ định an toàn (TUYỆT MẬT, {NATO, CRYPTO}).

Rõ ràng rằng, có các nhu cầu sắp xếp một chút các mức chỉ định an toàn và



Bell-La Padula model: *mô hình Bell-La Padula.* Hình 2. Luồng thông tin cho thấy nhu cầu về tính chất sao để ngăn ngừa chủ thể ác ý lấy thông tin từ một đối tượng tối mật và đặt nó vào một đối tượng mật.

điều đó đạt được bằng khái niệm trội. (lớp - 1, tập - loại - hình - 1) trội hơn (lớp - 2, tập - loại - hình - 2) khi và chỉ khi:

- lớp - 1 lớn hơn hoặc bằng lớp - 2;
- tập - loại - hình - 1 chứa tập - loại - hình - 2 như một tập con.

Như vậy (TỐI MẬT, {NATO, Hạt nhân}) có thể trội hơn (TỐI MẬT, {NATO}).

Một đối tượng sẽ có mức an toàn được chỉ định $f_o(O_j)$. Chủ thể (S_i) sẽ có mức an toàn (cực đại) $f_s(S_i)$ nhưng có thể chọn để hoạt động ở mức thấp hơn $f_c(S_i)$, mức này khi đó được gọi là mức an toàn hiện thời của chủ thể. Các quy tắc an toàn của hệ thống có thể buộc người sử dụng chấp nhận mức chỉ định thấp hơn này để thực hiện một số hoạt động, ví dụ ghi vào một tệp KHÔNG MẬT.

Như vậy, đối với một chủ thể và một đối tượng cho trước có ba mức an toàn quan trọng (f_s, f_o, f_c) và chúng tạo thành số hạng f của mô hình (b, M, f, H).

Bộ (b, M, f, H), tức là (tập truy nhập an toàn, ma trận được phép truy nhập, hàm mức, thứ bậc) biểu diễn trạng thái của mô hình. Mô hình định nghĩa ba đặc tính an toàn, đặc tính an toàn đơn giản (đặc tính ss), đặc tính sao (đặc tính *) và đặc tính an toàn tùy ý (đặc tính *ds*). Đặc tính an toàn đơn giản thỏa mãn khi (chủ thể, đối tượng, thuộc tính quan sát) là truy nhập hiện thời và mức an toàn của chủ thể trội hơn mức an toàn của đối tượng. Nói cách khác, chủ thể có mức an toàn thấp không thể đọc một một tệp có mức phân loại an toàn cao. Tính chất sao thỏa mãn, ở trạng thái

bất kỳ khi chủ thể có truy nhập quan sát đồng thời tới đối tượng - 1 và truy nhập thay đổi đối với đối tượng - 2 và mức an toàn của đối tượng - 2 trội hơn mức an toàn của đối tượng - 1. Quy tắc này nhằm ngăn ngừa virut con ngựa thành Tơroa hoạt động trong quá trình với một mức truy nhập an toàn cao, không chuyển thông tin từ đối tượng có mức phân loại an toàn cao sang đối tượng có mức phân loại an toàn thấp.

Trạng thái thỏa mãn tính chất an toàn tùy ý (tính chất *ds*) khi (chủ thể - 1, đối tượng - 1, thuộc tính - *x*) là truy nhập hiện thời, trong *b*, và thuộc tính - *x* được ghi trong thành phần (chủ thể - 1), đối tượng - 1) của M. Nói cách khác, mục nhập trong ma trận kiểm soát truy nhập tùy ý đối với chủ thể và đối tượng sẽ tương ứng với kiểu truy nhập đang tiến hành.

Hệ sẽ chuyển từ trạng thái này sang trạng thái khác như kết quả của một yêu cầu, ví dụ, bổ sung hoặc xóa một truy nhập đã thiết lập và sự đáp lại yêu cầu đó, tức là cho phép hoặc từ chối.

Định lý an toàn cơ bản của mô hình phát biểu rằng, an toàn có thể được đảm bảo một cách có hệ thống khi bản thân mỗi thay đổi đối với trạng thái hiện thời không vi phạm đến tính an toàn. An toàn có thể được đảm bảo một cách có hệ thống nếu bất cứ khi nào (chủ thể, đối tượng, thuộc tính truy nhập) được thêm vào tập truy nhập hiện thời, thì tất cả tính an toàn đơn giản, tính chất an toàn sao và tính chất an toàn tùy ý đối với trạng thái đó đều được thỏa mãn. Cách tiếp cận quy nạp này cho thấy rằng, sự bảo toàn tính an toàn từ trạng thái này sang trạng thái khác sẽ đảm bảo toàn bộ sự an toàn của hệ thống.

So sánh với Biba model. *Xem* access matrix model, discretionary security policy, dominate, mandatory security policy, object, Orange Book, simple security property, star security property, subject.

banecifiary ***người hưởng*** Trong hoạt động ngân hàng, bên cuối cùng được vào sổ bên có hoặc được trả tiền từ một cuộc chuyển tiền. *Đồng nghĩa với* ultimate beneficiary.

Berlekamp-Massey algorithm ***thuật toán Berlekamp-Massey*** Trong toán học, thuật toán xác định độ phức tạp tuyến tính của một dãy nhị phân hữu hạn. *Xem* linear complexity.

Best Wish ***virut Best Wish*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM, COM, OVL và EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* linear complexity.

beta testing ***thử beta*** Trong kỹ thuật tin cậy, phép thử một sản phẩm trong vận hành bởi những người sử dụng lựa chọn trước khi đem phát hành chính thức.

between-the-lines entry ***vào giữa chừng, vào giữa đường*** Trong an toàn máy tính, sự truy nhập do một người sử dụng không được phép nối lén chủ động vào một đầu cuối tạm thời không hoạt động của một người sử dụng hợp pháp được gán một kênh truyền thông. *Xem* access, active wiretapping; piggyback entry.

bias ***lệch, trệch; độ lệch*** (1) Trong toán học, lệch là điều kiện mà trong khi sinh các số giả ngẫu nhiên thì sự xuất hiện một số số nào đó có xác suất lớn hơn những số khác. *Xem* pseudorandom number. (2) Trong an toàn cơ sở dữ liệu, độ lệch là kết quả mất thông tin nảy sinh từ việc sử dụng các kỹ thuật nhiễu loạn trong kiểm soát suy luận. Nó được định nghĩa như hiệu giữa kỳ vọng của một giá trị thống kê bị nhiễu và giá trị thực của nó. *So sánh với* consistency. *Xem* inference control, information loss, perturbation.

biased ***chệnh, không cân xứng*** Trong toán học, chỉ một quá trình dùng trong việc sinh các số ngẫu nhiên tạo ra một số số có xác suất lớn hơn những số khác. *Xem* random numbers.

Biba model ***mô hình Biba*** Trong kiểm soát truy nhập, mô hình hệ thống kiểm soát truy nhập nhằm bảo vệ tính toàn vẹn của dữ liệu.

Trong mô hình này, các đối tượng và các chủ thể có mức phân loại an toàn phân cấp (thứ bậc) liên quan tới tính toàn vẹn hay "tính đáng tin cậy" của chúng. Như vậy, một chủ thể có thể có mức phân loại toàn vẹn $I(S)$ và một đối tượng có mức phân loại toàn vẹn $I(O)$; hơn nữa, các mức được sắp xếp sao cho, chẳng hạn $I(S) > I(O)$.

Mô hình Biba có hai tính chất an toàn có các tên tương tự với những tên sử dụng trong Bell-La Padula:

- Tính toàn vẹn đơn giản - nếu chủ thể S có thể sửa đổi một đối tượng O thì $I(S) > I(O)$.
- Tính chất sao toàn vẹn - nếu chủ thể S có truy nhập đọc tới đối tượng O có mức toàn vẹn $I(O)$, thì S có thể có truy nhập đọc đối với đối tượng P chỉ khi $I(O) >= I(P)$.

Trong mô hình này, một tệp có độ toàn vẹn cao phải không bị sai lạc bởi dữ liệu từ một tệp toàn vẹn thấp. Tính chất toàn vẹn đơn giản nhằm ngăn ngừa một cá nhân có mức phân loại toàn vẹn thấp sửa đổi một báo cáo có mức phân loại toàn vẹn cao. Như vậy, nếu điều quan trọng là đảm bảo cho dữ liệu trong một tệp chỉ bị sửa đổi bởi người có độ tin cậy cao, thì mô hình toàn vẹn đơn giản cùng với sự phân loại toàn vẹn thích hợp cho đội ngũ nhân sự và các tệp, sẽ cung cấp đảm bảo đó.

Tính chất sao liên quan tới việc ngăn ngừa luồng thông tin tương đối "khả nghi" có một mức phân loại toàn vẹn cao vào một tệp. Nó tương tự với tính chất sao của mô hình Bell-La Padula dùng để ngăn virut con ngựa thành Torroa làm rò thông tin có độ mật cao sang tệp có mức phân loại mật thấp. Tính chất sao của Biba đảm bảo rằng, một chủ thể truy nhập một tệp chỉ được phép ghi vào tệp cùng mức phân loại toàn vẹn hoặc thấp hơn và do đó, không thể làm sai lạc tệp có mức toàn vẹn cao bằng dữ liệu lấy từ tệp có mức phân loại kém tin cậy hơn. *So sánh với* Bell-La Padula model. *Xem* object, simple security property, star security property, subject.

bid ***giành điều khiển*** Trong truyền thông dữ liệu, sự cố gắng của một máy tính hoặc trạm giành điều khiển một mạch để nó có thể truyền dữ liệu.

bigram ***bộ đôi, cặp chữ*** Trong phân tích mật mã, một cặp các chữ cái liên tiếp. Trong các cuộc tấn công thống kê lên các mật mã, tần số biết được của các cặp chữ khác nhau trong một ngôn ngữ nào đó có thể được dùng để thử phá mã. *So sánh với* trigram. *Xem* information theory.

bijection ***song ánh*** Trong toán học, hàm ánh xạ một tập hợp các giá trị $\{p\}$ lên một tập hợp các giá trị $\{q\}$ sao cho mỗi tập có cùng số các phần tử và có quan hệ một - một giữa các phần tử. Như vậy mỗi giá trị trong $\{p\}$ gắn liền với chỉ một giá trị trong $\{q\}$ và ngược lại.

bimetallic-type heat detector ***máy dò nhiệt kiểu lưỡng kim*** Trong an toàn vật lý, thiết bị dò nhiệt gồm một băng lưỡng kim, hai dải kim loại thành phần có các hệ số giãn nở vì nhiệt khác nhau. Những thay đổi nhiệt độ khiến cho các dây uốn lệch nhau và điều này làm kích hoạt một tín hiệu báo động.

binary ***nhị phân*** Trong toán học và tin học, hệ đếm chỉ có hai trạng thái hoặc điều kiện. Hệ nhị phân được biểu diễn bằng các số 0 và 1.

binary arithmetic ***số học nhị phân*** Trong toán học và tin học, số học thực hiện với các số nhị phân. Các quy tắc số học cực kỳ đơn giản (ví dụ như 1 + 0 = 1, 1 + 1 = 10) và chúng có thể được thực hiện bằng các mạch logic đơn giản. *Xem* logic circuit.

binary code ***mã nhị phân*** Trong mã hóa, hệ thống mã hóa sử dụng các nhóm chữ số nhị phân 0 và 1, để biểu diễn một chữ cái, chữ số hoặc ký tự khác trong máy tính, ví dụ số 6 thập phân được biểu diễn là 110 theo hệ nhị phân, tức là (1 x 4) + (1 x 2) + (0 x 1). *Xem* binary.

binary coded decimal ***thập phân được mã (theo hệ) nhị phân, thập phân mã hóa nhị phân*** Trong tin học, phương pháp biểu diễn các số thập phân, trong đó mỗi chữ số của số được biểu diễn bởi một từ bốn bit. Bốn bit của từ bốn bit có thể biểu diễn các số trong khoảng 0 - 15, nhưng chỉ dùng các biểu diễn của các số 0 - 9. Ngoài ra, đôi khi người ta dùng cả byte để biểu diễn dấu. Dạng mã hóa này kém hiệu quả hơn các dạng nhị phân khác về mặt không gian nhớ, nhưng nó cho phép biểu diễn chính xác những số thập phân rất dài, và do đó thường được sử dụng trong những ứng dụng thuộc lĩnh vực giao dịch tài chính. *Xem* bit, byte, nibble.

binary digit ***chữ số nhị phân*** Trong toán học, ký tự 0 hoặc 1, thường viết tắt là "bit". *Xem* bit.

binary license ***giấy phép nhị phân*** Trong tin học, dạng phân phối phần mềm dưới dạng thực hiện được; người sử dụng không được phép sửa đổi mã chương trình.

binary number ***số nhị phân*** Trong toán học, số biểu diễn ở dạng nhị phân. *Xem* binary arithmetic, binary code.

binary symmetric source ***nguồn đối xứng nhị phân*** Trong mật mã học, thiết bị mà theo lý thuyết, có thể phát ra dãy các chữ số nhị phân thực sự ngẫu nhiên. *Xem* binary digit random numbers.

binary synchronous communications ***(giao thức) truyền đồng bộ nhị phân*** Trong truyền thông dữ liệu, giao thức điều khiển byte của hãng IBM gửi dữ liệu trong các khung được đánh dấu bằng các ký tự đồng bộ hóa. Sau hai ký tự đồng bộ hóa, mỗi khung có một ký tự khởi đầu phần tiêu đề, phần tiêu đề chứa thông tin điều khiển và địa chỉ, ký tự khởi đầu văn bản và ký tự kiểm tra độ dư thừa vòng. Giao thức hỗ trợ cả hoạt động điểm tới điểm lẫn hoạt động đa điểm. *Xem* byte control protocol, cyclic redundancy check, frame, header, multipoint connection, point to point.

binding analysis ***phân tích liên kết*** Trong an toàn thông tin, việc xác định xem liệu toàn bộ các chức năng đảm bảo an toàn cùng với những ảnh hưởng lẫn nhau của chúng như mô tả trong thiết kế kiến trúc có đáp ứng toàn bộ các mục tiêu an toàn hay không. *Xem* binding of functionality, information technology security evaluation criteria.

binding of functionality ***liên kết chức năng*** Trong an toàn thông tin, một tiêu chuẩn về hiệu quả trong ITSEC. Mặc dù các chức năng an toàn có thể thích hợp đối với những mục đích riêng lẻ của chúng, song có thể một số phối hợp nào đó các chức năng hoặc các cơ cấu gây cản trở hoặc xung đột với nhau. Trong đánh giá liên kết chức năng, người ta đã tiến hành nghiên cứu các quan hệ qua lại của các chức năng và cơ cấu an toàn, để đảm bảo chúng hỗ trợ lẫn nhau và tạo ra một tổng thể có hiệu quả và gắn bó. *Xem* information technology security evaluation criteria, security function, security mechanism.

biometrics ***công nghệ sinh trắc*** Trong kiểm soát truy nhập, các phương pháp tự động hóa kiểm chứng hoặc nhận dạng một cá nhân dựa trên các đặc trưng vật lý hoặc tập tính. Các kỹ thuật sinh trắc có thể được phân loại trên cơ sở một thuộc tính thụ động nào đó của cá thể, ví dụ như mẫu võng mạc mắt, hoặc một tác vụ đơn trị của một cá thể, ví dụ như ký chữ ký. Khái niệm sử dụng một thuộc tính vật lý duy nhất nào đó của người sử dụng có sức hấp dẫn lớn theo quan điểm xác thực, bởi vì dường như không có cơ chế nào để một kẻ tấn công có thể thực hiện gian lận thủ tục xác thực. Có thể đoán ra mật khẩu, hoặc ăn cắp thẻ bài nhưng không kẻ nào có được dấu vân tay của người khác.

Tổng quan

Các giai đoạn liên quan tới việc áp dụng có hiệu quả những hệ truy nhập sinh trắc như vậy gồm: thu nạp tương tự một thuộc tính của người sử dụng, phát triển một mẫu thuộc tính của người sử dụng, tức là ghi lại, so sánh mẫu nhập vào với mẫu đã lưu giữ của người sử dụng được phép, sẽ quyết định chấp nhận hoặc từ chối khi có yêu cầu truy nhập.

Bản chất của các phép đo sinh trắc như vậy là ở chỗ, chúng có thể hiển thị những biến đổi mỗi khi người sử dụng khởi nhập. Những thay đổi có thể này sinh do những yếu tố môi trường, như nhiệt độ, độ ẩm, do trạng thái của người sử dụng, ví dụ như căng thẳng, đổ mồ hôi hoặc sự hao mòn và trục trặc của thiết bị đo. Những thay đổi nhỏ ở

chữ ký đưa vào có thể không gây ra sự từ chối sai, tức là lỗi loại 1, hay tỷ lệ từ chối sai (FRR). Mặt khác, hệ thống phải không được bị khử nhạy tới mức chấp nhận các thuộc tính của cá nhân khác khi khớp với người sử dụng hợp pháp, gây ra chấp nhận sai, hay lỗi loại 2, hay như tỷ lệ chấp nhận sai (FAR). Việc giảm các tỷ lệ lỗi loại 1 thường phải trả giá là tăng tỷ lệ loại 2. Cơ chế thu nạp tương tự phải đảm bảo có sự phù hợp cao giữa các lần đo liên tiếp cùng các thuộc tính của một cá thể, trong khi vẫn đảm bảo đủ nhạy để giảm đến tối thiểu sự chấp nhận sai. Sự phát triển một mẫu sinh trắc phải lấy đủ được các đặc tính quan trọng đầu vào tương tự để đảm bảo rằng nó thực sự đồng nhất với đặc trưng của người sử dụng, đồng thời giảm đến tối thiểu số bit phải truyền và lưu giữ.

So sánh mẫu nhập vào và mẫu đã lưu là bài toán so khớp mẫu; các tiêu chuẩn để khớp mẫu phải sao cao các lỗi loại 1 và loại 2 đồng thời được giữ ở một mức thấp.

Ứng dụng

Các yếu tố cần xét đến trong khi xem xét một hệ kiểm soát truy nhập sinh trắc bao gồm:

- lĩnh vực ứng dụng;
- chi phí;
- các lỗi loại 1 và loại 2;
- hiệu suất;
- độ nhạy cảm với những yếu tố bên ngoài;
- khả năng chấp nhận của người dùng;
- những người sử dụng bị thiệt hại;
- trách nhiệm đối với người sử dụng;
- các tiêu chuẩn.

Các thiết bị sinh trắc có thể được xem xét trong rất nhiều lĩnh vực ứng dụng, kiểm soát truy nhập vật lý tại đầu vào, giấy phép tiến hành các giao dịch ở đầu cuối ATM hoặc EFTPOS, đăng nhập ở một đầu cuối, hoặc qua một mạng v.v. Các chi phí gắn liền với các thiết bị sinh trắc bao gồm: chi phí cơ bản về bộ đọc và thiết bị lưu mẫu kèm theo, chi phí bảo trì, điểm yếu dễ bị tấn công v.v. Chi phí của thiết bị sinh trắc hiện nay làm cho việc sử dụng chúng hạn chế ở những hệ coi an toàn là mối quan tâm hàng đầu. Chi phí của những thiết bị như thế không ngừng giảm và chắc chúng sẽ thông dụng hơn trong tương lai.

Có thể đạt được an toàn cao với các thiết bị sinh trắc, tùy thuộc vào việc đạt được các mức lỗi loại 1 và loại 2 thấp. Tuy nhiên, cần phải thận trọng khi giải thích các con số đã đánh giá cho những yếu tố tính năng đó. Việc đo các lỗi loại 1 là tương đối dễ dàng. Đơn giản là cần tiến hành một số lần thử liên tiếp đối với những người sử dụng điển hình trong những điều kiện thay đổi, nhiệt độ, độ ẩm, các thay đổi sinh lý v.v. Tuy nhiên, việc đo các lỗi loại 2 có thể lại liên quan tới những điều rất phức tạp. Rõ ràng có hai tình huống, một tình huống do các đặc trưng của một nhóm người sử dụng ngẫu nhiên; tình huống kia là một người sử dụng cố ý giả mạo là người khác.

Bài toán đánh giá tỷ lệ lỗi loại 2 là chọn một tập hợp người sử dụng để thử. Liên hệ các kết quả thử loại 2 với một mẫu ngẫu nhiên hoàn toàn, hoặc

các thành viên của mẫu được chọn phải có những đặc trưng gần với các đặc trưng của người sử dụng. Thực hiện các phép thử lỗi loại 2 với sự đảm bảo tính tương tự của các mẫu, ví dụ võng mạc mắt, chắc chắn là một nhiệm vụ khó. Bài toán các lỗi loại 2 có ý nghĩa thậm chí còn lớn hơn việc đo một hành vi vật lý. Làm sao ta có thể đảm bảo rằng, các đối tượng thử thành thạo trong việc giả dạng hành vi của người khác giống như một kẻ tấn công xác định. Tính có thể chấp nhận các tỷ lệ lỗi loại 1 và loại 2 rõ ràng phụ thuộc vào mức an toàn mà một lĩnh vực ứng dụng yêu cầu và vào mức bất tiện mà người dùng có thể chấp nhận được gắn liền với những từ chối sai.

Các hệ sinh trắc bao gồm việc đo một đặc trưng vật lý nào đó của người sử dụng, tiếp theo là so sánh với mẫu đã lưu. Nếu cho trước các biến liên quan tới phép đo, thì có lẽ cần nhiều hơn một phép đo, ít nhất là đôi khi như vậy. Toàn bộ quá trình đó chắc sẽ tốn thời gian hơn việc nhập mật khẩu hoặc nhét thẻ chất dẻo vào một bộ đọc. Khoảng thời gian trễ chấp nhận được của một hệ sinh trắc sẽ phụ thuộc vào lĩnh vực ứng dụng và mức an toàn cần có.

Các đặc trưng của người sử dụng và môi trường đo có lẽ bị thay đổi đáng kể theo thời gian. Việc quét vân tay sẽ bị ảnh hưởng bởi bụi bẩn, dầu mỡ, mồ hôi, sây sát v.v.. Có thể giảm số lần phản ánh sai bằng cách giảm độ nhạy của hệ thống với những biến đổi như thế, nhưng điều đó lại làm tăng xác suất của lỗi loại 2.

Các hệ sinh trắc có ưu điểm là chúng có ít yêu cầu hơn đối với những người sử dụng. Họ không nhất thiết phải nhớ những mật khẩu dài, đem theo các thẻ hoặc tiến hành những đối thoại phức tạp. Tuy nhiên, công chúng rất nhạy cảm với yêu cầu đo các đặc trưng cá nhân nào đó của họ. Lấy vẫy tay là một chủ đề đặc biệt nhạy cảm, bởi vì nó thường được tiến hành với các tội phạm.

Các hệ kiểm soát truy nhập do các đặc trưng vật lý của người sử dụng có thể gây cho người tàn tật khó khăn và bối rối. Các hệ nhận dạng tiếng nói rất có thể gây bối rối cho người nói lắp. Vấn đề chính sách của công ty hoặc luật pháp đối với cá nhân thua thiệt rõ ràng sẽ cần phải xem xét thận trọng khi ra quyết định sử dụng các hệ truy nhập sinh trắc.

Nếu các mẫu thuộc tính người sử dụng được lưu ở máy chủ trung tâm thì phải nhấn mạnh rằng, cả hệ máy chủ cả người sử dụng đều không thể chọn một mẫu khác. Không giống như mật khẩu hoặc PIN, người sử dụng không có cách nào thay đổi mẫu võng mạc mắt của họ. Hãy xét tình huống có thể nảy sinh nếu một kẻ tấn công truy nhập được vào một mẫu như thế. Khi đó anh ta có thể dễ dàng giả mạo là người sử dụng, đơn giản bằng cách gài một tín hiệu, tương ứng với mẫu của người sử dụng, như thế nó phát ra từ bộ đọc sinh trắc. Chỉ có nhờ cậy đến hệ chủ mới có thể loại bỏ được mẫu khỏi tệp được phép. Người sử dụng không chỉ bị từ chối truy nhập vào hệ thống mà có thể còn không có cách nào sử dụng được bộ quét võng mạc mắt để truy nhập. Việc

sử dụng mẫu võng mạc mắt đối với mắt khác chỉ có thể là một sự tạm hoãn.

Các bộ cảm biến sinh trắc đang xuất hiện trên thị trường và chúng xuất hiện trước cả các chuẩn quốc tế. Tuy nhiên trong một môi trường khép kín điều đó có thể không phải là một yếu tố quan trọng, song sự phát triển của những tiêu chuẩn như vậy sẽ trở thành vấn đề cấp thiết khi sử dụng chúng trong những mạng quốc gia và quốc tế, ví dụ như các hệ EDI hoặc EFT. *Xem* EDI, EFT, eye retina analysis, FAR, FRR, fingerprint analysis, hand geometry analysis, keystroke dynamics analysis, signature analysis, template Type 1 error, Type 2 error, veincheck, voice analysis.

bipolar ***lưỡng cực*** Trong truyền thông dữ liệu, chỉ tín hiệu nhận cả giá trị dương lẫn giá trị âm. *So sánh với* unipolar. *Xem* nonreturn to zero.

birthday problem ***bài toán ngày sinh*** Trong toán học, bài toán liên quan tới tính toán xác suất mà nếu n người chọn riêng lẻ một số ngẫu nhiên trong khoảng 1, 2,... n^2, trong đó $n < n^2$ thì có một xác suất đáng kể để hai người sẽ chọn cùng một số. Tên của bài toán xuất phát từ một sự kiện hơi ngạc nhiên là, với một nhóm 23 người được lựa chọn ngẫu nhiên thì có một cơ hội đồng đều để hai người trong số họ sẽ có cùng ngày sinh.

bistatic microwave sensor ***bộ cảm biến vi ba lưỡng ổn*** Trong an toàn vật lý, thiết bị phát hiện kẻ thâm nhập sử dụng máy phát vi ba và máy thu đường ngắm. Tổng tín hiệu nhận được bao gồm tổng vectơ của tín hiệu trực tiếp và các tín hiệu phản xạ từ các vật ở gần. Kẻ xâm nhập sẽ gây sự thay đổi trong tổng vectơ nhận được và báo động được kích hoạt. *Xem* microwave sensor.

BISYNC *Xem* binary synchronous communicaions.

bit ***bit*** *Xem* binary digit.

bit copier ***bộ sao bit, trình sao bit*** Trong bảo vệ phần mềm, chương trình đọc đĩa nguồn ở mức bit và ghi ở mức đó sang đĩa đích. Nếu đĩa nguồn được sao bảo vệ như thế thì nó sẽ là đĩa đích. *Xem* demon, weak bits.

bit interleaving ***xen kẽ bit, đan xen bit*** Trong truyền thông dữ liệu, phương pháp dồn kênh phân thời trong đó, kênh nhận một bit lần lượt từ mỗi đầu cuối chủ động và phân phối một bit lần lượt cho mỗi đầu cuối nhận. *So sánh với* character interleaving. *Xem* time division multiplexing.

BITNET ***mạng BITNET*** Trong truyền thông dữ liệu, viết tắt của Because It's Time NETwork (mạng Vì đã đến lúc), mạng quốc tế phát triển cho các cơ sở đại học.

bit oriented protocol ***giao thức hướng bit*** Trong truyền thông dữ liệu, giao thức không bắt buộc gán ký tự cho các bit dữ liệu đã truyền. *So sánh với* character oriented protocol. *Xem* bit, character, protocol.

bit parallel, byte serial ***bit song song, byte nối tiếp*** Trong truyền thông dữ liệu, sự truyền trong đó các bit riêng lẻ của một byte được gửi trên những đường riêng lẻ và các byte đầy

đủ được gửi tuần tự. *Xem* bit, byte, parallel transmission, serial transmission.

bit rate ***tốc độ bit*** Trong truyền thông dữ liệu, tốc độ tuyền các bit qua một liên kết truyền thông, thường biểu thị bằng bit trên giây (BPS). *Xem* baud, data transfer rate.

bit sequence independence ***(tính) độc lập dãy bit*** Trong truyền thông dữ liệu, chỉ mạng có khả năng chuyển dữ liệu số như một dãy các bit mà không có hạn chế nào đối với trình tự các bit. *Xem* bit, transparent data communication code.

bit sequence transparent ***trong suốt dãy bit, thông suốt dãy bit*** *Xem* bit sequence independence.

bits per inch ***bit trên insơ*** Trong tin học, số bit ghi được trên mỗi insơ của rãnh trên bề mặt ghi từ hóa.

bits per second ***bit trên giây*** *Xem* bit rate.

bit stream ***luồng bit, dòng bit*** Trong truyền thông dữ liệu, tín hiệu nhị phân không để ý tới sự nhóm theo ký tự. *Xem* bit.

bit string ***xâu bit*** Trong truyền thông dữ liệu, xâu các chữ số nhị phân trong đó, mỗi vị trí bit được xem xét như một đơn vị độc lập. *Xem* bit, string.

bit stuffing ***bổ sung bit, nhồi bit*** Trong truyền thông dữ liệu, kỹ thuật phân định ranh giới các khung bằng mẫu bit, ví dụ như 01111110. Khi năm bit 1 liên tiếp xuất hiện trong dữ liệu thông báo hoặc dữ liệu điều khiển thì bit 0 được bổ sung vào để tránh nhầm với dấu tách. *So sánh với* character stuffing. *Xem* synchronous data link control.

black ***phần đen*** Trong an toàn truyền thông, thông tin hoặc thiết bị và các đường dây không được chính thức coi là mật mà xử lý thông tin xếp vào loại mật đã mã. *So sánh với* red.

blacklist ***danh sách đen*** *Đồng nghĩa với* hot card list.

Black Monday ***virut Black Monday*** Trong an toàn máy tính, virut kết thúc và lưu thú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

blackout ***mất nguồn*** Trong an toàn vật lý, mất mát toàn bộ nguồn điện. *So sánh với* brownout.

blind dialing ***chọn số mò*** Trong truyền thông dữ liệu, phương tiện của một số modem cho phép modem chọn số khi âm chọn số được giả định có mặt nhưng không phát hiện được gì. Tiện ích này quan trọng trong một số hệ PBX sử dụng các đường không chuẩn mà một số modem sẽ hiểu như đường dây không hoạt động. *Xem* malicious code.

blob ***vết loang*** Trong an toàn máy tính, một dạng phá hủy của mã ác ý, mã này sẽ dần dần nắm quyền điều khiển trên một khoảng không gian nhớ ngày càng tăng cho tới khi hệ bị phá hủy. *Xem* malicious code.

block ***khối*** (1) Trong tin học, nhóm các từ, các tài liệu hoặc các tệp được xử lý như một đơn vị. (2) Trong tin học, tập hợp các bản ghi kề nhau được

nhớ như một đơn vị. (3) Trong truyền thông dữ liệu, nhóm các bit truyền như một đơn vị và được mã hóa để kiểm soát lỗi. *Xem* error detection code.

block cancel character ***ký tự hủy khối, ký tự xóa khối*** Trong mã hóa, ký tự thao tác đặc biệt nhằm làm cho một phần của khối đứng trước nó bị xóa. *Xem* block.

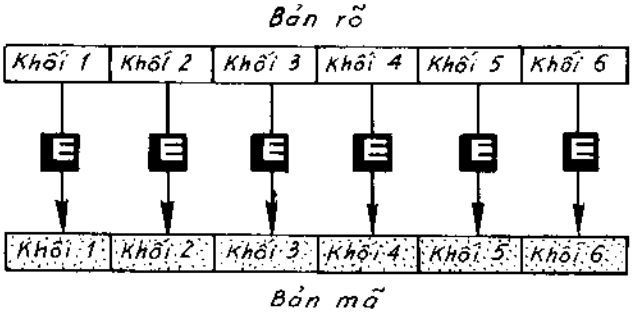
block character check ***kiểm tra ký tự khối*** Trong truyền thông dữ liệu, thủ tục kiểm soát lỗi dùng để phát hiện các lỗi trong một khối dữ liệu truyền qua mạng. *Xem* block, error detection code.

block cipher ***mật mã khối*** Trong mật mã, mã pháp trong đó bản rõ phải được ráp thành các khối với kích cỡ khối xác định bởi người thiết kế thuật toán mật mã; khối bản mã tương ứng chỉ phụ thuộc vào khóa mật mã, thuật toán và khối bản rõ. Như vậy, với một khóa mật mã đã cho bất kỳ, mã pháp sẽ cung cấp có hiệu quả một từ điển mã đồ sộ với các mục từ cho mọi khối bản rõ có thể và khối bản mã tương ứng. *So sánh với* block cipher chaining, stream cipher. *Xem* cryptopraphic key, electronic codebook.

block cipher chaining ***liên kết mật mã khối, xích mã khối*** Trong mật mã học, thủ tục sử dụng một mã khối trong đó bản mã ra phụ thuộc vào khóa, các khối bản rõ hiện thời và tất cả các khối bản rõ trước đó của thông báo. Việc liên kết khắc phục được điểm yếu mật mã của các mã khối. Điểm yếu này nảy sinh khi độ dài của thông báo vượt quá kích cỡ khối và các thông báo được định khuôn thức cao hoặc chứa độ dư thừa đáng kể.

Nếu thông báo mật mã bao gồm một số đáng kể các khối được tạo khuôn thức cao thì một số khối mã nhất định có thể xuất hiện trở lại trong các thông báo kế tiếp, do vậy tạo điều kiện cho một kẻ tấn công biên soạn được một từ điển mã các cặp bản rõ/bản mã.

Nếu một thông báo có độ dư thừa cao thì một kẻ tấn công sẽ có thể mở rộng sự phân tích tần số các đoạn bản rõ; các mã khối sẽ có xu hướng tạo ra các khối bản mã thể hiện cùng phân bố tần



block cipher: *mật mã khối.* Các mật mã khối mã hóa lần lượt mỗi khối văn bản.

số, do đó tạo ra thông tin hữu ích cho người phân tích mật mã.

Sự liên kết đảm bảo rằng, các mẫu trong các thông báo rõ không bị đưa vào bản mã. Hai khối bản rõ giống nhau trong các thông báo liên tiếp, sẽ tạo ra hai khối bản mã khác nhau miễn là các khối bản rõ trước đó không giống hệt nhau.

Tác dụng liên kết đạt được bằng cách cấp ngược trở lại các khối bản rõ hoặc bản mã trước đó và làm cho chúng ảnh hưởng tới quá trình mã/giải mã. Các khối bản rõ hoặc bản mã trước đó có thể được dùng để sửa đổi khóa hoặc đầu vào của thiết bị mã hóa/giải mã. Ví dụ, trong liên kết khối mã, đầu ra bản mã được cộng "loại trừ - hoặc" với khối bản rõ kế tiếp, kết quả được đưa vào thiết bị mã hóa.

Cần có những cách sắp xếp đặc biệt để xử lý khối ngắn cuối cùng khi độ dài của thông báo rõ không phải là một số nguyên lần kích cỡ khối. Đệm thêm các ký tự cố định, hoặc lựa chọn ngẫu nhiên là một giải pháp, nhưng giải pháp đó không thể chấp nhận được trong những trường hợp mà thông báo mã phải có cùng độ dài như thông báo rõ. Ví dụ, các tệp đã mã sẽ cần có cùng độ dài như các tệp bản rõ nếu chúng phải chiếm cùng vùng bộ nhớ. Hai kỹ thuật thông dụng cho trường hợp khối ngắn mà không làm giãn thông báo là chế độ mật mã dòng và lấy khéo bản mã.

Trong chế độ mã dòng, khối cuối cùng được mã hóa với một mã dòng; trong lấy khéo bản mã, khối bản mã áp chót được làm cho có cùng độ dài như khối bản rõ cuối cùng.

Liên kết gây mở rộng sai số; sự thay đổi giá trị bit của khối bản mã sẽ ảnh hưởng tới quá trình giải mã một số khối đến sau, nhưng bổ sung hoặc xóa đi một bit sẽ bóp méo hoàn toàn phần còn lại của thông báo rõ nhận được. Mật mã có kết nối được gọi là tự đồng bộ hóa nếu cuối cùng nó khôi phục được từ một lỗi, dưới dạng một bit thay đổi, trong bản mã đã truyền. *So sánh với* block cipher, stream cipher chaining. *Xem* blocksize, cipher block chaining ciphertext stealing, error extension, EXCLUSIVE OR, stream cipher.

block error rate ***tỷ lệ lỗi khối, suất lỗi khối*** Trong truyền thông dữ liệu, tỷ số số các khối nhận được không đúng trên tổng số các khối đã gửi đi. *Xem* block.

blocking law ***luật ngăn chặn, luật cấm*** Trong luật pháp, luật đặc biệt cấm sự tiết lộ, sao chép hay chuyển các tài liệu cho nhà chức trách của một nước khác dựa trên các đơn đặt hàng viết ra những tài liệu đó. Chúng được tòa án hoặc chính phủ của nước khác phát hành. *Xem* data protection.

block multiplexer channel ***kênh dồn khối*** Trong truyền thông dữ liệu, kênh của bộ dồn kênh truyền xen kẽ các chối dữ liệu. *Xem* block, channel, multiplexer.

block parity ***chẵn lẻ khối*** Trong truyền thông dữ liệu, phương pháp kiểm tra tính chẵn lẻ trong đó, một lỗi trong khối dữ liệu có thể được phát hiện và sửa mà không cần truyền lại khối. *Xem* error correction code, parity checking.

block size ***kích cỡ khối, kích thước khối*** Trong mật mã, số các bit trong một khối dùng trong mã khối. Kích cỡ khối phải đủ lớn để ngăn cản kiểu tấn công vét cạn thông báo. *Xem* block cipher, electronic codebook, message exhaustion.

block sum check ***kiểm tra tổng khối*** *Xem* longitudinal redudancy check.

Bloody ***virut Bloody*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trú; lây nhiễm cung khởi động đĩa mềm và bảng chia phần đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

Blood-2 ***virut Blood-2*** Trong an toàn máy tính, virut lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian vận hành, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

Blue Book ***Sách Xanh*** Trong an toàn dữ liệu, bản giải thích hệ quản lý cơ sở dữ liệu tin cậy thuộc các tiêu chuẩn đánh giá hệ máy tính tin cậy. Một trong những tiêu chuẩn của bộ Rainbow Series đôi khi bị gọi tên hơi sai vì bìa thực sự có màu hồng.

Bản giải thích bao gồm hai phần, hai phụ lục, một bảng từ vựng và danh sách tài liệu tham khảo. Phần thứ nhất nghiên cứu bài toán tổng quát hơn về đánh giá an toàn theo TCSEC, đối với các hệ thống vốn được xây dựng bằng cách ráp các phần - phần cứng, phần sun và phần mềm do các tổ chức và các hãng khác nhau tạo ra một cách độc lập. Nó đưa ra khái niệm các tập con TCB, bàn về sự đánh giá một hệ thống gồm những tập con TCB như thế và mức độ mà các khía cạnh của đánh giá tập con TCB có thể được tiến hành một cách độc lập. Phần thứ hai xem xét các yêu cầu đã giải thích đối với các hệ DBMS. *Xem* DBMS, Orange Book, TOB, TCB subset, TCSEC, Rainbow Series.

BNC connector ***bộ nối BNC*** Trong truyền thông, cáp đồng trục theo chuẩn công nghiệp nối với cơ cấu khóa chốt nganh; thường dùng nối thiết bị CCTV. *Xem* CCTV.

body print ***dấu ấn cơ thể*** Trong kiểm soát truy nhập, tổ hợp duy nhất của các thuộc tính vật lý, ví dụ nhịp mạch, mức hô hấp vốn đặc trưng cho một người. *Xem* biometrics.

book transfer ***chuyển tiền qua sổ sách*** Trong hoạt động ngân hàng, sự chuyển tiền giữa hai tài khoản cả hai đều được phục vụ bởi ngân hàng thực hiện giao dịch.

Boolean algebra ***đại số logic, đại số Boole*** Trong toán học, bộ môn toán học được đặt tên theo George Boole; nó cực kỳ quan trọng trong nghiên cứu các máy tính. Các biến trong hệ toán học này chỉ có thể nhận một trong hai giá trị, tức là ĐÚNG hoặc SAI, 1 hoặc 0. Có hai toán tử nhị phân, AND và OR, và toán tử đơn phân duy nhất NOT. *Xem* binary arithmetic, complement, logical expression, logical operator, logic circuit.

Boolean operator ***toán tử Boole*** Trong toán học, toán tử logic, AND, OR, NOT hoặc tổ hợp của chúng, ví dụ như NOT AND = NAND. *Xem* Boolean algebra, logical operator, XOR.

Boot ***virut Boot*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động của đĩa mềm và đĩa cứng và bảng phân chia đĩa cứng, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

boot sector virus ***virut cung khởi động*** Trong an toàn máy tính, virut lợi dụng cung khởi động của đĩa mềm hoặc đĩa cứng để đảm bảo nó được kích hoạt bất cứ khi nào máy tính khởi động từ đĩa đó. *Xem* virus.

bounds checking ***kiểm tra giới hạn*** Trong an toàn máy tính, việc thử các kết quả của chương trình máy tính để truy nhập vào bộ nhớ bên ngoài các giới hạn được phép của nó. *Xem* access. *Đồng nghĩa với* memory bounds checking.

bounds register ***thanh ghi giới hạn*** Trong an toàn máy tính, thanh ghi phần cứng chứa một dữ liệu chỉ ra biên của một bộ nhớ. *Xem* bounds checking.

Brain ***virut Brain*** Trong an toàn máy tính, virut kết thúc và thường trú, lây nhiễm cung khởi động của đĩa mềm và làm sai lạc cung khởi động. *Xem* virus names.

Brain Slayer ***virut Brain Slayer*** Trong an toàn máy tính, virut kết thúc và thường trú, lây nhiễm các tệp COM và EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

breach ***kẽ hở an toàn*** Trong an toàn máy tính, sự phá lỏng thành công và lặp đi lặp lại các cơ cấu kiểm soát an toàn có hoặc không có cơ chế ngăn cản, mà nếu hoàn thành có thể sẽ dẫn đến việc xâm nhập hệ thống. Ví dụ về những kẽ hở an toàn là: (*a*) Phân tích mã người dùng trong chế độ máy chủ. (*b*) Tiếp nhận không được phép mật khẩu nhận dạng hoặc các mật khẩu truy nhập tệp. (*c*) Truy nhập một tệp mà không sử dụng các cơ chế của hệ điều hành đã ấn định. (*d*) Truy nhập không được phép vào thư viện băng từ. *Xem* arrest, penetration.

break ***tạm ngừng, tạm ngắt*** Trong truyền thông dữ liệu, sự ngắt mạch đầu phát và nắm lấy điều khiển mạch ở đầu thu.

breakable ***có khả năng phá mã*** Trong mã thám, chỉ một mã pháp có thể xác định bản gốc hoặc khóa từ bản mã, hoặc xác định khóa từ các cặp bản gốc - bản mã. *Xem* cryptographic key, known plaintext.

break alarm ***báo động ngắt*** Trong an toàn vật lý, điều kiện báo động phát hiện kẻ xâm nhập do việc ngắt một mạch điện, ví dụ tách các lá kim loại có nối mạch gắn vào cửa sổ hoặc các khung cửa sổ. *So sánh với* beam break. *Xem* foil.

brevity lists ***(các) danh sách vắn tắt*** Trong an toàn máy tính, hệ thống mã được sử dụng để giảm thời gian cần thiết để truyền thông tin nhờ sử dụng một vài ký tự để biểu thị những câu dài, rập khuôn. *Xem* code system.

bridge ***cầu, cầu nối*** Trong truyền thông dữ liệu, thiết bị nối liên thông các mạng. Cầu bao hàm một cách có

hiệu quả tầng liên kết vật lý và dữ liệu của mô hình tham chiếu kết nối các hệ thống mở và như vậy có thể nối liên thông các mạng với những tầng liên kết dữ liệu khác nhau. *So sánh với* gateway, repeater, router. *Xem* data link layer, physical layer. (2) Trong truyền thông, thiết bị và các kỹ thuật dùng để làm khớp các mạch với nhau đảm bảo trục trặc truyền tối thiểu.

bridging sequential switcher ***bộ chuyển mạch cầu nối tuần tự*** Trong an toàn vật lý, bộ chuyển mạch video tuần tự với các đầu ra tách riêng cho các bộ giám sát lập trình trình tự và các bộ giám kiểm hoạt động mở rộng. Những bộ chuyển mạch như thế cho phép xem liên tục một cảnh chọn từ một dãy camera chuẩn. *Xem* sequential switcher, video switcher.

British Standards Institution ***Viện tiêu chuẩn Anh*** Trong tiêu chuẩn hóa, cơ quan quốc gia của Anh có vai trò tiêu chuẩn hóa tương tự Viện tiêu chuẩn quốc gia Mỹ.

British Telecom ***Telecom của Anh*** Bộ phận viễn thông thuộc PTT của Anh. *Xem* PTT.

broadband ***dải rộng*** Trong truyền thông, chỉ các phương tiện truyền mà dải thông của chúng lớn hơn dải thông khả dụng cho các mạch thoại và do đó có khả năng truyền dữ liệu tốc độ cao hơn. *Xem* bandwidth.

broadcast ***phát rộng, quảng bá*** Trong truyền thông, sự truyền đồng thời dữ liệu tới một số trạm. *Xem* Aloha, carrier sense protocol, Ethernet, local area network.

bromochlorodifluoromethane ***bromclodiflometan*** Trong an toàn vật lý, chất khí dùng để chữa cháy. *Đồng nghĩa với* halon 1211.

brownout ***(sự) giảm điện áp, nguồn yếu*** Trong an toàn vật lý, sự mất một phần công suất. *So sánh với* blackout.

browsing ***(sự) duyệt, xem lướt, xem trộm*** (1) Trong an toàn dữ liệu, tìm kiếm suốt bộ nhớ để định vị hoặc thu được thông tin mà không cần biết sự tồn tại hoặc khuôn dạng của thông tin đang tìm. (2) Trong an toàn dữ liệu, sự rà soát bất hợp pháp dữ liệu lưu ở một máy tính (ví dụ như dữ liệu mật hoặc phần mềm sở hữu riêng). Nó tương tự với nối lén thụ động các kênh truyền thông, nhưng nghiêm trọng hơn nhiều vì dữ liệu lưu trong máy tính có thời hạn sử dụng lâu hơn. Các cơ cấu kiểm soát truy nhập được thiết kế nhằm ngăn ngừa việc xem trộm. *Xem* access control, wiretap. *Đồng nghĩa với* scavenging.

BRP *Xem* business resumption planning.

BSC *Xem* binary synchronous communications.

BSI *Xem* British Standards Institution.

BT *Xem* British Telecom.

BTLE *Xem* between-the-lines entry.

buffer ***bộ đệm*** (1) Trong tin học, một vùng của bộ nhớ tạm thời dành để sử dụng khi thực hiện các thao tác nhập/xuất, mà dữ liệu được đọc vào đó hoặc được ghi ra từ đó. (2) Trong truyền thông dữ liệu, vùng nhớ dùng để bù trừ những chênh lệch về tốc độ luồng dữ liệu hoặc thời gian xuất hiện

các biến cố, khi chuyển dữ liệu từ thiết bị này sang thiết bị khác.

buffered network ***mạng có đệm*** Trong truyền thông dữ liệu, hệ thống sử dụng các bộ đệm gắn liền với mỗi đầu cuối để tăng tới tối đa hiệu quả hoạt động. *Xem* buffer.

bug ***con rệt điện tử; hỏng hóc, lỗi rối*** (1) Trong an toàn truyền thông, con rệp điện tử, *đồng nghĩa với* electronic listening device. (2) Trong tin học, hỏng hóc là lỗi ở một chương trình hoặc hệ thống. Thuật ngữ này được coi là bắt nguồn từ thời máy tính điện cơ sử dụng các rơle. Một lỗi không giải thích nổi đã được lần ra dấu vết là do cánh của một loài côn trùng mắc vào giữa các tiếp điểm của một rơle. *Xem* debug, relay.

building security systems ***(các) hệ an toàn cài sẵn*** Trong an toàn vật lý, hệ an toàn tích hợp cho một cài đặt để tạo ra sự bảo vệ chống hỏa hoạn, khói, đột nhập, gián điệp, phá hoại, trộm cắp, hoạt động không an toàn hoặc sai sót của thiết bị v.v..

bulletin board ***bảng thông báo*** Trong các ứng dụng, hệ thống truy nhập công cộng từ xa cho những người sử dụng máy tính cá nhân. Bảng thông báo hoạt động nhờ một người điều hành hệ thống (Sysop) và cung cấp rất nhiều dịch vụ đáp ứng các yêu cầu của đông đảo người sử dụng. Người sử dụng cần có một bộ chương trình phần mềm truyền thông và một modem để thiết lập quay số nối với hệ thống. Truy nhập vào các phương tiện của hệ thống được kiểm soát bởi Sysop và người sử dụng ban đầu phải được Sysop chấp nhận và sau đó tự đinh danh bằng mật khẩu khi khởi nhập hệ thống. Các phương tiện của bảng thông báo bao gồm:

- gửi các thông báo tới những người sử dụng khác;
- quét và đọc những thông báo do những người sử dụng khác gửi tới;
- tải lên và tải xuống các tệp.

Những người sử dụng được chờ đợi giúp đỡ lẫn nhau qua chia sẻ các ý tưởng, đặt ra những vấn đề về kỹ thuật và cung cấp câu trả lời cho những vấn đề đã đặt ra dựa trên sự hiểu biết và kinh nghiệm của họ. Phương tiện thông báo cũng có thể được sử dụng cho những vấn đề phi kỹ thuật, ví dụ như các quảng cáo BÁN và CẦN, cũng như phương tiện thư điện tử.

Phương tiện chuyển tệp cho phép người sử dụng cung cấp, và truy nhập phần mềm công cộng. Các chương trình có bản quyền cũng có thể được cung cấp trên cơ sở phần mềm dùng chung, tức là người sử dụng tải xuống chương trình và tự giác trả một phần cho người cung cấp nếu chương trình đó tỏ ra có ích.

Đã có một sự quan tâm nào đó về lĩnh vực an toàn máy tính khi các hacko sử dụng các bảng thông báo vi phạm bản quyền để phân phối thông tin liên quan tới xâm nhập qua điện thoại, phần mềm thâm nhập, gian lận thẻ tín dụng v.v. và để chia sẻ ý kiến chuyên môn. Hơn nữa, các phần mềm được tải xuống có thể chứa các virut máy tính. *Xem* electronic mail, hacker, MODEM, SYSOP, telephone intrusion virus.

Bundesdatenschutzgesetz ***luật Bundesdatenschutzgesetz*** Trong lập pháp, luật bảo vệ dữ liệu của Đức. *Xem* data protection - Germany.

Bundespost ***hãng Bundespost*** Hãng PTT của Đức. *Xem* PTT.

Burger ***virut Burger*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM, COM và EXE. *Xem* virus names.

burglar alarm pad ***đệm báo động trộm*** Trong an toàn vật lý, thiết bị phát hiện kẻ thâm nhập bao gồm lớp nền có khuôn các lá thép hoặc dây mịn. Một kẻ đột nhập bước vào làm rách lá hoặc đứt dây sẽ kích hoạt báo động. *Đồng nghĩa với* gird sensor. *Xem* foil.

burglary ***trộm cắp*** Trong lập pháp, sự xâm nhập bất hợp pháp vào một dinh cơ với mục đích ăn trộm.

buried-line intrusion pad ***đệm dò xâm nhập đường dây chôn*** Trong an toàn vật lý, máy dò kiểu địa chấn chôn ngầm gồm các đĩa gốm áp điện nằm bên trong một cáp đồng trục. Các đĩa được lắp giữa dây dẫn trung tâm và vỏ ở các khoảng đều đặn dọc theo cáp. Áp lực do chuyển động địa chấn lên các đĩa khiến cho chúng tạo ra các tín hiệu báo động. *Xem* piezoelectric detector, seismic sensor.

burn mark ***dấu đốt, dấu đánh dấu*** Trong bảo vệ phần mềm, kỹ thuật "lấy dấu tay" dùng laze để loại bỏ một vùng nhỏ chất liệu từ trên đĩa mềm. Một chương trình thử sẽ ghi vào, và sau đó cố đọc dữ liệu ra khỏi vùng đó. Nếu tác động đọc là thành công thì đĩa là bản sao và chương trình được bảo vệ sẽ bị vô hiệu hóa. *Xem* execute protection.

burst ***khối tín hiệu*** Trong truyền thông dữ liệu, dãy các tín hiệu được đếm như một thực thể đơn nhất phù hợp với tiêu chuẩn xác định nào đó.

bus ***bus, đường chủ, đường chính*** (1) Trong truyền thông dữ liệu, nhóm chung các đường phần cứng được dùng để truyền thông tin giữa các thiết bị hoặc thành phần số. (2) Trong truyền thông dữ liệu, cấu hình mạng trong đó các trạm làm việc được nối bởi các khớp nối chữ T với một cáp chính. *So sánh với* ring, star. *Xem* local area network.

business recovery planning ***kế hoạch hóa khôi phục kinh doanh*** *Đồng nghĩa với* business resumption planning.

business resumption planning ***kế hoạch hóa phục hồi kinh doanh*** Trong quản lý rủi ro, các sắp xếp để kế hoạch hóa các hoạt động khẩn cấp và khôi phục. Ba giai đoạn trong kế hoạch hóa khôi phục kinh doanh là: phòng ngừa, kế hoạch hóa và thử nghiệm.

Giai đoạn phòng ngừa gồm:

- phân tích hiểm họa;
- chương trình an toàn vật lý và bảo vệ;
- chương trình an toàn dữ liệu và bảo vệ.

Giai đoạn kế hoạch hóa bao gồm:

- phân tích chức năng/ứng dụng nguy cấp;
- thiết kế các thủ tục bình thường và khẩn cấp;
- các kiến trúc đối với: máy tính và viễn thông, xử lý thủ công và lưu giữ

bản ghi;

- thu nhận các tài nguyên dự phòng cho: lưu giữ ngoài tuyến, xử lý máy tính, xử lý thủ công, truyền thông dữ liệu và tiếng nói, kiểm tra quản lý;
- sắp xếp biên chế nhân sự cho đội đối phó thảm họa để đánh giá thiệt hại và lập kế hoạch khôi phục, các hoạt động khẩn cấp, quản lý đối phó - thảm họa.

Giai đoạn thử nghiệm gồm:

- thử nghiệm các hoạt động: các ứng dụng dựa trên xử lý máy tính, các ứng dụng dựa trên xử lý thủ công;
- thử nghiệm mô phỏng: đội đối phó khẩn cấp, đội quản lý thảm họa. *Xem* contingency plans, disaster recovery plan. *Đồng nghĩa với* business recovery planning.

bussback ***nối ra - vào, nối mạch phản hồi*** Trong truyền thông, việc một hãng truyền thông công cộng hoặc PTT nối một phần đầu ra của một mạch ngược trở lại phần đầu vào của một mạch. *Xem* loopback test.

byte ***byte, bai*** (1) Trong tin học, ký tự nhị phân được thao tác như một đơn vị và thường ngắn hơn một từ máy tính. Byte là đơn vị khả lập địa chỉ nhỏ nhất của bộ nhớ và thường dài tám bit. (2) Biểu diễn của một ký tự. *Xem* bit, word.

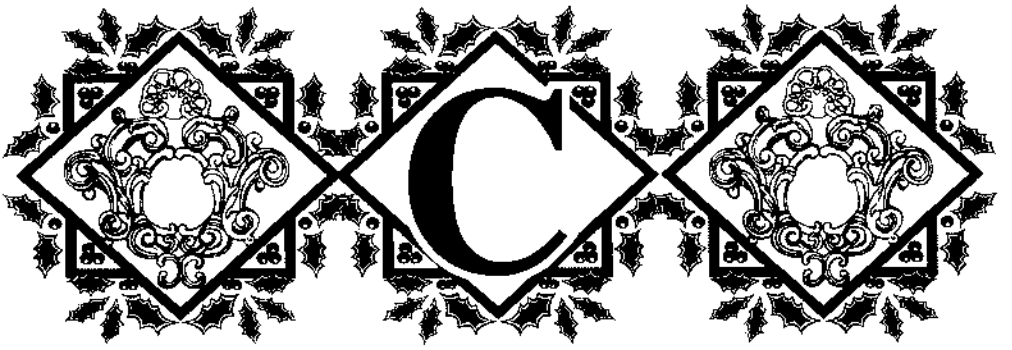
byte cipher feedback ***hồi tiếp mã theo byte*** Trong mật mã học, hồi tiếp mã trong đó, các đoạn được truyền đi và cấp ngược trở lại thanh ghi dịch, đều có độ dài một byte. *Xem* byte, cipher feedback.

byte control protocol ***giao thức kiểm soát byte*** Trong truyền thông dữ liệu, giao thức trong đó một thông báo được gửi đi với phần tiền đề tiếp theo là một trường thông tin. Cả máy gửi lẫn máy nhận đều cần để duy trì những số đếm khác nhau và để giải mã các mã điều khiển. *Xem* binary synchronous communications, header, protocol.

byte mode ***chế độ byte*** *Đồng nghĩa với* multiplex mode.

byte multiplex channel ***kênh dồn byte*** Trong truyền thông dữ liệu, kênh của bộ dồn kênh đan xen các byte dữ liệu từ những nguồn khác nhau. *Xem* multiplexer.

byte serial transmission ***truyền nối tiếp các byte*** Trong truyền thông dữ liệu, sự truyền dữ liệu trong đó, các byte kế tiếp theo nhau theo trình tự. Các bit riêng lẻ của mỗi byte có thể được truyền nối tiếp hoặc đồng thời. *Xem* serial transmission.



C1 *C1* *Xem* Division C.

C2 *C2* *Xem* Division C.

C2 by 92 *C2 năm 92* *Xem* NTISSP - 200

caboose *bit dừng* *Đồng nghĩa với* stop bit.

Caesar cipher *mã Caesar* Trong mật mã học, ví dụ sớm nhất về mã pháp đơn biểu, hoặc thay thế dùng trong các cuộc chiến tranh Gôlơ. *Xem* monoalphabetic cipher.

call *cuộc gọi* Trong truyền thông dữ liệu, sự truyền nhằm mục đích nhận dạng trạm truyền mà nó nhắm tới. *Xem* call accepted signal, call control character, call control procedure, call control signal, station.

call accepted signal *tín hiệu chấp nhận cuộc gọi* Trong truyền thông dữ liệu, tín hiệu điều khiển cuộc gọi được DTE được gọi truyền đi để báo rằng, nó chấp nhận cuộc gọi đang tới.

call back *gọi ngược* Trong an toàn máy tính, thủ tục được thiết lập để nhận dạng khẳng định một đầu cuối quay số vào một hệ máy tính bằng cách ngắt đầu cuối gọi, và tái thiết lập nối bằng cách hệ máy tính quay số điện thoại của đầu cuối gọi. *Xem* dial up control, port protection device, telephone intrusion. *Đồng nghĩa với* dial back.

call control character *ký tự điều khiển gọi* Trong truyền thông dữ liệu, ký tự được dùng để điều khiển cuộc gọi. Nó có thể được dùng cùng với các điều kiện tín hiệu xác định ở các mạch xen kẽ khác. *Xem* call control signal.

call control procedure *thủ tục điều khiển cuộc gọi* Trong truyền thông dữ liệu, sự cài đặt một tập các giao thức cần thiết để thiết lập và cắt một cuộc gọi. *Xem* call.

call control signal *tín hiệu điều khiển gọi* Trong truyền thông dữ liệu, một trong một tập hợp các tín hiệu cần

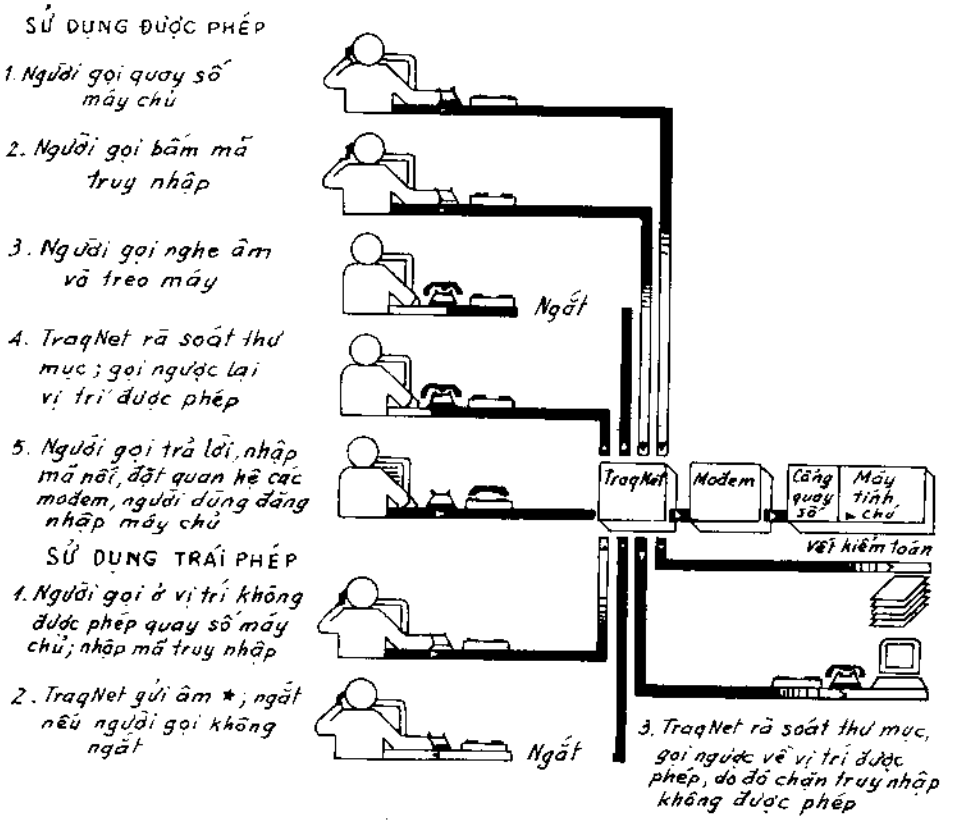
để thiết lập, duy trì và cắt một cuộc gọi. *Xem* call, call accepted signal, call not accepted signal, call progress signal, call request.

call not accepted signal ***tín hiệu không nhận cuộc gọi*** Trong truyền thông dữ liệu, tín hiệu điều khiển cuộc gọi được DTE được gọi gửi đi để báo rằng, cuộc gọi vừa tới không được chấp nhận. *So sánh với* call accepted signal. *Xem* call control signal, DTE.

call progress signal ***tín hiệu tiến hành cuộc gọi*** Trong truyền thông dữ liệu, tín hiệu điều khiển cuộc gọi truyền từ DCE tới DTE gọi để báo trạng thái của cuộc gọi đang được thiết lập, lý do tại sao không thể tiến hành nối, hoặc điều kiện bất kỳ nào khác của mạng. *Xem* call control signal, DCE, DTE.

call redirection ***tái định hướng cuộc gọi*** Trong truyền thông dữ liệu, phương tiện cho phép tự động chuyển các cuộc gọi tới một địa chỉ đã định danh khi đầu cuối người sử dụng bên nhận không hoạt động. *Xem* call.

call request ***yêu cầu gọi*** Trong truyền thông dữ liệu, tín hiệu điều khiển cuộc gọi do DTE gửi tới DCE



call back: *gọi ngược*. Hệ TraqNet 2000 từ LeeMah tạo ra kiểm soát truy nhập cho các mạng quay số.

(hoặc mạng) cho biết rằng, nó muốn thiết lập cuộc gọi. *Xem* call control signal, DCE, DTE.

Cambridge Ring ***Vòng Cambridge*** Trong truyền thông dữ liệu, một chuẩn mạng cục bộ (LAN) sử dụng cấu hình vòng cáp đồng trục hoặc cặp dây xoắn và tốc độ truyền 1 megabit mỗi giây. Nó sử dụng giao thức khe thông báo. *So sánh với* Ethernet. *Xem* bit, coaxial cable, local area network, message slot, ring, twisted pair.

CAN *Xem* cancel character.

cancel call ***hủy cuộc gọi*** Trong an toàn vật lý, một phương tiện ở một số bộ quay số điện thoại cho phép bỏ qua thủ công cuộc gọi được khởi phát bằng một tín hiệu báo động. *Xem* telephone dialer.

cancel character ***ký tự hủy*** Trong mã hóa, ký tự điều khiển chính xác dùng để báo rằng, dữ liệu đi kèm theo nó bị lỗi và phải được bỏ qua.

cancellation ***(sự) hủy bỏ*** Trong tin học, sự nhận dạng các tài liệu chuyển tác để ngăn ngừa sử dụng tiếp hoặc sử dụng lặp lại chúng sau khi chúng đã thực hiện xong chức năng của mình.

Cancer ***virut Cancer*** Trong an toàn máy tính, virut lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

candidate key ***khóa dự phòng, khóa thứ cấp*** Trong các cơ sở dữ liệu, khóa trong một cơ sở dữ liệu quan hệ có các tính chất của một khóa chính. Nó là tổ hợp các thuộc tính trong một quan hệ nhằm phân biệt một cách đơn nhất bộ thuộc tính với bộ thuộc tính khác bất kỳ trong quan hệ. Nếu một thuộc tính bất kỳ biến khỏi khóa dự phòng thì tính đơn nhất bị mất đi. Ví dụ, một cơ sở dữ liệu nhân sự có thể chứa tên và ngày sinh của nhân viên như những trường bên trong một quan hệ; hai nhân viên có thể có cùng tên và hai nhân viên khác có thể có cùng ngày sinh nhưng tổ hợp tên và ngày sinh có thể là đơn nhất và do đó là khóa có thể chấp nhận được. *Xem* attribute, key, primary key, relational database, tuple.

candidate TCB subset ***tập con TCB dự phòng*** Trong an toàn máy tính, sự nhận dạng phần cứng, phần sụn và phần mềm tạo thành tập con TCB đã đề xuất, cùng với thủ tục nhận dạng các chủ thể và đối tượng của nó; một trong những điều kiện đánh giá từng phần. *Xem* Blue Book, object, subset, TCB subset.

capability ***khả năng, năng lực*** (1) Trong kiểm soát truy nhập, dấu hiệu được dùng như một dấu định danh đối với một tài nguyên sao cho việc có dấu hiệu sẽ gán quyền truy nhập cho tài nguyên. (2) Trong an toàn máy tính, thẻ không làm giả được được hệ thống chấp nhận như bằng chứng không thể chối cãi rằng, người trình thẻ đó có truy nhập được phép vào đối tượng có tên trên thẻ. Nó thường được hệ điều hành và phần cứng hiểu như một địa chỉ đối với đối tượng. Mỗi năng lực còn chứa thông tin cấp quyền nhận dạng bản chất của chế độ truy nhập (ví dụ như chế độ đọc, chế độ ghi). *Xem* object.

C

capability list ***danh mục năng lực*** Trong kiểm soát truy nhập, danh sách các đối tượng mà một chủ thể nào đó có thể truy nhập được. *So sánh với* access control list. *Xem* access matrix model, capability.

capacitance sensor ***bộ cảm biến điện dung*** Trong an toàn vật lý, bộ cảm biến với hoạt động dựa trên sự phát hiện những thay đổi điện dung của một vật kim loại mang điện và đất.

capacitively coded card ***thẻ mã hóa bằng điện dung*** Trong an toàn vật lý, thẻ với thông tin được mã hóa dưới dạng các cung điện dung dùng trong kiểm soát truy nhập. *Xem* card reader.

capture ***phá bẫy*** Trong an toàn vật lý, sự khắc phục được bộ cảm biến bằng cách đi vòng.

card acceptor ***bên nhận thẻ*** Trong hoạt động ngân hàng, bên nhận thẻ tín dụng và trình dữ liệu giao dịch cho một cơ sở nhận. *So sánh với* card holder, card issuer. *Xem* acquirer.

card based mode ***chế độ dùng thẻ*** Trong hoạt động ngân hàng, chế độ trong đó các giao dịch được khởi động bằng việc sử dụng dữ liệu độc lập của khách hàng được ghi trên sọc từ ở thẻ chất dẻo.

card encoder ***bộ mã hóa thẻ*** Trong an toàn vật lý, thiết bị đặt mã duy nhất lên thẻ kiểm soát truy nhập. *Xem* card reader.

card holder ***người giữ thẻ*** (1) Trong hoạt động ngân hàng, người trình thẻ chất dẻo khi trả tiền hàng hóa hoặc dịch vụ. *So sánh với* card acceptor, card issuer. (2) Trong hoạt động ngân hàng, khách hàng gắn liền với số tài khoản chính yêu cầu giao dịch từ nơi nhận thẻ. *Xem* card acceptor, primary account number.

card identification code ***mã nhận dạng thẻ*** Trong an toàn vật lý, dãy số hoặc chữ - số được mã hóa trên thẻ truy nhập để kiểm tra thẻ và bảo vệ bản ghi. *Xem* card reader. *Đồng nghĩa với* system code.

card issuer ***cơ sở phát hành thẻ*** Trong hoạt động ngân hàng, tổ chức (hoặc đại lý của nó) cung cấp thẻ tín dụng cho người giữ thẻ để dùng trong giao dịch thường xuyên. Tổ chức cũng chịu trách nhiệm trả tiền cho nơi nhận thẻ đối với hàng hóa và dịch vụ nhân danh người giữ thẻ. *So sánh với* card acceptor, card holder. *Xem* acquirer.

card key ***khóa thẻ*** (1) Trong hoạt động ngân hàng, khóa cấu thành từ các dữ liệu ghi trên sọc từ của thẻ chất dẻo. Lý tưởng mà nói thì một số trong những dữ liệu đó phải là ngẫu nhiên. Tuy nhiên, điều đó không bắt buộc. *Xem* key management. (2) Trong an toàn vật lý, thẻ chất dẻo chứa thông tin đã mã hóa được dùng để mở một cửa bị khóa. *Xem* card reader. *Đồng nghĩa với* access card.

card mastering ***tạo thẻ gốc, tạo thẻ chủ*** Trong an toàn vật lý, chỉ việc mã hóa các thẻ kiểm soát truy nhập, cho phép chúng được truy nhập phổ biến vào một nhóm xác định các khóa. *Xem* card reader, master code card.

card reader ***máy đọc thẻ*** Trong an toàn vật lý, thiết bị đọc thông tin chứa

trên thẻ kiểm soát truy nhập. Thông tin có thể được mã hóa trong thẻ nhờ sọc từ tính, các chấm từ, các lỗ đục, dấu in nổi, các mạch tần số vô tuyến, các cung điện dung v.v.. Máy đọc có thể là loại máy đọc thông minh hoặc một thiết bị trực tuyến. Bản thân thẻ có thể chỉ chứa thông tin đã mã hóa hoặc có thể chứa một bộ vi xử lý và RAM. *Xem* capacitively coded card, intelligent token, off line card reader, on line card reader, magnetically encoded card, proximity card reader, RAM, single voiding card reader, smart card, system card reader, wipe through card reader.

card verification value ***giá trị xác minh thẻ*** Trong hoạt động ngân hàng, giá trị kiểm tra, thường gồm ba chữ số thập phân, nhận được, theo phương thức mật mã từ dữ liệu nhận dạng ghi trên sọc từ của thẻ ngân hàng hay tín dụng. Giá trị xác minh thẻ được tính toán tương tự như cách tính giá trị xác minh PIN. Sự có mặt giá trị xác minh thẻ trên một thẻ có thể được dùng để bảo vệ chống lại việc mã hóa gian lận dữ liệu mới lên thẻ bị mất hoặc bị ăn cắp. Nếu thẻ như vậy có dữ liệu mới ghi trên sọc từ, thì có thể trong lần giao dịch sau đó nhà buôn phải truyền dữ liệu sọc từ đi để tiến hành các kiểm tra về quyền được phép nhưng ghi giao dịch dựa vào dữ liệu tài khoản dập trên thẻ. Thủ tục này có thể cho phép sử dụng một cách có hiệu quả một thẻ sau khi nó bị báo mất.

Với một giá trị xác minh thẻ, quá trình cấp quyền sẽ tính toán giá trị kiểm tra từ bản kê nhận dạng dữ liệu, sử dụng các khóa mật và so sánh kết quả với giá trị xác minh thẻ lưu trên sọc từ. Giá trị xác minh thẻ cho phép kiểm tra dựa vào phép mã các dữ liệu tài khoản mới tùy ý vì kẻ tấn công không biết gì về các khóa mật mã cần thiết để tính toán giá trị xác minh thẻ. Tuy nhiên, nó không chống lại được việc sao dữ liệu từ một thẻ khác chứa giá trị xác minh thẻ đúng. *So sánh với* PIN verification value. *Xem* credit card, cryptographic key, magnetic stripe card.

Carioca ***virut Carioca*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

carrier ***sóng mang*** Trong truyền thông, điện áp hoặc sóng điện từ tần số liên tục có khả năng được điều biến bởi một tín hiệu thứ hai chứa thông tin cần truyền đi. *Xem* modulation.

carrier detect ***tín hiệu dò sóng mang*** *Đồng nghĩa với* received line signal detector.

carrier sense multiple access - collision detection ***đa truy nhập cảm biến sóng mang có dò xung đột*** Trong truyền thông dữ liệu, giao thức trong đó một nút có dữ liệu cần truyền sẽ nghe ngóng mạng cho tới khi mạng trở nên yên tĩnh. Quá trình nghe mạng vẫn tiếp tục khi truyền dữ liệu, nếu nó nghe thấy gì đó đã được truyền thì nó biết rằng cuộc truyền là thành công. Nếu không rõ ràng là hai hoặc nhiều nút đã truyền đồng thời và xung đột xảy ra làm dữ liệu bị sai lạc. Sau đó, các nút chờ một khoảng thời gian ngẫu nhiên trước khi định truyền lại. *Xem*

C

Aloha, carrier sense protocol. *So sánh với* control token, message slot. *Xem* local area network.

carrier sense protocol ***giao thức cảm biến sóng mang*** Trong truyền thông dữ liệu, giao thức dùng trong các hệ phát rộng trong đó, mỗi trạm giám sát đường truyền để kiểm tra xem có xung đột làm sai lạc dữ liệu của chúng và sau đó truyền lại dữ liệu. *Xem* Aloha, broadcast, carrier sense multiple access - collision detection.

carrier system ***hệ sóng mang*** Trong truyền thông, phương pháp sử dụng một đường duy nhất để thu được một số kênh. Các tín hiệu được điều biến bằng một tần số sóng mang khác nhau đối với mỗi kênh, và các tín hiệu thu được được giải điều chế ở đầu thu. *Xem* carrier, frequency division multiplexing.

Cascade ***virut Cascade*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy và làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

cash dispenser ***máy rút tiền mặt*** Trong hoạt động ngân hàng, máy cho phép khách hàng rút tiền mặt với điều kiện khách hàng phải có thẻ rút tiền mặt. *Xem* ATM.

cash highway ***đường truyền tiền mặt*** Trong hoạt động ngân hàng, tuyến giữa máy rút tiền mặt và nơi cất giữ. Thủ quỹ ngân hàng có thể vận hành máy rút tiền ở một vùng không an toàn với tiền được chuyển bằng xe ray có động cơ tốc độ cao từ nơi cất giữ an toàn ở ngân hàng.

CashWire ***dịch vụ CashWire*** Trong hoạt động ngân hàng, dịch vụ trả tiền thanh toán thực của BankWire của Hoa Kỳ. *Xem* banking networks, BankWire.

Casino ***virut Casino*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM. Ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và liên kết tệp. *Xem* virus names.

Casper ***virut Casper*** Trong an toàn máy tính, virut tự mã hóa, lây nhiễm các tệp COMMAND.COM và COM, làm sai lạc các tệp chương trình, OVL, dữ liệu và liên kết tệp, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

category ***loại hình, loại, hạng*** (1) Trong an toàn dữ liệu, nhóm các đối tượng được gắn một nhãn hạn chế không phân cấp (ví dụ như thông tin khoanh vùng, sở hữu). Các chủ thể phải có đặc quyền để truy nhập vào một loại hình. *Xem* compartment. (2) Trong an toàn dữ liệu, nhãn hạn chế được áp dụng cho dữ liệu đã phân loại hoặc chưa phân loại như một phương tiện tăng cường bảo vệ và hạn chế truy nhập hơn nữa đối với dữ liệu. Các ví dụ bao gồm thông tin khoanh vùng nhạy cảm (SCI), thông tin có sở hữu (PROPIN) và NATO. Các cá nhân chỉ có thể được truy nhập vào thông tin đó khi họ được cấp quyền truy nhập chính thức. *Xem* PROPIN, SCI. (3) Trong an toàn dữ liệu, một nhóm thông tin đã phân loại hoặc chưa phân loại nhưng nhạy cảm được gắn một nhãn hạn chế phụ để biểu thị rằng, cá nhân chỉ được

quyền truy nhập thông tin khi họ được ủy quyền thích hợp.

caution statement ***câu lệnh khuyến cáo*** Trong an toàn dữ liệu, một câu lệnh gán vào các đầu ra của máy tính có cấp phân loại cao nhất. Nó được xử lý trong thời gian sản phẩm được tạo ra và một yêu cầu rằng, mọi dữ liệu không được yêu cầu phải được kiểm soát ở mức đó và gửi trở lại ngay lập tức cho trung tâm máy tính gốc. *Xem* safeguarding statement.

CB *Xem* Certification Body.

CBC *Xem* cipher block chaining.

CBMS *Xem* computer based message system.

CBX *Xem* computerized branch exchange.

CCA *Xem* common cryptographic architecture.

CCEP *Xem* Commercial COMSEC Endorsement Program.

CCETT ***trung tâm CCETT*** Viết tắt của Centre Commune d'Etudes de Télévision et de Télécommunications (Trung tâm tổng hợp các nghiên cứu về truyền hình và viễn thông).

CCIR ***ủy ban CCIR*** Viết tắt của Comité Consultatif International Radio (Ủy ban tư vấn quốc tế về vô tuyến).

CCITT *Xem* Comité Consultatif International de Télégraphie et Téléphonie (Ủy ban tư vấn quốc tế về điện báo và điện thoại).

CCR *Xem* container clearance required.

CCTA ***tổ chức CCTA*** Viết tắt của U.K. Central Computer and Telecommunications Agency Cục máy tính và viễn thông trung ương Anh).

CCTV *Xem* closed circuit television.

CCU *Xem* communications control unit.

CDI *Xem* constrained data item.

cell restriction ***hạn chế ô*** Trong an toàn cơ sở dữ liệu, một dạng kiểm soát không nhớ trong đó quyết định hủy bỏ một thống kê phụ thuộc vào tập câu hỏi khi so sánh với bảng chứa các thống kê. *So sánh với* table restriction. *Xem* inference control, lattice model, memoryless control.

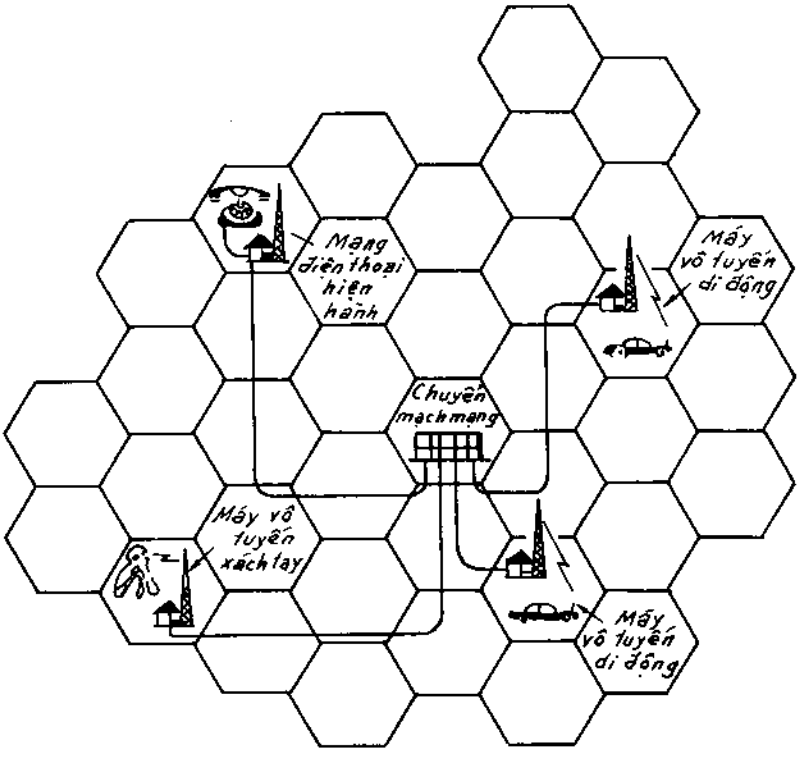
cell suppression ***triệt ô, giấu ô*** Trong an toàn cơ sở dữ liệu, một dạng hạn chế ô sử dụng kiểm soát trước, thường được các cơ quan tổng điều tra dân số sử dụng để bảo vệ dữ liệu được công bố dưới dạng bảng. Các ô chứa dữ liệu từ một vài bản ghi bị bị giấu cùng với những ô có liên quan mà có thể bị dùng để suy ra dữ liệu nằm ở những ô đã bị giấu. *So sánh với* audit expert, grouping, implied queries control, overlap control, query set size control. *Xem* a priori control, cell restriction.

cellular radio ***hệ điện thoại vô tuyến, điện thoại di động*** Trong truyền thông, phương pháp tạo ra dịch vụ điện thoại vô tuyến di động công cộng (ví dụ cho điện thoại ở ô tô). Tổng diện tích dịch vụ bao quát được chia thành những nhóm ô (vùng) thông thường người ta dùng 7, 12, 21 và 24 ô mỗi nhóm. Các ô trong một nhóm dùng chung tổng số kênh vô tuyến dành cho dịch vụ; các máy phát công suất nhỏ được dùng để các ô tương ứng ở những nhóm lân cận dùng cùng tần số

vô tuyến không bị nhiễu lẫn nhau. Bán kính ô có thể cao tới 32 km ở vùng nông thôn ít dân và thấp tới 1,1 km ở những vùng thành phố đông dân. Để giảm tới tối thiểu nhiễu chung kênh với các bán kính ô nhỏ có thể sử dụng anten vô tuyến phân quạt có góc bao quát 120^0.

Kỹ thuật chia ô cho phép những cuộc nói chuyện khác nhau sử dụng cùng các tần số trong các vùng cách nhau chỉ vài dặm. Khi người sử dụng điện thoại di động di chuyển từ ô này sang ô khác, cuộc gọi được chuyển (tức là trung tâm chuyển mạch so sánh cường độ tín hiệu khi nhận được ở các ô gần nhau). Nó rà soát tập hợp tần số đối với một kênh mở của ô nhận tín hiệu mạnh nhất và ra lệnh cho thiết bị di động điều hưởng về tần số đó. Hệ thống bây giờ có thể chấp nhận cuộc gọi khác xuất phát ở ô đầu tiên trên kênh đã bị chiếm trước đó. Để đảm bảo rằng chỉ có một số tối thiểu các cuộc gọi bị bỏ rơi, các ô thường phủ nhau.

Khi một cuộc gọi đang tiến hành di chuyển sang một ô bận, nơi không còn các kênh mở, nó có thể duy trì ở ô ban



cellular radio: *điện thoại vô tuyến.* Cấu trúc của mạng điện thoại vô tuyến.

đầu cho tới khi một kênh mở, hoặc người sử dụng di chuyển gần hơn tới ô thứ ba có kênh mở.

Các hệ vô tuyến tạo điều kiện gọi từ một điện thoại bình thường tới điện thoại di động ngay cả khi không biết vị trí của thuê bao được gọi và thiết bị của người đó không được sử dụng. Đài gốc trong mỗi ô sẽ truyền các tín hiệu nhận dạng đều đặn vốn được kiểm tra thường xuyên bởi mọi điện thoại di động trong vùng. Nếu máy di động phát hiện ra sự thay đổi tín hiệu cho biết nó chuyển từ ô này sang ô khác thì máy tự động truyền mã hiệu ngắn tới đài gốc mới để thông báo cho hệ thống rằng, nó đã, đi chuyển và thông báo vị trí mới nhất của nó.

cellular telephone ***điện thoại chia ô, điện thoại di động*** Trong truyền thông, điện thoại xách tay trong hệ thống điện thoại vô tuyến. *Xem* cellular radio.

central computer facility ***phương tiện máy tính trung tâm*** Trong tin học, một hoặc nhiều máy tính với các thiết bị ngoại vi, các thiết bị nhớ, các bộ xử lý trung tâm và thiết bị truyền thông trong một vùng được kiểm soát đơn lẻ. Phương tiện này không bao gồm các phương tiện máy tính từ xa, các thiết bị ngoại vi hoặc các thiết bị đầu cuối mà nằm bên ngoài vùng được kiểm soát đơn lẻ, ngay cả khi chúng được nối với phương tiện máy tính trung tâm nhờ các liên kết truyền thông đã được chấp thuận.

centralized adaptive routing ***định tuyến thích ứng tập trung*** Trong truyền thông dữ liệu, phương pháp định tuyến trong đó, trung tâm định tuyến mạng kiểm soát sự định tuyến dựa trên dữ liệu do mỗi nút cung cấp cho nó. *So sánh với* delta routing, directory routing, fixed routing, hot potato routing. *Xem* adaptive routing, node, routing.

centralized computer network ***mạng máy tính tập trung*** Trong truyền thông dữ liệu, cấu hình mạng máy tính trong đó, nút trung tâm cung cấp một năng lực tính toán, sự điều khiển hoặc những dịch vụ khác. *Xem* computer network, node.

central processing unit ***bộ xử lý trung tâm*** Trong tin học, thiết bị chứa các mạch điều khiển và thực hiện các lệnh.

central station ***trạm trung tâm*** Trong an toàn vật lý, doanh nghiệp hoặc tổ chức cung cấp một địa điểm trung tâm cho giám sát các hệ báo động của thuê bao. Tất cả các tín hiệu báo động thu được đều được ghi lại, khảo sát và báo cáo cho cảnh sát, các dịch vụ an ninh và cứu hỏa. Các liên kết truyền thông có thể là điện thoại, vô tuyến hoặc hữu tuyến. Dịch vụ có thể được cung cấp trên cơ sở vùng hoặc quốc gia có sử dụng các tuyến dịch vụ điện thoại vùng rộng. *So sánh với* monitoring station. *Xem* Grade AA central station, Grade A central station, Grade B central station, police connect. (2) Trong an toàn vật lý, điểm trung tâm đối với một hệ thống báo động do một ban an ninh giám sát.

Central Station Electrical Protection Association ***Hiệp hội bảo vệ điện trạm trung tâm*** Một tổ chức của Hoa Kỳ nhằm khuyến khích các tiêu chuẩn

công nghiệp đối với các trạm trung tâm. *Xem* central station.

CEPT ***hội nghị CEPT*** Viết tắt của Conference of European PTTs (hội nghị các Cty bưu chính viễn thông Châu Âu). *Xem* PTT.

CERT *Xem* Computer Emergency Response Team.

certificate ***thông báo chứng nhận, mã chứng nhận, chứng chỉ*** (1) Trong mật mã học, thông báo đảm bảo tính xác thực của dữ liệu chứa trong đó. Trong mật mã khóa công khai, điều quan trọng là người sử dụng khóa công khai có sự đảm bảo về tính xác thực của khóa ấy. Sự đảm bảo như vậy có thể cung cấp nhờ một chứng chỉ, do một cơ sở cấp chứng chỉ mà người sử dụng tin cậy phát hành. Nội dung của chứng chỉ có thể bao gồm danh tính người sở hữu khóa công khai, bản thân khóa công khai và thời hạn có hiệu lực của khóa này. Dữ liệu được ký (đánh dấu) bằng khóa mật của cơ sở cấp chứng chỉ.

Người sử dụng sẽ cung cấp chứng chỉ, còn nơi nhận sẽ giải mã chứng chỉ bằng khóa công khai của cơ sở cấp chứng chỉ. Khi đó nơi nhận có được đảm bảo rằng, danh tính của người dùng và khóa công khai tương ứng đã được ký bởi cơ sở tin cậy. *So sánh với* certification. *Xem* certificate revocation list, certification authority, digital signature, public key, public key cryptography, secret key. (2) Trong mật mã học, khóa công khai của một người sử dụng cùng với một thông tin khác nào đó được làm cho không thể giả mạo được nhờ chữ ký bằng khóa mật của cơ sở cấp chứng nhận phát ra nó. *Xem* certification authority, public key, secret key.

certificate identifier ***ký hiệu nhận dạng chứng nhận*** Trong mật mã học, là số nhị phân không lặp lại trong thời hạn an toàn của một cặp khóa công khai/khóa riêng dùng để tính toán chứng chỉ, hoặc nó sẽ là một tem thời gian duy nhất. *Xem* certificate, public key cryptography, security life.

certificate revocation list ***danh sách hủy bỏ chứng chỉ, danh sách thu hồi chứng chỉ*** Trong mật mã học, danh sách các chứng nhận bị hủy bỏ do cơ sở cấp chứng nhận truyền đi. Danh sách thông báo cho người sử dụng rằng, một chứng nhận không còn giá trị nữa, ví dụ do sự thất thoát một khóa mật gắn liền với khóa công khai được ký bởi chứng chỉ đang xét. *Xem* certificate, certification authority, public key, secret key.

certification ***(sự) chứng nhận*** (1) Trong mật mã học, phương pháp thử một hệ thống mật mã đã đề xuất bằng cách đặt nó dưới những tấn công được xem như thuận lợi nhất cho nhà mã thám. *Xem* cryptanalysis, worst case condition. (2) Trong an toàn máy tính, sự đánh giá về mặt kỹ thuật được tiến hành như một phần và hỗ trợ cho quá trình công nhận. Quá trình này thiết lập mức độ mà một ban thiết kế và thực hiện hệ máy tính riêng hoặc mạng riêng đáp ứng các yêu cầu an toàn đã định trước. *So sánh với* certificate. *Xem* accreditation. (3) Trong an toàn máy tính, tuyên bố xác định mức độ mà các

công nghiệp đối với các trạm trung tâm. *Xem* central station.

CEPT ***hội nghị CEPT*** Viết tắt của Conference of European PTTs (hội nghị các Cty bưu chính viễn thông Châu Âu). *Xem* PTT.

CERT *Xem* Computer Emergency Response Team.

certificate ***thông báo chứng nhận, mã chứng nhận, chứng chỉ*** (1) Trong mật mã học, thông báo đảm bảo tính xác thực của dữ liệu chứa trong đó. Trong mật mã khóa công khai, điều quan trọng là người sử dụng khóa công khai có sự đảm bảo về tính xác thực của khóa ấy. Sự đảm bảo như vậy có thể cung cấp nhờ một chứng chỉ, do một cơ sở cấp chứng chỉ mà người sử dụng tin cậy phát hành. Nội dung của chứng chỉ có thể bao gồm danh tính người sở hữu khóa công khai, bản thân khóa công khai và thời hạn có hiệu lực của khóa này. Dữ liệu được ký (đánh dấu) bằng khóa mật của cơ sở cấp chứng chỉ.

Người sử dụng sẽ cung cấp chứng chỉ, còn nơi nhận sẽ giải mã chứng chỉ bằng khóa công khai của cơ sở cấp chứng chỉ. Khi đó nơi nhận có được đảm bảo rằng, danh tính của người dùng và khóa công khai tương ứng đã được ký bởi cơ sở tin cậy. *So sánh với* certification. *Xem* certificate revocation list, certification authority, digital signature, public key, public key cryptography, secret key. (2) Trong mật mã học, khóa công khai của một người sử dụng cùng với một thông tin khác nào đó được làm cho không thể giả mạo được nhờ chữ ký bằng khóa mật của cơ sở cấp chứng nhận phát ra nó. *Xem* certification authority, public key, secret key.

certificate identifier ***ký hiệu nhận dạng chứng nhận*** Trong mật mã học, là số nhị phân không lặp lại trong thời hạn an toàn của một cặp khóa công khai/khóa riêng dùng để tính toán chứng chỉ, hoặc nó sẽ là một tem thời gian duy nhất. *Xem* certificate, public key cryptography, security life.

certificate revocation list ***danh sách hủy bỏ chứng chỉ, danh sách thu hồi chứng chỉ*** Trong mật mã học, danh sách các chứng nhận bị hủy bỏ do cơ sở cấp chứng nhận truyền đi. Danh sách thông báo cho người sử dụng rằng, một chứng nhận không còn giá trị nữa, ví dụ do sự thất thoát một khóa mật gắn liền với khóa công khai được ký bởi chứng chỉ đang xét. *Xem* certificate, certification authority, public key, secret key.

certification ***(sự) chứng nhận*** (1) Trong mật mã học, phương pháp thử một hệ thống mật mã đã đề xuất bằng cách đặt nó dưới những tấn công được xem như thuận lợi nhất cho nhà mã thám. *Xem* cryptanalysis, worst case condition. (2) Trong an toàn máy tính, sự đánh giá về mặt kỹ thuật được tiến hành như một phần và hỗ trợ cho quá trình công nhận. Quá trình này thiết lập mức độ mà một ban thiết kế và thực hiện hệ máy tính riêng hoặc mạng riêng đáp ứng các yêu cầu an toàn đã định trước. *So sánh với* certificate. *Xem* accreditation. (3) Trong an toàn máy tính, tuyên bố xác định mức độ mà các

biện pháp an toàn đáp ứng các chỉ tiêu kỹ thuật. Việc chứng nhận dựa trên các kết quả của phân tích rủi ro đã thực hiện. Nó không nhất thiết ngụ ý sự đảm bảo rằng, hệ đã mô tả không thể xâm nhập được. Nó là một đầu vào của quá trình phê chuẩn an toàn. *Xem* risk analysis. (4) Trong an toàn máy tính, đánh giá kỹ thuật về các đặc điểm an toàn và những biện pháp an toàn khác của một AIS được tiến hành như một phần và hỗ trợ cho quá trình công nhận. Nó thiết lập mức độ đáp ứng một tập hợp các yêu cầu an toàn đã xác định của việc thiết kế và thực hiện AIS riêng. *Xem* accreditation. (5) Trong an toàn máy tính, sự đảm bảo ghi chính thức của một cá nhân rằng, dựa trên sự đánh giá của các lần thử an toàn, hệ ADP đã phân loại và môi trường của nó đáp ứng được những đặc tả an toàn đã phê chuẩn nêu trong bản kế hoạch an toàn ADP. *Xem* ADP security.

certification authority ***cơ sở chứng nhận, cơ quan cấp chứng chỉ*** Trong mật mã học, một cơ sở được mọi người sử dụng tin cậy có quyền đưa ra và gán các chứng nhận. *Xem* certificate, certificate revocation list, certification path.

certification body ***cơ quan chứng nhận*** Trong an toàn thông tin, một tổ chức của nhà nước chịu trách nhiệm quản lý các đánh giá ITSEC trong nước đó. *So sánh với* information technology security evaluation facility. *Xem* information technology security evaluation criteria.

certification path ***tiến trình thực hiện chứng nhận*** Trong mật mã học, một dãy có thứ tự các chứng nhận về các đối tượng mà cùng với khóa công khai của đối tượng ban đầu trong quá trình, có thể được xử lý để thu được chứng chỉ của đối tượng cuối cùng trên đường dẫn. *Xem* certificate, certification authority.

Certified Protection Professional ***chuyên gia bảo vệ có chứng chỉ*** Quyết định của Hội an toàn công nghiệp Hoa Kỳ. *Xem* ASIS.

CESG ***nhóm CESG*** Viết tắt của U.K. Communications Electronics Security Group (nhóm an toàn điện tử truyền thông của Anh).

CFB *Xem* cipher feedback.

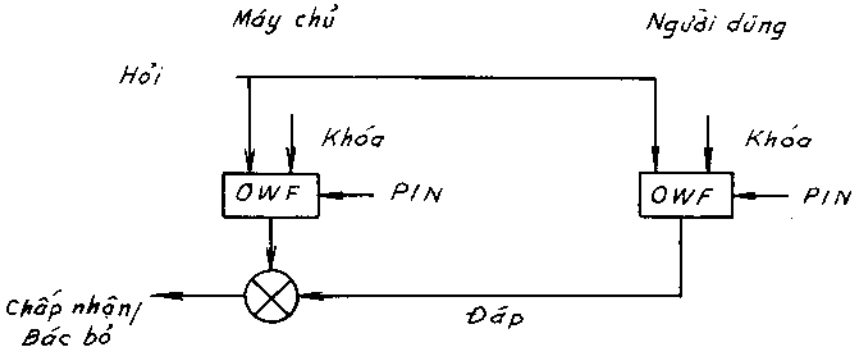
chaining ***liên kết, móc xích*** *Xem* block cipher chaining, stream cipher chaining.

challenge and reply authentication ***xác thực hỏi và đáp*** *Đồng nghĩa với* challenge/response.

challenge/response ***đòi hỏi/đáp ứng, hỏi/đáp*** Trong kiểm soát truy nhập, kỹ thuật trong đó máy chủ đáp ứng một yêu cầu nhập mạng bằng một câu hỏi (thách đố) đối với người sử dụng. Người sử dụng hợp pháp đáp lại câu hỏi đó bằng cách thực hiện một nhiệm vụ mà cần có sự hiểu biết, hoặc sự truy nhập tới thông tin mật mà chỉ người dùng (và có thể cả máy chủ) có khả năng sử dụng sau đó, người sử dụng gửi tiếp câu trả lời về máy chủ để kiểm tra. Vì câu hỏi khác nhau đối với mỗi đối thoại hỏi - đáp nên một kẻ nghe lén sau đó không thể giả mạo người sử dụng hợp pháp.

Các kỹ thuật đáp ứng đòi hỏi (hỏi/đáp)

có thể sử dụng mật mã đối xứng hoặc mật mã không đối xứng. Thông thường với mật mã đối xứng, câu hỏi của máy chủ có dạng một số ngẫu nhiên. Người sử dụng mã hóa số đó bằng khóa mật và trả lại bản mã như lời đáp. Máy chủ tìm khóa mật đã lưu ứng với mã định danh mà người dùng đã khai báo và giải mã lời đáp. Nếu kết quả giống với câu hỏi ban đầu thì máy chủ cho quyền truy nhập.



challenge/response: *đòi hỏi/đáp ứng.* Hoạt động của hệ đòi hỏi/đáp ứng. Với các mật mã không đối xứng thủ tục là tương tự trừ một điều là người sử dụng mã hóa câu hỏi bằng khóa mật còn máy chủ giải mã nó bằng khóa công khai của người sử dụng. Trong trường hợp này máy chủ không có khả năng giả dạng như người sử dụng. *Xem* asymmetric cipher, dynamic password, Fiat Shamir algorithm, public key, secret key, user id. *Đồng nghĩa với* challenge and replay authentication.

channel ***kênh, đường chuyển tin*** (1) Đường chuyền thông tin trong một hệ thống. Cũng có thể chỉ một cơ chế nhờ đó thực hiện đường chuyền tin. (2) Trong truyền thông dữ liệu, đường theo đó các tín hiệu có thể được gửi đi, ví dụ như kênh dữ liệu, kênh đầu ra mà có thể an toàn hoặc không an toàn trước một kẻ nghe lén. *So sánh với* convert channel. *Xem* eavesdropping. (3) Trong tin học, bộ xử lý chuyên dụng và hệ mạch hỗ trợ có chức năng kiểm soát các thao tác nhập/xuất. *Xem* input/output device.

channel bank ***khối dồn kênh*** Trong truyền thông, thiết bị thực hiện thao tác dồn kênh. Thường được dùng để dồn các kênh thoại. *Xem* multiplexer.

channel capacity ***dung lượng kênh*** Trong truyền thông dữ liệu, tốc độ cực đại mà thông tin có thể được truyền qua một kênh nào đó. Dung lượng kênh thường được đo theo baud, nhưng có thể được biểu thị theo bit trên giây khi nói tới thiết bị đầu cuối xác định. *Xem* baud, channel.

channel isolation *độ cách ly kênh* Trong truyền thông, số đo độ xuyên âm giữa hai kênh, được tính theo đexiben. *Xem* cross-talk, decibel.

channel overload *quá tải kênh* Trong truyền thông dữ liệu, điều kiện trong đó sự chuyển dữ liệu vào hoặc ra khỏi một bộ xử lý và các thiết bị I/O đạt tới một tốc độ tiến đến dung lượng của một kênh dữ liệu. *Xem* I/O.

Chaos *virut Chaos* Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động của đĩa mềm và đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp dữ liệu, tạo khuôn hoặc ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

Chaos Club *câu lạc bộ Chaos* Trong an toàn máy tính, câu lạc bộ các hackơ của Đức đã xâm nhập vào các hệ máy tính của Châu Âu và Hoa Kỳ. *Xem* Hanover Hacker.

CHAPS *hệ CHAPS* Trong hoạt động ngân hàng, viết tắt của Clearing House Automated Payment System (hệ chi trả tự động hóa ở phòng thanh toán bù trừ), một hệ điện tử liên ngân hàng để gửi các khoản chi trả đảm bảo, không điều kiện bằng đồng bảng Anh cho thanh toán cùng ngày từ một ngân hàng thanh toán nhân danh bản thân nó, hoặc từ các khách hàng của nó tới một ngân hàng thanh toán khác. *So sánh với* CHIPS. *Xem* banking networks, SWIFT.

character *ký tự* Trong các cấu trúc dữ liệu, biểu diễn của các chữ cái của bảng chữ cái (cả hoa lẫn thường), các chữ số 0-9 và các dấu câu. Biểu diễn thông thường nhất của các ký tự trong kỷ pháp nhị phân là mã ASCII, nhưng mã EBCDIC cũng được sử dụng. *Xem* ASCII, EBCDIC code.

character assembly *tạo mẫu ký tự, ráp ký tự* Trong truyền thông dữ liệu, quá trình nhờ đó các bit được xếp với nhau để tạo thành các ký tự khi các bit tới trên một liên kết dữ liệu. *So sánh với* character disassembly.

character code *mã ký tự* Trong mã hóa, phương pháp biểu diễn các ký tự nhờ một tập duy nhất các chữ số nhị phân. Hai bộ mã ký tự thông dụng nhất là ASCII và EBCDIC. *Xem* ASCII, EBCDIC code.

character disassembly *phân tích ký tự, tách ký tự* Trong truyền thông dữ liệu, quá trình nhờ đó các ký tự được phân tích thành các bit để truyền qua một đường liên kết dữ liệu. *So sánh với* character assembly. *Xem* bit.

character interleaving *đan xen ký tự* Trong truyền thông dữ liệu, phương pháp dồn kênh phân thời trong đó bộ dồn kênh lưu giữ ký tự đầy đủ trước khi truyền nó theo đường truyền. *So sánh với* bit interleaving. *Xem* time division multiplexing.

character mapping *ánh xạ ký tự* *Đồng nghĩa với* code conversion.

character oriented protocol *giao thức định hướng ký tự* Trong truyền thông dữ liệu, giao thức trong đó các tập bit đã truyền được nhận dạng như các ký tự riêng. *So sánh với* bit oriented protocol. *Xem* bit, character, protocol.

characterplexer ***bộ dồn ký tự*** Trong truyền thông dữ liệu, hệ trong đó dữ liệu từ kênh không đồng bộ tốc độ thấp được tổ chức trên cơ sở ký tự và mỗi ký tự đều được cho qua cửa vào đường trung chuyển tốc độ cao. *Xem* asynchronous transmission, synchronous transmission.

character set ***bộ ký tự*** (1) Trong mã hóa, tập hợp hữu hạn các ký tự khác nhau vốn được coi là đầy đủ đối với một áp dụng riêng. (2) Tập hợp các ký tự khả dụng ở một máy tính riêng. *Xem* character.

characters per second ***ký tự trên giây, cps, CHPS*** Trong truyền thông dữ liệu, số đo tốc độ truyền, thường là giữa thiết bị đầu cuối và máy tính. *So sánh với* baud.

character stuffing ***bổ sung ký tự*** Trong truyền thông dữ liệu, phương pháp chèn các ký tự điều khiển bổ sung vào một thông báo để thông báo không chứa một tập các ký tự tương ứng với việc định ranh giới các khung bằng một ký tự kết thúc khung đặc biệt. *So sánh với* bit stuffing.

character subset ***tập con ký tự*** Trong mã hóa, sự lựa chọn các ký tự từ bộ ký tự chứa tất cả các ký tự có một đặc điểm chung xác định. *Xem* character set.

character terminal ***đầu cuối ký tự, terminal ký tự*** Trong truyền thông dữ liệu, thiết bị đầu cuối không thể tạo ra các gói tin (bó tin) riêng của nó, nó được nối với một PAD (bộ ráp/dỡ gói tin) để nối với mạng chuyển mạch gói tin. *So sánh với* packet terminal. *Xem* packet switching, PAD.

charges ***(lệ) phí*** Trong hoạt động ngân hàng, lệ phí gắn liền với các dịch vụ tài chính.

check bit ***bit kiểm tra*** Trong mã hóa, chữ số nhị phân dùng trong quá trình xác định độ chính xác của dữ liệu đã xử lý hoặc đã truyền. *So sánh với* check digit, check key. *Xem* parity checking.

check digit ***chữ số kiểm tra*** Trong mã hóa, một hoặc nhiều chữ số dư thừa dùng để kiểm tra sự có mặt của các lỗi trong một tập kết hợp các chữ số. *So sánh với* check bit, check key. *Xem* checksum.

check key ***khóa kiểm tra*** Trong mã hóa, nhóm các ký tự lấy ra và gắn thêm vào một mục dữ liệu, mà có thể được dùng để phát hiện các lỗi trong mục dữ liệu trong quá trình xử lý. *So sánh với* check bit, check digit.

check kiting ***tạo séc khống*** Trong an toàn máy tính, một dạng con ngựa thành Tơroa có tác dụng bổ sung những khoản tiền nhỏ vào tài khoản của một kẻ gian lận trong một khoảng thời gian dài. Việc xử lý các séc của khách hàng bị trễ một cách cố ý và lợi nhuận kiếm được trong khoảng thời gian trì hoãn đó được ghi có vào cho tài khoản của kẻ gian lận. *So sánh với* salami technique. *Xem* malicious code.

checkpoint ***điểm kiểm tra*** Trong tin học, điểm điều khiển trong một chương trình hoặc tệp, được thiết lập cách quãng cho phép xử lý lại để tiếp tục lại được từ điểm đó, thay vì khởi động

chương trình hoặc tệp, nếu như xuất hiện một lỗi.

checkpoint restart ***khởi động lại ở điểm kiểm tra*** *Xem* checkpoint.

checksum ***tổng kiểm tra*** (1) Trong quá trình xác thực, một khối độ dài cố định được tạo ra như một hàm của mỗi bit trong thông báo. (2) Trong mã hóa, việc lấy tổng một tập hợp các mục dữ liệu nhằm các mục đích phát hiện lỗi. Các mục dữ liệu là các chữ số, các bit hoặc những xâu ký tự khác được xem như các chữ số nhằm mục đích tính toán. *Xem* error detection code, hash total.

chime ***tiếng chuông*** Trong an toàn vật lý, tín hiệu nghe dễ chịu dùng trong các hệ tiền báo hiệu để báo cho nhân sự được chọn về điều kiện hỏa hoạn trước khi phát ra báo động sơ tán. *Xem* presignal system.

Chinese Remainder Theorem ***định lý phần dư Trung Hoa*** Trong toán học, cho $m_1, m_2, \ldots m_k$, với k là số nguyên nguyên tố cùng nhau từ đôi một.

Giả sử

$M = m_1 . m_2 \ldots . m_k$

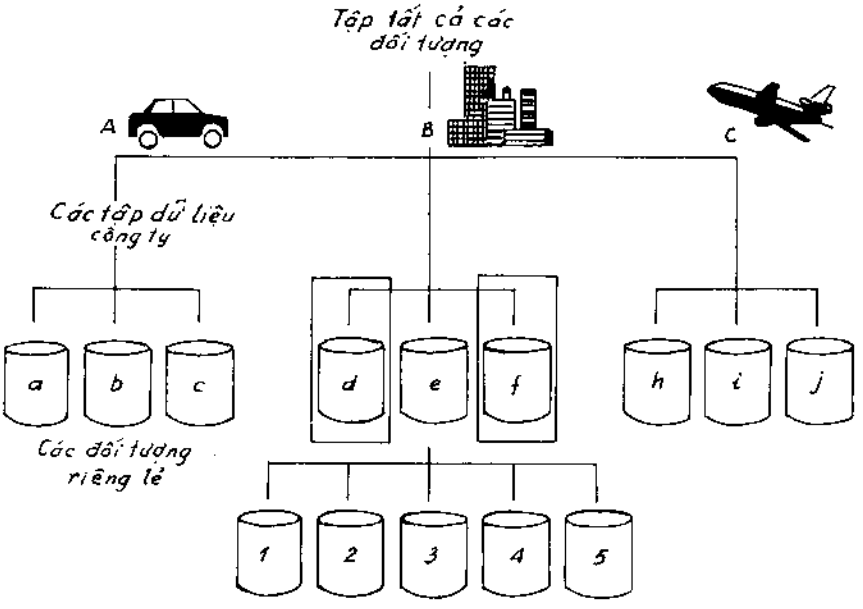
$x \equiv a_i \bmod m_i$, với $i = 1, 2, \ldots k$

$M_i = M/m_i$, với $i = 1, 2, \ldots k$

$M_i N_i \equiv 1 \bmod m_i$, với $i = 1, 2, \ldots k$

Thì

$x \equiv a_1 M_1 N_1 + a_2 M_2 N_2 \ldots + a_k m_k N_k \bmod M$



Chinese Wall model: *mô hình Vạn lý trường thành.* Sau khi truy nhập tệp 2, thì từ đó nhà phân tích tập dữ liệu c lớp xung đột B của công ty không thể truy nhập bất kỳ đối tượng nào trong các tập dữ liệu d hoặc f của công ty.

Xem modulo arithmetic, coprime.

Chinese Theorem ***định lý Trung Hoa*** Trong lý thuyết số, phép thử đối với các số nguyên tố, phát biểu rằng n là một số nguyên tố nếu nó chia hết cho $2^n - 2$.

Trong thực tế, phép thử không đúng với $n = 341$ vốn không phải là một số nguyên tố nhưng lại chia hết cho $2^{341} - 2$. *Xem* prime number.

Chinese Wall model ***mô hình Vạn lý trường thành*** Trong các mô hình hình thức, mô hình an toàn hình thức được xác định giống như mô hình bí mật cho thế giới thương mại.

Mô hình sử dụng các thuật ngữ chủ thể và đối tượng. Giống mô hình Bell-La Padula, nhưng nó có một khái niệm khác đáng kể về các luồng thông tin được phép. Khung cảnh của mô hình là khung cảnh của một tổ chức, ví dụ một tổ chức cung cấp các dịch vụ tư vấn, lưu trữ dữ liệu có liên quan tới một số công ty khách hàng. Chính sách an toàn của tổ chức là người sử dụng không thể truy nhập vào những gì liên quan tới một công ty nếu họ đã truy nhập dữ liệu từ một công ty thứ hai và truy nhập được đề nghị có thể xung đột về lợi ích.

Như vậy, một nhà phân tích thị trường trước đó đã từng truy nhập vào dữ liệu liên quan tới công việc tài chính của một nhà - sản - xuất - ôtô - *A* sau đó sẽ không được phép truy nhập dữ liệu của nhà - sản - xuất - ôtô - *B*. Sự hiểu biết của nhà phân tích về các công việc của nhà - sản - xuất - ôtô - *A* có thể được cho là xung đột lợi ích khi nghiên cứu nhà - sản - xuất - ôtô - *B*.

Sự hạn chế truy nhập chỉ áp dụng đối với các công ty mà theo một nghĩa nào đó, là những công ty cạnh tranh nhau. Nếu hai công ty không phải công ty cạnh tranh nhau thì không nảy sinh xung đột lợi ích như thế. Như vậy, người sử dụng đã truy nhập vào dữ liệu của nhà - sản - xuất - ôtô - *A* không bị ngăn cản truy nhập dữ liệu của nhóm khách - sạn - *C*. Do đó mô hình vạn lý trường thành phân chia các tổ chức thành các lớp xung đột lợi ích. Các đối tượng trong tổ chức được tổ chức phân cấp, tập hợp tất cả các đối tượng là gốc của cây, tập hợp các nút tiếp theo biểu thị các lớp xung đột (*A*, *B*, *C*), tức là những tập hợp của các tổ chức cạnh tranh lẫn nhau, bên trong mỗi lớp xung đột là những tập dữ liệu công ty (*a*, *b*, *c*,...,*j*). Những tập dữ liệu này đến lượt lại chứa những đối tượng riêng lẻ (1, 2,... 5), những đối tượng riêng lẻ đó là những chiếc lá cuối cùng của cây. Ban đầu một chủ thể có thể truy nhập một đối tượng bất kỳ, vào một tập dữ liệu bất kỳ, trong một lớp xung đột bất kỳ. Tuy nhiên, một khi một truy nhập như thế đã được thực hiện thì sau đó chủ thể bị giới hạn chỉ truy nhập những đối tượng nằm trong cùng tập dữ liệu công ty, hoặc những đối tượng từ lớp xung đột khác cho đến nay chưa truy nhập. Như vậy một nhà phân tích ban đầu có thể truy nhập đối tượng bất kỳ, ví dụ như tệp 2 từ tập dữ liệu *b*, trong lớp xung đột *A*; tệp này có thể tương ứng với tệp nhân sự từ tập dữ liệu của nhà - sản - xuất - ôtô - *B* trong lớp xung đột của các nhà sản xuất ôtô. Ô truy nhập tiếp theo, nhà phân tích chỉ có thể truy nhập hoặc đối

tượng bất kỳ khác trong tập dữ liệu của nhà - sản - xuất - ôtô - *B*, hoặc một đối tượng trong một lớp xung đột khác, ví dụ như đối tượng 1 từ tập dữ liệu *a* (nhóm khách - sạn - *A*) trong lớp xung đột *B* (lớp xung đột của các nhóm khách sạn). Truy nhập thứ hai sau đó cũng sẽ giới hạn những truy nhập tiếp theo trong lớp xung đột *B*.

Như vậy, bất kỳ khi nào một người sử dụng truy nhập một đối tượng trong một tập dữ liệu thì Vạn lý trường thành cũng sẽ được xây dựng quanh tất cả các tập dữ liệu trong cùng lớp xung đột và người sử dụng nằm bên ngoài thành đó. *So sánh với* Bell-La Padula model, Biba Models, Clark-Wilson model, information flow model. *Xem* formal model.

chip card ***các chip*** *Đồng nghĩa với* smart card.

chip modem ***modem chip*** Trong truyền thông dữ liệu, modem chứa trong một chip silic đơn. *Xem* MODEM.

CHIPS ***hệ CHIPS*** Ở ngành ngân hàng, viết tắt của Clearing House Interbank Payments System (hệ thống chi trả liên ngân hàng thanh toán bù trừ); dịch vụ chi trả viễn thông tư nhân do Hiệp hội thanh toán New York đối với các ngân hàng ở vùng New York vốn chi xử lý các khoản chi trả bằng đôla Mỹ. *So sánh với* CHAPS. *Xem* banking networks, SWIFT.

chosen cryptogram attack ***tấn công bản mã chọn trước*** Trong mật mã học, sự tấn công đòi hỏi một thông báo đã được ký bằng số bởi một người ký có chủ đích nhờ sử dụng thuật toán RSA. Giả sử khóa công khai, khóa riêng và modulo được người ký chỉ định dùng tương ứng là E, D và n. Kẻ tấn công chọn số C, trong đó $0 < C < n$ và cho nó là bản mã đã nhận được tương ứng với thông báo $M = C^E \bmod n$. Giả thiết này được chấp nhận vì nó qua được phép thử chữ ký số.

Bảo vệ chống sự tấn công này là khẳng định rằng, các thông báo đã ký có một độ dư thừa nào đó, vì kẻ tấn công không có cách nào để chọn số tương ứng với giá trị của M với những tính chất xác định. *Xem* digital signature, RSA.

chosen plaintext ***bản gốc chọn trước*** Trong mã thám, sự tấn công trong đó nhà phân tích mật mã có khả năng thu được bản mã tương ứng với bản gốc do anh ta chọn ra. Các hệ mật mã khóa công khai cung cấp cho các nhà phân tích mật mã phương tiện thu được một lượng không hạn chế bản gốc đã chọn vì khóa mã hóa là khóa công khai. *So sánh với* ciphertext only, known plaintext. *Xem* public key cryptography.

Christmas-J ***virut Christmas - J*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM và EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Christmas Violater ***virut Christmas Violater*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

CI *Xem* card issuer.

CIA *CIA* (1) Viết tắt của U.S. Central Intelligence Agency (Cục tình báo trung ương Hoa Kỳ). (2) Trong truyền thông, *xem* communications interface adapter.

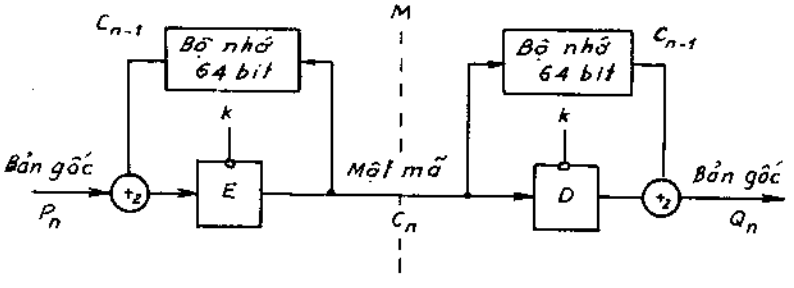
cipher ***mật mã, mã pháp*** Trong an toàn dữ liệu, kỹ thuật mật mã trong đó dãy các bit, hoặc các ký tự, được thay đổi nhờ một phép biến đổi bí mật. Mật mã mã hóa một đơn vị bản gốc kích thước cố định bằng một phép toán và độ dài của bản mã liên quan chặt chẽ với độ dài của bản gốc. *So sánh với* code. *Xem* block cipher, ciphertext, cryptography, plaintext, stream cipher.

cipher block ***khối mật mã*** (1) Trong mật mã học, kết quả bảo đảm an toàn cho một khối dữ liệu bằng cách áp dụng một hàm mật mã. Nói chung, trước và sau khi xử lý số bit trong khối không thay đổi. Ví dụ điển hình của các mã khối là đề xuất phác thảo của ISO, 8227: Xử lý thông tin - Mã hóa dữ liệu - Đặc tả thuật toán DEA1 (TC97/N1139) và chuẩn Thuật toán mã hóa dữ liệu (DEA) được ANSI (X3.92 - 1981) chấp nhận. *Xem* block cipher, DEA. (2) Trong mật mã học, khối dữ liệu được tạo ra bởi sự mã hóa một khối bản gốc độ dài định trước bằng một mã khối. Độ dài của khối mã có thể nhưng không nhất thiết phải bằng độ dài của bản gốc. *Xem* block cipher, ciphertext.

cipher block chaining ***liên kết khối mật mã, xích khối mã*** Trong mật mã học, một chế độ hoạt động khắc phục được điểm yếu trong mật mã của chế độ sổ mã điện tử. Đầu ra bản mã phụ thuộc vào khóa và tất cả các khối bản gốc trước đó của thông báo. Như vậy, các thông báo có khuôn thức cao sẽ không bị lặp lại các khối bản mã như trong chế độ sổ mã điện tử. Hoạt động này được minh họa trên sơ đồ. Thanh ghi dịch 64 bit được nạp một khối dữ liệu, gọi là vectơ khởi đầu.

Khối bản gốc 64 bit đầu tiên được cộng "loại trừ - hoặc" (EXCLUSIVE OR") với nội dung của thanh ghi dịch và khối 64 bit kết quả được mã bằng khóa k. Đầu ra bản mã 64 bit vừa được cấp vào thanh ghi dịch vừa được gửi tới máy thu. Đầu ra phép mã đầu tiên C_1 phụ thuộc vào P_1 và vectơ khởi đầu IV; đầu ra phép mã thứ hai phụ thuộc vào P_2 và C_1, tức là vào P_2, P_1 và IV.

Ở đầu thu, thanh ghi dịch cũng được



cipher block chaining: *liên kết khối mật mã.*

nạp cùng vectơ khởi đầu IV. Khối bản mã nhận được đầu tiên, C_1, được giải mã và đầu ra của khối giải mã được cộng "loại trừ - hoặc ("EXCLUSIVE OR") với nội dung của IV thanh ghi dịch, tái tạo lại khối bản rõ đầu tiên, P_1. Khối bản mã, C_1, cũng được đưa vào thanh ghi dịch sẵn sàng chờ nhận khối bản mã thứ hai, C_2. Thao tác liên kết khối mã có thể được mô tả ở dạng toán học để mã hóa:

$C_n = ek(P_n +_2 C_{n-1})$

trong đó $ek(M)$ = bản mã do mã hóa M bằng khóa k tạo ra, còn $+_2$ chỉ phép cộng modulo 2. Đầu ra của đơn vị giải mã Q_n được cho bởi

$Q_n = dk(C_n) +_2 C_{n-1}$

trong đó $dk(C_n)$ là khối dữ liệu được tạo ra nhờ giải mã khối bản mật mã C_n bằng khóa k. Từ đó

$Q_n = dk(ek(P_n +_2 C_{n-1})) +_2 C_{n-1}$

$= P_n +_2 C_{n-1} +_2 C_{n-1}$

$= P_n$.

Cả máy thu lẫn máy phát đều phải dùng chung giá trị chung của biến khởi đầu IV, được truyền từ máy gửi tới máy thu, thường được mã hóa bằng một khóa mật. Không thật cần thiết giữ bí mật IV để bảo vệ bí mật của bản gốc, nhưng phải ngăn cản một kẻ tấn công sửa đổi giá trị nhận được của IV. Nếu một kẻ tấn công có thể thay đổi IV thì khối đầu ra đầu tiên của thông báo gốc nhận được có thể bị thay đổi theo ý muốn của kẻ tấn công, các khối bản gốc sau đó sẽ không bị ảnh hưởng. Chính vì lý do này mà các IV thường được mã hóa để truyền đi.

Chế độ xích khối mã đòi hỏi rằng, các thông báo bao gồm một số bội các khối 64 bit. Khối thông báo cuối cùng có thể được đệm bằng các số không nhưng điều đó sẽ cung cấp cho nhà phân tích một thông tin hữu ích; các ký tự ngẫu nhiên cũng có thể được sử dụng thay cho các số không, nhưng máy thu cần biết cả quá trình đệm như vậy lẫn số ký tự đệm vào cuối thông báo. Chỉ thị đệm có thể được chèn vào như ký tự cuối cùng đã truyền đi và chỉ thị đó báo cho máy thu biết về số các ký tự đệm. Nếu yêu cầu độ dài của bản mã phải bằng độ dài của bản gốc là quan trọng, ví dụ, nếu một tệp đã mã hóa chiếm vùng nhớ trước đó đã cấp phát cho tệp văn bản gốc, thì việc đệm không được chấp nhận và phải áp dụng các giải pháp thay thế, ví dụ bằng cách "xén bớt" (ciphertext stealing) bản mã.

Lỗi một bit trong thông báo rõ (thông báo bản gốc) đưa vào sẽ ảnh hưởng tới mỗi khối bản mã được truyền kế tiếp, nhưng sẽ chỉ ảnh hưởng tới bit tương ứng trong bản gốc nhận được. Sự mất một bit, hoặc cộng thêm một bit tạp, vào bản mã sẽ gây mất đồng bộ giữa các dòng truyền đi và nhận được và sẽ làm sai lạc hoàn toàn bản gốc nhận được. Nếu một lỗi bit xuất hiện trong bản mã, thì các khối dữ liệu của bản gốc nhận được sẽ bị ảnh hưởng. Khối bị sai lạc đầu tiên sẽ phát sinh như kết quả giải mã khối bản mã đã thay đổi và khối bản gốc sẽ bị bóp méo, khối bản gốc thứ hai sẽ bị ảnh hưởng bởi phép cộng "loại trừ - hoặc" (EXCLUSIVE OR") khối văn bản mật mã bị sai lạc với đầu ra của thiết bị giải mã. Trong trường hợp này, chỉ có bit của khối bản gốc tương ứng với bit bị sai lạc của

khối bản mã sẽ bị ảnh hưởng. CBC do đó làm mở rộng lỗi. *So sánh với* cipher feedback, electronic codebook, output feedback. *Xem* block cipher chaining, ciphertext, ciphertext stealing, cryptographic key, DES, error extension, EXCLUSIVE OR, IV, plaintext, padding indicator, shift register.

cipher feedback ***hồi tiếp bản mã***

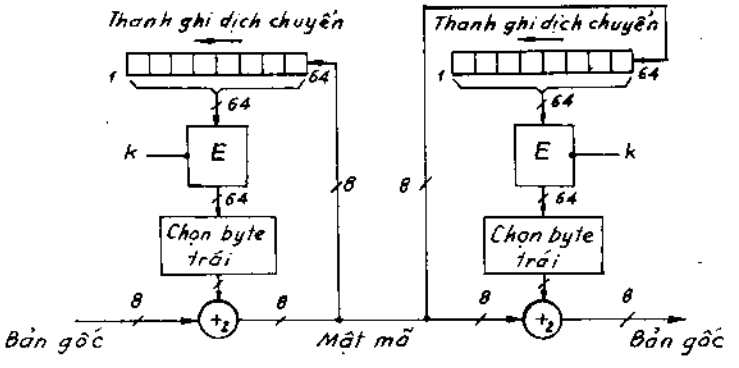
Trong mật mã học, chế độ hoạt động mã dòng thích hợp với những ứng dụng trong đó dữ liệu không thể được lập thành các khối 64 bit trước khi mã hóa. Trong một số ứng dụng, dữ liệu được xử lý như các bit, byte hoặc khung v.v. riêng lẻ, ví dụ thiết bị đầu cuối ký tự sẽ truyền các ký tự 8 bit riêng lẻ và những ký tự đó phải được truyền đi khi chúng được tạo ra, do đó không thể gom chúng lại thành các khối 64 bit để mã hóa.

Trong hồi tiếp bản mã, dòng bit giả ngẫu nhiên được cộng "loại trừ - hoặc" ('EXCLUSIVE OR') với dòng bản gốc để tạo thành dòng bản mã. Tại đầu thu cũng dãy giả ngẫu nhiên đó được cộng "loại trừ - hoặc" ('EXCLUSIVE OR') với dòng bản mã để tái tạo lại bản gốc. Dãy giả ngẫu nhiên được tạo ra từ chính dòng bản mã. Các thanh ghi dịch 64 bit được khởi tạo bằng một vectơ khởi tạo, IV, tại các đầu phát và thu. Nội dung của những thanh ghi này sau đó được đưa vào các khối mã DES các khối mã DES, sử dụng cùng khóa mật tại đầu phát và đầu thu.

Đoạn đầu ra 64 bit của khối DES có cùng độ dài như khối bản gốc cần mã hóa, sau đó được lựa chọn và được cộng "loại trừ - hoặc" với dòng dữ liệu. Như vậy, nếu dữ liệu cần mã ở dạng các khối 8 bit thì tám bit cực trái của đầu ra 64 bit của DES được chọn làm đoạn cho dòng giả ngẫu nhiên.

Khối bản mã, ví dụ ký tự 8 bit được đưa vào thanh ghi dịch của máy phát và truyền tới máy thu. Ở đầu thu nó được cấp vào thanh ghi dịch của máy thu và cũng được cộng "loại trừ - hoặc" với dòng giả ngẫu nhiên của máy thu, tạo ra bản gốc.

Nỗ lực mã DES với hồi tiếp bản mã lớn hơn so với chế độ CBC vì mỗi khối vào đòi hỏi mã một khối 64 bit; như vậy



cipher feedback: *hồi tiếp bản mã.*

nếu đầu vào được chia thành các byte thì phép mã 8 byte liên tiếp đòi hỏi tới 8 thao tác DES trong hồi tiếp bản mã và chỉ một thao tác DES trong CBC.

Vectơ khởi đầu, *IV*, có thể được truyền đi đơn giản như một phần mở đầu 64 bit ngẫu nhiên đối với một thông báo. Nếu phần mở đầu đó gây tốn phí quá lớn thì các thanh ghi dịch có thể được khởi đầu bằng một giá trị được thỏa thuận, ví dụ như toàn số không, và một phần mở đầu ngắn hơn được truyền đi; tuy nhiên việc sử dụng một phần mở đầu ngắn có thể là không khôn khéo nếu như các thông báo được tạo khuôn thức cao.

Hồi tiếp bản mã có tính mở rộng lỗi; một lỗi bit 1 trong bản mã sẽ tạo ra một lỗi bit tương ứng trong bản gốc được tiếp theo sau một số khối ra bị sai lệch vì lỗi mở rộng khắp thanh ghi. Nếu đầu vào là một dòng 8 bit thì 8 byte bị sai lệch ở đầu ra sẽ tiếp theo byte với lỗi bit một.

So sánh với cipher block chaining, electronic codebook, output feedback. *Xem* ciphertext, cryptographic key, DES, error extension, exclusive or, IV, plaintext, shift register, stream cipher.

cipher system ***hệ thống mã hóa*** Trong mật mã học, hệ thống lập mã (ghi mật mã) trong đó phép mã được áp dụng vào các phần tử bản gốc có độ dài như nhau. *Xem* cryptographic system, cryptography, plaintext.

ciphertext ***bản mã tín hiệu*** (1) Trong mật mã học, thông tin đã được mã hóa. *So sánh với* plaintext. (2) Trong mật mã học, văn bản hoặc tín hiệu không hiểu được được tạo ra thông qua việc sử dụng các hệ thống mật mã. *So sánh với* plaintext. *Xem* cipher system.

ciphertext key auto-key cipher ***mã pháp tự sinh khóa từ bản mã*** Trong mật mã học, kỹ thuật mật mã xích dòng trong đó, bản mã được cấp ngược trở lại thiết bị mã hóa để tạo ra dòng bit mật mã. *Xem* cipher feedback, cryptographic bit stream, stream cipher chaining.

ciphertext only ***tấn công chỉ có bản mã*** Trong mã thám, một tấn công trong đó nhà phân tích mật mã chỉ biết một lượng bản mã. Phương pháp mã hóa, ngôn ngữ bản gốc và có thể có một chỉ báo nào đó về những từ hoặc câu có thể sử dụng được. *So sánh với* chosen plaintext, known plaintext. *Xem* public key cryptography.

ciphertext searching ***tìm kiếm bản mã*** Trong mã thám, một kỹ thuật suy ra thông tin về bản gốc từ một khối bản mã. Ví dụ, sự duyệt qua một cơ sở dữ liệu lớn có thể phát hiện ra những bản ghi với những khối bản mã giống nhau và do đó, chẳng hạn, chỉ ra cá nhân có một tập hợp các thuộc tính giống nhau như khuynh hướng chính trị, tiền lương, điều kiện y tế v.v. *Xem* browsing.

ciphertext stealing ***xén bớt bản mã*** Trong mật mã học, chế độ hoạt động trong kỹ thuật liên kết mã khối để tránh mở rộng thông báo. Nếu độ dài của thông báo gốc không phải là một số nguyên lần kích thước khối thì các bit được lấy bớt từ khối bản mã áp chót và thêm vào khối bản rõ ngắn cuối cùng. Nếu kích thước khối là *n* bit và

khối cuối cùng chứa j bit ($j < n$) thì $n - j$ bit cuối cùng được loại bỏ khỏi khối bản mã áp chót và thêm vào đầu của khối bản rõ (gốc) cuối cùng, trước khi mã hóa. Do đó thông báo bản mã có cùng độ dài như bản rõ vì nó cũng chứa một khối ngắn j bit, tức là khối giáp cuối. Khi giải mã, khối bản mã cuối cùng được giải mã trước khối ngắn giáp cuối. $n - j$ bit đầu tiên của khối bản gốc đã khôi phục lại đó được bổ sung vào j bit của khối bản mã giáp cuối rồi mới được giải mã. Phương pháp này đảm bảo rằng, thông báo mật mã có cùng độ dài như bảo gốc ban đầu; điều đó có thể là một xem xét quan trọng nếu (chẳng hạn) bản mã được lưu giữ trong một vùng nhớ ban đầu là của bản gốc. *Xem* block cipher chaining, blocksize.

circuit ***mạch, mạch điện*** (1) Trong truyền thông, tuyến liên kết giữa hai hoặc nhiều điểm. (2) Trong điện tử học, đường chạy của dòng điện trong một vật dẫn hoặc một sơ đồ bố trí các vật dẫn.

circuit board ***tấm mạch, bo mạch*** *Đồng nghĩa với* printed circuit board.

circuit grade ***cấp mạch điện*** Trong truyền thông, khả năng mang thông tin của một mạch, khi cho trước tốc độ hoặc kiểu tín hiệu. Các cấp của mạch gồm dải tần rộng, thoại, dưới thoại (thoại con) và điện báo. *Xem* wideband channel, voice grade channel, subvoice grade channel.

circuit noise level ***mức ồn mạch, mức nhiễu của mạch*** Trong truyền thông, tỷ số tạp nhiễu mạch trên một mức chuẩn nào đó được chọn để quy chiếu. Tỷ số thường được đo theo đexiben trên tạp nhiễu chuẩn. *Xem* decibel, noise.

circuit switched digital circuitry ***sơ đồ mạch số chuyển mạch*** Trong truyền thông dữ liệu, kỹ thuật tạo ra những đường nối số từ đầu này tới đầu kia. Người sử dụng đặt các cuộc gọi bình thường và sau đó sử dụng cùng đường nối để truyền dữ liệu tốc độ cao. *Xem* circuit switching.

circuit switching ***chuyển mạch, (sự) đóng ngắt mạch*** Trong truyền thông dữ liệu, phương pháp trong đó đường nối được thiết lập theo nhu cầu và được duy trì giữa các trạm dữ liệu. Kỹ thuật này cho phép sự sử dụng dành riêng một mạch dữ liệu cho đến khi đường nối được giải phóng. *So sánh với* fast connect circuit switching, message switching, packet switching. *Xem* data station.

circumvention ***né tránh*** Trong an toàn vật lý, chỉ việc sử dụng các phương pháp né tránh vật lý để ngăn ngừa sự kích hoạt báo động, ví dụ trườn dưới sơ đồ vạch sẵn của máy phát hiện di động. *Xem* motion detector.

Cirrus ***mạng Cirrus*** Trong hoạt động ngân hàng, mạng EFTPOS của Hoa Kỳ. *Xem* EFTPOS.

CISA ***hệ CISA*** Viết tắt của Certified Information Systems Auditor (hệ kiểm toán các hệ thông tin có chứng nhận).

CKDS *Xem* cryptographic key data set.

Claims Language ***ngôn ngữ Claims*** Trong an toàn thông tin, ngôn ngữ đặc

tả bán chính thức, do bộ Thương mại và công nghiệp Anh đề xuất. Nó đòi hỏi người tài trợ phải chỉ rõ bộ chức năng an toàn có sử dụng một loạt các mẫu. *Xem* information technology security evaluation criteria.

Clark-Wilson model *mô hình Clark-Wilson* Trong các mô hình hình thức, một mô hình hình thức nhằm đáp ứng các yêu cầu an toàn dữ liệu của một môi trường thương mại.

Các thủ tục kế toán và kiểm toán do các công ty sử dụng đều dựa trên hai thủ tục kiểm soát cơ bản, chứng nhận và buộc tuân thủ. Chứng nhận cho biết rằng, các thủ tục kế toán được thiết kế và chứng thực sao cho bản ghi các giao dịch tài chính sẽ hoặc chứng tỏ rằng, chỉ các giao dịch hợp pháp đã được tiến hành, hoặc chỉ ra rằng, một tác động bất hợp pháp nào đó đã được thực hiện; các sổ sách hoặc cân bằng hoặc không. Như vậy việc ghi dữ liệu có một cấu trúc nội tại sao cho nó mô hình hóa chính xác tình trạng tài chính của thế giới thực tại của một tổ chức. Biện pháp phát triển bản ghi tài chính đó phải được một người có thẩm quyền chứng nhận để đảm bảo rằng, nó đáp ứng yêu cầu đó.

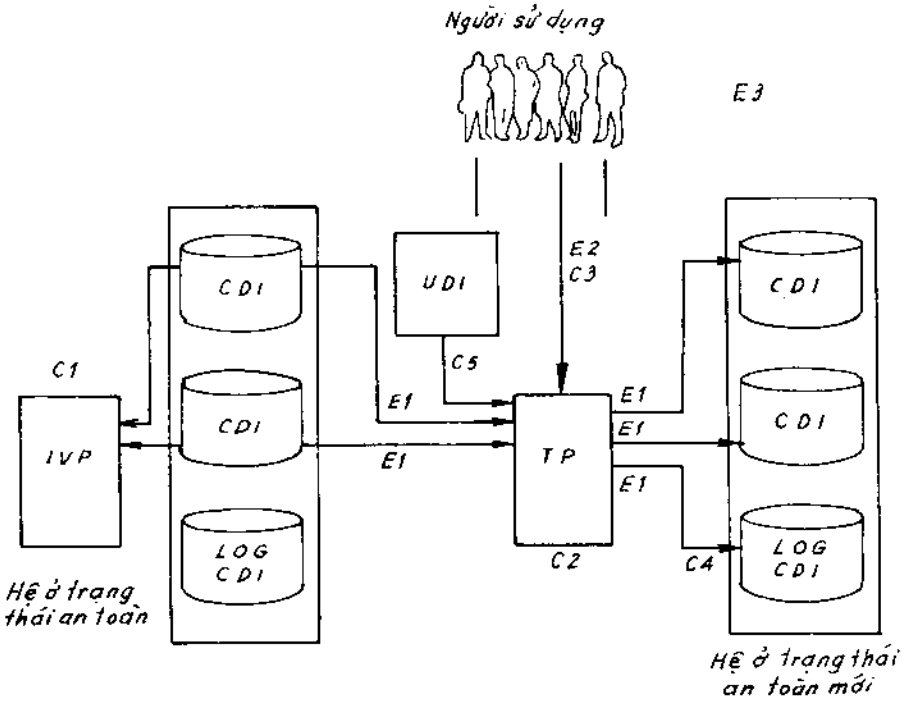
Tuy nhiên, sự đảm bảo các sổ sách cân bằng tự nó không đủ đảm bảo rằng không có hoạt động tài chính bất hợp pháp nào sẽ xảy ra. Nếu một người đã phạm vào một hành động bất hợp pháp không bị cản trở truy nhập tới mọi bản ghi tài chính, thì sẽ có thể tạo ra một trạng thái rõ ràng về tính toàn vẹn tài chính. Ví dụ, nếu như có thể ghi lên bản ghi tài chính rằng, hàng hóa đến một giá trị nào đó đã nhận được từ một nguồn bên ngoài và đã trả tiền cho hàng hóa đó, thì bản ghi tài chính có thể không cho cảnh báo nào về hoạt động bất hợp pháp. Tình huống như thế có thể xảy ra nếu một thủ phạm có khả năng ghi sai hóa đơn hàng hóa và cũng ghi sai khoản tiền trả cho người cung ứng không tồn tại.

Cách bảo vệ chống lại hành động như vậy là tách riêng các trách nhiệm; không một người nào có thể được phép thâm nhập vào mọi sổ sách. Nếu người chịu trách nhiệm ghi hóa đơn hàng hóa không được phép nhập một khoản trả, thì mục nhập sai trên hóa đơn hàng hóa không thể cân bằng với mục nhập khoản trả tương ứng. Như vậy, việc ghi từng phần một hoạt động bất hợp pháp sẽ làm cho sổ sách không cân bằng và điều này cho một manh mối về hành động trái phép. Bởi vậy cần có một dạng kiểm soát nào đó để đảm bảo sự tuân thủ liên tục việc tách bạch các nhiệm vụ.

Clark và Wilson đã phát triển một mô hình hình thức cho các hệ máy tính, phản ánh các yêu cầu của giới thương mại. Mô hình Clark - Wilson giới thiệu hai khái niệm an toàn mới: mục dữ liệu bắt buộc (CDI) và thủ tục biến đổi (TP). CDI đáp ứng có hiệu quả một dạng bút toán xác định trong sổ sách kế toán. TP là quá trình hợp pháp duy nhất mà có thể được thực hiện trên những tập CDI xác định, một TP có thể được xem giống như sự thực hiện một bút toán kép. Cần có các thủ tục chứng nhận để chỉ rõ rằng, các TP và các CDI có liên quan duy trì được tính toàn vẹn của bản ghi

tài chính. Ngoài sự chứng nhận như thế, cần có sự bắt buộc để đảm bảo rằng quy tắc tách riêng các công việc không bị vi phạm. Như vậy, các cơ chế bắt buộc sẽ giới hạn các TP có thể được áp dụng cho các CDI và những người sử dụng có thể gọi ra những TP xác định.

các TP và của các TP tới các CDI. CDI có thể không được truy nhập tùy ý để ghi lên các CDI khác; mỗi CDI chỉ có thể được xử lý theo một cách đáp ứng các yêu cầu chứng nhận. Hơn nữa, những người sử dụng chỉ có thể gọi tới những TP nào thỏa mãn sự tách riêng các yêu cầu chứng thực nhiệm vụ.



Clark-Wilson model: *mô hình Clark-Wilson.* E1 - các CDI chỉ thay đổi được bằng những TP được ủy quyền; E2 - những người sử dụng được phép đối với TP; E3 - những người sử dụng được xác thực; E4 - các danh sách ủy quyền chỉ thay đổi được bởi nhân viên an toàn; C1 - IVP phê chuẩn trạng thái CDI; C2 - các TP bảo toàn trạng thái có hiệu lực; C3 - sự tách riêng thích hợp nhiệm vụ; C4 - các TP ghi vào nhật ký; C5 - các TP phê chuẩn UDI.

Mô hình Clark-Wilson áp đặt một dạng kiểm soát truy nhập bắt buộc; trong trường hợp này, truy nhập liên quan tới truy nhập của người sử dụng vào

Những hạn chế đó là bắt buộc, cả các "chủ" của các CDI, cả người quản trị hệ thống đều không được tự ý vượt quá những hạn chế như thế.

Ở mô hình Clark-Wilson có bốn yêu cầu an toàn:

- hệ thống phải xác thực tách riêng và nhận dạng từng người sử dụng;
- hệ thống phải đảm bảo rằng, các mục dữ liệu đã đặc tả chỉ có thể được xử lý bởi một tập hợp hạn chế các chương trình và các kiểm soát trung tâm dữ liệu phải đảm bảo rằng, những chương trình đó đáp ứng quy tắc giao dịch theo quy định rõ ràng (xem dưới đây);
- hệ phải gắn với mỗi người sử dụng một tập hợp các chương trình hợp lệ cần chạy, còn trung tâm dữ liệu phải đảm bảo rằng, những tập hợp đó đáp ứng quy tắc tách riêng nhiệm vụ;
- hệ phải duy trì sổ ghi kiểm toán dùng ghi lại từng chương trình đã thực hiện và tên của người sử dụng ủy quyền.

Ngoài những tiêu chuẩn đó, có hai yêu cầu nữa đối với an toàn hệ thống:

- hệ máy tính phải chứa các cơ chế để đảm bảo rằng hệ thống buộc thực hiện những yêu cầu của nó;
- các cơ chế trong hệ thống phải được bảo vệ chống giả mạo hoặc sự thay đổi không được phép.

Mô hình xác định các mục dữ liệu trong hệ thống phải áp dụng tính toàn vẹn, gọi là các mục dữ liệu ràng buộc CDI. Điều căn bản là các mục dữ liệu về các giao dịch thương mại không được tạo ra hoặc sửa đổi theo cách tùy ý. Trạng thái của hệ thương mại sẽ được đặc trưng bằng một tập hợp các CDI, nếu tập hợp đó đáp ứng được một số tiêu chuẩn xác định trước. Ví dụ như chúng biểu diễn một tập hợp các sổ sách cân bằng, khi đó hệ thống ở trong trạng thái an toàn.

Lớp các thủ tục cần để kiểm tra xem tập hợp các CDI nhắc đến ở trên quả thực đáp ứng một trạng thái an toàn như vậy; những thủ tục đó được gọi là thủ tục phê chuẩn tính toàn vẹn, IVP. Như vậy việc áp dụng IVP cho một tập hợp các CDI để đảm bảo một trạng thái an toàn sẽ tương tự với kiểm tra để sổ sách của công ty cân bằng.

Bắt đầu từ một trạng thái an toàn là điều kiện cần những không phải đủ đối với một trạng thái an toàn tương lai nào đó. Tất cả những những thay đổi đối với CDI phải sao cho chúng chuyển hệ thống từ trạng thái an toàn này đến trạng thái an toàn khác. Trạng thái này của các công việc đạt được bằng cách hạn chế tất cả các tác động đối với các CDI ở những chuyển tác đã thiết lập rõ, gọi là các Thủ tục biến đổi, TP. Ví dụ, TP đáp ứng chuyển tác bút toán kép trong giới kế toán.

Phải thừa nhận rằng không phải tất cả các mục dữ liệu được nhập vào hệ thống đều là CDI. Dữ liệu được nhập vào một máy tính và nó có thể, do ngẫu nhiên hoặc với chú ý xấu, không đáp ứng được yêu cầu của một CDI. Hệ an toàn phải có một phương tiện nào đó xử lý những dữ liệu nhập như thế, tức là phê chuẩn tính hợp lệ của dữ liệu nhập và bổ sung đối với tập hợp hiện thời của các CDI, hoặc loại bỏ dữ liệu. Những mục dữ liệu như thế được gọi là các mục dữ liệu không ràng buộc UDI; chúng được xử lý bởi một TP riêng với nhiệm vụ kiểm tra mục dữ liệu và/hoặc chấp nhận nó như một CDI hợp

lệ, tức là biến đổi nó thành một CDI, hoặc loại bỏ nó.

Nếu hệ thống bắt đầu ở một trạng thái an toàn và nếu chỉ có các giao tác được phép mới được đảm bảo để di chuyển nó tới một trạng thái an toàn khác, thì an toàn hệ thống được đảm bảo cho bất kỳ dãy di chuyển nào như thế. Có một sự báo trước cho biết quan trọng mà chắc là gắn liền với lập luận đó: mỗi TP phải được thực hiện theo một trình tự chặt chẽ, sự hoàn thành từng phần TP có thể để hệ thống trong một trạng thái không an toàn, tức là chỉ có một bút toán được thực hiện. Nếu TP thứ hai bắt đầu từ trạng thái không an toàn đó, thì có thể không có sự bảo đảm hào đối với an toàn hệ thống trong tương lai.

Mô hình cho rằng, các IVP sẽ phê chuẩn các CDI, tức là đảm bảo trạng thái an toàn ban đầu, và các TP sẽ chuyển hệ thống từ trạng thái an toàn này sang trạng thái an toàn khác. Tuy nhiên, có hai khía cạnh của cách tiếp cận an toàn này:

- quá trình chứng nhận rằng, IVP và các TP đảm bảo trong thực tế những hoạt động an toàn như thế;
- thiết kế buộc tuân thủ chính sách an toàn.

Việc xác định rằng IVP và các TP đảm bảo tính toàn vẹn đối với một hệ thương mại đã cho sẽ phụ thuộc vào áp dụng riêng. Như vậy một cá nhân hoặc một nhóm được phép nào đó phải xác định IVP và các TP theo các quá trình do tổ chức sử dụng.

Các quy tắc chứng nhận của mô hình là:

- C1 - tất cả các IVP phải đảm bảo đúng rằng, mọi CDI đều ở trong trạng thái hợp lệ ở thời điểm IVP chạy;
- C2 - tất cả các TP phải được chứng nhận là hợp lệ, tức là chúng phải đưa một CDI tới một trạng thái cuối cùng hợp lệ với điều kiện là nó bắt đầu ở trong trạng thái hợp lệ. Đối với mỗi TP và mỗi tập hợp CDI mà nó có thể thao tác, nhân viên an toàn phải chỉ rõ một quan hệ xác định sự thực hiện đó. Như vậy, quan hệ có dạng: (TPi, (CDIa, CDIb, CDIc,...)), trong đó danh sách các CDI sẽ xác định một tập hợp cụ thể các đối số mà với chúng, TP được chứng thực;
- C3 - danh sách các quan hệ trong E2 (xem ở dưới) phải được chứng nhận đáp ứng sự tách riêng yêu cầu về công việc;
- C4 - tất cả các TP phải được chứng nhận để ghi vào một CDI gắn thêm duy nhất (nhật ký) tất cả các thông tin cần thiết để có thể khôi phục lại hoạt động thực chất;
- C5 - mọi TP lấy UDI như một giá trị vào đều phải được chứng nhận để chỉ thực hiện những biến đổi hợp lệ, nếu không thì không biến đổi nào được thực hiện, với mọi giá trị khả dĩ của UDI.

Bốn quy tắc buộc tuân thủ của mô hình là:

- E1 - hệ phải duy trì danh sách các quan hệ được chỉ ra trong quy tắc C2 (xem ở trên), và phải đảm bảo rằng, thao tác duy nhất của CDI bất kỳ được thực hiện bởi một TP, trong đó TP hoạt động trên CDI như được chỉ ra theo một quan hệ nào đó;

- E2 - hệ phải duy trì một danh sách các quan hệ có dạng (User ID, TPi, (CDIa, CDIb, CDIc...)), liên quan tới một người sử dụng, một TP và các đối tượng dữ liệu mà TP có thể tham chiếu nhân danh người sử dụng đó. Phải đảm bảo rằng, chỉ có những thực hiện được mô tả trong một trong các quan hệ là được tiến hành;
- E3 - hệ phải xác thực danh tính của mỗi người sử dụng định thực hiện một TP;
- E4 - chỉ có đại diện được phép chứng nhận các thực thể mới có thể thay đổi danh sách những thực thể như vậy khi được kết hợp với những thực thể khác; đặc biệt, thực thể gắn liền với một TP. Một đại diện có thể không có các quyền thực hiện nào đối với một thực thể song lại có thể chứng thực nó.

Các quy tắc C1, C2, và E1 cung cấp khung nền cơ bản để đảm bảo tính nhất quán bên trong của các CDI. C1 đòi hỏi rằng, tập hợp các IVP (thủ tục phê chuẩn tính toàn vẹn) phải được chứng nhận với mục tiêu là chúng sẽ đảm bảo để một tập hợp CDI cho trước phù hợp với đặc tả về tính toàn vẹn vào thời điểm IVP đó chạy, nói cách khác là "cân bằng sổ sách". C2 chứng nhận tương tự rằng, mỗi TPi thay đổi các CDI, đặc tả theo quan hệ (TPi, (CDIa, CDIb, CDIc,...)), từ trạng thái hợp lệ này sang trạng thái hợp lệ khác. Quy tắc buộc tuân thủ E1 có thể được so sánh (chẳng hạn) với việc buộc tuân thủ một thủ tục văn phòng để một giao dịch bán buôn với những dữ liệu xác định, được xử lý như một bút toán kép trong sổ sách.

E2 có liên quan tới một tập hợp các quan hệ bao gồm ID người sử dụng, các TP và các CDI. Quy tắc C3 chứng nhận rằng, những quan hệ đó tương ứng với sự tách riêng các yêu cầu phần việc của tổ chức. E2 đảm bảo rằng tập hợp đã được chứng nhận tương ứng của các quan hệ bị buộc tuân thủ, tức là một người sử dụng nào đó chỉ được phép thực hiện một TP nào đó có sử dụng một tập hợp nào đó các CDI như dữ liệu. E2 thực sự gộp cả E1 nhưng E1 được bao hàm để dễ cài đặt trong các hệ thống thực.

E3 buộc xác thực người sử dụng, tức là hệ thống đảm bảo sự phù hợp giữa ID người dùng với cá nhân khai báo danh tính đó tại thiết bị đầu cuối. C4 là quy tắc chứng nhận trên các TP nếu đảm bảo rằng, chúng ghi nhật ký các tác động của mình do đó cung cấp một vết kiểm toán.

Dữ liệu nhập vào hệ thống không được đảm bảo tạo thành CDI, người sử dụng được tự do nhập vào bất kỳ ký tự nào ở một đầu cuối, dữ liệu như thế được gọi là UDI (mục dữ liệu không ràng buộc). C5 là một quy tắc chứng nhận trên một TP có chức năng soạn thảo để đảm bảo rằng, toàn bộ dữ liệu nhập vào, tức là UDI, được kiểm tra về tính phù hợp với một CDI và hoặc qua được phép thử, do đó biến UDI thành CDI, hoặc loại bỏ UDI.

Quy tắc buộc tuân thủ cuối cùng E4 hạn chế quyền sửa đổi danh sách cho phép các cá nhân với các quyền chứng nhận và những cá nhân như thế không được quyền thực hiện các TP. *So sánh với* Bell-La Padula model, Biba model,

Chinese Wall model. *Xem* constrained data item, integrity validation procedure, transformation procedure, unconstrained data item.

Class A alarm system ***hệ báo động lớp A*** Trong an toàn vật lý, bản ghi đặc tính kỹ thuật phòng hỏa yêu cầu thao tác báo động ngay cả khi có một ngắt đơn, hoặc một sự cố tiếp đất, trong đường tín hiệu. *So sánh với* A fire, Class B alarm system.

Class A fire ***hỏa hoạn lớp A*** Trong an toàn vật lý, sự cháy của một vật liệu dễ cháy thông thường, ví dụ như gỗ, vải, giấy, chất dẻo v.v.. *So sánh với* Class B fire, Class C fire.

Class B alarm system ***hệ báo động lớp B*** Trong an toàn vật lý, bản ghi đặc tính kỹ thuật phòng hỏa đòi hỏi phát hiện tín hiệu báo động, một ngắt đơn hoặc sự cố tiếp đất trong đường tín hiệu. *So sánh với* Class A alarm system, Class B fire.

Class B fire ***hỏa hoạn lớp B*** Trong an toàn vật lý, hỏa hoạn liên quan tới hơi hoặc chất lỏng dễ cháy. *So sánh với* Class A fire, Class C fire.

Class C fire ***hỏa hoạn lớp C*** Trong an toàn vật lý, hỏa hoạn liên quan tới năng lượng điện. *So sánh với* Class A fire, Class B fire.

classification ***phân loại mật*** (1) Trong an toàn dữ liệu, việc gán thông tin hoặc tài liệu vào một loại trên cơ sở độ nhạy cảm của nó đối với sự tiết lộ hoặc sửa đổi hoặc sự phá hủy. Dựa trên Quy định hành chính của Hoa Kỳ 12356 vào năm 1982, các mức phân loại của Chính phủ Hoa Kỳ là: Tối mật (Top secret) - sự tiết lộ không được phép có thể gây ra tổn hại cực kỳ nghiêm trọng cho an ninh quốc gia. Tuyệt mật (secret) sự tiết lộ trái phép có thể gây hại nghiêm trọng tới an ninh quốc gia. Mật (Confidential) - sự tiết lộ không được phép có thể gây tổn hại cho an ninh quốc gia. (2) Trong an toàn dữ liệu, việc xác định rằng, thông tin cần thiết vì lợi ích của an ninh quốc gia, một mức độ bảo vệ đặc thù chống lại sự tiết lộ không được phép cùng với sự chỉ rõ rằng đã thực hiện việc xác định như thế. Sự phân loại dữ liệu được sử dụng cùng với các loại hình trong tính toán chỉ số rủi ro.

classification level ***mức phân loại*** Trong kiểm soát truy nhập, mức an toàn của một đối tượng. *So sánh với* clearance level. *Xem* object.

classified computer security program ***chương trình an toàn máy tính xếp vào loại mật*** Trong an toàn máy tính, tất cả các biện pháp an toàn công nghệ và các thủ tục quản lý được thiết lập và áp dụng cho các phương tiện ADP và các hệ thống ADP (bao gồm phần cứng máy tính, phần mềm và dữ liệu) để đảm bảo bảo vệ thông tin đã xếp vào loại mật. *Xem* ADP.

classified data/information ***dữ liệu/thông tin xếp vào loại mật*** Trong an toàn dữ liệu, dữ liệu chính thức đã được xác định đề yêu cầu bảo vệ vì lợi ích của an ninh quốc gia.

class of service ***lớp dịch vụ*** (1) Trong truyền thông, loại dịch vụ truyền thông mà một khách hàng thuê bao. (2) Trong truyền thông, loại thiết

bị điện thoại do một khách hàng sử dụng. (3) Trong truyền thông, các đặc quyền và hạn chế gọi của một đường truyền thông chuyển mạch nào đó.

CLC *Xem* communications link controller.

cleanroom approach ***phương pháp phòng sạch*** Trong tin học, phương pháp phát triển phần mềm nhằm giảm lỗi và tăng năng suất.

clearance ***(sự) thông, (sự) được phép; mức thông; mức truy nhập*** Trong kiểm soát truy nhập, sự cấp quyền cho một người sử dụng hệ thống truy nhập vào dữ liệu nhạy cảm. Bộ quốc phòng. Hoa Kỳ sử dụng một số mức thông: Chưa làm rõ (U). Thông tin chưa phân loại (N). Mức thông mật (C), mức thông tuyệt mật (S). Mức thông tối mật dựa trên điều tra cơ bản (TS(BI)). Mức thông tối mật dựa trên điều tra nền đặc biệt hiện thời (TS(SBI)), một hạng (IC). Đa hạng (MC). *Xem* clearance level, confidential clearance, multiple categories, one category, secret clearance, top secret clearance, unclassified information, uncleared.

clearance level ***mức thông, mức truy nhập*** Trong kiểm soát truy nhập, mức an toàn của một chủ thể. *So sánh với* classification level. *Xem* clearance, subject.

clear data ***dữ liệu rõ*** *Đồng nghĩa với* plaintext.

cleared funds ***quỹ đã bù trừ*** *Đồng nghĩa với* available funds.

clearing ***xóa, xóa về zero*** Trong an toàn máy tính, việc ghi đè thông tin đã phân loại trên vận tải tin từ tính sao cho có thể được sử dụng lại nó. (Điều này không làm giảm mức phân loại của vật tải tin.) *So sánh với* degauss. *Xem* clearing ADP media, object reuse, residue.

clearing ADP media ***giải phóng vật mang tin ADP*** Trong an toàn thông tin, thủ tục dùng để xóa hẳn thông tin đã phân loại nhớ trên vật mang tin nhưng không xóa toàn bộ như ở một thủ tục bỏ phân loại. *Xem* clearing, declassification of magnetic storage media.

cleartext ***bản rõ*** *Đồng nghĩa với* plaintext.

cleartext operation ***thao tác bản rõ*** Trong mật mã học, tiện ích của một thiết bị mã hóa hoặc bộ xáo trộn để nhận thông báo rõ ngay cả khi nó được thiết lập cho thao tác mã hóa hoặc xáo trộn. *Xem* cleartext, voice scrambling.

clear to send ***tín hiệu thông, tín hiệu gửi*** Trong truyền thông dữ liệu, tín hiệu dùng cùng với tín hiệu khác, tín hiệu yêu cầu gửi, như một giao thức bắt tay trong hoạt động bán song công. Tín hiệu được gửi từ một modem tới máy tính truyền, tiếp theo việc nhận một tín hiệu yêu cầu gửi, cho biết rằng modem sẵn sàng nhận các ký tự để truyền đi. *So sánh với* request to send. *Xem* half duplex, handshaking, MODEM, RS-232C.

clear zone ***vùng quang, vùng trống trải*** Trong an toàn vật lý, vùng ở cả hai phía của một hàng rào bao quanh không có rác rưởi, cây cối, cỏ dại, cây bụi v.v. sao cho khó giấu được những toan tính băng qua rào bảo vệ hoặc

C

chui qua nó. *Xem* perimeter barrier.

CLEF *Xem* commercial licensed evaluation facility.

clocking ***định thời*** Trong truyền thông dữ liệu, việc sử dụng các xung định thời để kiểm soát sự đồng bộ của dữ liệu và các ký tự điều khiển trong truyền thông nhị phân đồng bộ. *Xem* binary synchronous communications.

CLODO ***tổ chức CLODO*** Trong an toàn máy tính, tổ chức chống đối ngầm ban đầu ở Pháp, ủy ban nhằm thanh toán và làm mất tác dụng các máy tính.

closed circuit alarm ***báo động mạch kín*** Trong an toàn vật lý, báo động khởi phát do chập mạch. *Đồng nghĩa với* cross alarm.

closed circuit television ***truyền hình khép kín*** Trong an toàn vật lý, hệ các camera truyền hình và màn hình giám sát thường nối với nhau bằng cáp và dùng để giám sát các vùng được bảo vệ.

closed environment ***môi trường khép kín*** Trong an toàn máy tính, nguyên tắc theo đó, mỗi quá trình được cho không nhiều khả năng hơn mức cần thiết để thực hiện nhiệm vụ của nó. Trạng thái công việc bình thường là những quá trình hoàn toàn rời rạc tách biệt nhau; không có gì có thể dùng chung hoặc trao đổi được giữa chúng trừ những cách sắp xếp rõ ràng, mọi tương tác đều bị cấm trừ phi được phép rõ ràng.

closed hot site ***(địa) điểm nóng khép kín, vị trí nóng khép kín*** Trong quản lý rủi ro, một địa điểm nóng do một consocxium làm chủ hoặc nếu không thì được xây dựng cho một tập hợp riêng các công ty. *So sánh với* open hot site. *Xem* hot site.

closed security environment ***môi trường an toàn khép kín*** Trong an toàn máy tính, một môi trường bao hàm các hệ thống thỏa mãn cả hai điều kiện sau đây: (*a*) các nhà phát triển ứng dụng (kể cả các nhà bảo trì) đều có các sự cho phép và những sự ủy quyền đủ để cung cấp một giả định chấp nhận được rằng, họ không đưa vào logic ác ý. Mức truy nhập đủ được định nghĩa như sau: ở nơi nào mức phân loại tối đa của dữ liệu cần xử lý là mật hoặc thấp hơn thì các nhà phát triển được phân mức truy nhập và được cấp phép cùng mức như dữ liệu nhạy cảm nhất; nơi nào mức phân loại cực đại của dữ liệu cần xử lý là tuyệt mật hoặc cao hơn thì các nhà phát triển có ít nhất mức truy nhập tuyệt mật. (*b*) Sự kiểm soát cấu hình cung cấp một đảm bảo đủ để các ứng dụng được bảo vệ trước việc đưa vào logic ác ý trước và trong thời gian hoạt động của các ứng dụng hệ thống. *Xem* configuration control, malicious logic.

closed shop ***trung tâm tính toán khép kín*** (1) Trong an toàn vật lý, vùng hoạt động của máy tính với các kiểm soát đảm bảo rằng, nhân sự không đòi hỏi truy nhập, ví dụ như những nhà lập trình, bị hạn chế nhập vào vùng. (2) Trong các hoạt động, phương tiện sử dụng biên chế tin học riêng để thiết kế, phát triển, thử nghiệm và chạy các chương trình. *So sánh với* open shop.

closed user group ***nhóm người dùng khép kín*** Trong truyền thông, nhóm cho phép những người dùng cùng nhóm liên lạc với nhau, nhưng loại trừ các cuộc liên lạc với những người khác không phải là thành viên của nhóm.

cluster ***liên cung; chùm, đám*** (1) Trong các hệ điều hành, liên cung là các đơn vị không gian đĩa cấp cho một tệp. (2) Trong truyền thông dữ liệu, chùm là nhóm các thiết bị đầu cuối gộp lại ở một địa điểm riêng và được ghép nối với phương tiện truyền thông thông qua thiết bị điều khiển chùm. *Xem* cluster control unit.

cluster controller ***bộ điều khiển chùm*** *Đồng nghĩa với* cluster control unit.

cluster control unit ***thiết bị điều khiển chùm*** Trong truyền thông dữ liệu, thiết bị có thể điều khiển các thao tác nhập - xuất của nhiều hơn một thiết bị đầu cuối. *Đồng nghĩa với* cluster controller.

clutch head screw ***vít mũ có vấu*** Trong an toàn vật lý, vít có mũ phi chuẩn vốn đòi hỏi chìa vặn đặc biệt để vặn ra; nó làm thất vọng kẻ định mở trộm.

CNIL ***ủy ban CNIL*** Trong lập pháp, ủy ban nhà nước về xử lý dữ liệu và các đặc quyền của Pháp. *Xem* data protection - France.

CNP *Xem* communications network processor.

CNPDPI ***ủy ban CNPDPI*** Trong lập pháp, ủy ban quốc gia về bảo vệ dữ liệu cá nhân tự động hóa của Bồ Đào Nha. *Xem* data protection - Portugal.

COAM ***thiết bị COAM, thiết bị khách hàng*** Trong truyền thông dữ liệu, viết tắt của Customer Owned And Maintained communication equipment (thiết bị truyền thông do khách hàng làm chủ và bảo trì), ví dụ như các thiết bị đầu cuối.

coaxial cable ***cáp đồng trục*** Trong điện tử học, cáp tổn hao thấp, dùng cho các tần số cao, nó gồm một dây dẫn ở giữa và được cách điện với ống dây đồng bện.

CoCom ***ủy ban CoCom*** Viết tắt của Coordinating Committee for Multilateral Export Controls (ủy ban phối hợp kiểm soát xuất khẩu nhiều bên). Nó bắt đầu các hoạt động vào năm 1950 để kiểm soát việc xuất khẩu các vật liệu và công nghệ chiến lược cho các nước XHCN trước đây; các bên tham gia bao gồm Ôxtrâylia, Bỉ, Canada, Đan Mạch, Pháp, Đức, Hy Lạp, Italia, Nhật, Lucxămbua, Hà Lan, Na Uy, Bồ Đào Nha, Tây Ban Nha, Thổ Nhĩ Kỳ, Liên hiệp Anh và Hoa Kỳ.

code ***mã*** (1) Ký hiệu biểu diễn dữ liệu, thuận tiện cho xử lý tự động hóa. (2) Trong tin học, các lệnh hoặc các câu lệnh của một chương trình, hoặc tác động sinh ra chúng. (3) Trong truyền thông dữ liệu, hệ thống các ký hiệu dùng để biến đổi thông tin chữ - số thành dạng thích hợp để truyền đi trong truyền thông. (4) Tập hợp các quy tắc phác họa cách thức mà dữ liệu có thể được biểu diễn. *Xem* ASCII, Baudot code, character code. (5) Trong an toàn dữ liệu, phương pháp gửi các thông báo mật. Mỗi từ hoặc câu được thay thế

bằng nhóm tương ứng các ký hiệu lấy từ một cuốn mã từ điển. *So sánh với* cipher.

code analysis ***phân tích mã*** *Xem* static analysis.

code book ***sổ mã, từ điển mã*** Trong an toàn dữ liệu, sổ bí mật dùng để mã hóa một thông báo và chỉ người gửi và người nhận có. Ví dụ, một từ có thể được mã hóa theo vị trí vật lý và trang của nó trong sổ mã. *So sánh với* electronic codebook.

CODEC ***bộ lập - giải mã, codec*** Trong truyền thông, viết tắt của COder-DECoder (bộ lập mã - bộ giải mã), thiết bị để biến đổi các tín hiệu tương tự, ví dụ như tiếng nói, hình ảnh, âm nhạc thành dạng số hóa để truyền qua một phương tiện số và biến đổi lại chúng thành dạng tương tự. *So sánh với* MODEM. *Xem* analog signal.

code conversion ***chuyển đổi mã*** Trong truyền thông dữ liệu, quá trình thay đổi nhóm bit của một ký tự trong một mã thành nhóm bit tương ứng đối với ký tự ở mã thứ hai, ví dụ như từ mã ASCII thành mã EBCDIC. *Xem* ASCII, EBCIIC code. *Đồng nghĩa với* character mapping.

coded alarm system ***hệ báo động mã hóa*** Trong an toàn vật lý, hệ sử dụng các biến đổi xung hoặc tần số để phân biệt các tín hiệu báo động từ những bộ cảm biến khác nhau hoặc vùng bảo vệ khác nhau, ngay cả khi sử dụng một đường tín hiệu đơn.

coded character set ***bộ ký tự mã hóa*** Trong mã hóa, tập hợp các quy tắc để thiết lập một bộ ký tự và các quan hệ một - một giữa các ký tự trong bộ và các biểu diễn mã hóa của chúng.

coded key ***chìa khóa được mã*** Trong an toàn vật lý, phương pháp kiểm soát truy nhập dựa trên một vật phẩm mà người dùng có. Các khóa thường được dùng để truy nhập vào các vùng hoặc thiết bị thực tế; một khóa được mã có thể có dáng vẻ của một khóa thông thường nhưng nó còn có thể lưu giữ hàng ngàn hoặc hàng chục ngàn bit do đó tạo ra một mã nhận dạng duy nhất. *So sánh với* card key.

coded system ***hệ mã hóa*** Trong an toàn vật lý, hệ tiếp âm có ba hoặc nhiều vòng tín hiệu báo động mã hóa. Sau đó, có thể ngắt tín hiệu báo cháy hoặc thủ công hoặc tự động. *So sánh với* noncoded system. *Xem* master coded system.

code extension character ***ký tự mở rộng mã*** Trong bộ mã, ký tự điều khiển dùng để chỉ rằng một hoặc nhiều giá trị mã kế tiếp cần được thông dịch theo một mã đặc biệt. *Xem* escape character, shift codes.

code independent system ***hệ độc lập mã*** Trong truyền thông dữ liệu, chế độ truyền sử dụng một giao thức liên kết định hướng ký tự vốn không phụ thuộc vào bộ ký tự hoặc mã mà nguồn dữ liệu dùng. *Xem* link protocol.

code level ***mức mã*** Trong mã hóa, số các bit dùng để biểu diễn một ký tự. *Xem* byte.

code review ***xem lại mã, duyệt lại mã*** Trong an toàn máy tính, kỹ thuật ước lượng tĩnh trong đó các phần của mã nguồn được đánh giá để xác định xem

chúng có thực hiện theo các đặc tả thiết kế và có lỗi hay không. *So sánh với* penetration study, source code analyzer. *Xem* static evaluation.

code scrambling circuit ***mạch xáo trộn mã*** Trong an toàn vật lý, một mạch điện tử của hệ kiểm soát truy nhập cho phép tái gán ngẫu nhiên các mã cá nhân hóa theo lệnh. *Xem* card reader.

code set ***tập mã*** Trong mã hóa, tập hữu hạn và đầy đủ các biểu diễn được xác định theo một mã. *Xem* code.

code system ***hệ mã*** (1) Trong an toàn máy tính, hệ truyền thông bất kỳ dùng các nhóm ký hiệu để biểu diễn các phần tử của bản rõ độ dài khác nhau. *Xem* plaintext. (2) Theo nghĩa rộng nhất, phương tiện biến đổi thông tin thành dạng thích hợp cho truyền thông hoặc mã hóa, ví dụ như tiếng nói mã hóa, hệ mã Morse, hệ mã máy điện báo in chữ. *Xem* brevity lists, encryption. (3) Trong mật mã học, hệ mật mã trong đó các tương đương mật mã (thường gọi là các nhóm mã) trường gồm các chữ cái, chữ số hoặc cả hai trong những tổ hợp vô nghĩa được thay thế cho các phần tử bản gốc. Phần tử này có thể là các từ, các cụm từ hoặc các câu. *Xem* code.

code value ***giá trị mã*** Trong mã hóa, một phần tử của tập mã, ví dụ như giá trị mã chữ số nhị phân tám bit đối với ký tự xóa.

coercive force ***lực kháng từ*** Trong điện tử học, từ lực âm hoặc từ lực đảo tác dụng nhằm giảm độ cảm ứng từ. *Xem* coercivity, degauss.

coercivity ***độ kháng (từ)*** (1) Trong điện tử học, số đo lực kháng từ cần để giảm độ cảm ứng từ xuống bằng không. Thường được dùng để biểu thị mức độ dễ dàng mà một vật mang tin ADP từ tính có thể được khử từ. *Xem* coercive force, degauss. (2) Trong điện tử học, từ trường đảo cần thiết để giảm từ thông xuống bằng không, sau khi trường đã tăng lên để tạo ra sự bão hòa thông lượng từ và sau đó mới được giảm xuống bằng không.

cold site ***điểm nguội, điểm lạnh*** Trong quản lý rủi ro, trung tâm với các phương tiện phòng để máy cần thiết để tạo ra một địa điểm cho hoạt động của một trung tâm máy tính sau một thảm họa máy tính. Nó sẽ cung cấp không gian cho văn phòng và máy móc, các bộ nguồn, điều hòa không khí, các sàn nâng, hệ mạch điện v.v. nhưng thường có ít hoặc không có các bộ xử lý máy tính. Số thành viên của tổ chức cung cấp điểm nguội sẽ được giới hạn cũng như khoảng thời gian sử dụng những điểm như vậy. *Xem* contingency plans. *Đồng nghĩa với* shell site.

cold standby ***dự phòng nguội, dự phòng thứ cấp*** Trong hệ thống tin cậy, việc sử dụng máy tính dự phòng trong trường hợp sự cố hệ thống chính. Mọi dữ liệu trong bộ nhớ chính của máy tính ở thời điểm sự cố và không được ghi ở bộ nhớ dự phòng sẽ bị mất đi. *So sánh với* warm standby, hot standby.

cold start ***khởi động nguội*** Trong an toàn máy tính, hoạt động phải được tiến hành sau một sự cố nghiêm trọng trong một hệ máy tính, khi không truy

nhập trực tiếp được vào bộ nhớ và các giao tác mới xảy ra có thể đã bị mất. Hệ được nạp lại và khởi động ở chế độ IPL. *Xem* IPL.

collusion ***thông đồng, câu kết*** Trong lập pháp, hành động của hai hoặc nhiều người hợp tác cho các mục đích lừa lọc.

Colossus ***máy tính Colossus*** Trong mật mã học, máy tính điện tử chuyên dụng do Đài nghiên cứu bưu điện Anh chế tạo trong Thế chiến II và để dùng để mã thám các mật mã của Đức.

combination smoke detector ***máy phát hiện khói kết hợp*** Trong an toàn vật lý, máy phát hiện khói kết hợp cả thiết bị phát hiện khói ion hóa lẫn thiết bị phát hiện khói quang điện. *Xem* ionization smoke sensor, photoelectric beam smoke detector.

combinatorics ***toán tổ hợp*** Trong toán học, ngành toán học nghiên cứu các bài toán liệt kê và đếm, có liên quan tới xác suất và thống kê.

combined alarms ***(các) báo động phối hợp*** Trong an toàn vật lý, hệ chỉ kích hoạt các báo động dựa trên các tổ hợp các tín hiệu báo động từ các bộ cảm biến riêng.

combined station ***trạm kết hợp*** Trong truyền thông dữ liệu, trạm dùng trong các thủ tục HDLC. Trạm kết hợp tạo ra và thông dịch cả các lệnh lẫn các đáp ứng. *Xem* HDLC.

COMINT ***tin tình báo qua truyền thông*** Viết tắt của Communications Intelligence (tin tức tình báo qua truyền thông). Thông tin kỹ thuật và tình báo xuất phát từ truyền thông nước ngoài do những người không phải người nhận định thực rút ra được.

Comité Consultatif Internationale de Télégraphie et Téléphonie ***Ủy ban tư vấn quốc tế về điện báo và điện thoại*** Trong truyền thông, cơ quan cố vấn và tham mưu quốc tế được thành lập dưới sự bảo trợ của Liên Hợp Quốc để khuyến nghị các chuẩn truyền thông quốc tế. *Xem* protocol standards.

Commercial COMSEC Endorsement Program ***chương trình xác nhận an toàn truyền thông thương mại*** Một chương trình do NSA xây dựng để bảo vệ thông tin của chính phủ. *Xem* NSA COMSEC module.

commercial licensed evaluation facility ***phương tiện đánh giá đã đăng ký thương mại*** Trong an toàn thông tin, phương tiện đăng ký hoạt động ở Anh để tiến hành các đánh giá an toàn. *So sánh với* information technology security evaluation facility. *Xem* information technology security evaluation criteria.

commit ***lệnh cập nhật*** Trong các cơ sở dữ liệu, lệnh để cập nhật cơ sở dữ liệu theo tập hợp các giao tác nhập vào hệ thống. *So sánh với* rollback.

common carrier ***hãng truyền thông công cộng*** Trong truyền thông, hãng mà việc kinh doanh của nó là cung cấp các phương tiện truyền thông cho công chúng. Thuật ngữ này dẫn xuất từ khái niệm chuyên chở hàng hóa thương mại giữa các bang (của Hoa Kỳ). Ở Hoa Kỳ, một hãng truyền thông công cộng hình thành trong quyền hạn của các tổ chức bang có liên quan và nếu nó vận hành

các phương tiện giữa các bang thì nó sẽ phải tuân theo các quy định của FCC. Các hãng truyền thông công cộng có thể chuyển các thông báo từ xa, fax, truyền hình và dữ liệu. *So sánh với* VANS. *Xem* FCC, telemetry, PTT.

common cryptographic architecture ***kiến trúc mật mã phổ biến*** Trong mật mã học, kiến trúc mật mã phát triển cho các hệ IBM. *Xem* control vector.

communicating pair ***cặp truyền thông, cặp liên lạc*** Trong quản lý khóa, các bên logic trước đó đã thỏa thuận trao đổi dữ liệu. Một bên và trung tâm trao đổi các thông báo dịch vụ mật mã không phải là một cặp truyền thông. *Xem* cryptographic service message, logical party.

communication ***truyền thông, liên lạc*** Quá trình chuyển thông tin theo các phương tiện khác nhau từ một điểm, người hoặc thiết bị tới một điểm, người hoặc thiết bị khác. *Xem* telecommunications.

communication channel ***kênh truyền thông*** Trong truyền thông dữ liệu, môi trường vật lý và các thiết bị tạo nên phương tiện để truyền thông tin từ một thành phần của mạng tới (một hoặc nhiều) thành phần khác. *So sánh với* communication link.

communication link ***liên kết truyền thông*** Phương tiện vật lý nối vị trí này với vị trí khác nhằm mục đích truyền và thu thông tin. *So sánh với* communication channel.

communication processor ***bộ xử lý truyền thông*** *Xem* front end processor.

communication scanner ***bộ quét truyền thông*** Trong truyền thông dữ liệu, thiết bị giám sát các đường truyền để đáp ứng các yêu cầu phục vụ.

communications computer ***máy tính truyền thông*** Trong truyền thông dữ liệu, máy tính quản lý việc điều khiển các đường truyền và định tuyến dữ liệu trong một mạng. *Xem* routing.

communications control unit ***khối điều khiển truyền thông*** Trong truyền thông dữ liệu, thiết bị điều khiển sự truyền dữ liệu qua các đường truyền trong mạng.

communication server ***máy chủ truyền thông, bộ phục vụ truyền thông*** *Đồng nghĩa với* gateway.

communication service ***dịch vụ truyền thông*** Trong hoạt động ngân hàng, dịch vụ chuyển các thông báo giữa các thuê bao kể cả các giao dịch chuyển tiền lệ thuộc vào sự thanh toán qua các phương tiện khác.

communication link controller ***bộ điều khiển liên kết truyền thông*** Trong truyền thông dữ liệu, thiết bị thông minh cung cấp các chức năng giao tác định hướng đường truyền, ví dụ như phát hiện lỗi, đồng bộ hóa, các báo nhận, giữa một nhóm các modem và một máy tính hoặc bộ xử lý mạng truyền thông. *Xem* communications network processor.

communications medium ***phương tiện truyền thông, môi trường truyền thông*** Trong truyền thông dữ liệu, các mạch nối liên thông các mạng các đầu cuối hoặc các thiết bị vật lý mạng. Những mạch này có thể là mạch logic

hoặc mạch vật lý và tạo ra các đường truyền từ đầu này tới đầu kia giữa các quá trình truyền thông.

communications network processor *bộ xử lý mạng truyền thông* Trong truyền thông dữ liệu, thiết bị thông minh thực hiện các chức năng giao tác, ví dụ như nhớ đệm, chuyển đổi mã, quản lý hàng đợi giữa một máy tính với một hoặc nhiều bộ điều khiển liên kết truyền thông. *Xem* communications link controller.

communications security *an toàn truyền thông* (1) Sự bảo vệ bằng mọi biện pháp nhằm từ chối cấp cho những người không được phép thông tin có giá trị mà có thể nhận được từ việc có được và nghiên cứu các tín hiệu viễn thông, hoặc làm cho những người không được phép hiểu sai lệch các kết quả của việc có được và nghiên cứu như thế. An toàn truyền thông bao gồm an toàn mật mã, an toàn truyền dẫn, an toàn phát xạ và an toàn vật lý của các tư liệu và thông tin an toàn truyền thông. *Xem* cryptography, physical security, Tempest. (2) Sự bảo vệ đảm bảo tính xác thực của các tín hiệu viễn thông và nhờ áp dụng các biện pháp nhằm không cung cấp cho những người không được phép thông tin có giá trị mà có thể nhận được qua các tín hiệu viễn thông.

communication theory *lý thuyết truyền thông* Trong toán học, lý thuyết nghiên cứu sự truyền các thông báo khi có mặt tạp nhiễu. *Xem* information theory, noise.

commutative law *định luật giao hoán* Trong toán học, phép toán hai ngôi, tức là phép toán liên quan tới hai biến, thỏa mãn luật giao hoán nếu $x * y = y * x$, trong đó x và y là các biến và $*$ biểu thị phép toán hai ngôi (nhị nguyên). *So sánh với* associative law, distributive law. *Xem* Galois field.

compartment *vùng khoanh, ngăn, khoang* Trong an toàn dữ liệu, khoảng quy định áp dụng cho một kiểu thông tin nhạy cảm, cho biết các thủ tục xử lý đặc biệt cần sử dụng đối với thông tin và lớp tổng quát những người có thể truy nhập thông tin. Nó có thể liên quan tới việc quy định thông tin thuộc một hoặc nhiều loại hình. *Xem* category.

compartmentalization *(sự) chia ngăn, (sự) khoanh vùng* (1) Trong an toàn máy tính, sự cách ly các hệ điều hành, chương trình người dùng và các tệp dữ liệu với nhau trong bộ nhớ chính để bảo vệ trước truy nhập không được phép hoặc tranh chấp bởi những người sử dụng hoặc chương trình khác. *Xem* access. (2) Trong an toàn dữ liệu, phân chia dữ liệu nhạy cảm thành những khối nhỏ cách ly nhau nhằm giảm rủi ro cho dữ liệu. (3) Trong an toàn vật lý, nguyên tắc thiết kế theo đó sự cố hoặc biến cố có hại ở một phần của hệ thống không được phép lan rộng sang phần khác của hệ thống (ví dụ, khói hoặc khí có hại không được lan tỏa bên ngoài một vùng nào đó). *Xem* harmful event.

compartmented security mode *chế độ an toàn chia ngăn, chế độ an toàn khoanh vùng* (1) Trong an toàn máy tính, chế độ hoạt động cho phép hệ thống xử lý hai hoặc nhiều loại thông tin chia ngăn (thông tin cần sự

được phép đặc biệt) hoặc một loại thông tin chia ngăn bất kỳ với thông tin khác ngoài thông tin chia ngăn. Ở chế độ này, mọi người sử dụng hệ thống không cần được phân mức truy nhập đối với mọi loại thông tin chia ngăn đã xử lý, nhưng phải được phân mức truy nhập hoàn toàn đối với ít nhất là thông tin tối mật để truy nhập vào máy tính. *Xem* compartmentarization.

compatibility ***(tính) tương thích*** (1) Trong truyền thông dữ liệu, chỉ các cặp thiết bị đã đáp ứng được các yêu cầu về mã, tốc độ và sự biến đổi mức tín hiệu để có khả năng nối liên thông trực tiếp. (2) Trong tin học, chỉ các máy trên đó các chương trình có thể trao đổi với nhau mà không phải sửa đổi đáng kể.

compiler ***bộ biên dịch, trình biên dịch*** Trong tin học, chương trình được thiết kế để dịch chương trình nguồn viết bằng ngôn ngữ bậc cao sang chương trình ở dạng mã máy tương ứng. *Xem* high level language, machine code instruction, source program.

complement ***bù // số bù*** (1) Trong toán học, bù là thay đổi bit từ 0 thành 1 hoặc ngược lại trong số học nhị phân. *Xem* bit, Boolean algebra. (2) Trong toán học, số bù là số được rút ra bằng cách trừ một số nào đó từ một số xác định khác. Nó thường được dùng trong biểu diễn các số âm. *Xem* two's complement.

complete mediation ***dàn xếp hoàn toàn*** Trong an toàn máy tính, nguyên lý dàn xếp hoàn toàn, một trong những nguyên lý của các hệ thống an toàn phát biểu rằng, các kiểm tra truy nhập dựa trên thông tin kiểm soát truy nhập phải được thực hiện trong mọi tình huống gồm vận hành bình thường, bảo trì, phục hồi v.v.. *Xem* principles of cecure systems.

completeness check ***kiểm tra tính đầy đủ*** Trong xử lý dữ liệu, phép thử để các mục nhập dữ liệu được tạo ra ở các trường. Chúng không thể được xử lý ở trạng thái trống. *Xem* field.

complete set of residues ***tập đầy đủ số dư*** Trong lý thuyết số, tập hợp các số dư $(r_1, r_2 \ldots r_n)$ với một số nguyên n cho trước sao cho mỗi giá trị của một số nguyên b chỉ có một giá trị r_i, trong đó b là đồng dư với r_i theo modulo n. *Xem* congruent, residue.

complexity ***độ phức tạp*** Trong toán học, mức độ khó khăn của các bài toán cần tính toán khi đo bằng các tài nguyên cần để hoàn thành tính toán. Đây là lĩnh vực nghiên cứu tích cực và có các ứng dụng trong lĩnh vực mật mã học ngoài những lĩnh vực khác. *So sánh với* complexity analysis. *Xem* cryptography.

complexity analysis ***phân tích độ phức tạp*** Trong an toàn máy tính, phương pháp phân tích tĩnh xác định rõ các modun bên trong phần mềm có độ phức tạp cao theo một số đo nào đó, ví dụ theo số nhánh điều khiển trong modun. *So sánh với* complexity. *Xem* static analysis.

compliance testing ***kiểm tra tính phù hợp, kiểm tra tính tuân thủ*** Trong an toàn máy tính, việc kiểm tra chi tiết một khối lượng chuyển tác tương đối nhỏ sao cho, người kiểm tra

có thể biết được các điều khiển gắn sẵn trong hệ thống có hoạt động đúng hay không. *So sánh với* substantive testing.

component ***thành phần*** Trong truyền thông dữ liệu, một thiết bị hoặc tập hợp thiết bị, cấu thành từ phần cứng cùng với phần sụn của nó và/hoặc phần mềm thực hiện một chức năng riêng ở một mạng truyền thông máy tính. Thành phần là một bộ phận của một hệ lớn hơn và bản thân nó có thể gồm những thành phần khác. Các ví dụ là các modem, các bộ điều khiển viễn thông, các chuyển mạch thông báo, các thiết bị kiểm tra kỹ thuật, các máy tính chủ, các cổng nối, các mạng con truyền thông v.v.. *Xem* gateway, host computer, message switching, MODEM.

component reference monitor ***giám sát tham chiếu thành phần*** Trong kiểm soát truy nhập, khái niệm kiểm soát truy nhập liên quan tới một máy trừu tượng vốn dàn xếp tất cả các truy nhập tới các đối tượng bên trong một thành phần bởi các chủ thể bên trong thành phần đó. *Xem* component, reference monitor.

composite ***hợp số*** Trong lý thuyết số, số nguyên khác 1 chia hết cho một số nguyên khác không dư. *So sánh với* prime number.

compromise ***(sự) để lộ, (sự) làm lộ, (sự) thất thoát*** (1) Trong an toàn dữ liệu, sự vi phạm hệ thống an toàn đến mức có thể xảy ra tiết lộ không được phép thông tin nhạy cảm. *Xem* sensitive information. (2) Trong an toàn dữ liệu, sự tiết lộ không được phép hoặc sự mất mát thông tin nhạy cảm. *Xem* sensitive information. (3) Trong an toàn dữ liệu, chỉ sự tiết lộ không được phép thông tin nhạy cảm. Đối phương có thể nhận được thông tin tiết lộ đó nhờ nối lén, qua các kênh ngầm, con ngựa thành Toroa hoặc định tuyến sai thông báo. Nối lén tạo ra sự truy nhập trực tiếp vào thông tin truyền qua mạng. Các kênh ngầm cho phép một kẻ tấn công thu được tín hiệu về thông tin được bảo vệ qua việc giám sát những thay đổi trong các tài nguyên dùng chung v.v.. Con ngựa thành Toroa có thể thu thập thông tin nhạy cảm và phát thông tin đó cho kẻ tấn công khi nhận được các tín hiệu mã hóa từ kẻ tấn công. Các thông báo cũng có thể bị định tuyến sai và rời mạng ở những vị trí không được phép. *Xem* covert channel, Trojan Horse, wiretap. (4) Trong an toàn cơ sở dữ liệu, *đồng nghĩa với* personal disclosure.

compromising emanations ***(các) phát lộ, (các) phát xạ gây hại, (các) tín hiệu làm lộ*** (1) Trong an toàn máy tính, các tín hiệu liên quan tới dữ liệu không chủ ý hoặc mang tin tức mà nếu bị chặn và phân tích, sẽ làm lộ sự truyền thông tin đã phân loại mà một thiết bị xử lý thông tin bất kỳ thu nhận, nắm bắt hoặc xử lý theo cách khác. TEMPEST là tên rút gọn chưa phân loại liên quan tới các nhà nghiên cứu và các nghiên cứu về các phát xạ gây hại. Đôi khi nó được dùng đồng nghĩa với "phát xạ gây hại". *Xem* Tempest, van Eck phenomenom. (2) Trong an toàn máy tính, các bức xạ điện từ có thể chuyển tải dữ liệu và nếu bị chặn và phân tích có thể làm lộ thông tin nhạy cảm mà một hệ ADP bất

kỳ đang xử lý. *Xem* compromise, electromagnetic emanations, sensitive information, Tempest proofing, van Eck phenomenon.

COMPUSEC ***chương trình COMPUSEC*** Trong an toàn máy tính, chương trình an toàn máy tính của NSA Hoa Kỳ. *So sánh với* COMSEC, INFOSEC.

computationally infeasible ***không thể thực hiện về mặt tính toán*** Trong mã thám, nói tới sự tính toán có thể đạt được về lý thuyết song không thể thực hiện được về mặt thời gian với năng lực hiện tại hoặc năng lực dự đoán của máy tính.

computationally secure ***an toàn tính toán*** Trong mã thám, nói tới một mã pháp không thể bị phá bằng phân tích hệ thống với các tài nguyên sẵn có. *Xem* cryptanalysis. *Đồng nghĩa với* computationally strong.

computationally strong ***mạnh về tính toán*** *Xem* computationally secure.

computer ***máy tính*** (1) Thiết bị thực hiện các tính toán đã xác định trước trên một tập bất kỳ các dữ liệu vào hợp lệ và phân phối các kết quả với các mức chính xác xác định. (2) Thuật ngữ được dùng đối với máy tính số điện tử. *Xem* electronic digital computer, microcomputer.

computer abuse ***lạm dụng máy tính*** (1) Trong lập pháp, hoạt động không được phép cố ý hoặc cẩu thả làm ảnh hưởng tới tính sẵn sàng, độ tin cậy hoặc tính toàn vẹn của các tài nguyên máy tính.

Lạm dụng máy tính bao gồm gian lận, biển thủ, trộn cắp, làm hỏng cố ý, sử dụng bất hợp pháp, từ chối phục vụ và tham ô. Các mức lạm dụng máy tính gồm: (*a*) Lạm dụng nhỏ - các hoạt động thể hiện các vấn đề quản lý, như in lịch công tác hoặc chạy các trò chơi, vốn không ảnh hưởng tới tính sẵn sàng của hệ thống đối với các ứng dụng được phép; (*b*) Lạm dụng lớn - sử dụng không được phép (có thể mang tính tội phạm), từ chối phục vụ và nhiều lần lạm dụng nhỏ gây lãng phí; (*c*) Hành động tội phạm - gian lận, biển thủ, trộm cắp, phá hỏng ác ý, tham ô, tranh giành quyền lợi và truy nhập không được phép vào dữ liệu đã phân loại. *Xem* denial of service. (2) Trong an toàn máy tính, chỉ sự trộm cắp, gian lận, biển thủ hoặc phá hoại liên quan tới các máy tính bao gồm:

- thao tác bất hợp pháp đầu vào hoặc đầu ra của máy tính;
- truy nhập không được phép vào hệ thống thông qua các đầu cuối;
- sửa đổi hoặc sử dụng bất hợp pháp các chương trình ứng dụng;
- xâm phạm thiết bị xử lý dữ liệu và/hoặc trộm cắp thiết bị, các tệp hoặc bản in ra;
- phá hoại ngầm thiết bị của hệ thống máy tính;
- chặn xem dữ liệu bất hợp pháp.

Xem computer fraud control, computer security.

computer audit enquiry packages ***(các) bộ chương trình hỏi kiểm toán máy tính*** Trong kiểm toán, các bộ chương trình phần mềm kiểm toán máy tính chứa dựng một số đặc điểm chuẩn và có thể được tham số hóa để đáp ứng

các yêu cầu của người kiểm toán. *Xem* computer audit packages.

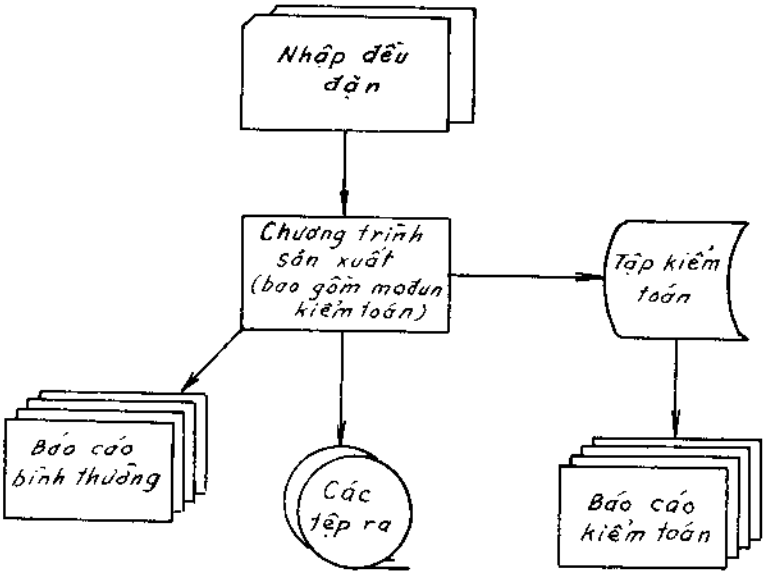
computer audit packages ***(các) bộ chương trình kiểm toán máy tính*** Trong kiểm toán, phần mềm để cho những người kiểm toán sử dụng, thường chứa những phương tiện để:

- so sánh các tệp chương trình hoặc dữ liệu và báo cáo về bất kỳ sự thay đổi nào;
- lấy mẫu các bản ghi trên cơ sở xác định trước hoặc ngẫu nhiên;
- phân tầng và phân tích những tệp dữ liệu lớn.

Xem computer audit enquiry packages, external auditor, internal auditor.

computer based message system ***hệ thông báo dựa trên máy tính*** *Đồng nghĩa với* electronic mail.

computer bureau ***văn phòng máy tính, văn phòng tính toán*** Về mặt pháp lý, theo Luật bảo vệ dữ liệu của Anh năm 1984, người điều khiển một văn phòng tính toán nếu người đó cung



computer audit packages: *(các) bộ chương trình kiểm toán máy tính.* Bộ giám sát kiểm tra tích hợp.

- lựa chọn và báo cáo về các bản ghi không thỏa mãn các tiêu chuẩn xác định;
- tái thực hiện các tính toán quan trọng để kiểm chứng;

cấp cho những người khác các dịch vụ về dữ liệu và một người cung cấp những dịch vụ như thế nếu:

(*a*) với tư cách là đại diện cho những người khác, anh ta làm cho họ được

tiến hành các công việc trên máy tính; hoặc (*b*) anh ta cho phép những người khác sử dụng thiết bị trong sở hữu của mình để xử lý. *Xem* data, data protection.

computer crime ***tội phạm máy tính*** (1) Trong lập pháp, theo Tội phạm máy tính của Bộ tư pháp Liên bang Hoa Kỳ: Sổ tay nguồn tòa hình sự (1979) - mọi hành động bất hợp pháp mà sự hiểu biết về công nghệ máy tính là cần thiết để khởi tố thành công. Tội phạm máy tính bao gồm các tội và tội có dẫn chứng mà có thể liên quan chủ động và thụ động tới máy tính khi bằng chứng có thể sử dụng về các hành động còn nằm trong máy tính. (2) Trong luật pháp, sự lừa đảo, biển thủ, truy nhập không được phép và những tội phạm "lao động trí óc" khác phạm phải với sự trợ giúp của hoặc trực tiếp liên quan tới hệ máy tính và/hoặc mạng máy tính. (3) Trong luật pháp, thuật ngữ làm hiểu sai vì đôi khi nó được dùng để chỉ những hoạt động không được phép mà chưa có định nghĩa pháp lý về tội phạm. Vấn đề lại phức tạp hơn bởi không có sự nhất trí về luật về tội phạm quốc tế. Một cá nhân phạm tội lừa đảo ở một termimal trên mạng do thao tác máy tính ở nước khác không nhất thiết vi phạm luật của nước nào. *Xem* computer abuse, computer fraud control, computer security.

Computer Emergency Response Team ***đội phản ứng khẩn cấp máy tính*** Trong an toàn máy tính, đội được thành lập theo Kinh nghiệm vụ virut Morris để phản ứng nhanh trước những sự thâm nhập vào các mạng và các hệ thống máy tính. *Xem* Morris worm.

computer facility ***phương tiện máy tính*** Các tài nguyên vật lý bao gồm các cấu trúc hoặc các bộ phận của các cấu trúc chứa đựng và hỗ trợ các khả năng. Đối với các máy tính nhỏ, các hệ độc lập và thiết bị xử lý văn bản, nó là vùng vật lý tại đó máy tính được sử dụng.

computer fraud control ***kiểm soát lừa đảo máy tính*** Trong an toàn máy tính, các biện pháp kiểm soát có hiệu quả chống lại lừa đảo máy tính bao gồm:

- phòng ngừa hoặc giảm bớt;
- phân tách các nhiệm vụ;
- kiểm soát nhập và xuất;
- kiểm soát sửa đổi bổ sung;
- kiểm tra xuyên suốt cấu trúc;
- lập hồ sơ rõ ràng;
- quay vòng công việc;
- chia tách kiến thức hoặc kiểm soát đối ngẫu;
- tăng mức độ khó khăn của che giấu/thực hiện;
- các thủ tục nhân sự tốt;
- đảm bảo tính trung thực và bảo hiểm tội phạm máy tính;
- phát hiện sớm;
- giám sát các vi phạm truy nhập;
- xem xét lại những tình huống bất thường;
- các vết kiểm toán;
- các mô hình phát hiện lừa đảo;
- phản ứng của người sử dụng lao động;
- tố cáo công khai.

Các biện pháp phòng ngừa ngăn chặn

lừa đảo xuất hiện phải được áp dụng và nếu các biện pháp hoàn toàn triệt để tỏ ra quá tốn kém hoặc không hữu ích thì phải sử dụng chiến lược thay thế của các biện pháp nhằm giảm tần số và mức độ bị lừa đảo.

Nhiệm vụ của nhân viên phải được tách bạch sao cho không có cá nhân nào có đủ tầm kiểm soát để gây ra một vụ gian lận. Tăng số lượng tối thiểu các cộng sự cần thiết để phân tích một vụ lừa đảo sẽ vừa làm giảm khả năng xuất hiện của nó, vừa dễ dàng phát hiện sự lạm dụng.

Các quá trình liên quan tới việc nhập dữ liệu vào máy tính, ví dụ như các chi tiết hóa đơn, hoặc nhận các thông tin ra từ máy tính, như các séc trả tiền, là cực kỳ nhạy cảm và phải được kiểm soát chặt chẽ. Mọi sự sửa đổi đối với các chương trình, dữ liệu hoặc các thủ tục phải được kiểm tra một cách độc lập. Phải tiến hành thử các kiểm tra xuyên suốt cấu trúc để đảm bảo rằng, hoạt động của máy tính được nhiều hơn một cá nhân am hiểu. Những người kiểm toán phải để tâm trí vào thiết kế hệ thống và thử nghiệm thu để tìm ra những hở vòng tiềm ẩn.

Việc lập hồ sơ rõ ràng đảm bảo rằng, thông tin về hoạt động hệ thống có thể sử dụng rộng rãi và không phải là lĩnh vực duy nhất của một cá nhân. Quay vòng công việc phải được áp dụng để tránh các tình huống trong đó, các cá thể bị cám dỗ và có cơ hội tìm ra những điểm yếu của hệ thống; các nhân viên cũng phải bị buộc nghỉ ngơi đều đặn. Sự kiểm tra đối ngẫu các hoạt động nhạy cảm liên quan tới các hoạt động tài chính, quản lý khóa mật mã v.v. đảm bảo rằng, không một cá thể nào có khả năng làm lộ hệ thống. Phải tránh các tình huống trong đó, một người phạm tội bị bắt quả tang có thể tự khai về lỗi thực sự đã xảy ra. Phải ban hành những nguyên tắc chỉ đạo có kỷ luật rõ ràng để thông báo một số hành động nào đó, ví dụ như nhập vào vùng nhạy cảm, là bị cấm. Phải thực hiện các thủ tục nhân sự tốt để xem xét các nhân viên có tiềm năng, giữ vững lòng trung thành của các nhân viên đang làm việc, phát hiện những thay đổi trong thái độ của các bệnh viện, giảm đến tối thiểu tổn thất tiềm tàng do các nhân viên đã bị sa thải gây ra v.v.. Cần phải xem xét tới những hoạt động nhạy cảm về kiểm soát nhân viên và việc bảo hiểm tội phạm máy tính.

Phát hiện sớm các ý đồ lừa đảo, ví dụ có thể phát hiện các thí nghiệm với các cơ cấu kiểm soát hệ thống bằng việc giám sát hệ thống một cách có hiệu quả. Tất cả các vi phạm truy nhập, ví dụ những ý đồ nhập mật khẩu không thành công, những ý đồ truy nhập các hoạt động đặc quyền phải được giám sát và nghiên cứu. Việc xem xét những sự cố và những mẫu động thái bất thường, những thay đổi thói quen hoặc các hoàn cảnh của cá nhân có thể giúp phát hiện sớm sự lừa đảo trong một số trường hợp. Các vết (biên bản) kiểm toán được dùng phải thích hợp với các mục đích an toàn và các báo cáo ngoại lệ được giám sát và xem xét đều đặn. Các mô hình phát hiện lừa đảo có thể được triển khai để chỉ ra những mẫu thuẫn trong hoạt động của một hệ

thống, hoặc những sai khác quan trọng giữa các bộ phận tương thích của hệ thống, ví dụ mẫu các giao dịch ở những đặc điểm khác nhau của công ty. Những người chủ phải đối phó lại sự lừa đảo của nhân viên bằng cách nhắc tới sự cảnh báo thích hợp của những người chủ khác về các hành động xấu của nhân viên và việc tố giác những người phạm tội sẽ làm nhụt chí những kẻ phạm tội tiềm ẩn khác. *Xem* audit trail.

computer inquiry 1980 ***điều tra máy tính - 1980*** *Ở* Hoa Kỳ, một quyết định của PCC nhằm hạn chế điều lệ của hãng truyền thông công cộng chỉ cho hãng dự phòng những dịch vụ cơ bản và bỏ các dịch vụ cải tiến khỏi điều lệ. Quyết định này khuyến khích cạnh tranh trên thị trường viễn thông và làm mở rộng phạm vi các dịch vụ và thiết bị khách hàng. *Xem* basic service, common carrier, enhanced services.

computerized branch exchange ***tổng đài nhánh máy tính hóa*** *Đồng nghĩa với* private automatic branch exchange.

computer matching ***so khớp máy tính*** Trong lập pháp, sự so sánh hai hoặc nhiều tập hợp các tệp dữ liệu để tìm kiếm các cá nhân bao hàm trong cả hai hoặc mọi tập hợp. *Xem* data protection, linkage.

Computer Misuse Act 1990 ***Luật về lạm dụng máy tính 1990*** Trong lập pháp, luật của Anh đề cập tới vấn đề lạm dụng máy tính. Nó xác định những tội lỗi khi xử lý các hacko, những kẻ tạo ra các virut máy tính, sâu máy tính và những mối đe dọa khác.

computer network ***mạng máy tính*** *Xem* data communications.

computer security ***an toàn máy tính*** (1) Việc bảo vệ các máy tính và các dịch vụ của chúng trước tất cả những nguy cơ tự nhiên và do con người gây ra và đưa ra một sự đảm bảo rằng, máy tính thực hiện những chức năng quan trọng của nó một cách đúng đắn và không có những tác dụng phụ gây hại nào. Nó bao gồm cả việc cung cấp độ chính xác của thông tin. *So sánh với* data security, information security. (2) Sự bảo vệ thông tin và các tài sản vật lý của một hệ máy tính. Sự bảo vệ thông tin nhằm ngăn ngừa việc tiết lộ xử lý, phá hủy và sửa đổi dữ liệu không được phép. Sự bảo vệ tài sản vật lý ngụ ý các biện pháp an toàn chống lại sự trộm cắp, phá hủy hoặc lạm dụng thiết bị (tức là các bộ xử lý, thiết bị ngoại vi, các phương tiện nhớ dữ liệu, các đường truyền thông và các giao diện).

Sự tiết lộ thông tin không được phép có thể được xem xét liên quan tới sự để lộ dữ liệu đã phân loại, bảo vệ hoặc giữ độc quyền. Các tổ chức quân sự, các doanh nghiệp, các cơ quan chính phủ v.v. có dữ liệu mật không được để lộ ra cho những người không được phép. Luật bảo vệ và giữ bí mật dữ liệu đặt trách nhiệm lên những người nắm giữ dữ liệu cá nhân phải duy trì mức tin cần của những dữ liệu đó; không làm được như vậy theo khuôn khổ của luật đó, có thể dẫn tới hành động hợp pháp chống lại người nắm giữ dữ liệu. Thông tin có sở hữu (ví dụ, phần mềm, các cơ sở dữ liệu truy nhập được bởi các hệ truy tìm thông tin trực tuyến thương

mại) tạo nên tài sản chính của các hãng phần mềm và các nhà xuất bản điện tử. Sự bảo vệ chống tiết lộ trái phép là vấn đề sống còn đối với tài chính của những cơ sở đó.

Xử lý dữ liệu liên quan tới sự thay đổi thuộc tính nào đó của dữ liệu như phân loại an toàn, các đặc quyền truy nhập tệp hoặc nơi tới của dữ liệu, khiến cho dữ liệu có giá trị đối với những người dùng bất hợp pháp hoặc làm cho chúng bị xử lý theo cách không được phép.

Các thiết bị nhớ điện tử và từ tính được thiết kế để xử lý thông tin rất không ổn định. Trong khi phá hủy dữ liệu lưu trên giấy có thể là nhiệm vụ tốn thời gian cực kỳ khó khăn, thì lại có thể phá hủy rất, nhanh thông tin trên máy tính bằng một đoạn mã ngắn chỉ thị ghi đè, bằng cách bỏ nguồn nuôi khỏi bộ nhớ khả biến, bằng cách khử từ các phương tiện nhớ từ tính, hoặc đơn giản bằng cách lấy trộm hộp đĩa mềm. Thiệt hại mà người chủ dữ liệu trước đây phải chịu có thể hoàn toàn không cân xứng với lợi ích, nếu có, mà kẻ tấn công hoặc nỗ lực cần để tấn công thu được.

Sự phun không được phép dữ liệu có thể dẫn đến sự chèn bất chính một mục vào cơ sở dữ liệu. Sự thay đổi dữ liệu không được phép có thể đem lại lợi ích cá nhân hoặc tài chính đáng kể cho kẻ tấn công và/hoặc bất lợi tương ứng cho người nắm giữ hoặc chủ của dữ liệu. Hơn nữa, khi không có những phòng ngừa đặc biệt thì có thể không phát hiện được những thay đổi như thế. Thông tin tài khoản ngân hàng, các điểm thi, các định mức tín dụng, các hồ sơ tội phạm, các giao dịch tài chính và hồ sơ y tế là những thông tin mà con người có thể muốn thay đổi vì lợi ích riêng của mình hoặc làm hại người khác.

An toàn tài sản vật lý liên quan tới các kỹ thuật an toàn truyền thống mà có thể kém huyền bí hơn so với các kỹ thuật của lĩnh vực an toàn thông tin, nhưng lại không kém phần quan trọng. Trộm cắp thiết bị tính toán hoặc thiết bị liên quan thường có thể gây mất mát cho người sở hữu mà mất mát đó hoàn toàn không tỷ lệ với lợi ích của kẻ cắp. Đĩa mềm bị đánh cắp có thể đáng giá một tuần tiền tiêu vặt đối với một cậu thiếu niên nhưng là mất mát dữ liệu tài chính không thể thay thế được đối với một công ty. Trộm cắp ác ý một tấm mạch in có thể làm ngừng một trung tâm máy tính trong một số giờ.

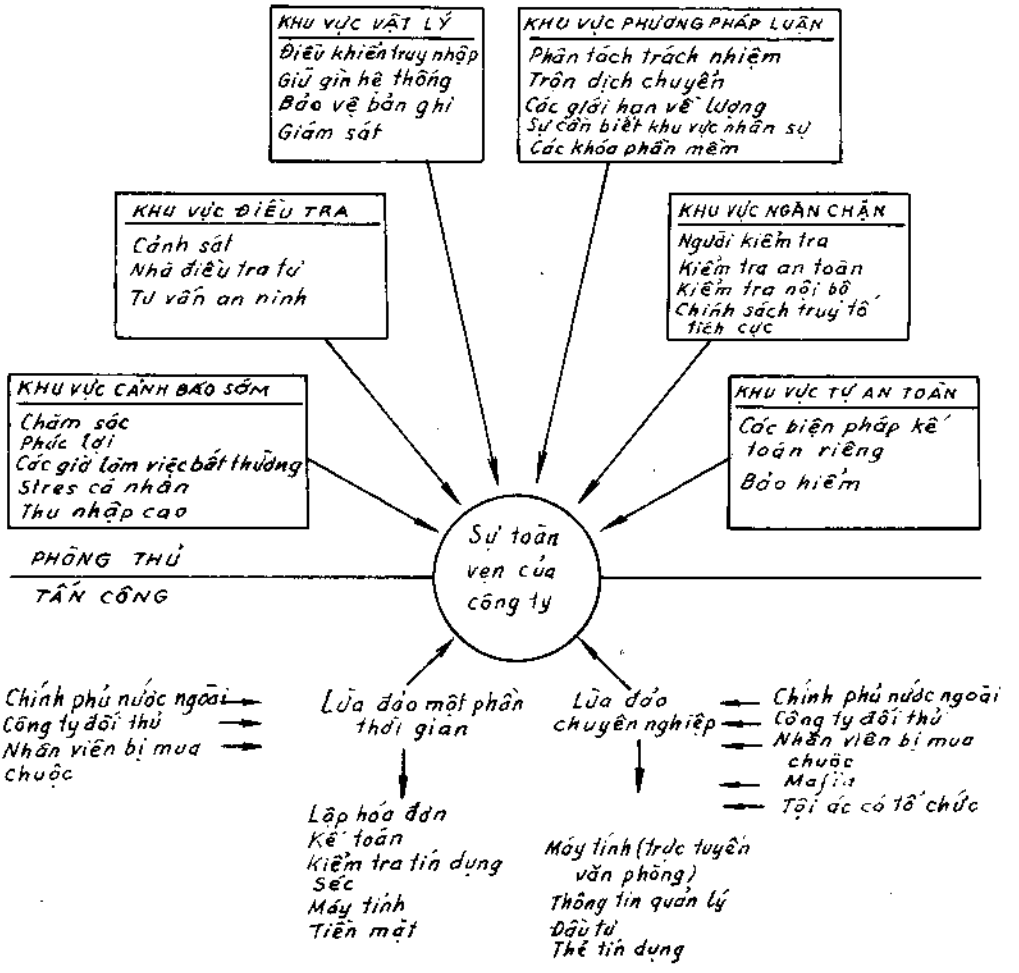
Phá hủy thiết bị có thể do ngẫu nhiên (ví dụ, thiên tai, hỏa hoạn, lụt lội v.v.) hoặc cố ý (ví dụ, phá hoại, hành động khủng bố). Mất mát mà tổ chức phải chịu có thể vượt xa chi phí cho thiết bị bị phá hủy. Việc lạm dụng không ác ý máy tính hoặc thiết bị truyền thông có thể do các nhân viên tiến hành các công việc riêng hoặc đơn giản, chơi trò chơi điện tử. Những ảnh hưởng có hại của họ tùy thuộc vào mức độ chúng tác động với hoạt động bình thường của tổ chức (ví dụ, thực hiện những hoạt động đó cũng ảnh hưởng tới thời gian đáp ứng của máy tính hoặc chiếm không gian nhớ đáng kể trên đĩa); hoặc tới mức làm tăng chi phí vận hành (ví dụ, cước phí truyền thông mạng công cộng). Lạm dụng phương tiện tính toán như

vậy cũng có thể làm tăng nguy cơ đưa virut máy tính vào.

Lạm dụng ác ý các phương tiện có thể chủ tâm nhằm làm quá tải hệ máy tính/truyền thông hoặc tấn công vào danh tiếng của tổ chức (ví dụ, hacko lạm dụng máy tính, công bố và quảng cáo những kỳ tích của họ). *Xem* access control, compromise, computer crime, data, data protection, data security, data subject, data user, disclosing, hacker, personal data, risk analysis.

Computer Security Act of 1987 ***Luật an toàn máy tính 1987*** Trong lập pháp, luật của Hoa Kỳ mà ngoài những cái khác ra thì còn gồm các điều khoản:

- Quy trách nhiệm về sự phát triển các nguyên tắc chỉ đạo an toàn máy tính và các chuẩn cho Viện tiêu chuẩn và công nghệ quốc gia.



computer security: *an toàn thông tin.*

- Yêu cầu rằng trong vòng sáu tháng sau khi ban hành luật thì các cơ quan Liên bang sẽ phải xác định xong các hệ thống hiện có và theo kế hoạch mà chứa (sẽ chứa) thông tin nhạy cảm, kể cả thông tin cá nhân.
- Yêu cầu về kế hoạch phát triển an toàn đối với mỗi hệ máy tính đã xác định trong vòng một năm ban hành luật.
- Yêu cầu đào tạo bắt buộc định kỳ về kiến thức an toàn máy tính và thực hành an toàn máy tính có chứng nhận đối với tất cả các nhân viên liên quan tới quản lý, sử dụng hoặc vận hành các hệ máy tính liên bang.

So sánh với Computer Security Act of 1988. *Xem* data protection - USA.

Computer Security Act of 1988 ***Luật an toàn máy tính 1988*** Trong lập pháp, luật của Hoa Kỳ thành lập Ban an toàn hệ thống máy tính và tư vấn bảo mật dưới sự bảo trợ của Viện tiêu chuẩn và công nghệ quốc gia. *So sánh với* Computer Security Act of 1987.

computer security incident ***sự cố an toàn máy tính*** Trong an toàn máy tính, sự cố gây hại gắn liền với một hệ ADP: (*a*) không tuân thủ các quy định hoặc chỉ dẫn an toàn của Bộ; (*b*) dẫn tới bị nghi ngờ hoặc làm tổn hại thực tế thông tin đã phân loại; hoặc (*c*) dẫn tới sự lạm dụng, làm mất mát hoặc hư hỏng tài sản hay thông tin của chính phủ. *Xem* ADP.

computer security plan ***kế hoạch an toàn máy tính*** Trong an toàn máy tính, bản ghi cách giải quyết đối với an toàn của một tổ chức để cho những người kiểm tra, người sử dụng, biên chế an ninh v.v. tham khảo. Kế hoạch phải chứa các đặc tả về phần cứng, phần mềm, kiểu dữ liệu vị trí vật lý, các mạng truyền thông và các chi tiết về nhân sự an toàn. Các biện pháp an toàn áp dụng cho nhân sự: tức là quyền tiếp cận thiết bị, dữ liệu, các quá trình, phải được nêu rõ cũng với các chi tiết kỹ thuật dùng cho an toàn truyền thông, kiểm soát truy nhập an toàn thông tin và an toàn chống rò rỉ bức xạ. Các chi tiết và những thủ tục về tình trạng khẩn cấp, các kế hoạch bất ngờ, các điều khoản dự phòng, các kế hoạch khôi phục sau sự cố và các thủ tục đào tạo cũng phải tạo thành một phần của kế hoạch an toàn. *Xem* contingency plans, compromising emanations, disaster rescovery plan.

computer security specialist ***chuyên gia an toàn máy tính*** Trong an toàn máy tính, một cá nhân có các trách nhiệm về vận hành hoặc tư vấn để lập kế hoạch, cài đặt, lắp đặt, vận hành và đánh giá các biện pháp an toàn và các kiểm soát an toàn.

computer security subsystem ***phân hệ an toàn máy tính*** Trong an toàn máy tính, các phương tiện bổ sung dưới dạng phần cứng, phần mềm hoặc phần sụn vào một hệ thống để tăng cường tính an toàn của nó. *Xem* firmware, hardware, software.

computer software quality ***chất lượng phần mềm máy tính*** Trong các hệ tin cậy, mức độ mà các thuộc tính của phần mềm cho phép nó thực hiện mục tiêu sử dụng cuối cùng xác định của nó. *Đồng nghĩa với* software quality.

computer virus ***virut máy tính*** *Xem* virus.

Comsec ***chương trình Comsec*** Trong an toàn truyền thông, chương trình an toàn truyền thông của NSA Hoa Kỳ. *So sánh với* COMPUSEC, INFOSEC. *Xem* communications security, NSA COMSEC module.

concealment system ***hệ che giấu*** Trong an toàn dữ liệu, phương pháp đạt độ bí mật trong đó sự tồn tại của thông tin nhạy cảm được ẩn giấu bằng cách lồng nó trong dữ liệu không liên quan. *Xem* confidentiality, sensitive information.

concentrator ***bộ tập trung*** Trong truyền thông dữ liệu, thiết bị nhớ đệm các dữ liệu tới và truyền lại nó qua những tuyến ra thích hợp.

conceptual design ***thiết kế khái niệm*** Hệ ứng dụng được mô tả và giới thiệu dưới dạng thích hợp cho người sử dụng.

conditioning ***điều phối*** Trong truyền thông dữ liệu, các thủ tục đảm bảo rằng, sự suy yếu của tín hiệu truyền ở mạch nằm trong các giới hạn xác định của biểu giá cước. Nó được dùng trên các đường điện thoại được thuê để truyền dữ liệu nhằm cải tiến tốc độ truyền.

conductive radiation ***phát qua dẫn điện*** Trong an toàn truyền thông, sự truyền các tín hiệu mang thông tin ngược qua các tuyến lưới điện hoặc cung cấp không dành cho truyền thông tin. *Xem* Tempest proofing.

conductive shielding ***chắn dẫn*** Trong điện tử học, vật liệu đặc biệt đặt quanh một thành phần (linh kiện) ngăn không cho nó phát ra bức xạ EMI/RF. *Xem* EMI/RF radiation, shielding effectiveness.

Confidential ***mật, bí mật*** *Xem* classification.

confidential clearance ***mức truy nhập mật, mức thông mật*** Trong kiểm soát truy nhập, một mức truy nhập của Bộ quốc phòng Hoa Kỳ đòi hỏi tư cách công dân Hoa Kỳ và điển hình là kiểm tra một số hồ sơ hạn chế nào đó. *So sánh với* multiple categories, one category, secret clearance, top secret clearance, unclassified information, uncleared. *Xem* clearance.

confidentiality ***độ bí mật, độ kín*** (1) Trong an toàn dữ liệu, đặc trưng an toàn máy tính đảm bảo cho các cá nhân được truy nhập các tài nguyên máy tính dựa trên mức thông an toàn và nhu cầu cần biết. Đặc trưng này bảo vệ chống lại sự thất thoát và sự tiết lộ do sơ suất. *Xem* data confidentiality, need-to-know. (2) Trong an toàn dữ liệu, khái niệm áp dụng cho dữ liệu vốn phải được lưu giữ tin cần và mô tả trạng thái và mức độ bảo vệ phải dự phòng cho những dữ liệu về các cá nhân cũng như các tổ chức như vậy. *Xem* data confidentiality. (3) Trong an toàn dữ liệu, tính chất đảm bảo để thông tin không còn hiệu lực hoặc bị tiết lộ cho những cá nhân, thực thể hoặc quá trình không được phép. *Xem* data confidentiality.

configurably dumb terminal ***đầu cuối cấu hình không thông minh*** Trong an toàn máy tính, terminal (đầu

cuối) mà có thể có các phương tiện nhớ và xử lý rộng rãi nhưng những phương tiện đó có thể bị vô hiệu hóa khiến trở thành thiết bị không thông minh (tức là không có bộ nhớ khả lập trình cho các mục đích an toàn máy tính). *Xem* dumb device.

configuration control ***kiểm soát cấu hình*** Trong an toàn máy tính, sự quản lý các thay đổi xảy ra đối với phần cứng, phần mềm, phần sụn và hồ sơ của một hệ thống trong suốt tuổi thọ phát triển và vận hành của hệ thống. *Xem* configuration management.

configuration management ***quản lý cấu hình*** (1) Trong an toàn máy tính, quá trình kiểm soát những sửa đổi đối với phần cứng, phần sụn, phần mềm và hồ sơ của hệ thống vốn tạo ra một sự bảo đảm đủ để hệ thống được bảo vệ chống lại việc đưa vào sự sửa đổi không đúng trước, trong khi và sau khi cài đặt hệ thống. *Xem* configuration control. (2) Trong an toàn máy tính, việc sử dụng các thủ tục thích hợp cho việc kiểm soát những thay đổi đối với cấu trúc phần cứng và phần mềm của một hệ thống nhằm đảm bảo rằng, những thay đổi như thế sẽ không làm giảm độ an toàn của dữ liệu.

confinement ***(sự) giới hạn*** (1) Trong an toàn dữ liệu, giữ cho dữ liệu ở trong mức an toàn đúng của nó. *So sánh với* data leakage. (2) Trong an toàn máy tính, sự cho phép một quá trình thi hành một chương trình mượn (nói chung, một chương trình tùy ý) truy nhập vào dữ liệu, đồng thời đảm bảo để dữ liệu không bị lạm dụng, sửa đổi phá hủy hoặc thất thoát.

confinement channel ***kênh hạn chế*** *Xem* covert channel.

confinement property ***tính chất giới hạn*** *Đồng nghĩa với* star property.

confirmed service ***dịch vụ được xác nhận*** Trong truyền thông dữ liệu, dịch vụ trong đó người gửi phát một yêu cầu, một chỉ báo về yêu cầu được chuyển cho người nhận đã định, người này đáp lại bằng phản ứng tạo ra một sự xác nhận cần chuyển cho người gửi. *So sánh với* unconfirmed service.

confusion ***(sự) gây xáo trộn, (sự) gây mập mờ*** (1) Trong mật mã học, kỹ thuật trong đó độ bền vững của một hệ mật mã được tăng lên bằng cách tạo ra một quan hệ phức tạp giữa bản mã và khóa mật mã. *So sánh với* diffusion. *Xem* ciphertext, cryptographic key, strength. (2) Trong mật mã học, đặc trưng của một mã pháp làm cho mỗi chữ cái của bức điện mã phụ thuộc vào tất cả các ký tự của khóa. *Xem* cryptogram, cryptographic key.

congruent ***đồng dư*** Trong toán học, cho các số nguyên b, c và $n \neq 0$, thì b là đồng dư với c modulo n khi và chỉ khi với một số nguyên m nào đó, $b - c = mn$.

connection ***kết nối, đường nối*** Trong truyền thông dữ liệu, đường liên lạc, theo nghĩa quan hệ qua lại trong mạng, giữa hai máy chủ trong một khoảng thời gian. Đường liên lạc được thiết lập (nhờ một máy chủ khởi xướng) nhằm mục đích chuyển thông tin (với máy chủ có liên quan); khoảng thời gian là thời gian cần để thực hiện mục đích của sự liên lạc (ví dụ như

chuyển tệp, một phiên nói chuyện, phân phát thư). Trong nhiều trường hợp, kết nối sẽ trùng hợp với kết nối máy chủ - máy chủ thiết lập thông qua TCP hoặc giao thức tương đương. Tuy nhiên, một kết nối (liên lạc) cũng có thể tồn tại chỉ khi dùng một giao thức như IP (IP không có khái niệm nào về một kết nối tồn tại trong một khoảng thời gian). Do đó thái niệm kết nối dùng ở đây độc lập với các giao thức riêng sử dụng trong liên lạc của hai máy chủ. *Xem* protocol, TCP/IP.

connectionless service ***dịch vụ không kết nối*** Trong truyền thông dữ liệu, dịch vụ truyền thông trong đó mỗi gói tin được truyền như một thực thể tách riêng, qua mạng, tới đích của nó. Các gói tin không cần truyền theo cùng đường và có thể tới đích theo cùng trình tự như khi truyền. *So sánh với* connection oriented service. *Xem* datagram sarvice.

connection oriented service ***dịch vụ định hướng kết nối*** Trong truyền thông, dịch vụ truyền thông trong đó thiết bị gửi thiết lập một kết nối, sử dụng kết nối trong thời gian chuyển thông tin và sau đó kết thúc kết nối. Cuộc gọi điện thoại đơn là một ví dụ dịch vụ định hướng kết nối. *So sánh với* connectionless service.

consistency ***tính nhất quán*** Trong an toàn cơ sở dữ liệu, chỉ việc không có các mâu thuẫn hoặc các nghịch lý này sinh khi sử dụng các kỹ thuật nhiễu loạn cho kiểm soát suy luận. Ví dụ, những kỹ thuật như thế có thể khiến cho một giá trị trung bình trả lại trong lời đáp cho một câu hỏi khác với giá trị trung bình tính bằng cách chia tổng nhận được cho số đếm nhận được. *So sánh với* bias. *Xem* inference control, perturbation.

console ***bàn điều khiển*** Ở các thiết bị ngoại vi, đầu cuối điều khiển của một hệ máy tính.

constant ratio code ***mã tỷ số không đổi*** *Đồng nghĩa với* M out of N code.

constrained data item ***mục dữ liệu ràng buộc*** Trong các mô hình hình thức, thuật ngữ dùng trong mô hình Clark-Wilson, nó biểu thị các mục dữ liệu vốn phải duy trì theo một quan hệ nào đó đối với nhau, ví dụ tương ứng với các sổ cân đối ngân sách trong một hệ thống kế toán. *So sánh với* unconstrained data item. *Xem* Clark-Wilson model.

construction vulnerability ***chỗ dễ tổn thương kết cấu, điểm yếu về cấu trúc*** Trong an toàn thông tin, chỗ dễ tổn thương lợi dụng một tính chất nào đó của đích đánh giá vốn đã đưa vào trong khi xây dựng nó. *So sánh với* exploitable vulnerability, operational vulnerability. *Xem* potential vulnerability. *Xem* information technology security evaluation criteria, target of evaluation, vulnerability.

contactless smart card ***thẻ thông minh không tiếp xúc, cạc thông minh không tiếp xúc*** Trong kiểm soát truy nhập, dạng thẻ thông minh không cần nối điện trực tiếp để chuyển dữ liệu giữa thẻ thông minh và bộ đọc. Thẻ được đặt gần sát bộ ghép nối thẻ và dữ liệu được trao đổi thông qua trường cảm ứng ở tần số vô tuyến. Thẻ này

có ưu điểm là không mòn và không rách khi tiếp xúc cơ khí. *Xem* smart card.

contained ***bị giới hạn, bị bao hàm*** Trạng thái ở bên trong các giới hạn, như trong các giới hạn của hệ thống, bất chấp mục đích hoặc chức năng và bao gồm mọi trạng thái nhớ, sử dụng hoặc xử lý.

container ***vật chứa, ngăn chứa*** Trong an toàn dữ liệu, cấu trúc thông tin nhiều mức. Một vật chứa có một phân loại và có thể chứa các đối tượng (mỗi đối tượng có phân loại riêng của mình) và/hoặc những vật chứa khác. *Xem* container clearance required, Landwehr's security model for military message systems, multilevel device, object.

container clearance required ***mức truy nhập vật chứa cần thiết, yêu cầu thông ngăn chứa*** Trong an toàn dữ liệu, thuộc tính của một số vật chứa tại đó, điều quan trọng là có mức truy nhập tối thiểu, do đó nếu một người sử dụng không có, ít nhất là mức truy nhập đó thì anh ta không thể nhìn thấy bất kỳ thực thể nào bên trong vật chứa. *Xem* container, Landwehr's security model for military message systems.

contamination ***ô nhiễm*** (1) Trong an toàn máy tính, tình huống trong đó dữ liệu hoặc chương trình của một người sử dụng tác động tới dữ liệu hoặc chương trình của người sử dụng khác theo một cách không mong muốn, hoặc ngẫu nhiên hoặc cố ý. (2) Trong an toàn dữ liệu, việc đưa dữ liệu có độ nhạy cảm và nhu cầu cần biết này vào dữ liệu có độ nhạy cảm thấp hơn hoặc nhu cầu cần biết khác. Điều này có thể dẫn tới dữ liệu bị ô nhiễm không nhận được mức bảo vệ cần thiết. *Xem* data contamination, need-to-know, sensitivity label.

content dependent access control ***kiểm soát truy nhập phụ thuộc nội dung*** Trong kiểm soát truy nhập, sự kiểm soát truy nhập trong đó truy nhập được xác định bằng giá trị của dữ liệu cần truy nhập. *So sánh với* context dependent access control.

contention ***tranh chấp*** (1) Trong truyền thông dữ liệu, tình huống mà hai hoặc nhiều thiết bị đồng thời định truy nhập một bộ phận thiết bị chung (ví dụ, hai terminal cố truy nhập một khối xử lý). (2) Ở các mạng dữ liệu, phương pháp điều khiển đường truyền trong đó các terminal yết cầu hoặc giành điều khiển truyền. Nếu kênh không sẵn sàng các terminal phải chờ cho tới khi nó rỗi. *Xem* contention control.

contention control ***kiểm soát tranh chấp*** Trong truyền thông dữ liệu, chiến lược kiểm soát đối với một mạng cục bộ (LAN) trong đó nút bất kỳ muốn truyền đều làm như thế. Nếu hai nút truyền ở cùng thời điểm sẽ xuất hiện xung đột và cả hai thông báo đều bị sai. Các nút truyền phát hiện xung đột (va chạm) và chờ một khoảng ngẫu nhiên trước khi truyền lại không báo. *Xem* Aloha, carrier sense multiple access-collision detection, contention, Ethernet, local area network.

contention delay ***trễ do tranh chấp*** Trong truyền thông dữ liệu, thời gian

chờ một phương tiện đang bị chiếm dụng bởi những thiết bị khác. *Xem* contention.

context dependent access control ***kiểm soát truy nhập phụ thuộc ngữ cảnh*** Trong kiểm soát truy nhập, sự kiểm soát truy nhập trong đó sự truy nhập được xác định theo tình huống riêng và dữ liệu được truy nhập dưới những tình huống đó. *So sánh với* content dependent access control.

contingency management ***quản lý ngẫu nhiên*** Trong quản lý rủi ro, sự quản lý tất cả các hành động được tiến hành trước, trong khi và sau một sự cố (điều kiện khẩn cấp), cùng với các thủ tục đã lập hồ sơ, đã thử mà nếu tuân theo chúng sẽ đảm bảo tính sẵn sàng của những hệ ADP quan trọng và sẽ tạo điều kiện bảo toàn tính liên tục của các hoạt động trong tình huống khẩn cấp. *Xem* ADP, contingency plans.

contingency plans ***(các) kế hoạch bất thường*** (1) Trong quản lý rủi ro, kế hoạch cho phản ứng khẩn cấp, cho các hoạt động dự phòng và sự khôi phục sau sự cố. Nó được hoạt động ADP duy trì như một phần của chương trình an toàn của mình. Bản kê nhất quán toàn diện về tất cả những hành động (kế hoạch) cần thực hiện trước, trong và sau sự cố (điều kiện khẩn cấp), cùng với các thủ tục đã lập hồ sơ, đã thử, mà nếu tuân theo, sẽ đảm bảo tính sẵn sàng của các tài nguyên ADP quan trọng và sẽ tạo điều kiện duy trì tính liên tục của các hoạt động trong tình huống khẩn cấp. *Xem* ADP, contingency management. (2) Trong quản lý rủi ro, các kế hoạch do một tổ chức soạn thảo ra để đáp ứng một loạt những vụ việc, những rủi ro và những sự cố có thể xảy ra: sai sót của nhân viên điều hành, mất nhân sự do ốm đau, chết hoặc đình công, hoạt động hackơ, trộm cắp, gian lận, sự phá hoại, sự thay đổi hoặc phá hủy phần mềm hoặc dữ liệu, hỏa hoạn, lũ lụt, mất nguồn, điều kiện thời tiết quá mức, nhiễu loạn điện, sự cố bảo vệ môi trường (điều hòa không khí, khói, bụi), tấn công khủng bố, va đập của máy bay, xe cộ, thiên thạch hoặc vệ tinh, hóa chất đổ tràn, sự cố kết cấu nhà, các sự cố là phản ứng hạt nhân hoặc những tác dụng bức xạ khác, động đất, núi lửa, lở đất...

Phản ứng với những hiện tượng đó phải cụ thể, ví dụ như các trách nhiệm cá nhân, các thủ tục dự phòng, các hợp đồng hỗ trợ lẫn nhau, các phương tiện truyền thông thay thế, các phương tiện xử lý thay thế, bảo hiểm, các kế hoạch thử nghiệm v.v..

Các tổ chức chuyên gia cung cấp một loạt những phương tiện quản lý phục hồi. Điểm nóng tạo ra một trung tâm trang bị đầy đủ với năng lực xử lý tương tự sẵn sàng trong một thời gian giới hạn xác định. Có thể chọn phương tiện vỏ bao, hoặc điểm nguội, chứa máy tính và tiện nghi văn phòng, các bộ nguồn, sàn nâng v.v. để lưu cất phần cứng của một tổ chức, nhưng không có năng lực xử lý. Những dịch vụ khác do những tổ chức chuyên gia như thế cung cấp bao gồm các công ty tư vấn, phối hợp những dịch vụ có những phương tiện tương thích dư thừa v.v..

Lập kế hoạch bất thường cũng phải bao gồm những thủ tục dự phòng và

phương tiện nhớ thay thế cho bộ nhớ từ tính, hồ sơ, các kế hoạch nối mạng hệ thống v.v. *Xem* business resumption planning, cold site, disaster recovery plan, emergency response plan, hot site, risk analysis.

contingency program ***chương trình dự phòng bất ngờ*** Trong an toàn máy tính, các hoạt động và các thủ tục hàng ngày, ví dụ như dự phòng các tệp dữ liệu quan trọng có đủ các yêu cầu về khả năng khôi phục. *So sánh với* contingency plans.

continuity check ***kiểm tra tính liên tục*** Trong truyền thông dữ liệu; việc kiểm tra được tiến hành để xác minh rằng, một đường thông tin tồn tại trong một kênh hoặc các kênh. *Xem* channel.

continuity of operations ***(sự) liên tục của các hoạt động, (sự) hoạt động liên tục*** Trong quản lý rủi ro, việc duy trì những dịch vụ thiết yếu đối với một hệ thông tin sau một sự cố lớn tại một trung tâm thông tin. Sự cố có thể do những nguyên nhân tự nhiên (như hỏa hoạn, lũ lụt hoặc động đất) hoặc do những sự cố có tính toán (như phá hoại ngầm). *Xem* contingency plans.

continuous synchronization ***đồng bộ hóa liên tục*** Trong an toàn truyền thông, một kỹ thuật xáo trộn tiếng nói trong đó, thông tin đồng bộ hóa cần thiết để giải mã thông báo nhận được được truyền đi liên tục hoặc cách quãng trong suốt thời gian truyền thông báo. *So sánh với* initial synchronization. *Xem* voice scrambling.

continuous wave ***sóng liên tục*** Trong truyền thông dữ liệu, chỉ phương pháp truyền trong đó sóng mang không đổi được bật và tắt theo các mẫu biểu diễn tín hiệu.

control cabinet ***phòng kiểm soát, phòng điều khiển*** Trong an toàn vật lý, thiết bị ở trung tâm nhận và giải thích các tín hiệu báo động từ một vùng bảo vệ và giám sát các tuyến báo động. Thiết bị sẽ chứa các bộ nguồn, các rơle, các bộ khuếch đại v.v. cần thiết. *Xem* alarm line.

control character ***ký tự điều khiển*** Trong mã hóa, ký tự mà sự xuất hiện của nó ở một ngữ cảnh riêng sẽ khởi phát một tác động điều khiển, ví dụ như ký tự trở về đầu dòng ở máy in.

control flow analysis ***phân tích luồng điều khiển*** Trong an toàn máy tính, phương pháp phân tích tĩnh, kiểm tra cấu trúc điều khiển của các chương trình ngôn ngữ bậc cao. Phương pháp này cho phép kiểm tra các chương trình về việc sử dụng chương trình con không đúng và các vi phạm các tiêu chuẩn điều khiển. *Xem* static analysis.

controllable isolation ***cách ly điều khiển được*** Trong an toàn máy tính, sự dùng chung có kiểm soát trong đó phạm vi hoặc lĩnh vực được phép có thể được giảm đối với một tập hợp hay một phạm vi hoạt động nhỏ tùy ý. *Xem* authorization, controlled sharing.

controlled access ***truy nhập có kiểm soát*** *Đồng nghĩa với* access control.

controlled access area ***vùng truy nhập có kiểm soát*** Trong an toàn vật lý, một phần hoặc toàn bộ một môi

trường mà ở đó, tất cả các kiểu và các khía cạnh truy nhập đều được kiểm tra và được kiểm soát. *Xem* controlled area.

controlled accessibility ***khả năng truy nhập kiểm soát được*** *Đồng nghĩa với* access control.

controlled area ***vùng được kiểm soát*** Trong an toàn vật lý, một vùng mà trong đó, bộ phận hoạt động không kiểm soát được sẽ không được phép truy nhập vào thông tin đã phân loại và là vùng được dùng cho mục đích chính là tạo ra sự kiểm soát hành chính, an toàn hoặc vùng đệm có các hạn chế an toàn đối với các vùng ngăn chặn hạn chế. Vùng này có thể được bảo vệ bằng các biện pháp an toàn vật lý như có canh gác hoặc hàng rào.

controlled rounding ***làm tròn có kiểm soát*** Trong an toàn cơ sở dữ liệu, dạng xáo trộn nhỏ căn cứ vào kết quả trong đó, dữ liệu thống kê được làm tròn để tổng các số được làm tròn bằng tổng đã làm tròn của các số. *So sánh với* random rounding, systematic rounding. *Xem* inference control, result based perturbation, perturbation.

controlled security mode ***chế độ an toàn có kiểm soát*** (1) Trong an toàn máy tính, chế độ hoạt động trong đó, các kiểm soát an toàn nội bộ ngăn chặn sự tiết lộ do sơ suất. Các kiểm soát nhân sự, vật lý và hành chính ngăn cản những ý đồ truy nhập không được phép. Hệ thống có thể có cả những người sử dụng truy nhập hệ thống không có cả mức thông (mức truy nhập được phép) an toàn lẫn nhu cầu cần biết đối với toàn bộ thông tin đã phân loại trong hệ thống. Truy nhập sẽ giới hạn ở những người sử dụng có mức thông an toàn tối thiểu nhỏ hơn mức phân loại cao nhất của thông tin đã xử lý một cấp. *Xem* administrative security, need-to-know, physical security. (2) Trong an toàn máy tính, chế độ hoạt động thuộc một kiểu chế độ an toàn nhiều cấp trong đó, một mức tin cậy hạn chế hơn được đặt vào cơ sở phần cứng/phần mềm của hệ thống, với các hạn chế kết quả về các mức phân loại và các mức thông (mà có thể được hỗ trợ). (3) Trong an toàn máy tính, một hệ ADP vận hành ở trong chế độ an toàn có kiểm soát khi ít nhất một cá nhân nào đó (người sử dụng) truy nhập hệ thống không có mức thông an toàn cũng như nhu cầu cần biết đối với toàn bộ tư liệu đã phân loại nằm trong hệ ADP. Tuy nhiên, sự tách riêng và sự kiểm soát người sử dụng lẫn tư liệu đã phân loại trên cơ sở mức thông an toàn và mức phân loại an toàn tương ứng về căn bản không thuộc sự kiểm soát của hệ điều hành như ở chế độ an toàn nhiều mức. *Xem* ADP, multilevel security mode, need-to-khow classification, clearance.

controlled sharing ***phân chia có kiểm soát*** Trong an toàn máy tính, điều kiện tồn tại khi sự kiểm soát truy nhập được áp dụng cho tất cả những người sử dụng và các thành phần của hệ thống ADP dùng chung tài nguyên. *Xem* access control, ADP, resource sharing.

controlled space ***không gian được kiểm soát*** Trong an toàn vật lý, không gian ba chiều bao quanh thiết bị

xử lý thông tin an ninh quốc gia mà bên trong đó những cá nhân không được phép sẽ: (*a*) bị từ chối tiếp cận không bạn chế và (*b*) vào có hộ tống bởi nhân sự được phép hoặc dưới sự giám sát liên tục bằng vật lý hoặc điện tử. *Xem* control zone.

controller ***bộ điều khiển*** Trong truyền thông dữ liệu, thiết bị có thể chứa một chương trình nhớ sẵn, hướng dẫn sự truyền dữ liệu trong mạng.

control mode ***chế độ điều khiển*** Trong truyền thông dữ liệu, trạng thái cần thiết đối với mọi đầu cuối trên một tuyến cho phép diễn ra các tác động điều khiển tuyến hoặc sự lựa chọn đầu cuối.

control panel ***bảng điều khiển*** *Xem* control cabinet.

control station ***trạm điều khiển*** Trong truyền thông, trạm trên mạng chịu trách nhiệm về các thủ tục điều khiển, ví dụ như hỏi vòng, lựa chọn, khôi phục và về khôi phục từ những tình huống bất bình thường như tranh chấp.

control token ***thẻ bài điều khiển, mã điều khiển*** Trong truyền thông dữ liệu, mẩu bit được chuyền quanh một mạng cục bộ nhằm mục đích điều khiển. Một nút bất kỳ khi nhận thẻ bài điều khiển có thể loại bỏ nó khỏi mạng, gửi thông báo và sau đó chuyển tiếp thẻ bài điều khiển. *So sánh với* daisy chain, message slot. *Xem* local area network.

control vector ***vectơ điều khiển*** Trong quản lý khóa, biến mật mã không mật, dùng trong kiến trúc mật mã thông thường của IBM để điều khiển việc sử dụng khóa. Vectơ điều khiển bao gồm một trường 64 bit, 128 bit hoặc > 128 bit cung cấp thông tin chi tiết được kết hợp với khóa mật mã, hoặc một biến mật mã tổng quát. Bộ (C, K) bao gồm vectơ điều khiển và khóa kết hợp K được thiết kế sao cho, việc xử lý mật mã liên quan tới khóa K chỉ có thể được thực hiện nếu xử lý có yêu cầu là được phép bởi vectơ điều khiển.

Vectơ điều khiển được cung cấp trong bản gốc và do đó có thể được thông dịch bên ngoài phần cứng mật mã chuyên dụng. Tuy nhiên, nó phải được ghép với khóa, hoặc trong trường hợp tổng quát, ghép với biến mật mã, sao cho một vectơ điều khiển khác không thể thay thế được cho giá trị ban đầu. Điều này có thể đạt được bằng cách kết hợp vectơ điều khiển với khóa mã khóa độ dài gấp đôi — KK, dùng để bảo vệ K trong bộ nhớ hoặc khi truyền. Hoặc là mã xác thực dựa trên các giá trị của cả C lẫn K có thể gắn liền với vectơ điều khiển.

Phương pháp kết hợp vectơ điều khiển với khóa mã hóa KK liên quan tới việc tạo ra hàm băm 128 bit của vectơ điều khiển. Trong trường hợp cấu trúc dữ liệu 64 bit, vectơ điều khiển được ghép với chính nó và sau đó trường mở rộng hai bit được thiết lập để chỉ báo rằng, vectơ điều khiển đã lấy từ trường 64 bit. Đối với vectơ điều khiển 128 bit, hàm băm là hàm đồng nhất là khi đó, trường mở rộng được thiết lập để chỉ báo rằng, cấu trúc dữ liệu ban đầu là 128 bit. Hàm băm mật mã được dùng cho các cấu trúc dữ liệu quá 128 bit nhằm tạo ra trường 128 bit và trường

mở rộng lại được thiết lập để chỉ báo rằng, cấu trúc dữ liệu ban đầu có độ dài vượt quá 128 bit. Kết quả của các phép toán hàm băm thảo luận ở trên sau đó được cộng modulo 2 với khóa mã khóa DES KK; khóa 128 bit kết quả được sử dụng để mã hóa khóa K.

Như vậy, nếu một vectơ điều khiển bất hợp pháp được cung cấp với khóa K, thì khóa mã khóa hình thành bằng phép cộng mudulo của KK với vectơ điều khiển đã băm sẽ không tương ứng với khóa ban đầu dùng để mã hóa K và phép toán giải mã cuối cùng sẽ tạo ra giá trị sai của K. *So sánh với* tagged keys. *Xem* common cryptographic architecture, cryptographic variable, DES, key encrypting key.

control zone ***vùng kiểm soát*** Trong an toàn vật lý, vùng không gian có bán kính biểu thị theo fut bao quanh thiết bị mà được dùng để xử lý thông tin nhạy cảm và nằm dưới sự kiểm soát vật lý và kỹ thuật, đủ để ngăn ngừa sự thâm nhập không được phép hoặc sự thất thoát. *Xem* compromise, controlled space, sensitive information. *Đồng nghĩa với* security perimeter.

Convention on Mutual Administrative Assistance in Tax Matters ***Công ước hỗ trợ hành chính lẫn nhau trong các vấn đề về thuế*** Trong lập pháp, thỏa thuận giữa các nước cho phép trao đổi tự động dữ liệu về thuế mà không cần sự tán thành của chủ thể dữ liệu. *Xem* data protection, data subject.

conversation ***hội thoại, đàm thoại*** Trong truyền thông dữ liệu, sự trao đổi qua lại thông tin giữa hai hệ thống hoặc hai người sử dụng hệ thống.

converter ***bộ chuyển đổi (mã)*** *Xem* code conversion.

cookie monster ***mã "con quỷ bánh bao"*** Trong an toàn máy tính, một dạng mã ác ý tạo ra hình "con quỷ bánh bao" xuất hiện ở các màn hình đầu cuối máy tính, cùng với dòng chữ "Ta muốn một chiếc bánh bao". Hình ngốn dần văn bản hiện hình cho tới khi người sử dụng rõ "Cookie" (bánh bao) ở bàn phím đầu cuối. *So sánh với* flying dutchman. *Xem* malicious code.

Co-ordinated Universal Time ***giờ quốc tế phối hợp*** Thang thời gian do Viện giờ quốc tế (International Time Bureau) duy trì để lập cơ sở của việc phổ biến phối hợp các tín hiệu tần số và thời gian chuẩn. *Đồng nghĩa với* Greenwich Mean Time.

coprime ***nguyên tố cùng nhau*** Trong lý thuyết số, tính chất của một cặp số nguyên có ước số chung lớn nhất là một (ví dụ, 8 và 15). *Xem* prime number. *Đồng nghĩa với* mutually prime.

coprocessor ***bộ đồng xử lý*** Trong tin học, dạng đa xử lý trong đó hai hoặc nhiều bộ xử lý dùng chung cùng dòng lệnh. Kỹ thuật này cho phép các bộ xử lý được thiết kế cho một khoang riêng các nhiệm vụ và do đó thực hiện chức năng phân cho chúng với hiệu suất cao. *Xem* processor.

copy protected ***(được) khóa chống sao chép, (được) bảo vệ chống sao chép*** Trong bảo vệ phần mềm, chỉ các phần mềm phân phối trên đĩa mềm được làm cho "không thể sao chép được"

nhờ biện pháp vật lý. *Xem* copy protection, software protection, unprotect.

copy protection ***khóa chống sao chép, bảo vệ chống sao chép, cấm sao chép*** Trong bảo vệ phần mềm, các kỹ thuật dùng để ngăn chặn sao chép bất hợp pháp phần mềm. Thuật ngữ này được đặt ra sai vì mọi chương trình đều có thể được sao lại nhưng với một số biện pháp bảo vệ làm nó có thể không thể chạy được sau khi đã sao. *So sánh với* execute protection.

copyright ***bản quyền*** (1) Tài liệu hợp pháp thiết lập quyền sở hữu một sáng tạo nghệ thuật (ví dụ, cuốn phim, tác phẩm văn học, tác phẩm âm nhạc). (2) Trong phần mềm và xuất bản, quyền ngăn cản sao chép. Người giữ bản quyền có quyền ngăn cản sao chép dạng trong đó ý tưởng được biểu thị nhưng không phải bản thân ý tưởng. Các chương trình trình máy tính được bảo vệ bằng cùng những luật pháp bảo vệ các tác phẩm văn học ở những nước có luật pháp về bản quyền. Tuy nhiên, sử dụng ý tưởng hoặc một thuật toán thu được bằng cách nghiên cứu mã nguồn của một chương trình có bản quyền tự nó không phải là sự vi phạm bản quyền.

cord trap ***bẫy dây*** Trong an toàn vật lý, dụng cụ đơn giản phát hiện kẻ xâm nhập, gồm một sợi dây căng ngang vùng được bảo vệ và nối với các chuyển mạch ở mỗi đầu. Dây dịch chuyển kích hoạt báo động.

core ***lõi, lõi sợi quang*** Trong truyền thông, phần ở giữa của sợi quang dẫn phần chính ánh sáng. *Xem* fiber optics.

coroutine ***đồng thường trình, đồng thủ tục*** Trong lập trình, thủ tục mà có thể chuyển điều khiển sang thường trình bất kỳ khác, tự treo và tiếp tục chạy sau đó. *So sánh với* subroutine. *Xem* procedure.

corporate security policy ***chính sách an toàn tập thể*** Trong an toàn thông tin, tập hợp các đạo luật, các quy tắc và các thủ tục điều chỉnh cách thức quản lý, bảo vệ và phân phối tài sản chứa thông tin nhạy cảm trong một tổ chức người sử dụng.

corrective maintenance ***bảo trì có hiệu chỉnh*** Trong tin học, hoạt động phát hiện, cô lập và hiệu chỉnh các sự cố sau khi xuất hiện. *So sánh với* preventive maintenance.

correctness ***tính đúng đắn*** Trong an toàn máy tính, theo nghĩa chặt chẽ, tính chất của một hệ thống được đảm bảo như kết quả của các hoạt động xác minh hình thức. Tính đúng đắn không phải là một tính chất tuyệt đối của một hệ thống, mà nó ngụ ý tính nhất quán chung của một đặc tả và thực hiện nó. *Xem* formal proof, formal verification, proof of program correctness, verification.

correctness proof ***chứng minh tính đúng đắn*** Trong an toàn máy tính, chứng minh toán học về tính nhất quán giữa bản đặc tả (tính năng kỹ thuật) và việc thực hiện nó. Chứng minh này có thể áp dụng ở mức mô hình an toàn tới đặc tả hình thức, ở mức đặc tả hình thức tới mã HOL (logic bậc cao), ở mức trình biên dịch hoặc ở mức phần cứng. Ví dụ, nếu một hệ thống có thiết kế và cài đặt đã kiểm chứng thì tính đúng

đắn chung của có phụ thuộc vào tính đúng đắn của bộ biên dịch và phần cứng. Một khi hệ thống được chứng minh là đúng đắn thì có thể hy vọng nó được thực hiện như đã đặc tả, nhưng không nhất thiết như đã dự liệu nếu các bản đặc tả không đầy đủ hoặc không thích hợp. *Xem* formal security policy model, proof of program correctness, verification.

correct refinement ***làm mịn đúng*** Trong an toàn thông tin, sự làm mịn một hàm đã mô tả ở một mức trừu tượng được coi là đúng nếu toàn bộ các tác dụng đã mô tả ở mức trừu tượng thấp hơn sẽ thể hiện ít nhất là tất cả các tác dụng mô tả ở mức trừu tượng cao hơn. *Xem* information technology security evaluation criteria.

correspondent banks ***(các) ngân hàng đại lý*** Trong hoạt động ngân hàng, các ngân hàng trao đổi các danh sách chữ ký hoặc các mã ủy quyền, hoặc cả hai, hoặc cam kết trao đổi các dịch vụ, hoặc có một tài khoản hoặc các tài khoản của nhau, hoặc tổ hợp bất kỳ của những cái đó.

corrupt data ***dữ liệu sai lạc*** Trong an toàn dữ liệu, dữ liệu bị sửa đổi ngẫu nhiên hay ác ý (ví dụ nối trộm chủ động dây). *Xem* data integrity, active wiretapping.

corruption ***sai lạc, hư hỏng*** Trong của hệ thống nhớ và truyền thông dữ liệu, quá trình khiến cho dữ liệu bị thay đổi theo cách không mong muốn hoặc trong khi truyền hoặc trong khi lưu giữ (ví dụ, đĩa mềm hư hỏng). *Xem* floppy disk.

cost-risk analysis ***phân tích chi phí - rủi ro*** Trong quản lý rủi ro, sự đánh giá các chi phí cho rủi ro hoặc mất mát hoặc hư hại tiềm ẩn của dữ liệu trong hệ thống xử lý dữ liệu tự động mà không cần bảo vệ dữ liệu chống các chi phí bảo vệ dữ liệu. *Xem* automatic data-processing system, compromise, risk analysis.

COTS ***có bán, bán chạy*** Trong tin học, viết tắt của Commercial off The Shelf (có sẵn để bán), chỉ phần mềm có thể thu được từ một hãng bán.

counter ***bộ đếm*** Trong mật mã học, cơ cấu đếm tăng dùng giữa hai bên để kiểm soát các quá trình phân phối khóa liên tiếp. *Xem* key management.

countermeasure ***biện pháp đối phó*** (1) Trong quản lý rủi ro, phương pháp bất kỳ: vật lý, phần cứng, phần mềm, nhân sự, thủ tục v.v. dùng để đối phó lại một mối hiểm họa đối với hệ thống. *Xem* threat. (2) Trong an toàn thông tin, biện pháp an toàn kỹ thuật hoặc phi kỹ thuật đóng góp vào mục đích an toàn của mục tiêu đánh giá. *Xem* information technology security evaluation criteria, target of evaluation.

counterparty ***(bên) đối tác*** Trong hoạt động ngân hàng, khách hàng mà ngân hàng ký kết một giao dịch. *Xem* counterparty group.

counterparty group ***nhóm đối tác*** Trong hoạt động ngân hàng, việc kết hợp các đối tác thành những nhóm chung, ví dụ như công nghiệp, nông thôn. *Xem* counterparty.

counterparty risk ***rủi ro đối tác*** *Xem* counterparty. *Đồng nghĩa với* credit risk.

country of domicile ***nước sở tại*** Trong hoạt động ngân hàng, nước mà ở đó khách hàng có cơ sở. *Đồng nghĩa với* country of residence.

country of residence ***nước cư trú*** *Đồng nghĩa với* country of domicile.

cover payment ***trả bảo lãnh*** Trong hoạt động ngân hàng, việc hoàn trả của một ngân hàng đại lý cho một khoản tiền trả. *Xem* correspondent banks.

covert ***ngầm, che giấu*** Được nguy trang.

covert channel ***kênh ngầm, kênh bí mật*** Trong an toàn máy tính, kênh truyền thông cho phép một quá trình chuyển thông tin vi phạm chính sách an toàn hệ thống. Một kênh ngầm thường truyền thông bằng cách khai thác một cơ cấu không nhằm mục đích truyền thông. *So sánh với* covert channel. *Xem* covert storage channel, covert timing channel, security policy.

cover time ***thời gian bảo vệ*** Trong an toàn dữ liệu, khoảng thời gian được tin là mã pháp sẽ chống lại được một cuộc tấn công cụ thể. *Xem* minimal cover time.

covert storage channel ***kênh nhớ ngầm, kênh nhớ bí mật*** Trong an toàn máy tính, kênh ngầm liên quan tới việc một quá trình ghi trực tiếp hoặc giám tiếp một vị trí nhớ và quá trình khác đọc trực tiếp hoặc gián tiếp vị trí nhớ. Các kênh nhớ ngầm thường liên quan tới tài nguyên hữu hạn (ví dụ, các liên cung trên đĩa) được chia sẻ bởi hai đối tượng ở các mức an toàn khác nhau. *So sánh với* covert timing channel. *Xem* covert channel.

covert timing channel ***kênh định thời ngầm, kênh định thời bí mật*** Trong an toàn máy tính, kênh bí mật trong đó, một quá trình báo hiệu thông tin cho quá trình khác bằng cách điều chỉnh việc sử dụng các tài nguyên hệ thống của nó (ví dụ, thời gian bộ xử lý trung tâm) theo cách sao cho thao tác đó ảnh hưởng tới thời gian đáp ứng thực mà quá trình thứ hai quan sát được. *So sánh với* covert storage channel. *Xem* covert channel.

CPP *Xem* Certified Protection Professional.

CPU *Xem* central processing unit.

cracker ***cracơ, kẻ phá khóa*** Trong lập pháp, hackơ chuyên về khắc phục các hệ thống bảo vệ phần mềm. *So sánh với* crasher. *Xem* hacker.

CRAMM ***hệ CRAMM*** Trong quản lý rủi ro, hệ phương pháp luận phân tích rủi ro. *Xem* risk analysis methodologies.

crash ***tai biến*** Trong an toàn máy tính, sự phá hỏng do sự cố phần mềm hoặc phần cứng gây ra. Xem crasher.

crasher ***kẻ phá hoại*** Trong lập pháp, hackơ cố ý gây cản trở nghiêm trọng cho hoạt động của hệ máy tính. *So sánh với* cracker. *Xem* hacker.

CRC *Xem* cyclic redundancy check.

credentials ***dữ liệu ủy nhiệm*** (1) Trong xác thực, dữ liệu được truyền đi để thiết lập danh tính đã yêu cầu về một thực thể. (2) Trong kiểm soát truy nhập, dữ liệu được chuyển từ thực thể này sang thực thể khác, dùng để thiết lập các quyền truy nhập của thực thể gửi. *Xem* access right.

credit advice ***giấy báo có*** Trong hoạt động ngân hàng, giấy do ngân hàng phục vụ tài khoản báo về khoản có cho tài khoản của người giữ tài khoản đó (chủ tài khoản). *Xem* account servicing bank.

credit card ***thẻ tín dụng*** Trong hoạt động ngân hàng, thẻ cho phép người mang thẻ mua hàng hóa hoặc dịch vụ từ rất nhiều loại cửa hàng và sau đó hoàn trả cho một cơ sở tài chính thích hợp trên cơ sở định kỳ. *So sánh với* debit card.

credit party ***bên có*** Trong hoạt động ngân hàng, bên được vào sổ có hoặc được trả bởi ngân hàng thu. *So sánh với* beneficiary, debit party.

credit risk ***rủi ro tín dụng*** Trong hoạt động ngân hàng, rủi ro sinh ra qua khả năng của đối tác thực hiện các cam kết trả tiền của họ. *Xem* counterparty. *Đồng nghĩa với* counterparty risk.

criteria ***chuẩn cứ, tiêu chuẩn, tiêu chí*** Trong an toàn thông tin, chỉ các định nghĩa về các tính chất và các ràng buộc mà hệ chức năng và sự đảm bảo hệ thống phải đáp ứng. *Xem* ITSEC, TCSEC.

critical data processing workload ***lượng công việc xử lý dữ liệu tới hạn*** Trong quản lý rủi ro, phần trong toàn bộ khối lượng công việc sẽ sinh ra mất mát nghiêm trọng nếu bị hỏng trong một khoảng thời gian xác định. *Xem* critical functions, criticality, critical processing.

critical functions ***(các) chức năng tới hạn*** Trong các hoạt động, các chức năng quan trọng đối với các hoạt động của một tổ chức và có thể, đối với sự sống còn của nó. *Xem* critical data processing workload, criticality, critical processing.

criticality ***tính tới hạn*** Trong an toàn máy tính, khái niệm liên quan tới nhiệm vụ mà hệ thống tự động hóa hỗ trợ và mức độ mà nhiệm vụ đó phụ thuộc vào hệ thống. Mức độ phụ thuộc này tương ứng với sự tác động lên nhiệm vụ trong trường hợp từ chối phục vụ, sửa đổi hoặc phá hủy dữ liệu hoặc phần mềm. *Xem* critical data processing workload, critical processing.

critical processing ***xử lý tới hạn, xử lý quan trọng*** Trong an toàn máy tính, các ứng dụng được xác định như có một tầm quan trọng trong hoạt động của một tổ chức mà chỉ có thể chấp nhận mất chút ít hoặc không mất tính sẵn sàng của chúng. *So sánh với* discretionary processing. *Xem* critical data processing workload, critical functions.

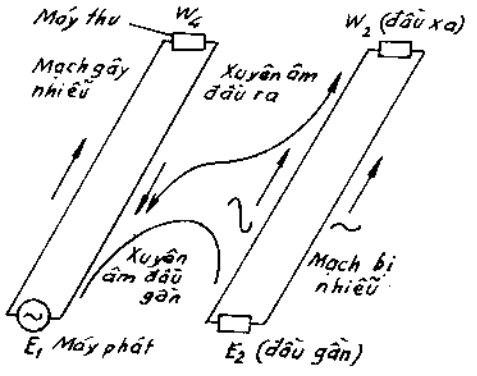
critical technology ***công nghệ tới hạn, công nghệ quan trọng*** các công nghệ bao gồm (*a*) các mảng bí quyết kỹ thuật thiết kế và sản xuất (kể cả các dữ liệu kỹ thuật); (*b*) sản xuất chủ chốt, thanh tra và thiết bị thử nghiệm; (*c*) vật liệu chủ chốt và (*d*) các hàng hóa kèm theo bí quyết kỹ thuật vận hành, ứng dụng hoặc bảo trì tinh vi mà có thể đóng góp đáng kể vào tiềm năng quân sự của bất kỳ quốc gia hoặc nhóm quốc gia nào và có thể tỏ ra bất lợi cho an ninh của Hoa Kỳ. *Xem* keystone equipment, know-how. *Đồng nghĩa với* Military Critical Technology.

CRL *Xem* certificate revocation list.

cross alarm ***báo động chéo*** *Đồng nghĩa với* closed circuit alarm.

crossfire ***nhiễu cảm ứng*** *Đồng nghĩa với* crosstalk.

crosstalk ***xuyên âm*** Trong truyền thông, sự chuyển không mong muốn năng lượng từ kênh truyền thông này sang kênh truyền thông khác. *Đồng nghĩa với* crossfire.



crosstalk: *xuyên âm.* Xuyên âm này sinh ở đoạn ngắn của hai mạch song song. Dây dẫn ở gần hơn với mạch gây nhiễu có điện áp xuyên âm lớn hơn so với dây dẫn ở xa hơn; hiệu điện áp là hiệu dụng ở các đầu nối E_2 và W_2.
Năng lượng ở mạch nhiễu được giả định truyền từ đông sang tây.

cross zone ***vùng chéo, vùng giao nhau*** (1) Trong an toàn vật lý, mạch báo cháy cần các tín hiệu từ hai bộ cảm biến khác nhau để kích hoạt. (2) Trong an toàn vật lý, Sơ đồ mạch điện thế kết hợp các đầu vào tín hiệu báo động nhằm tạo ra những đầu ra xác định. *Xem* combined alarms.

cryptanalysis ***phân tích mật mã, mã thám*** (1) Trong mật mã học, việc phân tích một hệ thống mật mã và/hoặc những đầu vào và đầu ra của nó để rút ra các biến mật và/hoặc các dữ liệu nhạy cảm kể cả bản gốc. *Xem* cleartext. (2) Trong mật mã học, các bước và các thao tác được thực hiện trong việc biến đổi các thông báo đã mã hóa thành bản gốc mà ban đầu không cần biết khóa dùng trong thuật toán mã hóa. *Xem* chosen plaintext, ciphertext only, encrypt, encryption algorithm, key, known plaintext, plaintext.

cryption ***quá trình mật mã, thao tác mật mã*** Trong mật mã học, quá trình mã hoặc giải mã. *Xem* decrypt, encrypt.

cryptogram ***tài liệu mã hóa, bản mã, điện mật*** Trong lập mã, một thông báo đã được mã hóa, *Đồng nghĩa với* ciphertext.

cryptogram space ***không gian bản mã*** Trong lập mã, toàn bộ tập hợp các thông báo mã mà có thể được tạo ra bằng cách mã tất cả các thông báo trong không gian thông báo bằng tất cả các khóa trong không gian khóa. *So sánh với* message space, key space.

cryptographic algorithm ***thuật toán mật mã*** Trong an toàn dữ liệu, tập hợp các quy tắc xác định thủ tục cần để mã và giải mã dữ liệu. *Xem* cipher.

cryptographic API ***API mật mã*** Trong lập mã, giao diện lập trình ứng dụng (API) mật mã - một giao diện giữa các chương trình ứng dụng và các dịch vụ mật mã, cho phép các chương trình ứng dụng gọi các dịch vụ mật mã theo một khuôn thức xác định. Nó cho phép

các chương trình ứng dụng gọi ra các dịch vụ mật mã ở mức độ nào đó theo những khuôn lệnh xác định trước và do đó, giảm nhẹ nhiều chi tiết cài đặt mật mã, quản lý khóa v.v. cho người lập trình ứng dụng. API mật mã cũng tăng cường khả năng liên vận hành và tính linh hoạt của các chương trình ứng dụng. *Xem* common cryptographic architecture.

cryptographic authentication ***xác thực mật mã*** Trong công việc xác nhận, sự sử dụng các kỹ thuật liên quan đến mã hóa để tiến hành sự xác nhận. *Xem* message authentication.

cryptographic bit stream ***dòng bit mật mã*** Trong an toàn dữ liệu, dòng các bit được kết hợp với bản gốc để tạo ra bản mã trong phép mã dòng. *Xem* stream cipher. *Đồng nghĩa với* key stream, running key.

cryptographic checkfunction ***hàm kiểm tra mật mã*** Trong lập mã, thông tin được rút ra bằng cách thực hiện quá trình mật mã trên dữ liệu; do đó nó là kết quả của một hàm toán học của khóa và dữ liệu *Xem* cryptographic key, MAC.

cryptographic checksum ***tổng kiểm tra mật mã*** Trong lập mã, tổng kiểm tra được tính toán có sử dụng khóa mật. *Xem* checksum, MAC.

cryptographic checkvalue ***giá trị kiểm tra mật mã*** Trong lập mã, thông tin được rút ra nhờ thực hiện phép biến đổi mật mã trên một đơn vị dữ liệu.

cryptographic control ***kiểm soát mật mã*** Trong lập mã, việc sử dụng các kỹ thuật mật mã để bảo vệ thông tin khi truyền qua một tuyến liên kết hoặc khi được nhớ trong máy tính. *Xem* wiretapping.

cryptographic device ***bộ phận mật mã, công cụ mật mã*** Trong mật mã học, một thực hiện thủ tục mật mã.

cryptographic equipment ***thiết bị mật mã*** Trong quản lý khóa, thiết bị thực hiện các chức năng mật mã (ví dụ như mã hóa, xác thực, sinh khóa). *Xem* authentication, cryptographic facility, encryption, key generation.

cryptographic facility ***phương tiện mật mã*** Trong quản lý khóa, mođun chống làm giả chứa một thiết bị có thể thực hiện một thuật toán mật mã, ví dụ như DES, và còn chứa bộ nhớ để nhớ một số hữu hạn khóa. Trong một hoạt động điển hình, một khóa dữ liệu được mã theo khóa chính sẽ được đưa vào thiết bị cùng với dữ liệu được mã theo khóa dữ liệu. Khóa cính được giữ trong bộ nhớ không khả biến bên trong thiết bị. Một hoạt động hai giai đoạn đầu tiên sẽ giải mã khóa dữ liệu bằng khóa chính và sau đó, giải mã dữ liệu bằng khóa dữ liệu. Như vậy khóa dữ liệu không bao giờ được lộ ra bên ngoài phương tiện. *Xem* key encrypting key, key management, tamper resistant module. *Đồng nghĩa với* cryptographic equipment.

cryptographic key ***khóa mật mã*** (1) Trong lập mã, một tham số dùng cùng với một thuật toán nhằm mục đích phê chuẩn, xác thực, mã hóa, giải mã, lập hoặc hủy chữ ký. *Xem* authentication, cryptographic algorithm,

decipherment, encipherment, signature construction, signature deconstruction validation. *Đồng nghĩa với* key. (2) Trong mật mã học, tham số (ví dụ như số 64 bit mật đối với DES) dùng bởi quá trình mật mã, làm cho quá trình được xác định hoàn toàn và chỉ những người có khóa đó có thể sử dụng. (3) Trong mật mã học, tham số xác định phép biến đổi từ bản gốc sang bản mã và ngược lại. Một khóa DEA là một tham số 64 bit chứa 56 bit độc lập và 8 bit có thể được dùng như các bit chẵn lẻ. *Xem* ciphertext, DEA, parity bit.

cryptographic key data set ***tập dữ liệu khóa mật mã*** Trong quản lý khóa, tập các khóa được mã bằng các khóa mã khóa và được lưu giữ trong bộ nhớ dự phòng. *Xem* backing storage, key encrypting key.

cryptographic keying material ***tư liệu tạo khóa mật mã*** *Xem* keying material.

cryptographic period ***chu kỳ mật mã*** Trong lập mã, khoảng thời gian xác định, chu kỳ sử dụng hoặc số các biến cố mà trong đó một khóa mật mã sẽ được thay đổi. *Xem* cryptographic key.

cryptographic seal ***con dấu mật mã*** *Xem* digital signature.

cryptographic service message ***thông báo dịch vụ mật mã*** Trong quản lý khóa, thông báo về vận chuyển các khóa hoặc thông tin có liên quan dùng để kiểm soát quan hệ tạo khóa. *Xem* ANSI X9.17 - 1985, cryptographic key, keying relationship, service message.

cryptographic system ***hệ thống mật mã*** (1) Trong lập mã, về mặt hình thức một hệ thống mật mã bao gồm năm thành phần:

- không gian thông báo;
- không gian bản mã;
- không gian khóa;
- họ các phép biến đổi mã;
- họ các phép biến đổi giải mã.

Không gian thông báo bao gồm toàn bộ tập hợp các thông báo có thể được mã hóa v.v.. Phép biến đổi mã hóa sử dụng một khóa mã hóa trong không gian khóa để ánh xạ thông báo trong không gian thông báo lên bản mã trong không gian bản mã, thuật toán giải mã thực hiện phép biến đổi ngược lại bằng khóa giải mã tương ứng.

Nói chung, các hệ thống mật mã phải thỏa mãn các yêu cầu:

- các thuật toán mã hóa và giải mã phải có hiệu lực đối với mọi khóa;
- các hệ thống phải vận hành đơn giản;
- tính an toàn cần phụ thuộc vào tính bí mật của các khóa chứ không phụ thuộc vào tính bí mật của các thuật toán mã hoặc giải mã.

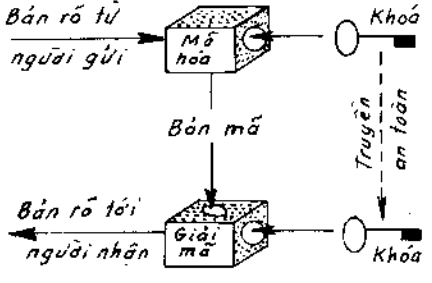
Xem mapping. (2) Trong mật mã học, các tài liệu, cơ cấu, thiết bị và các phương pháp có liên quan vốn được dùng như một khối để cung cấp phương tiện mã hóa (lập mật mã hoặc lập mã) đơn nhất. *Xem* encode, encrypt.

cryptographic throughput factor ***hệ số năng suất mật mã*** Trong lập mã, số đo mức mở rộng thông báo do quá trình đệm thêm vào gây ra. Nó được định nghĩa như tỷ số độ dài theo bit của thông báo trên độ dài tương ứng cũng theo bit của bản mã tương ứng. *Xem* padding.

cryptographic transparency *(độ) trong suốt mật mã* Trong lập mã, một kỹ thuật trong đó, người sử dụng có đặc quyền có thể truy nhập tư liệu mã hóa ở trạng thái đã giải mã mà không cần biết về quá trình giải mã.

cryptographic variable *biến mật mã* Trong lập mã, một tham số của thuật toán mật mã tạo ra sự an toàn có tính chất bí mật của nó, ví dụ như khóa riêng trong một hệ thống mật mã khóa công khai. *Xem* cryptographic key, public key cryptography.

cryptography *phép ghi mật mã, phép lập mã* (1) Trong mật mã học, bộ môn nghiên cứu các nguyên lý, các phương tiện và các phương pháp biến đổi dữ liệu nhằm che giấu nội dung thông tin của nó, ngăn ngừa sự sửa đổi không phát hiện được của nó. (2) Trong mật mã học, nghệ thuật hoặc khoa học nghiên cứu các nguyên lý, các phương tiện và các phương pháp để làm cho bản gốc không thể hiểu được và để biến đổi các thông báo đã mã hành dạng hiểu được. *Xem* encrypt, plaintext. (3) Trong mật mã học, khoa học và sự nghiên cứu cách ghi bí mật. Mật mã là phương pháp ghi bí mật, nhờ đó văn bản gốc được biến đổi thành văn bản mật mã. Quá trình biến đổi văn bản gốc thành văn bản mật mã được gọi là viết mật mã hoặc mã hóa; quá trình ngược lại biến đổi văn bản mật mã thành văn bản gốc được gọi là đọc mã hoặc giải mã. Cả mã hóa lẫn giải mã đều được kiểm soát bằng một hoặc nhiều khóa mật mã.



cryptography: *phép ghi mật mã.* Mã hóa và giải mã.

Phép ghi mật mã cổ điển giữ bí mật cho thông tin gửi qua các kênh mà ở đó có thể có sự nghe lén hoặc chặn bắt các thông báo. Người gửi chọn một mã pháp và khóa mã và, hoặc giao nó trực tiếp cho người nhận hoặc gửi gián tiếp nó quá kênh chậm nhưng an toàn, thường là qua người mang thư tin cẩn. Các thông báo và thông tin trả lời được truyền qua kênh không đảm bảo ở dạng mã.

Hệ mật mã tương tự với tổ hợp khóa chữ bí mật có thể thiết lập lại để khóa an toàn một kéo sắt. Tổ hợp được giữ bí mật và có thể được thay đổi bất cứ khi nào nó bị nghi ngờ là đã rơi vào tay kẻ xấu. Mặc dù những người không được phép biết tập hợp tất cả các khóa hoặc tổ hợp khả dĩ nhưng có thể họ không có khả năng phát hiện ra tổ hợp chính xác với chi phí thời gian và tiền bạc hợp lý. Nỗ lực thử mọi tổ hợp khả dĩ là thước đo độ an toàn của khóa hoặc mật mã.

Phép lập mã hiện đại bảo vệ dữ liệu truyền qua các đường thông tin cao tốc hoặc thông tin lưu giữ trong các hệ

máy tính. Có hai mục tiêu chính: (*a*) tính bí mật để ngăn ngừa sự để lộ dữ liệu không được phép; và (*b*) tính xác thực để ngăn ngừa sửa đổi dữ liệu không được phép. Tính xác thực liên quan tới việc:

- cung cấp danh tính của một cá nhân hay hệ thống;
- cho biết người khởi đầu dữ liệu chính là người có danh tính đã khai báo;
- cung cấp các nội dung của dữ liệu mà không bị thay đổi trái phép.

Các mã pháp hiện đại như tiêu chuẩn mã dữ liệu (DES), FEAL hoặc RSA, tạo ra mức độ an toàn cao trong những điều kiện bình thường, chỉ có thể bị phá vỡ bởi một kẻ tấn công có sự hiểu biết về khóa đang dùng. Nói chung, thuật toán sử dụng để mã/giải mã với các hệ thống mật mã hiện đại đều đã được công bố, nhưng khóa được giữ kín. *Xem* cryptanalysis, cryptographic key, cryptology, data encryption standard, digital signature, key management, public key cryptography, RSA.

crypto-key ***khóa mật mã*** *Đồng nghĩa với* cryptographic key.

cryptology ***mật mã học*** Lĩnh vực bao gồm cả phép lập mã và thám mã. *Xem* cryptanalysis, cryptography.

cryptomanagement ***quản lý mật mã*** Trong lập mật mã, các thủ tục vốn phải được thực hiện và vận hành để đảm bảo rằng, các hệ thống mật mã tạo ra mức độ an toàn cần thiết.

crypto-operation ***thao tác mật mã*** Trong lập mã, sự áp dụng chức năng các phương pháp mật mã. (*a*) Ngoại tuyến: Mã hóa hoặc giải mã được thực hiện như một thao tác độc lập, tách biệt với sự truyền văn bản đã mã, như bằng tay hoặc bằng máy không nối với đường tín hiệu. (*b*) Trực tuyến: Việc sử dụng thiết bị mật mã nối trực tiếp với một đường tín hiệu, thực hiện các quá trình liên tục mã hóa, truyền hoặc thu và giải mã. *Xem* off line crypto-operation, on line crypto-operation.

cryptoperiod ***chu kỳ khóa mã, thời hạn khóa*** Trong quản lý khóa, khoảng thời gian trong đó một khóa cụ thể được phép sử dụng, hoặc khoảng thời gian các khóa dành cho một hệ thống nào đó có thể vẫn còn tác dụng. *Xem* cryptographic key.

cryptosystem ***hệ thống mật mã*** *Xem* cryptographic system.

cryptotext ***bản mã*** *Đồng nghĩa với* ciphertext.

CSDC *Xem* circuit switched digital circuitry.

CSM ***CSM*** Viết tắt của Cryptographic Service Message (thông báo dịch vụ mật mã). *Xem* ANSI X9.17 - 1985, cryptographic service message.

CSMA-CD *Xem* carrier sense multiple access-collision detection.

CSTVRP ***chương trình CSTVRP*** Viết tắt của Computer Security Technical Vulnerability Reporting Program (chương trình báo cáo điểm yếu kỹ thuật an toàn máy tính).

CTS *Xem* clear to send.

CUG *Xem* closed user group.

current utilization ***lượng tiền sử***

dụng hiện thời, lượng tiền lưu chuyển hiện tại Trong hoạt động ngân hàng, lượng tiền thực tế luân chuyển hiện thời; lượng tiền đó sẽ là lượng ban đầu được rút ra (cam kết ban đầu nếu rút hoàn toàn) trừ đi mọi khoản thanh toán lại nhận được. *Đồng nghĩa với* loan utilization.

Curse Boot ***virut Course Boot*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động ở đĩa mềm và đĩa cứng, làm sai lạc cung khởi động và ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

custodian of data ***người trông coi dữ liệu*** Trong an toàn dữ liệu, một cá nhân hoặc một nhóm người được giao phó việc trông nom và chịu trách nhiệm về sự an toàn của những dữ liệu xác định.

customer ***khách hàng*** (1) Trong an toàn máy tính, một người hoặc một tổ chức nhận các sản phẩm mà một hệ thống tự động hóa tạo ra nhưng không được truy nhập vào hệ thống. *So sánh với* user. *Xem* access. (2) Trong hoạt động ngân hàng, cá nhân khởi động một giao dịch.

customer code ***mã khách hàng*** Trong an toàn vật lý, mã dùng trong các hệ thống báo động hoặc kiểm soát truy nhập để nhận dạng một bộ phận thiết bị hoặc khách hàng. *Xem* access control.

customer type ***kiểu khách hàng*** Trong hoạt động ngân hàng, nhóm tổ chức ngang hàng mà khách hàng thuộc vào, ví dụ như ngân hàng tư nhân, ngành phục vụ nhà nước.

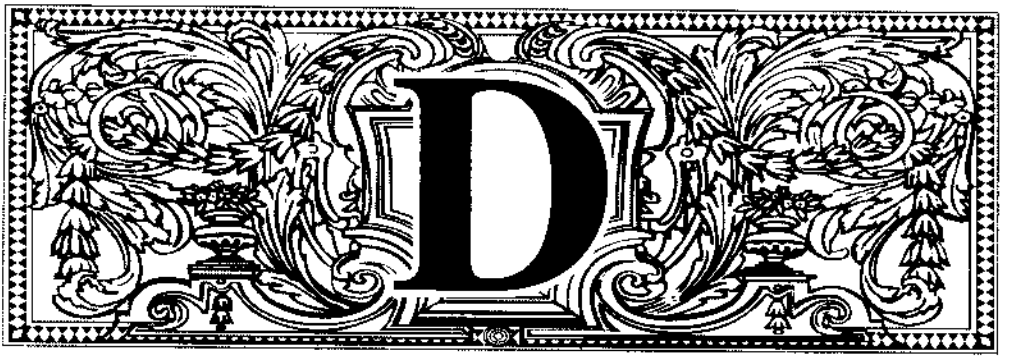
cutoff frequency ***tần số cắt*** Trong điện tử học, các giới hạn tần số trên hoặc dưới của dải tần hữu dụng của một bộ lọc. *Xem* filter.

CVV *Xem* card verification value.

cyclical band shift invertor ***bộ đảo dịch dải tần theo vòng*** Trong an toàn truyền thông, một dạng bộ đảo dịch dải tần trong đó, các tần số sóng mang được chọn nhờ đầu ra của máy sinh số giả ngẫu nhiên. *Xem* band shift invertor, voice scrambling.

cyclic code ***mã chu trình, mã tuần hoàn, mã xyclic*** *Xem* Gray code.

cyclic redundancy check ***kiểm dư vòng, phương pháp CRC*** Trong mã hóa, phương pháp để phát hiện các lỗi trong khi truyền hoặc chuyển dữ liệu nhờ sử dụng mã đa thức và một ký tự kiểm vòng. *Xem* error detection code, polynomial, code.



D *Xem* Division D.

DAA ***DAA*** (1) Trong lập mã, viết tắt của data authentication algorithm (thuật toán xác thực dữ liệu). *Xem* authentication. (2) Trong an toàn máy tính, *xem* Designated Approving Authority. (3) Trong truyền thông, *xem* data access arrangement.

DAC ***DAC*** (1) Viết tắt của Data Authentication Code (mã xác thực dữ liệu). *Đồng nghĩa với* MAC. (2) Trong kiểm soát truy nhập, *xem* discretionary access control.

daemon ***daemon*** (1) Trong tin học, quá trình tạm treo chờ một loại biến cố nào đó xuất hiện, khi đó nó được tự động kích hoạt, thực hiện công việc của nó và hoặc kết thúc hoặc tự tạm treo chờ biến cố tiếp theo. *So sánh với* demon, Trojan Horse. *Xem* Morris worm. (2) Trong an toàn máy tính, *đồng nghĩa với* internal subject.

daisy chain ***xích vòng, nối kết mạng vòng*** Trong truyền thông dữ liệu, một kỹ thuật ở mạng cục bộ để chuyển giấy phép truyền cho một nút; các đường dây chuyên dụng được dùng để chuyển thông tin điều khiển từ nút này sang nút tiếp theo. *So sánh với* control token, message slot. *Xem* local area network.

Dark Avenger ***virut Dark Avenger*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

DARPA ***cơ quan DARPA*** Viết tắt của Defense Advanced Research Projects Agency (Cơ quan dự án nghiên cứu tiên tiến), ban đầu là ARPA. *Xem* ARPA.

DASD ***thiết bị DASD*** Trong tin học, viết tắt của direct access storage device (thiết bị nhớ truy nhập trực tiếp).

data ***dữ liệu*** (1) Thông tin với biểu diễn vật lý xác định. (2) Biểu diễn các

sự kiện, khái niệm, thông tin hoặc các lệnh ở dạng thích hợp cho truyền thông, thông dịch hoặc cho xử lý bởi con người hoặc bởi hệ thống thông tin tự động hoá (AIS). (3) Các chương trình, tệp hoặc thông tin khác lưu giữ trong, hoặc xử lý bởi một hệ máy tính. (4) Thông tin với biểu diễn xác định (cách dùng từ ngữ lỏng lẻo để chỉ mọi hoặc toàn bộ thông tin mà có thể được máy tính tạo ra, xử lý, lưu giữ. (5) Trong lập pháp, theo định nghĩa bởi Luật bảo vệ dữ liệu Anh 1984, thông tin ghi dưới dạng có thể xử lý được bởi thiết bị vận hành tự động để đáp lại các lệnh đưa ra cho mục đích đó. *Xem* data protection. (6) Biểu diễn các sự kiện, khái niệm hoặc các lệnh theo cách hình thức hóa để cho nó có thể được truyền thông, thông dịch hoặc xử lý bởi con người hoặc các phương tiện tự động. *So sánh với* information.

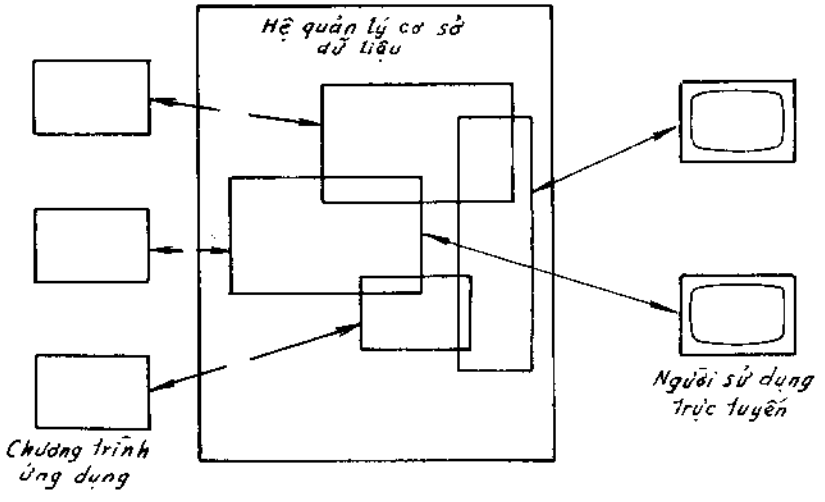
data above voice ***hệ dữ liệu (bên) trên tiếng nói*** Trong truyền thông dữ liệu, hệ để mang các dữ liệu số ở một phần phổ vô tuyến vi ba bên trên tần số dùng cho truyền tiếng nói. *So sánh với* data in voice, data under voice.

data access arrangement ***bộ gá truy nhập dữ liệu, DAA*** Trong truyền thông, thiết bị chứa biến áp cách ly, để nối thông thiết bị người dùng với mạng điện thoại. Nó được thiết kế để ngăn ngừa các điện áp hoặc tín hiệu có hại thâm nhập mạng.

data access management ***quản lý truy nhập dữ liệu*** *Xem* MODEM.

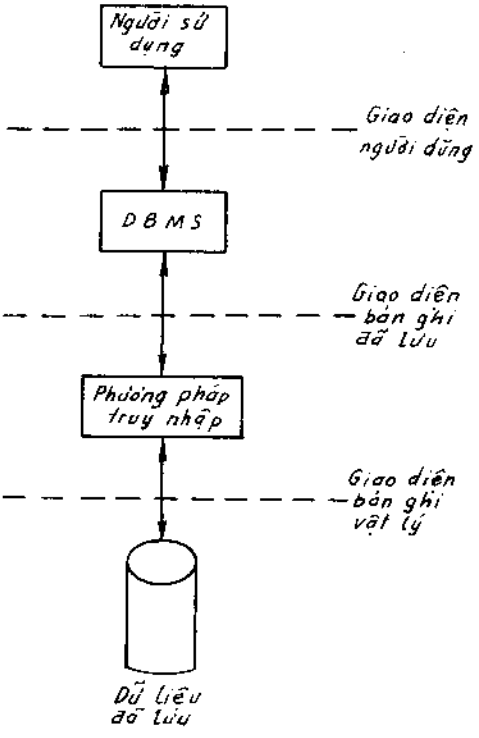
data acquisition ***thu nhận dữ liệu*** Trong tin học, quá trình nhận dạng, cách ly và thu thập dữ liệu nguồn cần xử lý tập trung. *Xem* data capture.

databank ***ngân hàng dữ liệu*** *Đồng nghĩa với* database.



database: *cơ sở dữ liệu.* Hình 1. Hệ các tệp không tích hợp.

database *cơ sở dữ liệu* (1) Tập hợp rộng rãi và toàn diện của các bản ghi được tập hợp và tổ chức theo cách có nghĩa để phục vụ một mục đích riêng. (2) Trong tin học, tập hợp dữ liệu vận hành lưu giữ được sử dụng bởi hệ các ứng dụng của một doanh nghiệp. Tiền thân của các hệ cơ sở dữ liệu là các tập hợp các tệp riêng lẻ được duy trì bởi các phòng ban của doanh nghiệp nhằm các mục đích tiền đặc tả và được xử lý bởi các chương trình ứng dụng riêng lẻ. Cách sắp xếp đó đã không có hiệu quả xét theo nỗ lực lập trình cần để vận hành hệ thống, không quản lý được toàn bộ quy mô thông tin có trong dữ liệu đã nhớ và đã rất không linh hoạt cho các doanh nghiệp đang phát triển.



database: *cơ sở dữ liệu.* Hình 2. Dữ liệu đã tích hợp.

Các hệ cơ sở dữ liệu tích hợp dữ liệu đã nhớ và phần mềm đặc biệt gọi là các hệ quản lý cơ sở dữ liệu (DBMS) tạo một bộ đệm giữa dữ liệu được lưu và các chương trình ứng dụng.

Các ưu điểm từ cách tiếp cận này là:

(*a*) các hệ nhớ vật lý được tách khỏi chương trình ứng dụng;

(*b*) có thể giảm độ dư thừa của dữ liệu được lưu;

(*c*) các vấn đề về tính không nhất quán của dữ liệu lưu giảm đi;

(*d*) dữ liệu đã lưu có thể được dùng chung giữa những người sử dụng;

(*e*) có thể buộc tuân thủ các chuẩn kiểm soát dữ liệu;

(*f*) những hạn chế cho an toàn có thể được áp dụng;

(*g*) có thể duy trì được tính toàn vẹn của dữ liệu;

(*h*) tạo điều kiện cho những câu vấn tin không theo thể thức.

Sự có mặt của DBMS ngụ ý rằng, các chương trình riêng lẻ có thể liên lạc dữ liệu với DBMS vốn có trách nhiệm truy nhập hoặc cập nhật mục tương ứng trong bộ nhớ vật lý. Sự độc lập dữ liệu vật lý này cho phép thay đổi các cách bố trí bộ nhớ vật lý (ví dụ để điều chỉnh các khối dữ liệu lớn hoặc tối ưu hoá truy nhập dữ liệu) mà không cần sửa đổi các chương trình ứng dụng. Sự tích hợp dữ liệu được lưu đảm bảo rằng, các mục dữ liệu không nhất thiết phải sao đôi trên các tệp (ví dụ, thông tin về nhân viên được lưu giữ trên các tệp nhân sự và bảng lương). Sự giảm

dư thừa dữ liệu này cũng làm giảm đến tối thiểu mối nguy hại do tính không nhất quán của dữ liệu (ví dụ, nếu phòng nhân sự đã điều chỉnh tệp riêng của họ khi một nhân viên thôi việc, thì có thể có sự không nhất quán với mục tương ứng trên tệp bảng lương cho tới khi phòng kế toán cũng tiến hành điều chỉnh). Sự dùng chung dữ liệu giữa các phòng ban rõ ràng trở nên dễ dàng nhờ dùng cơ sở dữ liệu và điều này cung cấp thông tin thích hợp nhiều hơn cho các nhà quản lý (ví dụ, có thể lập mối tương quan giữa mọi khía cạnh về năng lực của nhân viên với tiền lương).

Những ưu điểm chính của các hệ cơ sở dữ liệu trở nên rõ ràng khi khối lượng dữ liệu được lưu tăng lên và các hệ chuyển từ chế độ xử lý theo khối sang chế độ xử lý tương tác. Các mối nguy hiểm về dữ liệu không chính xác, không hợp lệ hoặc không an toàn trở nên nghiêm trọng trong những tình huống đó, nhưng với bộ nhớ tích hợp dữ liệu, có thể quy trách nhiệm về kiểm soát tổng thể cơ sở dữ liệu cho người quản trị cơ sở dữ liệu (DBA). DBA có quyền hạn và trách nhiệm để đảm bảo rằng, các tiêu chuẩn cài đặt đã được tuân thủ. Điều này khắc phục được các vấn đề nảy sinh từ các khuôn thức dữ liệu có phong cách riêng do các nhà lập trình riêng lẻ tạo ra và tạo điều kiện cho bảo trì lẫn trao đổi giữa các cài đặt.

Giá trị và bản chất tin cần của dữ liệu tập thể đã buộc các tổ chức phải có thái độ nghiêm ngặt hơn đối với truy nhập dữ liệu. Sự tồn tại bộ nhớ điện tử trung tâm đã làm tăng các nguy cơ truy nhập không được phép. Chức năng của DBA là buộc tuân thủ sự điều khiển trung tâm và do đó là sống còn đối với các tổ chức.

Điều quan trọng là bảo vệ dữ liệu khỏi bị hư hỏng ngẫu nhiên cũng như cố ý và DBA phải khởi phát và bắt tuân thủ các thủ tục điều hành và các điều khiển tính hợp lệ để tối thiểu hóa nguy cơ chèn hoặc sửa đổi không đúng (ví dụ, dữ liệu nhập bị loại bỏ nếu nó có khuôn thức không đúng hoặc không tuân theo các tiêu chuẩn quy định trước).

Những phát triển cơ sở dữ liệu ban đầu tập trung vào thiết kế các mối quan hệ qua lại giữa các mục dữ liệu và việc tối ưu hóa các chiến lược truy nhập. Hai biện pháp chính là cơ sở dữ liệu phân cấp và cơ sở dữ liệu mạng. Cơ sở dữ liệu phân cấp có cấu trúc cây với các mục riêng lẻ được truy nhập bởi các tìm kiếm dọc theo các nhánh từ nút cha tới nút con. Theo cách tiếp cận thứ hai, các cơ sở dữ liệu mạng cho phép các con trỏ giữa các mục dữ liệu và điều này vi phạm các yêu cầu về cây chỉ cho phép mỗi nút có một cha.

Các chỉ số và các tệp đảo cho phép truy nhập dễ dàng tới các mục riêng lẻ và giảm thời gian truy nhập đĩa. Các tệp đảo cho phép tìm kiếm nhanh theo các thuộc tính khác bằng khoá chính. Ví dụ, nếu tệp nhân viên được sắp xếp theo vần abc tên nhân viên, thì tìm kiếm tất cả các nhân viên ở một phòng cụ thể đòi hỏi tìm kiếm toàn diện tất cả các nhân viên trong tổ chức. Tập đảo chứa phòng và tên nhân viên, được sắp xếp theo tên phòng có thể cung cấp thông tin cần thiết trong thời gian ngắn.

Tuy nhiên, các cách tiếp cận đã nhắc đến ở trên đối với thiết kế cơ sở dữ liệu buộc cơ sở dữ liệu phải có cấu trúc chặt chẽ và dẫn đến những sắp xếp chỉ số rất phức tạp. Khái niệm cơ sở dữ liệu quan hệ do E. F. Codd đưa ra đã cách mạng hóa các khái niệm cơ sở dữ liệu và loại bỏ được nhu cầu đối với những chỉ số phức tạp.

Cơ sở dữ liệu quan hệ dựa trên cấu trúc dữ liệu khá dĩ đơn giản nhất (tức là các bảng hoặc tệp hai chiều). Những bảng đó, gọi là các quan hệ, có thể được xử lý để cho diện mạo dữ liệu thích hợp với áp dụng cụ thể. Sự phát triển này còn tạo ra thêm một mức độ độc lập dữ liệu nữa (tức là tính độc lập dữ liệu logic). Những người sử dụng có thể được cung cấp có hiệu quả một cơ sở dữ liệu riêng, là tập hợp con của cơ sở dữ liệu toàn bộ, phù hợp với những yêu cầu riêng của họ. Cơ sở dữ liệu riêng này không liên quan tới bất kỳ sự phân chia hoặc sắp xếp lại dữ liệu đã nhớ nào. Do đó nó không còn gây ra các nguy cơ về nhân đôi lại hoặc về tính không nhất quán vốn có trong việc tạo ra nhiều cơ sở dữ liệu "cá nhân".

Sự dự phòng các khung nhìn cục bộ còn đơn giản hóa các thủ tục an toàn vì những người sử dụng riêng lẻ chỉ được trang bị sơ đồ con phù hợp với cấp an toàn của họ.

Xu hướng hiện đại là sử dụng các cơ sở quan hệ truy nhập tương tác bằng các ngôn ngữ truy vấn đơn giản, hoặc xử lý bằng các ngôn ngữ thế hệ thứ tư. Trong khi những cơ sở dữ liệu ban đầu chủ yếu đã được xử lý bằng các chương trình ứng dụng trong chế độ lô, thì các hệ hiện nay được thiết kế để chấp nhận cả chế độ này lẫn chế độ truy nhập trực tuyến đối với các câu hỏi không dự tính trước và các cập nhật của tập hợp người dùng rộng rãi và phân tán.

Truy nhập trực tuyến trong môi trường nhiều người dùng đòi hỏi cả giao diện người dùng đơn giản lẫn DBMS phức tạp vốn đảm bảo sự an toàn và tính toàn vẹn trong mọi điều kiện làm việc. Cơ sở dữ liệu phải được bảo vệ trước các chuyển tác dở dang, có thể khiến cho cơ sở dữ liệu rơi vào trạng thái không nhất quán (ví dụ, giao dịch ngân hàng thiên vị ghi có một tài khoản nhưng không ghi nợ tài khoản tương ứng kia. Trong trường hợp sự cố hệ thống, còn phải có khả năng khôi phục lại cơ sở dữ liệu. Những người dùng cạnh tranh nhau phải được bảo vệ để khỏi cản trở nhau nếu cả hai đều cập nhật cùng bản ghi.

Cộng đồng những người dùng cơ sở dữ liệu đang nhanh chóng mở rộng. Một đầu của phạm vi mở rộng đó có những cơ sở dữ liệu đồ sộ được thiết kế cho các cơ sở tập thể và các cơ sở dữ liệu công cộng phục vụ những người sử dụng quốc gia và quốc tế. Ở đầu kia của phạm vi đó, có vô số những DBMS máy vi tính được thiết kế cho các doanh nghiệp nhỏ và những người sử dụng chuyên nghiệp (ví dụ, dBase). *Xem* application program, database administrator, database security, data independence, DBA, flat file, fourth-generation language, hierarchical database, inverted file, lockout, logical data independence, network database,

primary key, query language, relational database, rollback, schema, subschema, tree structure. *Đồng nghĩa với* databank.

database administrator ***người quản trị cơ sở dữ liệu, DBA*** Trong các cơ sở dữ liệu, người chịu trách nhiệm về hệ thống cơ sở dữ liệu, nhất là về việc xác định các quy tắc truy nhập sửa đổi và lưu giữ dữ liệu. *Xem* database.

database language ***ngôn ngữ cơ sở dữ liệu*** *Xem* database manegement system, data description language, data manipulation language, query language.

database management system ***hệ quản lý cơ sở dữ liệu, DBMS*** Trong các cơ sở dữ liệu, tập hợp các chương trình tạo điều kiện tạo và bảo trì một cơ sở dữ liệu và thi hành chương trình có sử dụng cơ sở dữ liệu. *Xem* data independence.

database producer ***người tạo ra cơ sở dữ liệu, tổ chức tạo ra cơ sở dữ liệu*** Trong truy tìm thông tin trực tuyến, người hoặc tổ chức biên soạn cơ sở dữ liệu. Người tạo ra cơ sở dữ liệu có thể là một hãng buôn bán, một tổ chức chuyên môn hoặc cơ quan của chính phủ. Không nhất thiết người tạo ra cơ sở dữ liệu phải là người làm cho cơ sở dữ liệu khả dụng đối với người bán cơ sở dữ liệu. *So sánh với* database vendor.

database security ***an toàn cơ sở dữ liệu*** Sự áp dụng các cơ sở dữ liệu đã tăng lên nhanh trong những năm gần đây; đã có sự phát triển mạnh của các cơ sở dữ liệu riêng ở các máy tính và các máy tính mini và sự mở rộng dung lượng của các hệ lớn phục vụ đông đảo người dùng của một tổ chức, một quốc gia và quốc tế.

Tổng quan

Sự tích hợp các hồ sơ của một tổ chức thành một cơ sở dữ liệu duy nhất, làm tăng rủi ro truy nhập trái phép và sửa đổi ác ý dữ liệu của tổ chức. Hơn nữa, sự xuất hiện luật pháp bảo vệ dữ liệu đã đặt trách nhiệm pháp lý lên những người giữ dữ liệu cá nhân phải bảo vệ thông tin đó trước sửa đổi ác ý và truy nhập trái phép. Do đó các vấn đề an toàn cơ sở dữ liệu đang tăng cả tầm cỡ vấn đề lẫn những bất lợi liên quan tới tính an toàn không đầy đủ.

Trong trường hợp lý tưởng, các cấu trúc an toàn đối với cơ sở dữ liệu phải đáp ứng những yêu cầu nêu dưới đây.

(*a*) Không người hoặc nhóm người nào có thể truy nhập, sửa đổi, thêm hoặc xoá dữ liệu một cách bất hợp pháp.

(*b*) Không một người hoặc nhóm người không được phép nào có thể suy ra giá trị của mục bí mật bằng cách xử lý các câu hỏi hoặc thực hiện các tính toán đối với dữ liệu đã phát ra.

(*c*) Các cấu trúc an toàn phải linh hoạt và người dùng được cấp những đặc quyền thích hợp theo hoạt động và nhu cầu của họ.

(*d*) Các cơ chế an toàn không được làm suy giảm đáng kể tính năng của hệ quản lý cơ sở dữ liệu.

(*e*) Khả năng truy nhập hệ thống không bị giảm đối với những người dùng hợp pháp.

(*f*) Không nên mở rộng đáng kể đối với dữ liệu đã nhớ.

(*g*) Chi phí cho các cấu trúc an toàn

phải phù hợp với chức năng của cơ sở dữ liệu.

Các vấn đề an toàn đối với tất cả các cơ sở dữ liệu rơi vào hai nhóm lớn – sự bảo toàn tính toàn vẹn và sự an toàn – nhưng bản chất của vấn đề liên quan tới chức năng, kích thước và tập hợp người dùng của cơ sở dữ liệu.

Bảo toàn tính toàn vẹn là trách nhiệm của DBMS; các nội dung của cơ sở dữ liệu phải được bảo vệ chống những lỗi nảy sinh do bấm phím sai, cập nhật không nhất quán, các cập nhật hỏng một phần v.v. An toàn hệ thống cơ sở dữ liệu được thiết kế để đảm bảo ngăn chặn những người sử dụng không được phép, ác ý v.v. truy nhập cơ sở dữ liệu.

Nội dung cơ sở dữ liệu phải được bảo vệ chống sửa đổi ngẫu nhiên bởi những người sử dụng ngây thơ, lỗi chương trình v.v. cũng như chống lại kẻ tấn công. An toàn chống lại truy nhập ác ý có thể được chia thành kiểm soát truy nhập DBMS, mã hóa tệp, kiểm soát suy luận và các bộ lọc cho những hệ nhiều mức.

Kiểm soát truy nhập DBMS

DBMS tạo ra một giao diện giữa người sử dụng và các tệp dữ liệu; do đó đối với DBMS, có thể tạo ra một khung nhìn về cơ sở dữ liệu, thích hợp cho một người sử dụng riêng. Như vậy DBMS có thể cung cấp hiệu quả cho mỗi người sử dụng một cơ sở dữ liệu cá nhân hạn chế, chỉ chứa những mục dữ liệu tương ứng với mức đặc quyền của người sử dụng. Tuy nhiên, DBMS không thể cung cấp sự đảm bảo an toàn trong mọi tình huống. Những hạn chế của an toàn cơ sở dữ liệu là:

- đôi khi người sử dụng có thể đi vòng qua DBMS và truy nhập trực tiếp các tệp cơ sở dữ liệu;
- có thể xử lý các cơ sở dữ liệu thống kê nhằm làm lộ thông tin liên quan tới các cá nhân;
- DBMS có thể không có khả năng ngăn chặn người sử dụng suy diễn thông tin đã phân loại bằng cách xử lý các câu truy vấn trong phạm vi mức đặc quyền của họ;
- những kẻ tấn công có thể gài virut con ngựa thành Tơroa vào trong DBMS;
- DBMS có thể quá phức tạp nên không cho phép kiểm chứng hình thức các thủ tục an toàn.

Nếu một cơ sở dữ liệu nằm bên trong một hệ máy tính, nơi những người sử dụng có truy nhập riêng rẽ vào hệ điều hành, hoặc các phương tiện mang tin chứa các tệp dữ liệu, thì một kẻ tấn công có thể chỉ đơn giản đi vòng qua DBMS và truy nhập trực tiếp các tệp dữ liệu. Ví dụ, đĩa mềm chứa một tập hợp các tệp cơ sở dữ liệu máy vi tính có thể bị lấy khỏi máy tính và bị nghiên cứu chi tiết ở máy vi tính của kẻ tấn công.

Mã hóa

Dữ liệu có thể được mã hoá để ngăn ngừa tấn công trực tiếp; tuy nhiên, một sự mã hóa như thế sẽ trực tiếp ảnh hưởng tới hoạt động của DBMS và có một số ràng buộc đối với thuật toán mã hóa và chế độ mã hóa.

- Về mặt lý thuyết hệ mã hóa phải an toàn hoặc đòi hỏi một hệ số công việc cao để phá. Các dữ liệu được lưu giữ thường có giá trị trong một khoảng

thời gian dài và do đó nhạy cảm với sự phân tích mật mã mà có thể cần một khoảng thời gian dài.

- Thời gian mã hóa, và đặc biệt là thời gian giải mã, không được ảnh hưởng nhiều tới hoạt động của người sử dụng trực tuyến. Trong một số hệ thống, việc mã hóa có thể được thực hiện theo các lô dữ liệu cập nhật, nhưng khi đó, thời gian giải mã sẽ ảnh hưởng trực tiếp tới những truy nhập bình thường của người sử dụng.
- Dữ liệu đã mã không nên quá lớn so với dữ liệu rõ.
- Sự mã hóa phải dựa trên bản ghi để DBMS không bị buộc truy lục một khối lượng lớn dữ liệu khi giải mã một bản ghi.
- Sơ đồ mã hóa phải tương thích với phương tiện DBMS để tạo ra các sơ đồ con của người sử dụng.
- Các trường bên trong cơ sở dữ liệu phải được mã bằng các khóa khác nhau. Khi đó, một người sử dụng truy nhập bất hợp pháp tới được các trường đã phân loại đã mã phải không có khả năng suy diễn các giá trị bản gốc của họ thông qua những thao tác được phép trên những trường khác.
- Bản ghi tự nó phải được mã hóa như một thực thể. Nếu bản ghi chỉ đơn thuần chứa một tập hợp các trường mã hóa riêng lẻ thì sẽ tồn tại các nguy cơ thay thế một trường mã hóa từ bản ghi này sang bản ghi kia, và so khớp mẫu. Trong trường hợp sau, một người sử dụng có thể so khớp các giá trị của các trường trong các bản ghi khác nhau; nếu tồn tại trường mã hóa đã so khớp trong một bản ghi trong phạm vi mức đặc quyền của người sử dụng, thì có thể suy diễn giá trị của trường bản mã phù hợp.
- Sơ đồ mã hóa phải cho phép những người sử dụng được trao nhiều mức đặc quyền đọc và ghi.
- DBMS phải không bị sơ đồ mã hóa buộc phải duy trì các bản sao nhân đôi các mục dữ liệu để cho phép đưa ra sơ đồ con khác.
- Phải có thể vận hành sơ đồ mã hóa với những bản ghi được bổ sung cục bộ.

Kiểm soát suy luận - tổng quan

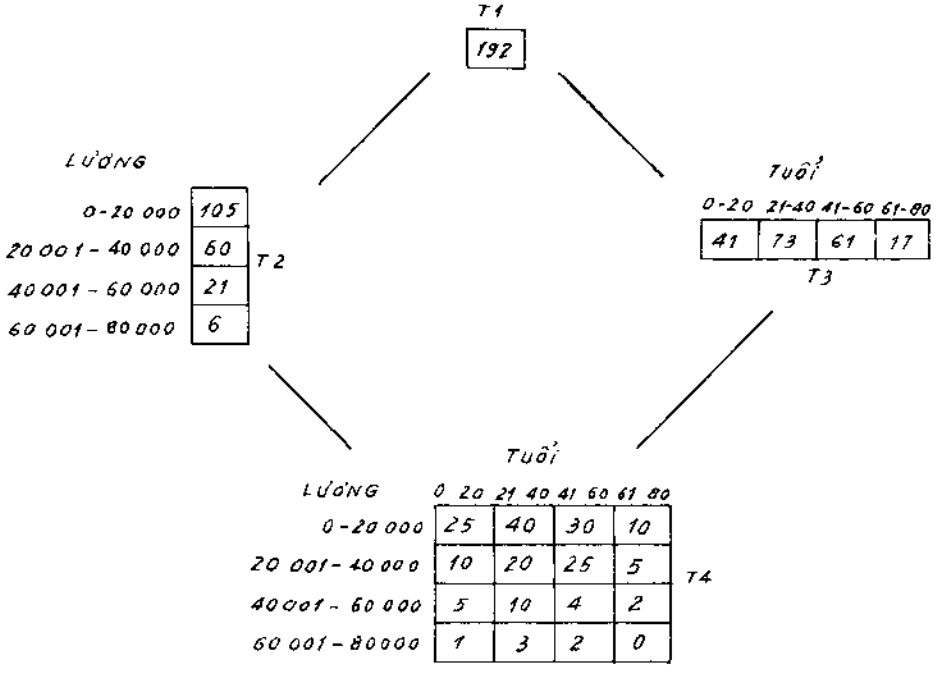
Một số hệ an toàn cơ sở dữ liệu không mã hóa dữ liệu được lưu nhưng buộc người sử dụng truy nhập cơ sở dữ liệu thông qua DBMS. Trong những trường hợp đó, bản thân DBMS có thể được thao tác để lộ thông tin bí mật.

Một trường hợp đặc biệt này sinh ở những nơi người sử dụng có thể nhận hợp pháp các dữ liệu thống kê liên quan tới một tập hợp người sử dụng nào đó, nhưng không được phép truy nhập các chi tiết cá nhân về một cá nhân bên trong tập hợp đó. Như vậy, có thể là hợp pháp khi tiếp cận được tỷ lệ trường hợp mắc một bệnh ở một thành phố, nhưng không thể xác định được liệu một cư dân cụ thể nào đó của thành phố có bị mắc bệnh đang nói tới hay không. Khía cạnh này của an toàn cơ sở dữ liệu được gọi là kiểm soát suy luận.

Thiết lập giới hạn dưới đối với số các bản ghi có thể gắn liền với một câu hỏi là không đủ vì có thể dùng những câu

hỏi chồng chéo lên nhau (phủ nhau) để suy ra thông tin có liên quan tới một cá nhân. Ví dụ, nếu giới hạn dưới của 100 bản ghi mỗi câu hỏi được thiết lập thì "A Smith" có thể truy nhập hợp pháp tới mức lương trung bình của 99 nhân viên và "A Smith". Câu hỏi thứ hai về mức lương trung bình của cũng các cá thể đó và "B Jone" cung cấp thông tin đủ cho "A Smith" suy ra mức lương của "B Jone". Nếu hệ thiết lập giới hạn dưới về số các bản ghi gắn với một câu hỏi và số cực đại các phần tử chung trong hai câu hỏi, thì một kẻ tấn công sẽ buộc phải thực hiện một số lớn các câu hỏi để suy ra một mục liên quan tới một cá thể. Điều này làm bài toán của anh ta trở nên khó hơn nhưng không phải là không thể giải được.

Các phương pháp kiểm soát suy luận có thể được xem xét theo mức an toàn, độ mất mát thông tin và chi phí. An toàn liên quan tới một con số tương đối các thống kê nhạy cảm. Có thể suy ra chúng bằng cách xử lý các câu hỏi hợp pháp và mức độ khó khăn trong việc thực hiện điều đó. Độ mất mát thông tin là số đo số các thống kê không nhạy cảm bị hạn chế một cách không cần thiết bởi sự kiểm soát. Chi phí của kiểm soát suy luận này sinh từ việc thực hiện hệ thống kiểm soát và tổng phí tính toán/lưu trữ trong việc đánh giá xem



database security: *an toàn cơ sở dữ liệu.* Mô hình giản.

các câu hỏi có được xử lý hay không. Các phương pháp kiểm soát suy luận có thể được phân loại thành:

- hạn chế đối với tập hợp các câu hỏi được phép;
- bổ sung tạp nhiễu vào các thống kê đã phát ra.

Kiểm soát suy luận - hạn chế đối với những câu hỏi được phép

Trong nghiên cứu các hạn chế đối với các câu hỏi được phép thì việc biểu diễn cơ sở dữ liệu theo một mô hình giàn là điều hữu ích.

Ta hãy xét cơ sở dữ liệu thống kê chứa các chi tiết về một tập hợp cần khảo sát với những thuộc tính tuổi và lương. Thuộc tính tuổi được chia thành các khoảng 0-20, 21-40, 41-60, 61-80 và lương thành các khoảng 0-20.000, 20.001-40.000, 40.001-60.000 và 60.001-80.000. Mô hình giàn đối với cơ sở dữ liệu được minh hoạ ở hình vẽ. Cơ sở dữ liệu có thể biểu diễn số người thuộc một trong các khoảng thuộc tính đó, tình huống này có thể được biểu diễn như một bảng hai chiều với mỗi ô chứa các số đếm tương ứng. Có thể rút ra một bản dữ liệu thô hơn bằng cách xem xét hoặc tuổi hoặc lương một cách riêng rẽ. Trong trường hợp này, các bảng chỉ cung cấp những chi tiết về số người trong một độ tuổi hoặc khoảng lương (xem hình minh hoạ), tức là các con số trong các ô của bảng đó biểu thị tổng của các cột (đối với tuổi) hoặc hàng (đối với lương) của bảng hai chiều.

Ở đỉnh của mô hình giàn là bảng một ô đơn giản cho biết số người trong tập hợp khảo sát. Bảng ở đáy giàn là bảng dễ có khả năng để lộ thông tin về một cá nhân nhất. Ví dụ, rõ ràng là chỉ có một người của tập hợp khảo sát, trong độ tuổi 0-20, có lương trong khoảng từ 60.001 và 80.000. Giả sử có một thuộc tính thứ ba trong cơ sở dữ liệu, ví dụ như số lần phạm tội, thì có thể suy ra số lần phạm tội đối với một cá nhân nếu biết rằng cá nhân đó thuộc độ tuổi 0 tới 20 và có lương trong khoảng 60.001-80.000.

Các bảng ở cao hơn trong giàn không cung cấp chi tiết nhỏ như thế, ví dụ bảng tuổi chỉ cho thông tin về phân bố tuổi của tập hợp người sử dụng, không có mối liên quan nào với lương. Tính chất nhạy cảm của một thống kê có thể được xác định bằng tiêu chuẩn n - đáp ứng, k% trội, tức là một thống kê nhạy cảm là thống kê trong đó *n* bản ghi hoặc ít hơn cấu thành trên k% của tổng số.

Rủi ro tiết lộ của một bảng được cho bởi số phần trăm các ô nhạy cảm của bảng. Thất thoát hoặc tiết lộ cá nhân xuất hiện khi có thể suy luận một thống kê cho tới giờ chưa biết về một cá nhân.

Sự tiết lộ thụ động nảy sinh khi có thể dùng thống kê để suy ra rằng, các nhân không có một thuộc tính cụ thể, ví dụ như trên hình vẽ, mọi cá nhân trên tuổi 60 không thể kiếm được quá 60.000.

Các kỹ thuật hạn chế trong kiểm soát suy luận có thể được áp dụng ở mức bảng hoặc mức ô, và được dùng để ngăn ngừa truy nhập tới các bảng hoặc các ô chứa các thống kê nhạy cảm. Các kỹ thuật hạn chế bảng hoặc ô được phân loại như kỹ thuật không nhớ, dựa

D

trên kiểm toán và tiên nghiệm.

Các kỹ thuật không nhớ sử dụng những tiêu chuẩn không dựa trên việc duy trì một bản ghi chứa các câu hỏi trước đó đã đặt ra mà cũng không dựa trên danh sách thống kê được phép, tức là quyết định cho phép lập một câu hỏi vào thời điểm mà câu hỏi được đặt ra và không thực hiện tính toán trước tiêu chuẩn. Các kiểm soát dựa trên kiểm toán duy trì một bản ghi chứa các câu hỏi và cố xác định xem, liệu kết quả của câu hỏi đưa ra tương quan với dữ liệu thu được từ các câu hỏi trước đó có dẫn tới một sự thất thoát hay không. Các kiểm soát tiên nghiệm xác định trước xem liệu có một tập hợp các thống kê nào đó có thể phát ra mà không gây thất thoát hay không.

Hạn chế bằng xác định xem có một bảng ngoại lệ nào đó có thể được cung cấp để trả lời các câu hỏi hay không; ba kỹ thuật thông thường là:

- kiểm soát theo lệnh;
- kiểm soát theo kích thước tương đối của bảng;
- ước lượng rủi ro một cách tường minh.

Kiểm soát theo lệnh là một kỹ thuật không nhớ đơn giản, chỉ cho phép các câu hỏi khi các thuộc tính chứa trong đó không vượt quá một giá trị xác định nào đó. Kỹ thuật này hạn chế có hiệu quả biểu diễn cơ sở dữ liệu ở những bảng phía trên của mô hình giàn. Ví dụ, nếu chỉ một thuộc tính được phép ở một câu hỏi thì chỉ ba bảng phía trên trong hình minh họa (tức là $T1$ $T2$ và $T3$) có thể được truy nhập. Tuy nhiên, kỹ thuật này không xem xét số các ô trong một bảng có liên quan với tổng số các bản ghi. Một bảng hai chiều có 100 ô dành cho một tập hợp 200 bản ghi dễ làm thất thoát hơn là cùng bảng dành cho 10.000 bản ghi. Tương tự, việc giảm số ô bằng cách ghi các thuộc tính trên các khoảng lớn hơn (ví dụ 0-40.000 thay cho 0-20.000) có thể làm giảm nguy cơ thất thoát đối với một bảng nhiều chiều nào đó.

Kiểm soát theo kích thước tương đối của bảng, còn gọi là tiêu chuẩn s_m/N, dựa trên tỷ số của số ô trong một bảng trên tổng số bản ghi. Nếu con số trung bình các bản ghi gắn liền với một ô giảm xuống dưới một giá trị ngưỡng nào đó thì bảng bị hạn chế. Cách kiểm soát này không tính tới sự phân bố các bản ghi trên bảng, ví dụ như ở hình, những người quá trẻ và những người quá già không dễ kiếm được lương cao. Những kỹ thuật khác nhau đã được thử nghiệm để xác định một cách tường minh mức rủi ro đi kèm với việc phát ra một bảng nào đó, ví dụ thông qua xem xét phân bố tần số của các thuộc tính.

Các kỹ thuật hạn chế ô nhằm xác định xem tính sẵn có của một ô đặc biệt có dẫn tới tiết lộ dữ liệu cá nhân hay không. Với các kỹ thuật này, quyết định được đưa ra là xóa một ô nào đó hoặc nhóm ô nào đó, chứ không phải toàn bộ bảng; do đó mất mát thông tin nhỏ hơn mất mát thông tin gắn liền với các kỹ thuật hạn chế bảng.

Ba phương pháp sử dụng cách tiếp cận này là:

- kiểm soát kích thước tập hợp câu hỏi;
- kiểm soát các câu hỏi có ngụ ý;

- kiểm soát sự chồng chéo;
- chuyên gia kiểm toán;
- xóa ô;
- kết nhóm.

Kiểm soát kích thước tập hợp câu hỏi là kỹ thuật hạn chế ô không nhớ đơn giản vốn không cho phép các câu hỏi liên quan tới một tỷ lệ quá thấp hoặc quá cao của các bản ghi thích hợp trong cơ sở dữ liệu. Sự hạn chế đối với các câu hỏi tạo thành một tỷ lệ quá thấp các bản ghi tự nó đã rõ ràng; sự hạn chế đối với các câu hỏi tạo thành một tỷ lệ quá cao các bản ghi nảy sinh do có thể suy ra dữ liệu chứa trong các bản ghi không bao hàm trong câu hỏi. Như vậy một câu hỏi cho trên 99 trong 100 bản ghi, tiếp theo bằng một câu hỏi giống hệt thứ hai cho toàn bộ 100 bản ghi, sẽ cung cấp thông tin trực tiếp về bản ghi bỏ sót từ câu hỏi đầu tiên. Có thể phá vỡ sự kiểm soát này bằng cách sử dụng các bộ theo dõi để nhét thừa các số bản ghi trong một câu hỏi. Ví dụ như ở hình minh hoạ, một câu hỏi về số người trong độ tuổi 0-20 với mức lương giữa 60.000 và 80.000 có thể được loại bỏ hẳn bởi cách kiểm soát này. Tuy nhiên, nếu câu hỏi được áp dụng cho khoảng lương 0-20.000 cũng như 60.000 tới 80.000 thì nó rất có thể được phép. Câu hỏi được phép thứ hai đối với bộ theo dõi, tức là độ tuổi 0-20, mức lương 0-20.000 khi đó có thể được dùng để suy ra thống kê nhạy cảm.

Kiểm soát các câu hỏi có ngụ ý hạn chế nỗ lực cản trở các tấn công dùng bộ theo dõi bằng cách kiểm tra các kích thước của các tập hợp câu hỏi ngụ ý đối với mỗi câu hỏi. Tập hợp câu hỏi có ngụ ý là một tập hợp mà có thể tính toán từ câu hỏi thực sự và những câu hỏi được phép khác. Tuy nhiên, kỹ thuật này có thể yêu cầu tính toán quá mức vì có thể có nhiều tập hợp câu hỏi có ngụ ý đối với mỗi câu hỏi riêng lẻ. Kiểm soát câu hỏi chồng chéo sử dụng một vết kiểm toán và giới hạn các câu hỏi trong đó, các tập hợp câu hỏi có nhiều hơn một số lượng nhỏ xác định các bản ghi chung. Tuy nhiên, kỹ thuật này có thể gây ra tổn thất thông tin quá mức, ví dụ một câu hỏi phủ một phần đáng kể cơ sở dữ liệu hầu như có thể khiến cho một câu hỏi có liên quan bất kỳ nào khác bị cấm.

Trong kỹ thuật chuyên gia kiểm toán, một vết kiểm toán được sử dụng để phát triển một ma trận nhị phân cho biết liệu có một câu hỏi nào đó có thể để lộ thông tin về một cá nhân hay không. Các cột của ma trận nhị phân tương ứng với các cá nhân; các hàng biểu thị một cơ sở cho một tập hợp các câu hỏi có thể rút ra được từ những câu hỏi trước đó. Nếu một câu hỏi dẫn đến sự điều chỉnh ma trận với một hàng chứa tất cả các số không, trừ một cột, thì câu hỏi đó có thể tiết lộ thông tin về cá nhân tương ứng với cột đó.

Kỹ thuật tiên nghiệm được dùng để xác định những ô cần phải xóa trong kỹ thuật *xóa ô*. Giấu thông tin trong một ô riêng lẻ là không đủ vì dữ liệu đó có thể được suy ra dễ dàng từ những bảng mức cao hơn trong gian. Ví dụ, hãy xét bảng *T4* (hình minh họa), nếu ô tương ứng với độ tuổi 0-20, lương 60.001-80.000, được để trống thì có thể suy ra dữ liệu đơn giản bằng cách cộng

các ô còn lại ở cột tuổi và trừ kết quả từ ô 0-20 ở bảng mức cao hơn 1/3. Các ô kế bên của 1/4 do đó cũng bị xóa cho tới khi thống kê nhạy cảm được bảo vệ. Tính toán tiên nghiệm có thể được thực hiện một lần đối với cơ sở dữ liệu đầy đủ và do đó, không bao hàm tính toán quá mức đối với mỗi câu hỏi. Tuy nhiên, có thể không thực hiện được toàn bộ tải trong tính toán nếu các thống kê được đưa ra đối với một số lớn các thuộc tính hoặc nếu cơ sở dữ liệu bị điều chỉnh nhiều lần.

Trong kỹ thuật kết nhóm, hoặc bao lại, các thuộc tính được nhóm lại để đảm bảo không ô nào có thể để lộ dữ liệu cá nhân. Như vậy ở hình minh họa, sự kết nhóm của các khoảng lương cao hơn thành một khoảng duy nhất 40.001 tới 80.000 có thể đảm bảo rằng, không ô nào tương ứng với dưới 2 bản ghi.

Kiểm soát suy luận - bổ sung tạp nhiễu

Các phương pháp nhiễu loạn làm thay đổi các thống kê trả lại người sử dụng theo cách sao cho, thông tin được cung cấp là đầy đủ với mục đích đã định của nó nhưng không thể xử lý làm lộ dữ liệu chính xác liên quan tới một cá nhân. Ví dụ, nguy cơ thất thoát có thể được giảm bằng cách bổ sung những con số ngẫu nhiên, hoặc tạp nhiễu vào các mục dữ liệu cá nhân khi chúng được trích ra theo các tiêu chuẩn chọn lọc và được dùng để tính toán mọi thống kê, ví dụ như một giá trị trung bình. Tác dụng tổng cộng của các số ngẫu nhiên, cả giá trị dương lẫn âm, phải không làm ảnh hưởng đáng kể tới thống kê đã tính toán. Tuy nhiên, nó đủ để làm cho các dữ liệu bất kỳ được suy ra bất hợp pháp. Ví dụ, nó có thể là hiệu của hai số bị nhiễu lớn, trở nên vô nghĩa.

Nhược điểm của các kỹ thuật nhiễu loạn là chúng có thể làm mất thông tin do các yếu tố về mức vênh và nhất quán. Mức vênh là hiệu số giữa kỳ vọng của một thống kê bị nhiễu và giá trị thực của nó. Thiếu nhất quán liên quan tới các mâu thuẫn có thể nảy sinh khi sự lặp lại cùng câu hỏi tạo ra các kết quả khác nhau, ví dụ như giá trị trung bình trả về có thể khác với giá trị trung bình tính toán được bằng cách chia kết quả của các câu hỏi tạo ra tổng và số đếm tương ứng.

Các kỹ thuật nhiễu loạn có thể được phân loại thành dựa trên bản ghi hoặc kết quả. Ở các câu hỏi dựa trên bản ghi, hoặc một mẫu các bản ghi thỏa mãn câu hỏi được chọn ra và toàn bộ thống kê được ước lượng từ mẫu, hoặc các bản ghi riêng lẻ được làm nhiễu khi chúng được dùng để tính thống kê. Các phương pháp dựa trên kết quả đưa nhiễu vào kết quả câu hỏi sau khi nó đã được tính toán đúng, ví dụ như bằng cách làm tròn kết quả.

Các phương pháp gây nhiễu dựa trên bản ghi là: các câu hỏi lấy mẫu ngẫu nhiên và các nhiễu dữ liệu ngẫu nhiên. Trong trường hợp các câu hỏi lấy mẫu ngẫu nhiên, thủ tục chọn lựa được áp dụng cho mỗi bản ghi khi nó được trích ra theo các tiêu chuẩn câu hỏi. Các tiêu chuẩn chọn lọc sẽ xác định xem liệu có dùng bản ghi trong thống kê cần thiết hay không. Thống kê được ước lượng từ một mẫu thuộc tập hợp câu hỏi và do đó khó, nếu không phải là không

thể, nhận ra được dữ liệu về một bản ghi cá nhân.

Nhiễu dữ liệu ngẫu nhiên bổ sung một số ngẫu nhiên vào dữ liệu của mỗi bản ghi được trích ra để tính toán thống kê chung. Phương pháp này lệ thuộc vào các cuộc tấn công lấy trung bình, trong đó cùng một câu hỏi sẽ được lặp lại vài lần sao cho, tổng tác dụng của tạp nhiễu thêm vào có thể được giảm liên tục. Nhược điểm thứ hai của phương pháp này là nó có thể gây những khó khăn cho người sử dụng do những điểm không nhất quán, ví dụ nó có thể trả về các số đếm âm.

Các phương pháp gây nhiễu dựa trên kết quả gồm:

- làm tròn có hệ thống;
- các khoảng hệ thống;
- làm tròn ngẫu nhiên;
- làm tròn có kiểm soát.

Làm tròn hệ thống liên quan tới việc làm tròn các dữ liệu theo một giá trị đinh trước nào đó. Phương pháp này có thể dẫn tới sự không nhất quán, ví dụ như tổng làm tròn của các số có thể khác với tổng của các số được làm tròn.

Biểu diễn dữ liệu làm tròn có hệ thống có thể được đưa ra dưới dạng các khoảng có hệ thống, như vậy nếu số 13 được làm tròn đến bội gần nhất của 5 thì nó được biểu diễn trong khoảng 10-14 thay cho số 15.

Làm tròn ngẫu nhiên chọn ngẫu nhiên cực dưới và cực trên của khoảng làm tròn, ví dụ như số 7 có thể được biểu diễn bằng 5 hoặc 10. Phương pháp này không bị vênh nhưng để tránh những sự không nhất quán, thì kết quả làm tròn phải sao cho các câu hỏi tương đương luôn cho cùng kết quả.

Làm tròn có kiểm soát tránh được sự không nhất quán của các tổng được làm tròn vốn khác với tổng của các số được làm tròn.

Các bộ lọc

An toàn của những hệ cơ sở dữ liệu lớn được người sử dụng dùng với những mức phân loại an toàn khác nhau đặt ra những vấn đề riêng. Tính chất phức tạp của một DBMS lớn làm giảm nhẹ các thủ tục kiểm chứng hình thức mà có thể đem đến sự đảm bảo rằng, dữ liệu có một mức phân loại an toàn *d* không bao giờ được phân phối cho người sử dụng có mức phân loại an toàn kém *d*. Có bốn kiểu tấn công có thể dẫn đến sự tiết lộ không được phép dữ liệu đã phân loại:

- truy nhập trực tiếp;
- truy nhập gián tiếp bằng suy luận;
- phát hành trực tiếp bởi con ngựa thành Torroa;
- rò rỉ bởi con ngựa thành Torroa.

Nguy cơ truy nhập trực tiếp sẽ đơn giản đáp lại yêu cầu của người sử dụng về dữ liệu ở mức phân loại lớn hơn so với mức phân loại được phép đối với người sử dụng. Sự tấn công gián tiếp bằng suy luận cho phép người sử dụng đặt ra một câu hỏi liên quan tới sự lựa chọn các bản ghi theo giá trị của các mục dữ liệu vốn có mức phân loại cao hơn so với mức phân loại của người sử dụng. Dữ liệu thực được trả về cho người sử dụng là ở mức được phép của người sử dụng nhưng nó cho phép anh ta suy ra thông tin có mức an toàn cao hơn. Ví dụ, nếu các tên của một số hệ thống vũ khí là tối mật nhưng các tên

của những hãng cung ứng các linh kiện để sản xuất những hệ thống đó lại chỉ được phân loại là mật, thì một câu hỏi về các tên của các hãng cung cấp đối với hệ thống vũ khí tối mật ZEUS sẽ để lộ danh sách những hãng cung ứng cho hệ thống vũ khí tối mật đó.

Các virut con ngựa thành Tơroa có thể tìm ra các dữ liệu được phân loại và làm cho những người sử dụng không được phép có thể sử dụng được nó. Sự tấn công trực tiếp của con ngựa thành Tơroa cung cấp thông tin đã phân loại bằng cách thay đổi nhãn an toàn của nó, hoặc tái định vị dữ liệu vào một bản ghi với mức phân loại an toàn thấp hơn. Sự tấn công gây rò rỉ bởi con ngựa thành Tơroa sẽ mã hóa thông tin đã phân loại và cung cấp nó cho người sử dụng không được phép, rõ ràng như câu trả lời cho một câu hỏi hợp pháp. Sau đó người sử dụng giải mã lời đáp và trích ra thông tin đã phân loại. Ví dụ, người sử dụng con ngựa thành Tơroa có thể thiết lập một bảng không phân loại (không mật) với 26 tên thành phố. Nếu con ngựa thành Tơroa cần giải phóng một tên có nghĩa tối mật, thì nó có thể mã hóa tên thành các con số, với mỗi chữ cái thay thế bằng một con số biểu thị vị trí ở bảng chữ cái của nó, và sau đó trả lại tên các thành phố tương ứng với những con số đó.

Các mối đe dọa cho một cơ sở dữ liệu nhiều mức khiến việc thiết kế một DBMS sao cho nó đảm bảo an toàn hệ thống là cực kỳ khó khăn. Một phương pháp đã đề xuất tách riêng chức năng an toàn và giao nó cho một bộ lọc nằm giữa người sử dụng và DBMS. Việc tách sự truy nhập cơ sở dữ liệu và hệ kiểm tra an toàn ngụ ý là, nhu cầu kiểm chứng an toàn hình thức chỉ được áp dụng cho bộ lọc, và như vậy không cần mở rộng phần mềm phức tạp của DBMS. Trong một phương pháp, bộ lọc đưa một tổng kiểm tra mật mã vào mỗi mục dữ liệu vốn cần phải dán nhãn phân loại an toàn. Tổng kiểm tra là một MAC được tính toán có hiệu quả trên mục dữ liệu và nhãn phân loại nhờ sử dụng một khóa mật chỉ bộ lọc biết. Bản thân dữ liệu được lưu giữ dưới dạng rõ và do đó, có thể thao tác bởi DBMS; tuy nhiên, mọi ý đồ bất hợp pháp cố sửa đổi dữ liệu đã lưu giữ, hoặc thay đổi mức phân loại an toàn của nó sẽ bị bộ lọc phát hiện khi nó phê chuẩn tổng kiểm tra. Kỹ thuật này, gọi là khóa toàn vẹn, có biệt hiệu sơn phun vì mỗi mục dữ liệu bị đặt mức phân loại của nó không thể tẩy ra được.

Bộ lọc chịu trách nhiệm kiểm tra mức phân loại an toàn của dữ liệu và so sánh nó với mức phân loại của người sử dụng trước khi đưa ra dữ liệu. Nhãn phân loại có thể được lưu giữ với dữ liệu dưới dạng rõ hoặc mã, hoặc các nhãn có thể được lưu giữ bên trong bộ lọc. Cách đầu để lộ nguy cơ về các cuộc tấn công bởi virut con ngựa thành Tơroa bắt và phát hành dữ liệu phân loại mức cao. Việc mã hóa đơn giản các nhãn bằng một khóa đơn là không an toàn vì tất cả các nhãn tối mật (chẳng hạn) sẽ có cùng giá trị bản mã. Trong những tình huống này, kẻ tấn công có thể hợp tác với con ngựa thành Tơroa để xác định các nhãn phân loại bản mã, ví dụ, bằng cách chèn các mục có các

nhãn phân loại thấp để con ngựa thành Tơroa có thể phát triển một danh sách phương án bản mã của những nhãn như thế và từ đó, xác định các bản mã tương ứng có những mức phân loại cao hơn.

Có thể tăng mức an toàn của các nhãn bằng một khóa mật mã là hàm của khóa mật và bản thân dữ liệu, ví dụ như, id của bản ghi và tên thuộc tính; phương pháp này cung cấp có hiệu quả một khóa tách riêng hoàn toàn khỏi dữ liệu và lưu giữ trong bộ lọc an toàn. Nhược điểm chính của cách tiếp cận này là nó làm tăng các chức năng của bộ lọc đối với việc lưu giữ và truy lục các nhãn, điều đó nhất định sẽ làm tăng thêm tính phức tạp của phần mềm lọc và mâu thuẫn với quan niệm cho bộ lọc phải đủ đơn giản để có thể kiểm chứng an toàn hình thức.

Các nhãn phân loại có thể được áp dụng cho toàn bộ các quan hệ, các thuộc tính, các bản ghi hoặc các mục dữ liệu riêng lẻ. Cũng vậy, các tổng kiểm tra mật mã có thể được áp dụng ở mức quan hệ, thuộc tính, bản ghi hoặc mục dữ liệu. Dữ liệu chuyển giao cho bộ lọc phải làm sao cho có thể tính toán và phê chuẩn được tổng kiểm tra, nếu tổng kiểm tra được tính toán trên một khối lớn dữ liệu, thì một câu hỏi đơn giản liên quan tới một mục dữ liệu sẽ liên quan tới việc truy lục và chuyển những khối dữ liệu lớn tới bộ lọc. Mặt khác, các tổng kiểm tra được tính toán trên các mục dữ liệu đơn lẻ sẽ gây ra nguy cơ là những mục như thế có thể được chuyển bất hợp pháp từ bản ghi này sang bản ghi khác.

Chức năng của bộ lọc là tính toán các tổng kiểm tra có sử dụng một khóa mật đã nhớ và phê chuẩn các tổng kiểm tra của dữ liệu mà DBMS trả về cho nó và xác định xem câu trả lời cho các câu hỏi có nằm trong phạm vi mức đặc quyền của người sử dụng hay không. Các chức năng của bộ lọc phải được giữ càng đơn giản càng tốt để tạo điều kiện xác minh hình thức tính an toàn của nó. Như vậy bộ lọc không nên có các chức năng truy nhập và truy lục phức tạp của DBMS. Tuy nhiên, các tấn công của con ngựa thành Tơroa vẫn có thể nếu các nhãn an toàn và các tổng kiểm tra không được lưu giữ bởi bộ lọc độc lập với việc xử lý dữ liệu của DBMS. Ví dụ, một con ngựa thành Tơroa đơn giản có thể không điều chỉnh được mức phân loại an toàn của một mục dữ liệu. Như vậy nếu con ngựa thành Tơroa phát hiện rằng, bộ lọc đã thay đổi tổng kiểm tra của mục dữ liệu nào đó khi bản thân dữ liệu không thay đổi thì rõ ràng là, mức phân loại đã bị thay đổi. Con ngựa thành Tơroa khi đó có thể đơn giản khôi phục lại tổng kiểm tra trước đó và nhãn phân loại đã mã hóa của nó về giá trị ban đầu, và bộ lọc có thể không có khả năng phát hiện các hoạt động của con ngựa thành Tơroa.

Các tấn công của con ngựa thành Tơroa khó triệt được ngay cả khi bộ lọc có nhiệm vụ mở rộng là lưu giữ các nhãn và các tổng kiểm tra. Ví dụ, một cuộc tấn công có thể theo những giai đoạn sau:

- (*i*) kẻ cộng tác với con ngựa thành Tơroa khởi phát một câu hỏi khiến cho DBMS truy lục một tập hợp các

D

bản ghi có các mức phân loại an toàn thay đổi;

- (*ii*) con ngựa thành Toroa ghi nhớ tất cả những bản ghi đó;
- (*iii*) bộ lọc chỉ cho qua những bản ghi trong phạm vi mức truy nhập an toàn của người sử dụng;
- (*iv*) khi đó người sử dụng đưa ra một câu hỏi mà sẽ chỉ trả lại những bản ghi do bộ lọc đưa ra trong câu trả lời câu hỏi thứ nhất;
- (*v*) con ngựa thành Toroa ghi nhớ các tập hợp bản ghi được DBMS truy nhập theo yêu cầu của câu hỏi thứ hai và xóa chúng khỏi tập hợp đã thu thập ở (*ii*);
- (*vi*) con ngựa thành Toroa để rò các bản ghi có mức phân loại cao còn lại cho người sử dụng.

Xem a priori control, attribute, audit based control, audit expert, audit trail, bias, cell restriction, cell suppression, compromise, consistency, controlled rounding, cryptographic checksum, data protection, DBMS, disclosure risk, field, filter, grouping, implied queries control, inference control, information loss, key management, lattice model, memoryless control, multilevel database security, nagative disclosure, n-respondent, k%-dominance, operating system, order control, overlap control, personal disclosure, query set size control, random data perturbation, random rounding, random sample queries, record, relative table size control, sensitive statistic, spray paint, statistical database, subschema, systematic ranges, systematic rounding, table restriction, tracker, Trojan Horse, update inconsistency, view, work factor.

data bits ***(các) bit dữ liệu*** Trong truyền thông dữ liệu, số bit được truyền trên mỗi ký tự, không bao gồm các bit kiểm tra và định thời. *Xem* bit.

data bus coupler ***bộ ghép bus dữ liệu*** Trong truyền thông, một thành phần nối một số ống dẫn sóng quang và tạo ra hệ hai chiều thực chất bằng cách trộn và tách tất cả các tín hiệu trong nó. *Xem* data bus, fiber optics.

data capture ***thu nạp dữ liệu, bắt dữ liệu*** Trong tin học, tác động thu dữ liệu nhờ các thiết bị ngoại vi (ví dụ, terminal điểm trả tiền). *Xem* point-of-sale terminal.

data carrier detect ***tín hiệu dò sóng mang dữ liệu, tín hiệu DCD, DCD*** Trong truyền thông dữ liệu, tín hiệu giao tiếp từ modem tới thiết bị đầu cuối dữ liệu cho biết rằng tín hiệu sóng mang chất lượng thích hợp đang được thu nhận. *Xem* carrier, data terminal equipment.

data cell ***ô dữ liệu*** Ở các cấu trúc dữ liệu, đơn vị dữ liệu nhỏ nhất không thể phân chia tiếp được nữa (ví dụ, một bit). *So sánh với* cell. *Xem* bit.

data chain ***chuỗi dữ liệu*** Ở các cấu trúc dữ liệu, các khối dữ liệu liên kết với nhau bởi các con trỏ. *Xem* chained file.

data channel ***kênh dữ liệu*** *Xem* channel.

data circuit ***mạch dữ liệu*** Trong truyền thông dữ liệu, mạch cho phép thực hiện liên lạc hai chiều giữa hai thiết bị đầu cuối dữ liệu bất kỳ như máy tính, thiết bị hiển thị v.v.

data circuit terminating equipment ***thiết bị kết thúc mạch dữ liệu, DCE*** Trong truyền thông dữ liệu, bộ phận thiết bị nằm ở mỗi đầu của mạch dữ liệu cung cấp mọi chức năng cần để thiết bị lập, bảo trì và gánh cuối một mạch. Nó cũng thực hiện sự biến đổi và mã hóa tín hiệu giữa thiết bị cuối dữ liệu và đường điện thoại. *So sánh với* data terminal equipment. *Xem* modem.

data collection ***thu thập dữ liệu*** Trong tin học, hoạt động tích lũy dữ liệu từ nhiều vị trí vào một chỗ trước khi xử lý.

data communications ***truyền thông dữ liệu, liên lạc dữ liệu*** Sự trao đổi các thông báo, mã hóa dưới dạng dữ liệu nhị phân, giữa hai bên truyền thông (hoặc những người sử dụng đầu cuối) thường tách riêng về mặt địa lý qua một mạng truyền thông.

Tổng quan

Các bên liên lạc có thể là con người hoặc ứng dụng dựa trên máy tính như các hệ xử lý chuyển tác. Các loại thông báo cần trao đổi bao gồm:

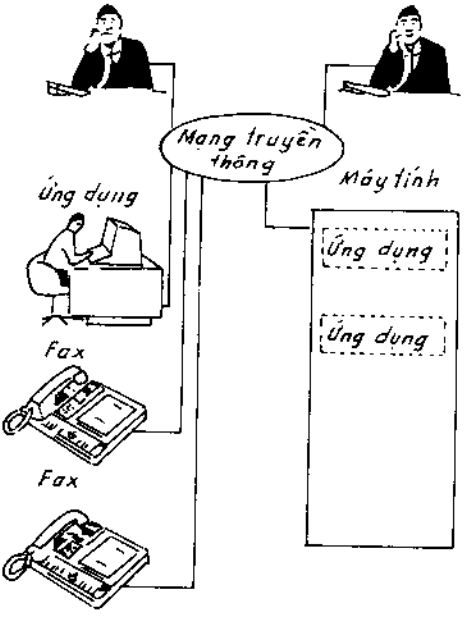
- thoại (ví dụ như nói chuyện điện thoại);
- dữ liệu (ví dụ như giao tác của máy trả nhân tiền tự động);
- hình ảnh (ví dụ như truyền hình);
- đồ họa (ví dụ như fax);
- văn bản (ví dụ như nội dung một cuốn sách);

hoặc tổ hợp bất kỳ của những loại đó.

Gắn với mỗi bên truyền thông là một thiết bị phía người sử dụng để tiến hành liên lạc hoặc hỗ trợ các ứng dụng truyền thông. Trong trường hợp đàm thoại, các thiết bị người sử dụng đầu cuối là các ống điện thoại, trong khi đó trong trường hợp một giao dịch ngân hàng, các thiết bị phía người sử dụng là máy trả nhân tiền tự động (ATM) và một dạng nào đó của hệ máy tính chủ hỗ trợ ứng dụng hoạt động ngân hàng của ATM (hình 1).

Mạng truyền thông là một tập hợp liên thông các thành phần vật lý để chuyển các thông báo giữa các thiết bị phía người sử dụng theo một tập hợp các tham số "chất lượng dịch vụ" được nhất trí từ trước. Những tham số đó quyết định phạm vi mà:

- dịch vụ do mạng truyền thông cung cấp phụ thuộc vào sự ngắt hoặc sự



data communications: *truyền thông dữ liệu*. Hình 1. Mạng truyền thông.

mất tính liên tục (tính sẵn sàng/độ tin cậy của dịch vụ mạng);

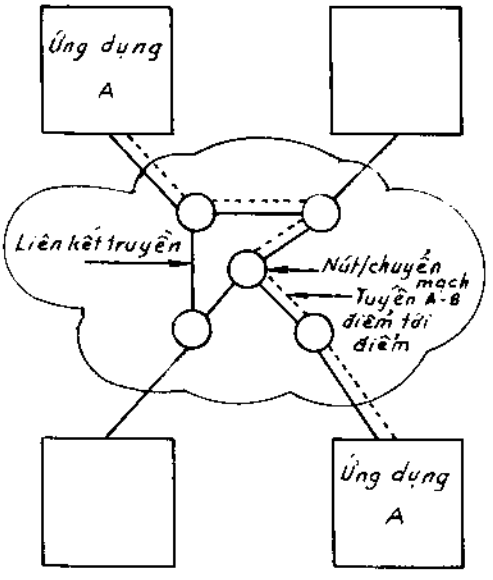
- tính bí mật của các thông báo được trao đổi có thể bị tổn thương (tính chất kín của thông báo);
- các thông báo được trao đổi bị sai lạc hoặc sửa đổi (tính toàn vẹn của thông báo);
- các thời gian trễ trong phân phát thông báo trên mạng truyền thông.

Tập hợp các thành phần vật lý cấu thành một mạng truyền thông bao gồm các liên kết truyền dẫn và các nút mạng. Các liên kết truyền dẫn là những đường truyền các thông báo khi chúng đi qua mạng. Nhiều loại phương tiện truyền được dùng để tạo các liên kết truyền dẫn gồm dây đồng (các cáp đôi xoắn, cáp đồng trục), thủy tinh (các cáp sợi quang) và không khí/chân không (để truyền bức xạ điện từ).

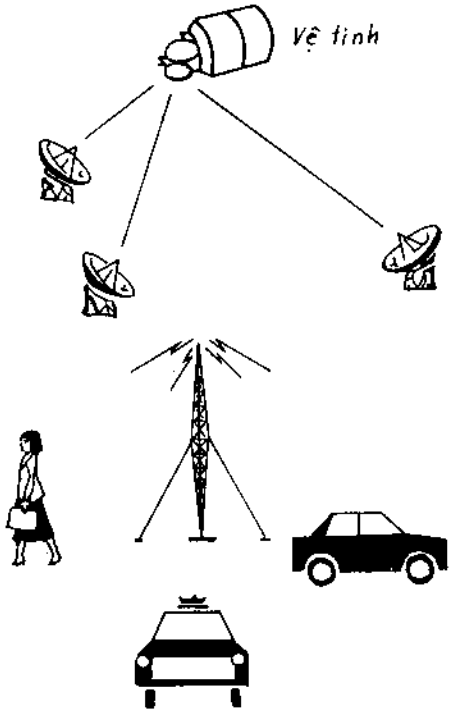
Các nút mạng, cũng gọi là các chuyển mạch hoặc các bộ xử lý thông báo giao tiếp (IMP), thường là các bộ xử lý máy tính để kết thúc các đoạn liên kết truyền dẫn riêng lẻ và định tuyến các thông báo giữa các thiết bị phía người dùng. Chúng cũng tạo ra giao diện giữa các thiết bị phía người dùng và mạng truyền thông.

Các mạng

Hai loại mạng truyền thông cơ bản là mạng truyền thông chuyển mạch và mạng truyền thông quảng bá.



data communications: *truyền thông dữ liệu.* Hình 2(a). Mạng chuyển mạch.



data communications: *truyền thông dữ liệu.* Hình 2(b). Mạng quảng bá.

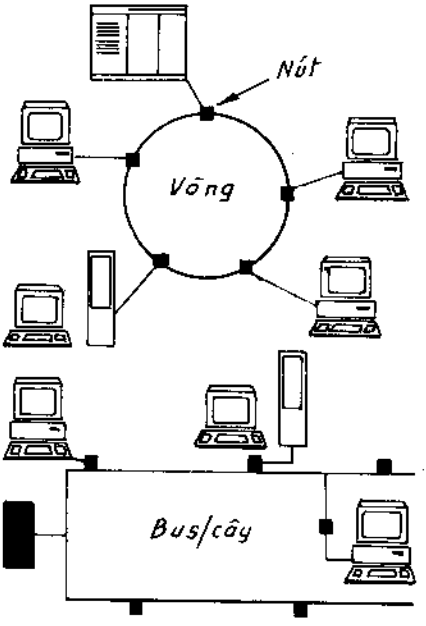
Mạng truyền thông chuyển mạch (hình 2a) bao gồm một tập hợp ghép nối các nút mạng và các đoạn liên kết truyền dẫn mà cùng tạo ra nhánh điểm tới điểm để trao đổi các thông báo giữa các thiết bị phía người dùng. Một ví dụ về kiểu mạng này là mạng điện thoại chuyển mạch công cộng (PSTN) dùng cho liên lạc thoại. Loại mạng chuyển mạch quan trọng khác, được thiết kế cho các thông báo dữ liệu (ví dụ như các giao dịch tài chính trong mạng ngân hàng), là mạng dữ liệu chuyển mạch gói (PSDN).

Ở mạng truyền thông quảng bá (phát rộng) có một đường liên kết truyền dùng chung duy nhất giữa tất cả các thiết bị phía người dùng. Các ví dụ về loại mạng này bao gồm các hệ thống vệ tinh, mạng điện thoại di động chia vùng (hình 2b) và các mạng cục bộ (LAN) (hình 2c).

Các tín hiệu truyền

Nút mạng nối các thiết bị phía người dùng với mạng. Nó biến đổi các thông báo từ kiểu và khuôn thức do các thiết bị phía người dùng sử dụng thành các tín hiệu truyền vật lý, sao cho chúng có thể được truyền qua đoạn liên kết truyền. Các thông báo cần truyền hoặc ở dạng số (ví dụ như một cuộc đàm thoại). Các ví dụ về các tín hiệu truyền vật lý bao gồm các mức điện áp trên một dây dẫn điện, cường độ chùm sáng trong cáp sợi quang và các sóng vô tuyến. Các tín hiệu truyền vật lý cũng hoặc ở dạng số (tức là mức tín hiệu chỉ có những giá trị rời rạc), hoặc ở dạng tương tự (tức là có mức tín hiệu thay đổi liên tục).

Những mạng truyền thông đầu tiên được thiết kế cho truyền thông tin thoại dùng các phương pháp báo hiệu truyền tương tự. Do đó, những mạng như vậy cần biến đổi các thông báo dữ liệu (do các hệ máy tính số tạo ra) thành các tín hiệu truyền tương tự. Quá trình này được gọi là điều biến và được thực hiện bởi một modem (bộ điều biến/giải điều). Mặt khác, các mạng truyền thông hiện đại được thiết kế để sử dụng các công nghệ truyền số và do đó, về cơ bản chúng là một hệ chuyển bit. Khi sử dụng những mạng đó, các thông báo tương tự như các cuộc đàm thoại và hình ảnh đầu tiên phải được biến đổi thành các tín hiệu truyền số nhờ bộ codec (bộ lập/giải mã). Điều biến mã xung (PCM) thường được dùng



data communications: *truyền thông dữ liệu.* Hình 2(c). Mạng cục bộ

để biến đổi một tín hiệu tương tự thành dạng số.

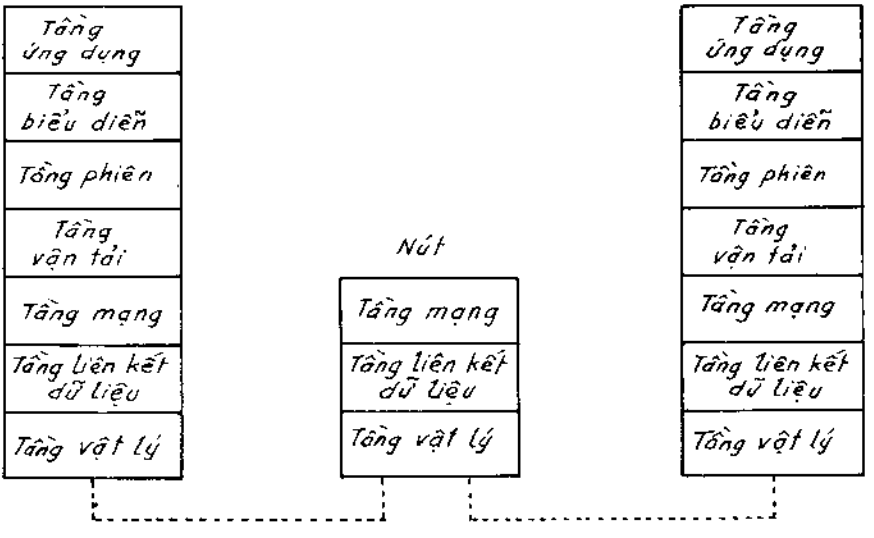
Các giao thức truyền thông

Mạng truyền thông được yêu cầu cung cấp một dịch vụ cho các thiết bị phía người dùng mà thỏa mãn một tập hợp xác định các tiêu chuẩn về "chất lượng dịch vụ", chẳng hạn tính toàn vẹn của thông báo.

Cần có một số quá trình để cho mạng truyền thông có thể kiểm soát và quản lý việc vận chuyển các thông báo giữa các thiết bị phía người dùng. Những quá trình đó là những sự thực hiện các quy tắc (hoặc giao thức) mà định rõ, ví dụ:

- cách quản lý sự trao đổi chung các thông báo;
- khuông dạng các thông báo cần trao đổi;
- cách ghi địa chỉ và định tuyến các thông báo;
- các thủ tục để phát hiện các lỗi truyền và khởi phát tác động hiệu chỉnh, tức là kiểm soát lỗi;
- các thủ tục để ngăn ngừa nút gửi khỏi làm tràn ngập nút nhận do truyền nhiều dữ liệu hơn khả năng nút nhận có thể xử lý, tức là điều khiển luồng.

Tập hợp toàn bộ các quy tắc chi phối sự trao đổi thông tin giữa các thiết bị phía người dùng, nhất là đối với các ứng dụng dữ liệu, có khả năng cực kỳ lớn. Do đó các quy tắc thường được nhóm lại thành các tầng, trong đó một tầng giao thức cho trước chứa một tập hợp các chức năng liên quan (ví dụ như sự trao đổi dữ liệu qua một liên kết truyền đơn lẻ, định tuyến thông báo qua một mạng).



data communications: *truyền thông dữ liệu.* Hình 3. Kiến trúc truyền thông.

Các tầng tạo thành hệ phân cấp giao thức hoặc kiến trúc truyền thông. Ví dụ về các kiến trúc truyền thông phân tầng bao gồm kiến trúc mạng hệ thống (SNA) do IBM phát triển, giao thức kiểm soát truyền/giao thức internet (TCP/IP) do Bộ quốc phòng Mỹ phát triển và mô hình tham chiếu kết nối các hệ thống mở (OSI RM) (hình 3) được phát triển dưới sự bảo trợ của Tổ chức tiêu chuẩn hóa quốc tế ISO.

Kiến trúc truyền thông OSI RM cung cấp một cơ sở để thảo luận về những đặc trưng tổng quát của những kiến trúc như vậy. Ví dụ, các giao thức mức vật lý (tầng vật lý) xác định cách thức cả hai tín hiệu điều khiển và dữ liệu được biểu diễn (ví dụ như giá trị các mức điện áp đối với logic 0 và 1). Ngoài ra, tầng vật lý xác định những đặc trưng tín hiệu truyền khác như thời khoảng của một tín hiệu và trình tự các tín hiệu cần để thực hiện việc chuyển dữ liệu. Tầng vật lý cũng xác định những đặc trưng cơ học, như kích thước của các bộ nối liên kết truyền và số lượng và sự bố trí các chân và các lỗ cắm. Một trong những chuẩn giao diện vật lý được dùng rộng rãi nhất là RS-232-C của Liên hiệp các ngành công nghiệp điện tử (EIA).

Vai trò của tầng liên kết dữ liệu trong kiến trúc truyền thông là điều khiển và quản lý quá trình trao đổi dữ liệu (phân biệt với các tín hiệu truyền) qua một liên kết truyền dẫn đơn. Yêu cầu cơ bản là đặt những dấu phân tách quanh các đoạn dữ liệu đã truyền để đảm bảo sự đồng bộ giữa máy gửi và máy nhận. Trong truyền không đồng bộ, các đoạn dữ liệu đã truyền là ký tự đơn (ví dụ 8 bit) được tách ra bởi các bit khởi và dừng. Các ký tự được truyền một cách độc lập (không đồng bộ) qua liên kết truyền dẫn. Trong truyền đồng bộ (định hướng bit), đơn vị chuyển dữ liệu là

01111110 Cờ (8 bit)	Địa chỉ (8 bit)	Kiểm soát (8 bit)	Thông tin	Tổng kiểm tra khung (FCS) (16 bit)	01111110 Cờ (8 bit)

Kiểm soát:

I: Thông tin	0	N(S)		P/F	N(R)
S: Giám sát	1	0	S	P/F	N(R)
U: Không đánh số	1	1	M	P/F	M

data communicatins: *truyền thông dữ liệu.* Hình 4. Khung truyền

khung (frame) truyền được phân tách nhau bởi một mẫu bit dành riêng như trường cờ (hình 4). Khung truyền chứa các đoạn thông báo người dùng đầu cuối có thể có độ dài tùy ý nhưng thường nằm trong khoảng 500-2000 bit. Tầng liên kết dữ liệu chịu trách nhiệm duy trì tính toàn vẹn của các đoạn dữ liệu riêng lẻ truyền qua liên kết. Với mục đích này, mỗi đoạn dữ liệu (tức là ký tự hoặc khung) mang thông tin kiểm soát lỗi bổ sung (do nút truyền tạo ra), cho phép nút nhận kiểm chứng (tới một mức cần thiết) rằng, không có sự sai lạc các đoạn dữ liệu trong khi truyền. Đối với truyền không đồng bộ định hướng ký tự, một bit chẵn lẻ đơn được gắn vào mỗi ký tự. Đối với truyền đồng bộ định hướng khung, một tổng kiểm tra khung (FCS) (thường 16 bit) được dùng để kiểm chứng từng đoạn dữ liệu riêng lẻ.

Các khung truyền cũng mang thông tin điều khiển bổ sung, dưới dạng các số thứ tự, do nút nhận dùng để phát hiện sự mất mát hoặc sự lặp các khung. Ở các sơ đồ kiểm soát phòng lỗi trong mỗi đoạn dữ liệu, có đủ thông tin kiểm soát lỗi, cho phép nút nhận phát hiện một lỗi truyền ở đoạn dữ liệu đó và cố gắng hiệu chỉnh lỗi. Các sơ đồ kiểm soát lỗi hồi tiếp yêu cầu nút nhận báo nhận các đoạn dữ liệu theo thứ tự và đúng, hoặc yêu cầu truyền lại trong trường hợp phát hiện có vấn đề (ví dụ như các đoạn dữ liệu sai lạc, các đoạn dữ liệu mất hoặc bị lặp).

Ở mức liên kết dữ liệu, nút gửi thực hiện một mức kiểm soát lỗi bổ sung trong quá trình truyền qua một cơ cấu "ấn định thời khoảng". Nếu không nhận được tín hiệu báo nhận đối với một đoạn dữ liệu trong một khoảng thời gian xác định trước, thì nút gửi khởi phát một hoạt động hiệu chỉnh, như tự động truyền lại đoạn dữ liệu (cho tới một giới hạn xác định).

Việc kiểm soát luồng được thực hiện ở mức liên kết dữ liệu, theo một trong hai cánh. Ở cách thứ nhất, nút nhận truyền một đoạn dữ liệu giám sát/điều khiển (ví dụ như ký tự điều khiển XOFF đối với truyền không đồng bộ, một khung (frame) tín hiệu báo máy thu không sẵn sàng (RNR) đối với truyền đồng bộ) cho nút gửi để ngăn sự truyền tiếp tục. Khi nút nhận đã sẵn sàng để truyền tiếp, thì nó gửi một đoạn dữ liệu giám sát/điều khiển tương ứng (ví dụ, ký tự điều khiển XON đối với truyền không đồng bộ, một khung (frame) báo máy thu sẵn sàng (RR) đối với truyền đồng bộ). Trong cơ chế điều khiển luồng cơ bản thứ hai được dùng ở các sơ đồ truyền định hướng khung, nút gửi sẽ ngừng truyền khi số các khung đã truyền không nhận được tín hiệu báo nhận tương ứng, đạt tới một giới hạn xác định trước. Giới hạn được gọi là Cửa sổ gửi và sự truyền lại tiếp tục khi các tín hiệu báo nhận tới nút nhận.

Tầng liên kết dữ liệu cũng kiểm soát sự truy nhập liên kết truyền trong các mạng phát rộng (ví dụ các mạng cục bộ) trong một số các thiết bị đầu cuối cùng chung một liên kết chung. Các sơ đồ quyết định (trọng tài) truy nhập liên kết bao gồm các cơ chế hỏi vòng, các cơ chế chuyền thẻ bài (khi được dùng trong các LAN dùng giao thức vòng thẻ

bài và bus thẻ bài), và các cơ chế đua tranh như truy nhập đa cảm biến sóng mang/dò xung đột (CSMA/CD) dùng trong hệ LAN Ethernet.

Chức năng hàng đầu của tầng mạng trong kiến trúc ở hình 3 là cung cấp định tuyến điểm tới điểm các đoạn dữ liệu, giữa các thiết bị phía người dùng, thông qua mạng truyền thông. Yêu cầu về các khả năng định tuyến này nảy sinh trong các mạng truyền thông chuyển mạch, tức là các mạng trong đó đường điểm tới điểm được tạo ra bởi một tập hợp kết nối các liên kết truyền và các nút (ví dụ như mạng dữ liệu chuyển gói PSDN). Trong những mạng như thế, một nút mạng truyền thông có thể lựa chọn một số liên kết truyền dẫn đến đích cuối cùng.

Ở mức tầng mạng, các đoạn dữ liệu được gọi là các gói tin và một gói đơn thường có độ dài dưới 2000 bit. Tùy thuộc vào kiểu thông báo được trao đổi giữa các thiết bị phía người dùng, một gói tin có thể chứa một thông báo đầy đủ hoặc một phần thông báo.

Tầng mạng hoạt động theo một trong hai chế độ cơ bản. Ở chế độ mạch ảo (hoặc định hướng nối kết), các thiết bị phía người dùng đầu tiên trao đổi các gói giám sát/điều khiển, thiết lập một tuyến điểm tới điểm giữa các thiết bị phía người dùng. Ngay khi thiết lập được tuyến qua mạng truyền thông, tất cả các gói sau đó chứa các thông báo giữa các thiết bị phía người dùng sẽ sử dụng tuyến này. Về hoạt động, cách thức này tương tự với mạng điện thoại chuyển mạch công cộng (PSTN) trong đó, một mạch điểm tới điểm được thiết lập giữa các thiết bị phía người dùng trong thời gian kết nối cuộc gọi.

Chế độ hoạt động cơ bản khác của tầng mạng là chế độ gói dữ liệu (hoặc không kết nối). Ở chế độ này, các gói tin (hoặc gói dữ liệu) chứa các thông báo đã được các nút mạng xử lý như các thực thể khép kín. Mỗi gói được định tuyến độc lập qua mạng và sự phân phát điểm tới điểm dựa trên cơ sở "cố hết sức". Do đó, ở chế độ hoạt động gói dữ liệu, các gói có thể tới theo trình tự bất kỳ, trong khi ở chế độ hoạt động mạch ảo thì trình tự của gói được duy trì. Chế độ hoạt động gói dữ liệu tương tự với hệ thống bưu điện.

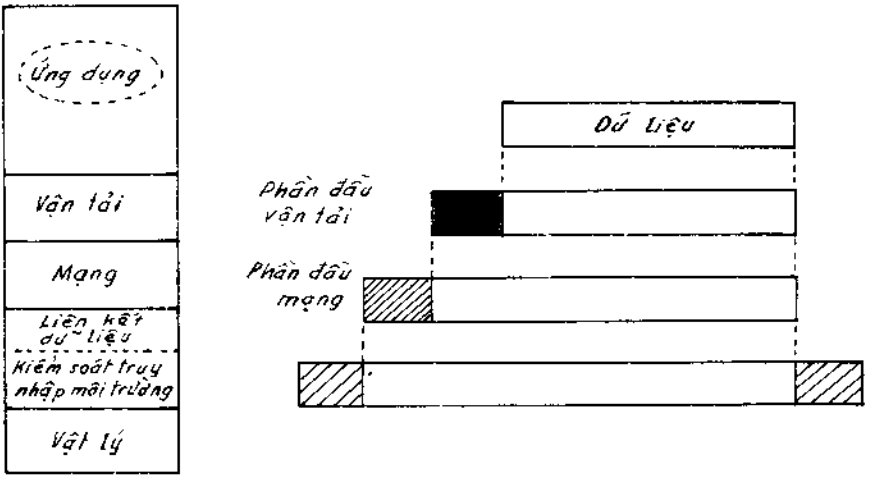
Các mục tiêu chính trong định tuyến mạng là phân phát các gói một cách tin cậy (và đúng) trong mạng với độ trễ tối thiểu và chi phí ít nhất. Một số chiến lược định tuyến khác nhau đã được phát triển để đạt được những mục tiêu đó, mặc dù phần lớn đều dựa trên dạng thư mục (hoặc bảng) nào đó lưu giữ ở mỗi nút mạng. Ở mức đơn giản nhất, thư mục chứa một tập hợp thông tin chỉ cho biết cần chọn liên kết truyền nào để tới được một nút riêng. Sơ đồ "định tuyến cố định" này (hình 5) có ưu điểm đơn giản, nó có tính năng kém trong các tình huống tải đỉnh (tức là trong các khoảng thời gian tắc nghẽn trầm trọng) và cũng thiếu tính linh hoạt khi có sự cố thành phần. Các chiến lược khác sử dụng nhiều phương pháp thích ứng cho phép các nút mạng giám sát các điều kiện mạng qua việc trao đổi thông tin giám sát/điều khiển và phản ứng động.

Chức năng chính của tầng vận tải trong

minh họa này là tạo ra sự quản lý điểm tới điểm về sự trao đổi các thông báo giữa các thiết bị phía người dùng. Yêu cầu đối với các chức năng quản lý trao đổi như thế (ví dụ như tính toàn vẹn thông báo điểm tới điểm) nảy sinh trong trường hợp mạng truyền thông sử dụng chế độ hoạt động gói dữ liệu (không kết nối) ở mức tầng mạng, nơi có thể không có sự đảm bảo toàn bộ các gói tin sẽ được phân phát. Tương tự ở chế độ hoạt động mạch ảo, nút mạng có thể gặp các vấn đề phần cứng, phần mềm hoặc truyền dẫn vốn đòi hỏi nó thiết lập lại hoặc một đường nối mạch ảo đơn hoặc nhiều đường nối.

cầu gói tin của tầng mạng. Sau đó nó gắn thêm cho mỗi đoạn dữ liệu như vậy một thông tin giám sát/kiểm soát lỗi, chẳng hạn một tổng kiểm tra được tính toán và các số hiệu thứ tự đoạn dữ liệu. Thủ tục tổng kiểm tra cho phép tầng vận tải tương ứng ở bên nhận phát hiện các lỗi truyền mà các thủ tục kiểm soát lỗi ở các tầng liên kết dữ liệu đã không phát hiện ra. Thông tin đánh số thứ tự đoạn dữ liệu cho phép phát hiện các đoạn dữ liệu bị mất hoặc lặp lại.

Các tầng phiên, tầng biểu diễn và tầng ứng dụng trong mô hình tham chiếu của OSI cung cấp các chức năng liên quan tới việc quản lý một ứng dụng mà



data communications: *truyền thông dữ liệu.* **Hình 5. Phân cấp giao thức.**

Với tư cách giữ một phần vai trò quản lý, tầng vận tải có thể được yêu cầu phân chia các thông báo, từ các thiết bị phía người dùng, thành các đoạn dữ liệu có kích thước thoả mãn các yêu

các thiết bị phía người sử dụng đang dùng.

Chuẩn X.25 của CCITT là chuẩn được dùng rộng rãi để truy nhập các mạng chuyển mạch gói. Chuẩn xác định một

giao thức ba tầng cho chế độ hoạt động mạch ảo bao gồm mức vật lý, mức liên kết và mức gói tin.

Giao thức kiểm soát truyền dẫn/giao thức liên mạng (TCP/IP) do Bộ quốc phòng Hoa Kỳ phát triển cung cấp những chức năng tương tự các chức năng đã mô tả đối với các tầng vận tải và mạng trong ví dụ ở trên. Trong kiến trúc TCP/IP, tầng giao thức liên mạng (IP) cung cấp dịch vụ gói dữ liệu (không kết nối) cho tầng giao thức kiểm soát truyền dẫn (TCP). Tầng TCP tạo ra sự kiểm soát lỗi điểm tới điểm và kiểm soát luồng tin cậy.

Mạng số dịch vụ kết hợp (ISDN) là một sự phát triển quan trọng trong truyền thông dữ liệu; tất cả các chức năng báo hiệu và chuyển mạch của mạng đều được thực hiện nhờ sử dụng các phương pháp số. Điều đó sẽ có tác động lớn lao tới một loạt các dịch vụ do mạng cấp và chi phí và độ tin cậy của những dịch vụ đó. *Xem* application layer, asynchronous transmission, ATM, CCITT, cellular radio, codec, connectionless service, CSMA-CD, datagram, data link layer, Ethernet, fiber optics, fixed routing, flow control, forward error control, local area network, interface message processor, international standards organization, ISDN, MODEM, network layer, open systems interconnection, packet, packet switching network, physical layer, polling, presentation layer, protocol, pulse code modulation, RS-232C, session layer, sliding window protocol, start bit, stop bit, synchronous transmission, system network architecture, token ring, token bus, transmission control protocol/ internet protocol, transport layer, virtual circuit, XON-XOFF protocol, X.25.

data compression ***nén dữ liệu*** (1) Trong mã hóa, sự giảm kích thước của dữ liệu nhờ các kỹ thuật mã hóa khai thác các dư thừa trong dữ liệu. *So sánh với* data compaction, data reduction. *Xem* redundancy. (2) Trong các hệ thống nhớ, kỹ thuật tiết kiệm không gian nhớ bằng cách loại bỏ các khe, các trường trống, các dư thừa hoặc những dữ liệu không cần thiết để giảm bớt độ dài của các bản ghi hoặc các khối. *Xem* null suppression.

data confidentiality ***tính bí mật của dữ liệu*** Trong an toàn dữ liệu, trạng thái tồn tại khi dữ liệu được lưu giữ bí mật và được bảo vệ tránh những tiết lộ không được phép. *So sánh với* data integrity. *Xem* ADP availability, application confidentiality, application integrity, confidentiality.

data connection ***kết nối dữ liệu*** Trong truyền thông dữ liệu, sự hợp mạng của một số các mạch được thiết kế để mang các tín hiệu dữ liệu. Cần có thiết bị chuyển mạch đặc biệt để dữ liệu có thể được truyền giữa các thiết bị cuối dữ liệu. *Xem* data terminal equipment, switching.

data contamination ***(sự) ô nhiễm dữ liệu*** Trong an toàn máy tính, quá trình hoặc tác động cố ý hoặc ngẫu nhiên dẫn tới sự thay đổi tính toàn vẹn của dữ liệu ban đầu. *Xem* data diddling.

data corruption ***(sự) sai lạc dữ liệu*** Trong an toàn dữ liệu, sự vi phạm cố ý hoặc ngẫu nhiên tính toàn vẹn của

dữ liệu. *Xem* data integrity.

data coupler ***bộ ghép dữ liệu*** Trong truyền thông dữ liệu, thiết bị cho phép nối các modem của khách hàng với mạng điện thoại. Nó giới hạn công suất đưa vào đường truyền và cung cấp các chức năng điều khiển mạng và báo hiệu. *Xem* MODEM.

datacrime ***virut Datacrime*** Trong an toàn dữ liệu, virut tự mã hóa, lây nhiễm các tệp COM, làm sai lạc các tệp chương trình và OVL, tạo khuôn và ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

Datacrime-B ***virut Datacrime-B*** Trong an toàn máy tính, virut tự mã hóa, lây nhiễm các tệp COM, làm sai lạc các tệp chương trình và OVL, tạo khuôn và ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

Datacrime II ***virut Datacrime II*** Trong an toàn máy tính, virut tự mã hóa, lây nhiễm các tệp COM và EXE, làm sai lạc các tệp chương trình và OVL, tạo khuôn và ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

Datacrime II-B ***virut Datacrime II-B*** Trong an toàn máy tính, virut tự mã hóa, lây nhiễm các tệp COMMAND.COM, COM và các tệp EXE, làm sai lạc các tệp chương trình và OVL, định dạng và ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

data-dependent protection ***bảo vệ phụ thuộc dữ liệu*** Trong an toàn dữ liệu, sự bảo vệ dữ liệu ở mức phù hợp với mức nhạy cảm của các bộ phận dữ liệu riêng lẻ chứ không phải với mức nhạy cảm của toàn bộ tệp chứa cả các bộ phận dữ liệu.

data description language ***ngôn ngữ mô tả dữ liệu*** Ở các cơ sở dữ liệu, ngôn ngữ để mô tả dữ liệu. Những ngôn ngữ như thế cung cấp các định nghĩa rất chi tiết về các cấu trúc và các quan hệ của dữ liệu. Trong một số trường hợp, ngôn ngữ chỉ liên quan tới cấu trúc logic của cơ sở dữ liệu, trong những trường hợp khác nó cũng liên quan tới các mô tả liên quan tới cách mà dữ liệu được tổ chức ở các thiết bị nhớ vật lý. *So sánh với* data manipulation language.

data dictionary ***từ điển dữ liệu*** Ở các cơ sở dữ liệu, kho chứa tập trung thông tin về dữ liệu được lưu, cung cấp các chi tiết về ý nghĩa, quan hệ với dữ liệu khác, nguồn gốc, cách sử dụng và khuôn thức. Nó là một phần quan trọng của hệ quản lý cơ sở dữ liệu cung cấp thông tin về bản chất và cách sử dụng dữ liệu đã nhớ, do đó cho người quản trị cơ sở dữ liệu có sự điều khiển chung đối với một cơ sở dữ liệu phát triển. *Xem* database administrator; database management system.

data diddling ***gian lận dữ liệu*** Trong an toàn dữ liệu, sự thay đổi các giá trị dữ liệu đã nhớ cho các mục đích bất hợp pháp. *Xem* data contamination.

data element ***mục dữ liệu, phần tử dữ liệu*** *Đồng nghĩa với* data item.

data-encrypting key ***khóa mã dữ liệu*** Trong quản lý khóa, khóa mật mã dùng để mã hóa (và giải mã) dữ liệu. *So sánh với* key-encrypting key. *Đồng nghĩa với* data key, primary key.

data encryption algorithm ***thuật toán mã dữ liệu, DEA*** Trong an toàn

dữ liệu, chuẩn mã ANSI, ANSI X3.92 - 1981, đồng nhất với hàm mật mã vốn tạo thành một phần của chuẩn mã dữ liệu, Công bố 46 của FIPS. *Xem* American National Standards Institute, data encryption standard.

data encryption standard ***chuẩn mã dữ liệu, DES*** Trong lập mã, chuẩn mã hóa dữ liệu lặc tả một thuật toán được thực hiện trong các thiết bị phần cứng điện tử và được sử dụng để bảo vệ dữ liệu máy tính bằng mật mã. Thuật toán là một mật mã tích sử dụng các khối dữ liệu 64 bit và một khóa 64 bit. Chuẩn này được Viện tiêu chuẩn quốc gia Hoa Kỳ đưa ra vào tháng giêng 1977, như Công bố 46 của FIPS. Nó đã trở thành thuật toán bắt buộc đối với các cơ quan liên bang Hoa Kỳ từ tháng sáu năm 1977.

DES dựa trên một mật mã tích trước đó, gọi là Lucifer và do IBM phát triển. Nó sử dụng các khối dữ liệu 64 bit và một khoá 64 bit. Tuy nhiên, khóa mật mã sử dụng 8 bit chẵn lẻ và như vậy theo quan điểm mật mã, nó chỉ là khóa 56 bit. Luồng dữ liệu trong thuật toán DES được minh hoạ trên hình 1.

Dữ liệu được tiến hành chuyển vị và thay thế lần lượt trong các hộp P (IP, IP^{-1}, E và P) và các hộp S. Khóa cũng phải qua các phép chuyển vị trong các hộp hoán vị $PC1$, $PC2$ và các thanh ghi dịch C và D. Có 16 vòng thao tác đối với dữ liệu và mỗi vòng gồm các phép tính toán với một khóa 48 bit khác nhau phát triển từ khóa mật mã 64 bit gốc. Các phép tính toán với dữ liệu được minh hoạ ở sơ đồ thanh ở hình 2.

Khối dữ liệu vào là khối đầu tiên chịu hoán vị trực tiếp, IP. Trong trường hợp này, các bit đơn giản được sắp xếp lại như ở bảng 1.

Bảng 1

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Như vậy bộ tám đầu tiên của đầu vào xuất hiện tương ứng ở các vị trí bit 40, 8, 48, 16, 56, 24, 64 và 32 của đầu ra. Cả hoán vị này cả đầu vào của nó đều không bị ảnh hưởng bởi khóa; nó được coi như đã được tính đến để thuận tiện cho việc thực hiện nhưng nó không có chức năng mật mã. Đầu ra của giai đoạn này được tách thành hai khối 32 bit, khối bên trái được chuyển qua thanh ghi 32 bit $L32$, còn khối bên phải qua $R32$. 32 bit của $R32$ sau đó được hoán bị theo phép hoán vị mở rộng E (bảng 2).

Bảng 2

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Bảng 3

Các hộp *S*

Các cột

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
12	1	10	15	9	2	6.	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	23	12
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Trong trường hợp này, một số trong các đầu vào xuất hiện ở 2 vị trí ra, ví dụ như bit 4 xuất hiện ở các vị trí ra 5 và 7. Theo cách này, khối đầu vào 32 bit vừa được chuyển vị vừa được mở rộng thành khối ra 48 bit. Đầu ra của khối *E* được cộng modulo 2 với đầu ra của giai đoạn thứ nhất của bộ sinh khoá và kết quả phải qua mã pháp thay thế trong tám hộp *S*. Những hộp *S* đó hoạt động song song, mỗi hộp nhận các đầu vào 6 bit và sinh ra các đầu ra 4 bit (bảng 3).

Đầu vào 48 bit được chia thành tám khối 6 bit, mỗi khối đưa vào một hộp *S*. Mỗi hộp *S* có thể được xem như một ROM chứa các dữ liệu được tổ chức thành 4 hàng và 16 cột, do đó mỗi vị trí trong ma trận đối với hộp *S* tương ứng với một trong 64 đầu vào có thể. Phần tử ma trận được xác định theo hàng, được chọn bằng các bit 1 và 6 của đầu vào, ví dụ như 1xxxx0 chọn hàng 2. Các bit từ 2...5 của đầu vào quyết định cột của phần tử ma trận, ví dụ nếu khối 6 bit đầu tiên của đầu vào là 110000 thì hàng 2 (10) cột 8 (1000) của hộp *S* đầu tiên được chọn cho đầu ra 1111 (15 theo hệ thập phân).

Các đầu ra 4 bit của 8 hộp *S* được tập hợp lại thành khối ra 32 bit mà sau đó được hoán vị theo phép hoán vị trực tiếp *P* (bảng 4). Hoán vị này đơn giản chuyển vị đầu vào 32 bit thành đầu ra 32 bit, ví dụ như bit 1 của đầu vào được chuyển vị thành bit 9 của đầu ra. Đầu ra 32 bit của *P* được cộng "loại trừ - hoặc" (EXCLUSIVE OR) với nội dung của thanh ghi *L*32 và kết quả được đặt vào một bộ nhớ tạm 32 bit.

Bảng 4

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Các nội dung của thanh ghi *R*32 được chuyển sang thanh ghi *L*32 và sau đó *R*32 được điều chỉnh bằng nội dung của thanh ghi 32 bit tạm thời. Việc đó hoàn thành vòng đầu tiên trong 16 vòng; khi đó bộ sinh khóa tạo ra khóa 48 bit mới và quá trình được lặp lại với nội dung mới của *L*32 và *R*32.

Sau 16 phép lặp như thế, nội dung của các thanh ghi *L* và *R* được đưa chéo vào các khối đầu vào 32 bit bên phải và bên trái của hộp hoán vị IP^{-1}, tạo ra hoán vị ngược của *IP* và đầu ra của thủ tục mã hóa.

Khóa DES có 64 bit nhưng chỉ có 56 bit có thể được chọn độc lập, 8 bit còn lại là các bit chẵn lẻ và do đó không có chức năng mật mã. Bộ sinh khóa nhận một khóa 64 bit nhập vào hộp hoán vị *PC*1 mà ở đó, các bit thứ tám đều được loại bỏ và các bit còn lại được hoán vị theo dữ liệu ở bảng 5, tức là bit 57 xuất hiện như bit đầu ra 1, bit 8 được loại bỏ và bit 9 được chuyển vị thành bit 7.

Bảng 5

PC1

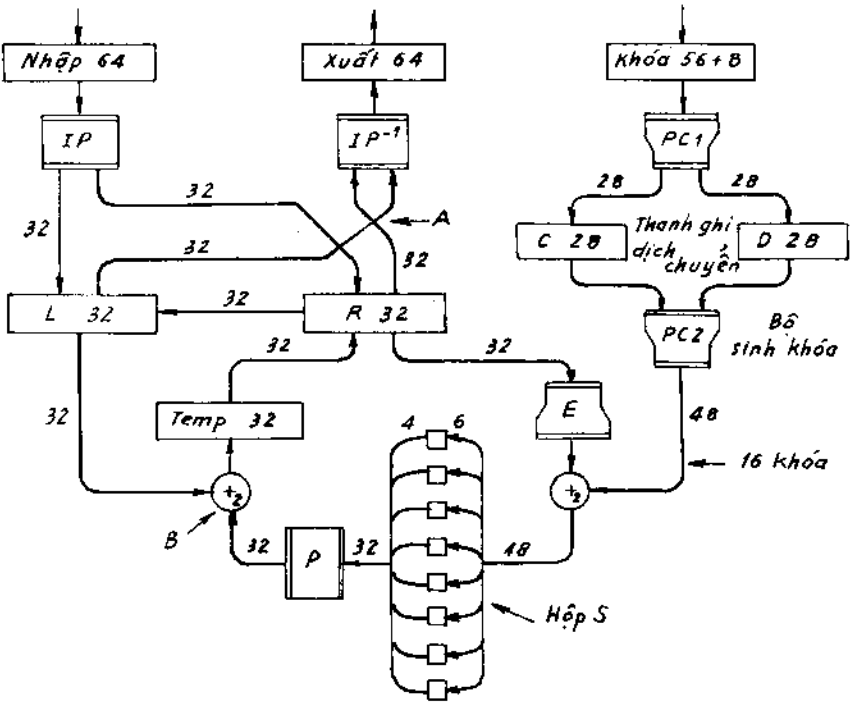
	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
C	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
D	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

28 bit bên trái nhất của đầu ra được chuyển sang thanh ghi dịch *C* và bên phải nhất sang thanh ghi dịch *D*. Dữ liệu ở những thanh ghi đó được dịch về bên trái 1 hoặc 2 bit, trước mỗi vòng trong 16 vòng (bảng 6).

Bảng 6

Các phép dịch khóa để mã hóa

Khóa	*Số dịch sang bên trái*
k_1	1
k_2	1
k_3	2
k_4	2
k_5	2
k_6	2
k_7	2
k_8	2
k_9	1
k_{10}	2
k_{11}	2
k_{12}	2
k_{13}	2
k_{14}	2
k_{15}	2
k_{16}	1



data encryption standard: *tiêu chuẩn mã dữ liệu.* Hình 1. Cấu trúc logic.

Nội dung của những thanh ghi này sau đó được đưa vào hộp hoán vị $PC2$ đã chọn (bảng 7), cung cấp đầu ra khóa 48 bit vốn được cộng "loại trừ - hoặc" (EXCLUSIVE OR) với đầu ra của hoán vị E.

Bảng 7

PC2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Quá trình giải mã liền một mạch và lặp lại có hiệu quả hoạt động mã hóa với thứ tự các khóa $k_1, k_2, \ldots k_{16}$ đảo ngược. Quá trình giải mã có thể được mô tả tốt nhất theo biểu diễn đại số các phép biến đổi.

Giả sử R_j, L_j, K_j biểu diễn nội dung của các thanh ghi $L32$, $R32$ và khóa 48 bit (hình 1) ở vòng thứ j. Trong quá trình mã hóa:

$$L_j = R_{j-1} \qquad \text{pt1}$$

$$R_j = L_{j-1} +_2 F(R_{j-1}, k_j) \qquad \text{pt2}$$

trong đó $F(R_{j-1}, k_j)$ là đầu ra của hộp P ở vòng thứ j và $+_2$ biểu thị phép EXCLUSIVE OR. Những phương trình đó có thể được viết lại:

$$R_{j-1} = L_j$$

$$R_j +_2 F(R_{j-1}, k_j) = L_{j-1} +_2 F(R_{j-1}, k_j) + F(R_{j-1}, k_j)$$

khi đó $A +_2 A = 0$

Do đó $R_{j-1} = L_j$ pt3

và $L_{j-1} = R_j +_2 F(R_{j-1}, k_j)$ pt4

thay thế L_j cho R_{j-1} ở phương trình 4 ta có

$$L_{j-1} = R_j +_2 F(L_j, k_j) \qquad \text{pt5}$$

Quá trình mã hóa và giải mã được minh họa trên hình 3. Ở giai đoạn mã hóa thứ nhất:

$$R_2 = L_1 +_2 F(R_1, k_1)$$

$$L_2 = R_1$$

Nếu bây giờ chúng ta tuân theo quá trình từ $L16$, $R16$, $L16$ được chuyển vị bởi IP^{-1} để trở thành nửa bên phải của khối bản mã, ở giai đoạn giải mã, nó chịu phép biến đổi ngược và sau đó chuyển sang thanh ghi $R0$. Do đó ở giai đoạn giải mã thứ nhất, $R0$ chứa $L16$, tương tự $L0$ chứa $R16$. Bây giờ từ các phương trình 3 và 5; ta có

$$R_{15} = L_{16} \qquad \text{pt3}$$

và $L_{15} = R_{16} +_2 F(L_{16}, k_{16})$ pt4

Do đó hoạt động mã hóa trên nội dung của $L0$ (= $R16$) và $R0$ (= $L16$) với khóa k_{16} sẽ có tác dụng chuyển các giá trị $L15$ và $R15$ tương ứng sang các thanh ghi $R1$ và $L1$. Tiếp tục theo cách này sẽ dẫn đến bản rõ ban đầu ở cuối quá trình giải mã.

Những phương trình đó cho thấy rằng, sự giải mã được thực hiện nhờ thực hiện có hiệu quả quá trình mã hóa với trình tự 16 khóa $k_1, k_2, \ldots k_{16}$ đảo ngược lại. Việc tạo ra các khóa theo trình tự đảo ngược để giải mã được thực hiện bởi bộ sinh khóa. Trong quá trình mã, nội dung của các thanh ghi dịch 28 bit C và D được dịch về bên phải tổng cộng 28 lần, như vậy khóa đầu tiên để giải mã k_{D1} tương ứng với k_{16}. Tập hợp các phép dịch sau đó đối với C và D trong quá trình giải mã được cho ở bảng 8.

Bảng 8

Các phép dịch khóa để giải mã

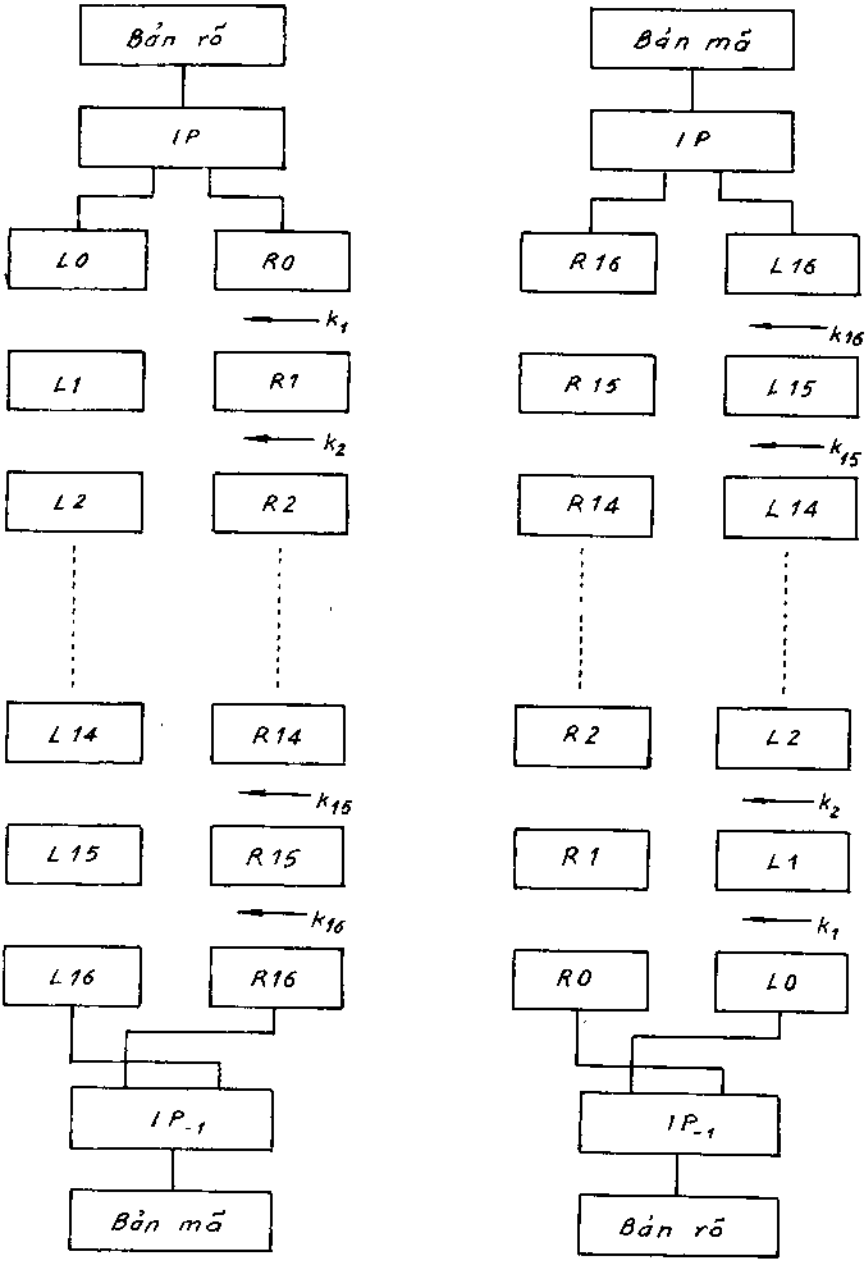
Khóa	*Số lần dịch về bên phải*
k_1	0
k_2	1
k_3	2
k_4	2
k_5	2
k_6	2
k_7	2
k_8	2
k_9	1
k_{10}	2
k_{11}	2
k_{12}	2
k_{13}	2
k_{14}	2
k_{15}	2
k_{16}	1

Các quá trình mã hóa và giải mã phụ thuộc vào trình tự các khóa được tạo ra bởi bộ sinh khóa. Nếu đối với một khóa cá biệt $k_1 = k_{16}$, $k_2 = k_{15}$ v.v. thì trong các quá trình mã hóa và giải mã có cùng trình tự; trong trường hợp này phép mã hóa kép sẽ tạo ra thông báo bản gốc ban đầu; những khóa như thế được gọi là khoá yếu.

Tình huống tương tự nảy sinh trong trường hợp các cặp khóa A, B có tính chất $A_1 = B_{16}$, $A_2 = B_{15}$... Trong trường hợp này, phép mã hóa bằng một khóa, tiếp đó lại được mã với khóa thứ hai sẽ tạo ra bản gốc ban đầu; các cặp khóa như thế được gọi là khóa bán yếu.

Tính an toàn của DES là chủ đề của một cuộc tranh cãi sôi nổi và là chủ đề khảo sát của Thượng viện Hoa Kỳ. Cuộc tranh cãi tập trung vào độ dài của khóa DES và vào khả năng để các hàm cửa sập mật được thiết kế vào các hộp S, không có hồ sơ về thiết kế và các lý do xây dựng các hộp S chưa bao giờ được đưa ra. Độ dài thực sự của khóa DES là 56 bit và khả năng của một máy DES chuyên dụng với nhiều bộ xử lý song song có thể rà soát mọi khóa có thể, đã được tranh cãi nhưng kết luận của Ủy ban lựa chọn của Thượng viện là độ an toàn của DES là thích hợp đối với lĩnh vực sử dụng được đề xuất trong khoảng thời gian đã định của nó. Độ dài hiệu quả của các khóa DES có thể được tăng lên nhờ mã hóa bội và kỹ thuật này được dùng cho các khóa mã khóa trong một số sơ đồ quản lý khoá. DES biến đổi có hiệu quả khối bản gốc 64 bit thành khối bản mã 64 bit nhờ sử dụng khóa 56 bit. Nó có ưu điểm không mở rộng thông báo và khóa tương đối ngắn. Thực ra, đối với một khóa đã cho, DES có thể được xem như một sổ mã với 2^{64} mục từ. Như vậy chế độ DES thông thường thực tế được gọi là sổ mã điện tử và nó có một điểm yếu mật mã nếu các thông báo được tạo khuôn thức cao được mã hóa bằng cùng khóa. Một kẻ tấn công có thể phát hiện sự có mặt của các khối bản mã thường hay xuất hiện và có thể suy ra các cặp bản gốc - bản mã hoặc ít nhất, thu được một thông tin nào đó về bản chất của lưu lượng.

Những chế độ hoạt động DES khác, tức là kết nối khối mã, hồi tiếp mật mã và hồi tiếp đầu ra có thể khắc phục được những thiếu sót đó của hoạt động sổ mã điện tử. DES có thể thực hiện bằng



data encryption standard: *tiêu chuẩn mã hoá dữ liệu.* Hình 2. Sơ đồ thang.

phần mềm hoặc phần cứng, các thực hiện LSI có thể cho thời gian tính toán cỡ micro giây, do đó tạo ra tốc độ dữ liệu cao cho các kênh truyền thông an toàn. *Xem* ciphertext, cryptographic key, electronic codebook, EXCLUSIVE OR, FIPS, Lucifer, multiple DES encipherement, parity bit, P box, plaintext, product cipher, S box, semiweak key, substitution cipher, trapdoor, weak key.

data exchange ***trao đổi dữ liệu*** Trong an toàn thông tin, các chức năng đảm bảo an toàn của dữ liệu trong khi truyền qua các kênh truyền thông. *Xem* information technology security evaluation criteria.

data flow analysis ***phân tích luồng dữ liệu*** Trong an toàn máy tính, phương pháp phân tích tĩnh kiểm tra các mẫu dữ liệu dùng trong chương trình, tìm kiếm để tham chiếu tới các biến không được xác định hoặc thiết lập, các biến đã thiết lập nhưng chưa được xác định, các biến đã thiết lập và không được sử dụng v.v... *Xem* static analysis.

data flow control ***kiểm soát luồng dữ liệu*** *Xem* information flow control.

data frame ***khung dữ liệu*** Trong truyền thông dữ liệu, gói dữ liệu truyền qua một mạng biểu diễn toàn bộ hoặc một phần thông báo. *So sánh với* acknowledgement frame. *Xem* frame.

datagram ***gói dữ liệu, đơn vị dữ liệu*** Trong truyền thông dữ liệu, gói tin độc lập trong một hệ chuyển gói tin chứa đủ thông tin định tuyến để nó đến được địa chỉ đích cần thiết. *Xem* datagram, service, packet.

datagram service ***dịch vụ gói dữ liệu*** Trong truyền thông dữ liệu, dịch vụ không kết nối trong đó, không có sự báo nhận đến của các gói dữ liệu riêng lẻ. *So sánh với* connectionless service. *Xem* datagram.

data haven ***nơi dữ liệu trú ẩn*** Trong lập pháp, một vùng không có luật bảo vệ dữ liệu. *Xem* data protection.

data independence ***tính độc lập dữ liệu*** Ở các cơ sở dữ liệu, tính chất của cấu trúc dữ liệu loại bỏ sự ghép chặt chẽ với những chương trình người dùng, do đó cấu trúc logic hoặc vật lý của cơ sở dữ liệu có thể được thay đổi mà không ảnh hưởng tới cách nhìn của người lập trình ứng dụng về dữ liệu. *Xem* logical data independence, physical data independence.

data input voice answerback ***trả lời nhập dữ liệu bằng tiếng nói, tiếng đáp lại dữ liệu nhập, DIVA*** Trong truyền thông dữ liệu, hệ trong đó người dùng gửi dữ liệu nhập tới máy tính qua terminal (ví dụ, điện thoại bấm phím) và nhận được tiếng đáp lại từ máy tính mà có thể hoặc là giọng người thực được ghi sẵn hoặc tiếng nói tổng hợp. *Xem* audio response unit, speech synthesizer.

data integrity ***tính toàn vẹn dữ liệu*** (1) Trong an toàn dữ liệu, tính chất đảm bảo dữ liệu không bị thay đổi hoặc phá hủy trái phép. *So sánh với* data confidentiality. (2) Trong an toàn dữ liệu, trạng thái tồn tại khi các dữ liệu được máy tính hóa cũng giống như dữ liệu trong các tài liệu nguồn và không bị những sửa đổi hoặc hủy hoại ngẫu

nhiên hoặc cố ý. *So sánh với* data confidentiality.

data in voice ***dữ liệu (truyền) dạng tiếng nói, dữ liệu tiếng*** Trong truyền thông dữ liệu, kiểu truyền thông trong đó dữ liệu số thay thế các mạch tiếng nói trong kênh sóng cực ngắn. *So sánh với* data under voice, data above voice.

data item ***mục dữ liệu*** Trong các cơ sở dữ liệu, đơn vị dữ liệu nhỏ nhất có ý nghĩa độc lập (ví dụ, tên nhân viên trong bản ghi cá nhân). *Xem* field record. *Đồng nghĩa với* data element, datum.

data keeper ***người giữ dữ liệu*** Trong lập pháp, người có trách nhiệm đảm bảo thực hiện các cuộc kiểm tra đều đặn về độ chính xác và xác đáng của dữ liệu cá nhân. *Xem* data protection.

data key ***khóa dữ liệu*** Trong quản lý khóa, khóa dùng để mã và giải mã hoặc xác thực dữ liệu. *So sánh với* key encrypting key. *Xem* cryptographic key.

data leakage ***rò rỉ dữ liệu*** Trong an toàn dữ liệu, dòng thoát ngẫu nhiên của thông tin mật mà nếu không thì được coi là an toàn đối với một cá nhân hoặc các cá nhân. *Đồng nghĩa với* seepage.

data level ***cấp dữ liệu*** Trong an toàn dữ liệu. (*a*) Cấp I. Dữ liệu đã phân loại. (*b*) Cấp II. Dữ liệu chưa phân loại cần bảo vệ đặc biệt, ví dụ Luật bảo mật, chỉ sử dụng chính thức, các tài liệu kỹ thuật bị giới hạn phân phối hạn chế. (*c*) Cấp III. Tất cả các dữ liệu chưa phân loại khác.

data link ***liên kết dữ liệu*** (1) Trong truyền thông dữ liệu, phương tiện vật lý nối hai vị trí (ví dụ, dây điện thoại). (2) Trong truyền thông dữ liệu, môi trường truyền dẫn vật lý, giao thức và các thiết bị và chương trình có liên quan và cho phép truyền dữ liệu từ nguồn dữ liệu tới nơi tiếp nhận dữ liệu. *Xem* data link layer, data sink, data source, protocol. *Đồng nghĩa với* information link.

data link control standard ***chuẩn điều khiển liên kết dữ liệu*** Trong truyền thông dữ liệu, tập hợp các quy ước gửi và nhận dữ liệu tới và từ một mạng dữ liệu.

data link encryption ***mã liên kết dữ liệu*** Trong an toàn dữ liệu, sự mã hóa của dữ liệu qua mạch vật lý. Với dạng mã hóa này dữ liệu đưa vào các nút trung gian và nút cuối cùng ở dạng rõ. *So sánh với* end-to-end encryption, node encryption. *Xem* network encryption, plaintext. *Đồng nghĩa với* link encryption, link-to-link encryption.

data link layer ***tầng liên kết dữ liệu*** Trong truyền thông dữ liệu, tầng trong mô hình liên thông các hệ thống mở của ISO. Chức năng của tầng này là biến đổi một kênh truyền không tin cậy thành kênh truyền tin cậy để tầng trên nó (tức tầng mạng) sử dụng. Luồng bit dữ liệu thô được tổ chức thành các khung, mỗi khung chứa một tổng kiểm tra để phát hiện lỗi. *So sánh với* application layer, network layer, physical layer, presentation layer, session layer, transport layer. *Xem* bit stream, checksum, frame. Open Systems Interconnection.

DataLock ***virut DataLock*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

data management ***quản lý dữ liệu*** Ở các cơ sở dữ liệu, sự tổ chức và thực hiện các chức năng nhằm tạo ra dữ liệu được lưu, truy nhập nó, điều chỉnh các thiết bị nhập/xuất và buộc tuân thủ các quy ước lưu giữ dữ liệu.

data manipulation language ***ngôn ngữ thao tác dữ liệu, ngôn ngữ xử lý dữ liệu, DML*** Ở các cơ sở dữ liệu, ngôn ngữ mà người lập trình dùng để xử lý việc chuyển dữ liệu giữa cơ sở dữ liệu và chương trình ứng dụng. Nó thường nằm trong ngôn ngữ khác cung cấp khung sườn cho nó và những thủ tục xử lý dữ liệu. *So sánh với* data description language.

data mining ***khai thác dữ liệu, truy lục dữ liệu*** Trong lập pháp, rà soát các cơ sở dữ liệu để tìm các dữ liệu cá nhân mà có thể được dùng cho các hoạt động tiếp thị v.v.. *Xem* data protection.

data modelling ***mô hình hóa dữ liệu*** Trong các cơ sở dữ liệu, chỉ việc xác định các nhóm dữ liệu cơ bản và các mối quan hệ của chúng.

data modification ***sửa đổi dữ liệu*** Trong an toàn dữ liệu, sự thay đổi dữ liệu theo cách không được phép và không thể phát hiện được.

data origination ***khởi sinh dữ liệu, (sự) hình thành dữ liệu*** Trong tin học, sự dịch thông tin từ dạng ban đầu của nó sang dạng máy đọc được hoặc trực tiếp thành tín hiệu điện.

data origin authentication ***xác thực nguồn gốc dữ liệu*** (1) Trong xác thực, sự chứng thực rằng nguồn dữ liệu đã nhận được đúng như đã khai báo. (2) Trong xác thực, sự nhận dạng khẳng định nguồn hoặc nơi gửi dữ liệu đó.

data owner ***người sở hữu dữ liệu, chủ dữ liệu*** Trong an toàn dữ liệu, người hoặc nhóm người được ủy quyền theo luật định chịu trách nhiệm về một loại hoặc phạm trù thông tin riêng; cá nhân hoặc tổ chức chịu trách nhiệm về dữ liệu thực tế chứa trong tổ chức. *Xem* ownership.

dataplex ***dồn kênh dữ liệu*** Trong truyền thông dữ liệu, thuật ngữ chung dùng ở Anh để chỉ các dịch vụ có liên quan tới dồn kênh. *Xem* multiplexing.

dataplug ***phích dữ liệu, ổ dữ liệu*** Trong truyền thông, tên độc quyền cho một thiết bị cho phép cả đàm thoại điện thoại lẫn dữ liệu được dồn kênh trên cáp đôi xoắn nối với một tổng đài tự động nhánh lẻ (PABX). *Xem* multiplexing, private automated branch exchange.

data processing ***xử lý dữ liệu*** Trong các ứng dụng, sự thực hiện có hệ thống các thao tác trên dữ liệu để đạt được mục tiêu mong muốn. Những thao tác đó có thể bao gồm xử lý, trộn, sắp xếp và tính toán dữ liệu. *Xem* automatic data processing system.

data protection ***bảo vệ dữ liệu*** Trong lập pháp, các thủ tục được chấp nhận để giảm tối thiểu sự lạm dụng các dữ liệu cá nhân. Các mối quan tâm về bảo vệ dữ liệu cá nhân vẫn còn là lĩnh

vực tranh cãi sôi nổi từ những năm 1960.

Người ta đã sớm nhận ra rằng, các hệ thống máy tính lưu giữ dữ liệu cá nhân là một hiểm họa tiềm ẩn cho cá nhân. Trong khi mà luật pháp hoặc hiến pháp của các bang riêng lẻ (của Hoa Kỳ) có thể chưa công nhận quyền về tính riêng tư, song khả năng lưu giữ và xử lý những lượng dữ liệu khổng lồ liên quan tới các thành viên dân cư riêng lẻ đã chứa đựng những nguy cơ đáng kể trong phần quan trọng của thế kỷ này. Trong suốt lịch sử, các chính phủ đã tìm kiếm cách nhận diện các thành viên dân cư, những người được coi là mối đe dọa cho cơ sở của các niềm tin tôn giáo hoặc chính trị, hoặc các nền tảng dân tộc của họ v.v.. Những chính phủ như thế hoặc đã thiết lập những cơ sở dữ liệu thủ công hoặc tự động hóa khổng lồ riêng về dữ liệu cá nhân của họ, hoặc đã khai thác các cơ sở dữ liệu mà ban đầu là phát triển cho các mục đích hợp pháp.

Khả năng tiềm tàng của những cơ sở dữ liệu như vậy đã tăng lên một cách kỳ lạ do những tiến bộ về máy tính và các hệ truyền thông. Khối lượng các mục dữ liệu riêng lẻ, mỗi mục thu thập cho một mục đích giới hạn, có thể được ráp lại qua các hệ truyền thông quốc tế và có tương quan với nhau trên các cơ sở dữ liệu lớn. Các phương pháp trí tuệ nhân tạo, như các mạng thần kinh hoặc các hệ chuyên gia, có thể rà soát các cơ sở dữ liệu như thế để tìm các mẫu có dấu hiệu về những đặc điểm "không mong muốn" cảm nhận được: những người lạm dụng các kế hoạch phúc lợi, những kẻ né tránh nộp thuế, những dân nhập cư bất hợp pháp, những kẻ buôn bán ma túy, người không đăng ký nghĩa vụ quân sự v.v..

Có những nguy cơ đáng kể đối với cá nhân được ghi trên những cơ sở dữ liệu như thế. Nguy cơ lớn nhất là dữ liệu được ghi không chính xác, do thu nạp dữ liệu kém hoặc đánh máy sai, hoặc đơn giản là đã lạc hậu. Những dữ liệu không chính xác như vậy có thể gây hại cho cá nhân, ví dụ như bị từ chối một khoản vay ngân hàng, bị từ chối việc làm hoặc trả bảo hiểm, và cá nhân bị ảnh hưởng sẽ thường chẳng có cách nào sửa, ngay cả khi đã biết về lỗi dữ liệu đằng sau quyết định đó.

Sự tương hợp máy tính cung cấp cho những người sử dụng các cơ sở dữ liệu rời rạc cơ hội để tham khảo chéo dữ liệu cá nhân, ví dụ kiểm tra lối sống so với các bản khai thu nhập cá nhân. Việc sử dụng các phương pháp trí tuệ nhân tạo có thể cung cấp những cách rà soát thậm chí tinh vi hơn, ví dụ như những người hành nghề y lợi dụng đặc biệt nhiều dịch vụ bệnh lý, các mẫu lữ hành và hành vi có dấu hiệu của những kẻ buôn bán ma túy. Trong nhiều trường hợp, thậm chí không thể có khả năng hỏi tại sao hệ thống đã nhận dạng được một cá nhân cụ thể, và cá nhân ít có cơ hội để chống án.

Khu vực tư nhân thường tìm cách khai thác khối lượng các dữ liệu cá nhân cho các mục đích tiếp thị, hoặc để bảo vệ chống lại việc lạm dụng các phương tiện tín dụng, dữ liệu thu thập một cách rõ ràng cho một mục đích, ví dụ như việc sử dụng thẻ tín dụng có thể được

bán cho các tổ chức tiếp thị, ví dụ các danh sách người mua đồ cũ qua thư.

Tổ chức hợp tác và phát triển kinh tế đã thừa nhận những mối liên can tới các cuộc chuyển dữ liệu cá nhân qua biên giới trong năm 1969 và ban hội thẩm Ngân hàng dữ liệu của nó đã xem xét những vấn đề bảo mật dữ liệu máy tính. Năm 1980 OECD đã chấp nhận các Nguyên tắc chủ đạo của cơ quan này về bảo vệ tính riêng tư và các luồng dữ liệu qua biên. Những nguyên tắc chủ đạo đó có tính chất tư vấn và không ràng buộc pháp lý đối với bất kỳ nước thành viên nào.

Hội đồng Châu Âu đã thông qua Quy ước về bảo vệ cá nhân đối với việc xử lý tự động dữ liệu cá nhân vào năm 1981. Quy ước ràng buộc về mặt pháp lý đối với bất kỳ nước thành viên nào phê chuẩn nó và sự phê chuẩn đòi hỏi nước thành viên thông qua luật bảo vệ dữ liệu quốc gia riêng của nước thành viên đó.

Châu Âu dẫn đầu trong việc phê chuẩn các luật bảo vệ dữ liệu và điều đó đã có tác dụng rõ rệt. Các nước không thông qua các luật có hiệu quả có thể thấy rằng, các tổ chức của họ bị ngăn cản chuyển dữ liệu cá nhân với các nước đã có những luật như thế và những sự ngăn cấm như vậy có thể tác động tới các hoạt động thương mại.

Luật pháp bảo vệ dữ liệu thay đổi đáng kể từ nước này qua nước khác. Hơn nữa, có những thay đổi rộng bên trong các quốc gia, về các luật do các bang hợp thành hoặc các chính quyền địa phương thông qua. Hầu như tất cả những luật như thế đều bảo vệ những tệp dữ liệu cá nhân tự động hóa do các cơ quan chính phủ trung ương hoặc bang xử lý; một số luật cũng áp dụng cho các hệ lưu giữ thủ công dữ liệu cá nhân. Trong nhiều trường hợp, khu vực tư nhân không xét đến trong luật.

Trong phần lớn các trường hợp, các luật đều miễn trừ cho các cơ quan thi hành pháp luật và các dữ liệu lưu giữ cho an ninh quốc gia. Tuy nhiên, các nước Tây Âu có quan điểm rằng, luật pháp phải bảo vệ chống lại khả năng lạm dụng những tệp như thế.

Trong nhiều trường hợp nhưng không phải tất cả, luật bảo vệ dữ liệu thành lập một ban giám sát việc thực hiện các quy định bảo vệ dữ liệu có hiệu quả. Ban này được coi là có hiệu quả nhất khi nó không thuộc bộ máy quan liêu thông thường của chính phủ mà có thể báo cáo trực tiếp cho quốc hội hoặc cơ quan tương đương.

Đối với các tổ chức ở các quốc gia có luật pháo bảo vệ dữ liệu có hiệu quả, có một sự cám dỗ rõ ràng muốn xuất khẩu dữ liệu cá nhân sang các quốc gia không áp đặt những hạn chế đối với việc lưu giữ và xử lý nó. Tuy nhiên, những nơi cất trữ tiềm tàng dữ liệu như vậy có thể nhận ra rằng, việc thiếu các luật bảo vệ dữ liệu có thể dẫn đến sự ngăn cản xuất khẩu dữ liệu cá nhân từ các quốc gia đã thông qua những luật như thế. Những hạn chế như vậy đối với các luồng dữ liệu qua biên có thể có tác động quan trọng tới những nước nhỏ vốn đã bắt đầu thu hút các hệ thống ngân hàng nước ngoài.

Tình hình luật pháp bảo vệ dữ liệu trên thế giới vẫn còn lộn xộn và sôi động.

Nói chung, phần lớn các quốc gia Tây Âu, Bắc Mỹ, Ôxtrâylia, Niu Di Lân, Israen và Nhật đều đã thông qua một dạng luật pháp bảo vệ dữ liệu nào đó, mặc dù có những biến đổi đáng kể trong luật pháp đó. *So sánh với* freedom of information. *Xem* computer matching, data haven, data protection - Australia, data protection - Austria, data protection - Belgium, data protection - Canada, data protection - Council of Europe, data protection - Cyprus, data protection - EC, data protection - Finland, data protection - France, data protection - Germany, data protection - Greece, data protection - Guernsey, data protection - Iceland, data protection - Ireland, data protection - Isle of man, data protection - Israel, data protection - Japan, data protection - Jersey, data protection - Luxembourg, data protection - Netherlands, data protection - New Zealand, data protection - Normay, data protection - OECD, data protection - Portugal, data protection - Slovenia, data protection - Spain, data protection - Sweden, data protection - U.K., data protection - USA.

data protection - Australia ***bảo vệ dữ liệu - Ôxtrâylia*** Trong lập pháp, Đạo luật bảo vệ tính riêng tư Ôxtrâylia, 1988 là luật Liên bang kiểm soát việc thu thập, lưu giữ, an toàn và việc sử dụng dữ liệu cá nhân của các cơ quan chính phủ Liên bang. Theo những điều khoản của luật này, các cơ quan chính phủ Liên Bang hằng năm phải thông báo cho Ủy viên bảo mật theo luật định về mức độ, mục đích và nội dung của dữ liệu cá nhân trong các hệ thống của họ. Đạo luật bảo vệ tính riêng tư bổ sung năm 1990 đã mở rộng các trách nhiệm của Ủy viên bảo mật tính đến cả ngành kinh doanh tư vấn tín nhiệm. Ba bang ở Ôxtrâylia: Queensland, New South Wales và Victoria cũng đã có hành động để thông qua các luật bảo vệ dữ liệu. *Xem* data protection.

data protection - Austria ***bảo vệ dữ liệu - áo*** Trong lập pháp, đạo luật bảo vệ dữ liệu của Áo ban hành năm 1978 và áp dụng cho các thể nhân và pháp nhân. Luật pháp đòi hỏi thông báo và đăng ký các thủ tục liên quan tới xử lý dữ liệu cá nhân. *Xem* data protection.

data protection - Belgium ***bảo vệ dữ liệu - Bỉ*** Trong lập pháp, luật bảo vệ dữ liệu phác thảo đã được đệ trình cho Hội đồng nhà nước năm 1990. Luật này áp dụng cho cả các hệ xử lý dữ liệu cá nhân tự động hoá lẫn thủ công. Nó cũng áp dụng đối với dữ liệu cá nhân của công dân Bỉ được xử lý ở nước ngoài và có thể truy nhập được từ các hệ thống trong nước Bỉ. *Xem* data protection.

data protection - Canada ***bảo vệ dữ liệu - Canada*** Trong lập pháp, Đạo luật về quyền con người của Canada, 1977. Nó đã lập ra chức vụ Ủy viên bảo mật và cho công dân quyền truy nhập tới dữ liệu cá nhân do các cơ quan chính phủ lưu giữ. Đạo luật ngân hàng Canada tiếp sau đó, 1980, đã đặt các giới hạn lên luồng dữ liệu qua biên đối với các dữ liệu tài chính cá nhân. Năm 1982 Đạo luật bảo vệ tính riêng tư đã được thông qua, giải quyết cả bảo mật lẫn quyền tự do truy nhập thông tin. Đạo luật bảo vệ tính riêng tư tăng thêm quyền hạn của Ủy viên bảo mật; luật

này chỉ áp dụng cho các thể chế và cơ quan của chính phủ Liên bang. Tuy nhiên, các hệ máy tính của chính phủ Liên bang hằng năm sẽ cung cấp thông tin chi tiết về bản chất của các tệp cá nhân đã xử lý. Luật bảo vệ dữ liệu cũng đã được thông qua ở các tỉnh Quebec và Ontario. *Xem* data protection.

data protection - Council of Europe ***bảo vệ dữ liệu - Hội đồng Châu Âu*** Trong lập pháp, năm 1981 Hội đồng Châu Âu đã thông qua Công ước bảo vệ các cá nhân đối với việc xử lý tự động dữ liệu cá nhân. Công ước đòi hỏi sự phê chuẩn của mỗi nước thành viên và để cho phép phê chuẩn, mỗi nước thành viên phải thông qua các luật bảo vệ dữ liệu riêng của họ. *Xem* data protection.

data protection - Cyprus ***bảo vệ dữ liệu - Síp*** Trong lập pháp, năm 1986 Síp đã ký Công ước Hội đồng Châu Âu về Bảo vệ cá nhân đối với xử lý tự động dữ liệu cá nhân. *Xem* data protection, data protection - Council of Europe.

data protection - Denmark ***bảo vệ dữ liệu - Đan Mạch*** Trong lập pháp, năm 1978 Quốc hội Đan Mạch đã thông qua hai luật bảo vệ dữ liệu: Đạo luật đăng ký các cơ quan công của Đan Mạch và Đạo luật đăng ký tư nhân Đan Mạch giải quyết tương ứng các khu vực công cộng và tư nhân. Đạo luật đăng ký tư nhân Đan Mạch quy định những hạn chế tương đối chặt chẽ đối với các luồng dữ liệu cá nhân qua biên giới. Những đạo luật đó đã được bổ sung vào năm 1988 để gộp thêm yêu cầu bắt buộc về đăng ký tất cả các tệp dữ liệu chứa dữ liệu nhạy cảm công với điều chỉnh chặt chẽ hơn đối với ngành kinh doanh tư vấn tín nhiệm. *Xem* data protection, transboder data flow.

data protection - EC ***bảo vệ dữ liệu - EC*** Trong lập pháp, tháng 7 năm 1990, Cộng đồng Châu Âu đã đưa ra đề xuất bảo vệ dữ liệu cá nhân. Chỉ thị của Cộng đồng Châu Âu áp dụng cho việc xử lý các tệp dữ liệu cá nhân xử lý và lưu giữ thủ công và tự động hóa, và các hệ thống khu vực tư nhân và khu vực công. *Xem* data protection, data protection - Council of Europe.

data protection engineering ***công nghệ bảo vệ dữ liệu*** Trong an toàn dữ liệu, hệ phương pháp luận và các công cụ dùng để thiết kế và thực hiện các cơ chế bảo vệ dữ liệu. *Xem* data protection.

data protection - Finland ***bảo vệ dữ liệu - Phần Lan*** Trong lập pháp, năm 1987 Phần Lan đã thông qua Đạo luật về hồ sơ dữ liệu cá nhân và nó đã trở thành luật vào năm 1988. Đạo luật mở rộng cho các khu vực cả công lẫn tư, các hồ sơ xử lý và lưu trữ thủ công hay tự động hóa. Những người sử dụng dữ liệu phải thông báo cho Ủy viên kiểm tra bảo vệ dữ liệu về việc thiết lập một hồ sơ dữ liệu cá nhân. *Xem* data protection.

data protection - France ***bảo vệ dữ liệu - Pháp*** Trong lập pháp, năm 1978 Pháp đã thông qua Luật về tin học và tự do của nước này. Cơ quan bảo vệ dữ liệu - Ủy ban quốc gia về xử lý dữ liệu và quyền tự do (CNIL) đã được thành lập. CNIL yêu cầu đăng ký các

khai báo đối với dữ liệu cá nhân được xử lý bởi khu vực nhà nước. CNIL cũng nhận được các yêu cầu cho các ý kiến về xử lý dữ liệu cá nhân bởi khu vực công. Không giống như luật pháp ở nhiều quốc gia, các hồ sơ công an không được miễn trừ khỏi luật bảo vệ dữ liệu. *Xem* data protection.

data protection - Germany ***bảo vệ dữ liệu - Đức*** Trong lập pháp, Luật liên bang về bảo vệ chống lạm dụng dữ liệu cá nhân đã được thông qua năm 1977 và có hiệu lực vào năm 1978. Luật đề ra chức vụ Ủy viên bảo vệ dữ liệu Liên bang. Chỉ có các thể nhân, không phải pháp nhân hoặc hợp nhân, là được luật bảo vệ; hơn nữa, luật chỉ áp dụng cho các cơ quan ủy quyền và cơ quan hành chính Liên bang. Các cơ quan ủy quyền của nhà nước nằm trong quyền hạn của mỗi Bang có các luật bảo vệ dữ liệu riêng; những luật đó cũng bảo vệ việc sử dụng dữ liệu cá nhân ở khu vực tư nhân. *Xem* data protection.

data protection - Greece ***bảo vệ dữ liệu - Hy Lạp*** Trong lập pháp, dự luật. Luật bảo vệ dữ liệu đã được đệ trình lên quốc hội Hy Lạp năm 1987. Luật áp dụng cho các khu vực tư nhân và công và cho các hồ sơ dữ liệu cá nhân tự động hóa và thủ công. Dự luật lập ra Ủy ban bảo vệ dữ liệu để xem xét sự tuân thủ theo luật. *Xem* data protection.

data protection - Guernsey ***bảo vệ dữ liệu - Đảo Guernsey*** Trong lập pháp, Luật bảo vệ dữ liệu (thẩm quyền của khám sai) đã được thông qua năm 1986. Về cơ bản luật tương tự với Đạo luật bảo vệ dữ liệu của Anh. *Xem* data protection, data protection - Jersey, data protection - U.K.

data protection - Iceland ***bảo vệ dữ liệu - Aixơlen*** Trong lập pháp, Luật bảo vệ dữ liệu cuối cùng được thông qua năm 1989. Luật này vẫn tiếp tục quy định Ủy ban bảo vệ dữ liệu để giám sát việc tuân thủ luật. Luật áp dụng cho các khu vực cả công lẫn tư, các hồ sơ xử lý hoặc lưu trữ thủ công và tự động hóa, thể nhân và pháp nhân. *Xem* data protection.

data protection - Ireland ***bảo vệ dữ liệu - Ailen*** Trong lập pháp, Đạo luật bảo vệ dữ liệu Ailen được thông qua năm 1988 và được bổ sung theo Các quy tắc (Y tế) (Sửa đổi truy nhập) bảo vệ dữ liệu năm 1989. Đạo luật có những điểm tương tự với Đạo luật bảo vệ dữ liệu Anh nhưng nó có định nghĩa chặt chẽ hơn về dữ liệu cá nhân. Ủy ban bảo vệ dữ liệu được thành lập để tăng cường việc tuân thủ luật. Đạo luật không áp dụng đối với các hồ sơ xử lý và lưu giữ thủ công cũng như các chủ dữ liệu là pháp nhân. *Xem* data protection - U.K.

data protection - Isle of Man ***bảo vệ dữ liệu - Đảo Man*** Trong lập pháp, Đạo luật bảo vệ dữ liệu, về cơ bản tương tự với Đạo luật bảo vệ dữ liệu của Anh, đã được thông qua năm 1988. *Xem* data protection - U.K.

data protection - Israel ***bảo vệ dữ liệu - Israen*** Trong lập pháp, Luật bảo vệ tính riêng tư có những điều khoản tương tự với luật pháp của Châu Âu, đã được thông qua năm 1981. *Xem* data protection.

data protection - Japan ***bảo vệ dữ liệu - Nhật Bản*** Trong lập pháp, Nghị viện Nhật đã thông qua Đạo luật về bảo vệ dữ liệu cá nhân xử lý bằng máy tính năm 1988. Đạo luật này áp dụng cho các hồ sơ tự động hóa các cơ quan chính phủ quốc gia xử lý. Tổng giám đốc Cơ quan quản lý và phối hợp có trách nhiệm quản lý việc tuân thủ luật của chính phủ. Một số quận và chính quyền thành phố đã thông qua các sắc lệnh bảo vệ dữ liệu. *Xem* data protection.

data protection - Jersey ***bảo vệ dữ liệu - Đảo Jersey*** Trong lập pháp, Luật bảo vệ dữ liệu (Đảo Jersey) đã được thông qua năm 1987. Nó áp dụng cho các hồ sơ dữ liệu cá nhân tự động hóa chứ không phải thủ công và không áp dụng cho các chủ thể dữ liệu là pháp nhân hay công ty (hợp) nhân. *Xem* data protection, data protection - Guernsey, data protection - U. K.

data protection - Luxembourg ***bảo vệ dữ liệu - Lucxămbua*** Trong lập pháp, Luật của Lucxămbua về việc sử dụng dữ liệu liên kết tên trong xử lý máy tính đã được thông qua năm 1979. Luật này bảo vệ cả khu vực công lẫn khu vực tư. *Xem* data protection.

data protection - Netherlands ***bảo vệ dữ liệu - Hà Lan*** Trong lập pháp, Đạo luật bảo vệ dữ liệu Hà Lan có hiệu lực năm 1989. Đạo Luật điều chỉnh các hồ sơ chứa dữ liệu cá nhân cả tự động hóa lẫn thủ công. Luật này quy định thành lập Phòng đăng ký và phòng đó đề ra các quy tắc điều chỉnh kinh doanh các hệ dữ liệu cá nhân. *Xem* data protection.

data protection - New Zealand ***bảo vệ dữ liệu - Niu Di Lân*** Trong lập pháp, các vấn đề bảo vệ dữ liệu đã được tính đến trong luật pháp như Đạo luật công ty, 1955, Đạo luật y tế, 1956, Đạo luật trung tâm máy tính Wanganui, 1976, Đạo luật ban y tế vùng, 1983 và Đạo luật nhận con nuôi trưởng thành, 1985. Đạo luật Ủy ban quyền con người Niu Di Lân, 1977, đảm bảo các trách nhiệm của Ủy ban quyền con người để xem xét các vấn đề bảo mật bao gồm bảo mật dữ liệu cá nhân. *Xem* data protection.

data protection - Norway ***bảo vệ dữ liệu - Na Uy*** Trong lập pháp, Đạo luật đăng ký dữ liệu cá nhân năm 1978 của Na Uy trở thành luật vào năm 1980 và đã được sửa đổi vào năm 1987. Luật bảo vệ các hồ sơ dữ liệu cá nhân xử lý và lưu giữ thủ công và tự động hóa, khu vực công và khu vực tư. Chức thanh tra dữ liệu đã được luật quy định. Bổ sung luật năm 1987 bao gồm những tham khảo về các hoạt động báo cáo tín dụng, marketing trực tiếp và marketing từ xa. *Xem* data protection.

data protection - OECD ***bảo vệ dữ liệu - OECD*** Trong lập pháp, năm 1980 Hội đồng của Tổ chức hợp tác và phát triển kinh tế đã thông qua các Đường lối chỉ đạo về Bảo mật và các đường dữ liệu cá nhân qua biên. *Xem* data protection, transborder dataflow.

data protection - Portugal ***bảo vệ dữ liệu - Bồ Đào Nha*** Trong lập pháp, Quốc hội Bồ Đào Nha đã thông qua Luật về bảo vệ dữ liệu cá nhân máy tính hoá năm 1991. Luật áp dụng cho các hồ sơ cá nhân tự động hóa khu vực công

hoặc tư, cho các thể nhân. Ủy ban quốc gia về bảo vệ dữ liệu cá nhân tự động hóa (CNPDPI) đã được luật quy định thành lập. *Xem* data protection.

data protection - Slovenia ***bảo vệ dữ liệu - Slovenia*** Trong lập pháp, Slovenia đã thông qua Đạo luật bảo vệ dữ liệu vào năm 1990. Đạo luật chấp nhận những nguyên tắc cơ bản của Các đường lối chỉ đạo của OECD về bảo vệ bí mật và các luồng dữ liệu qua biên của dữ liệu cá nhân và Hội đồng hiệp ước Châu Âu về dữ liệu cá nhân. *Xem* data protection, data protection - OECD, data protection - Counsil of Europe.

data protection - Spain ***bảo vệ dữ liệu - Tây Ban Nha*** Trong lập pháp, hiến pháp của Tây Ban Nha có một điều khoản đảm bảo quyền riêng tư của công dân, kể cả ngăn ngừa lạm dụng thông tin cá nhân. *Xem* data protection.

data protection - Sweden ***bảo vệ dữ liệu - Thụy Điển*** Trong lập pháp, đạo luật bảo vệ dữ liệu đầu tiên đã từng được thông qua ở Thụy Điển vào năm 1973. Đạo luật này điều chỉnh cả khu vực công lẫn khu vực tư. Ban thanh tra dữ liệu đã được thành lập để giám sát những yêu cầu rất chặt chẽ của đạo luật này. Sự chú ý đặc biệt đã được dành cho việc xuất khẩu dữ liệu cá nhân vì người ta sợ rằng các tổ chức có thể đơn giản lờ Ban thanh tra dữ liệu và xuất khẩu dữ liệu để xử lý ở đâu đó khác. Các thủ tục gắn liền với việc đăng ký và xuất khẩu các giấy phép hoạt động nặng nề tới mức đạo luật đã được sửa đổi vào năm 1982 để làm cho các thủ tục bớt rắc rối hơn. *Xem* data protection.

data protection - UK ***bảo vệ dữ liệu - Liên hiệp Anh*** Trong lập pháp, Cuộc tranh cãi về bảo vệ dữ liệu ở Anh đã trở nên sôi nổi từ đầu những năm 1970. Vấn đề này đã được xem xét bởi Ủy ban thanh niên (1972), hai Sách Trắng (1975) và Ủy ban Lindop (1976). Mối quan tâm thể hiện vào đầu những năm 1980 khi không thông qua được Công ước Hội đồng Châu Âu. Đã có nguy cơ rằng các cơ quan chính phủ và các công ty khu vực tư nhân không còn được phép chuyển dữ liệu cá nhân nhạy cảm tới và từ các nước Châu Âu vốn đã thông qua các luật bảo vệ dữ liệu.

Đạo luật bảo vệ dữ liệu của Anh được thông qua năm 1984 và dựa trên tám nguyên tắc bảo vệ dữ liệu phù hợp rộng rãi với các khuyến nghị của Công ước hội đồng Châu Âu về bảo vệ các cá nhân đối với việc xử lý tự động dữ liệu cá nhân. Tám nguyên tắc đó là:

- thông tin chứa trong dữ liệu cá nhân sẽ thu được và dữ liệu cá nhân phải được xử lý đúng đắn và hợp pháp;
- dữ liệu cá nhân chỉ được lưu giữ cho một hoặc nhiều mục đích xác định và hợp pháp;
- dữ liệu cá nhân được lưu giữ cho một mục đích bất kỳ hoặc các mục đích phải không được sử dụng hoặc bị tiết lộ theo bất kỳ cách nào không tương thích với mục đích hoặc những mục đích đó;
- dữ liệu cá nhân được lưu giữ cho một hoặc các mục đích bất kỳ phải đầy đủ và thích đáng và không quá mức so với mục đích hoặc các mục đích đó;
- dữ liệu cá nhân phải chính xác và ở

chỗ nào cần thiết sẽ được cập nhật;

- dữ liệu cá nhân lưu giữ cho một hoặc các mục đích bất kỳ phải không được lưu giữ lâu hơn mức cần thiết cho mục đích hoặc các mục đích đó;
- chủ thể dữ liệu phải được quyền:

- truy nhập trong các thời khoảng hợp lý và không trễ quá mức hoặc phí tổn quá mức vào dữ liệu cá nhân mà người đó là chủ thể;

- nơi nào thích hợp phải sửa hoặc xóa những dữ liệu như thế;

- các biện pháp an toàn thích hợp phải được thực hiện chống lại truy nhập bất hợp pháp đề hoặc sửa đổi, tiết lộ hoặc phá hủy dữ liệu cá nhân và chống lại mất mát ngẫu nhiên hoặc phá hủy dữ liệu cá nhân.

Ngoài ra, đạo luật quy định chức vụ mới của Người ghi đăng ký dữ liệu, một chức vụ cấp quốc gia và một Diễn đàn bảo vệ dữ liệu. Trách nhiệm của Người ghi đăng ký là lập ra và duy trì một bản đăng ký những người sử dụng dữ liệu và những người tiến hành các dịch vụ văn phòng máy tính. Diễn đàn lắng nghe những lời kêu cầu nhân danh những người sử dụng phản đối những quyết định hoặc những hành động của Người ghi đăng ký. Đạo luật đòi hỏi rằng, những những sử dụng dữ liệu cá nhân tự động hóa ở khu vực công và tư, phải đăng ký các hệ thống của họ với Người ghi đăng ký và tuân thủ các nguyên tắc, ngoại trừ những nhóm được miễn trừ xác định liệt kê dưới đây.

- dữ liệu cá nhân do một cá nhân giữ để sử dụng trong gia đình, như các mục đích cá nhân, gia đình hoặc giải trí;
- dữ liệu cá nhân mà luật yêu cầu làm dữ liệu công cộng, như danh sách tự động hóa những người bỏ phiếu do Nhân viên đăng ký bầu cử duy trì;
- dữ liệu cá nhân chỉ dùng để tính toán, trả lương và trợ cấp, giữ các tài khoản hoặc duy trì các sổ sách ghi các khoản mua và bán để đảm bảo thực hiện các khoản trả tiền;
- dữ liệu cá nhân dùng để phân phối các bài báo hoặc thông tin cho các chủ thể dữ liệu và chỉ một lượng rất nhỏ dữ liệu được duy trì nếu chủ thể dữ liệu phản đối duy trì những dữ liệu đó thì không áp dụng miễn trừ;
- dữ liệu cá nhân lưu giữ bởi một câu lạc bộ không phải tổ chức, tất cả các chủ thể dữ liệu phải là thành viên của câu lạc bộ và nếu họ phản đối bảo trì thông tin thì miễn trừ không được áp dụng;
- thông tin mà chỉ được xử lý để chuẩn bị văn bản, ví dụ như xử lý văn bản;
- dữ liệu cá nhân được lưu giữ cho các lý do an ninh quốc gia;
- những lĩnh vực khác bao gồm hệ thống thuế, y tế và công tác xã hội, điều chỉnh dịch vụ tài chính, các giấy hẹn gặp của quan tòa, đặc quyền nghề nghiệp hợp pháp, dữ liệu cá nhân được chuyển thành công khai và dự phòng.

Đạo luật tín dụng tiêu dùng, 1974, cho chủ thể dữ liệu quyền truy nhập dữ liệu cá nhân của các cơ quan báo cáo tín dụng tiêu dùng và do đó, những dữ liệu như thế cũng được miễn trừ theo Đạo luật bảo vệ dữ liệu.

Theo Đạo luật bảo vệ dữ liệu, sẽ là vi phạm nếu xử lý hoặc trao đổi tự động

dữ liệu cá nhân:

- mà không đăng ký như người sử dụng;
- mà bị Người ghi đăng ký ngăn không cho làm điều đó;
- cho các mục đích hoặc các trao đổi chưa được đăng ký.

Cá nhân là đối tượng của thông tin chứa trong một tệp máy tính được quyền kiểm tra thông tin đó, nhận một bản sao của bản ghi và thực hiện các hoạt động chống tổn thất ở nơi nào dữ liệu không chính xác hoặc đã bị lạm dụng. Các thủ tục an toàn có hiệu quả phải được các cơ quan xử lý dữ liệu cá nhân tiến hành để bảo vệ chống sự truy nhập không được phép. Ngoài ra, Đạo luật về lạm dụng máy tính, 1990, coi truy nhập các hệ máy tính theo cách không được phép và sửa đổi dữ liệu theo cách bất kỳ đều là bất hợp pháp. *Xem* Computer Misuse Act - 1990, data protection, Lindop Committee, privacy, Younger Committee.

data protection - USA ***bảo vệ dữ liệu - Hoa Kỳ*** Trong lập pháp, luật pháp bảo vệ dữ liệu đã được ban hành ở cấp Liên bang và Bang ở Hoa Kỳ, nhưng luật pháp đó kém chặt chẽ hơn so với luật hiện thời có hiệu lực ở một số nước Châu Âu.

Đạo luật báo cáo đúng tín dụng, 1970, đòi hỏi các cơ quan tín dụng phải lập sổ sách của họ có thể sử dụng cho các chủ thể dữ liệu và hạn chế sự tiết lộ thông tin tín dụng cho các cơ quan được phép. Đạo luật cũng đưa ra các thủ tục để sửa các lỗi trong dữ liệu cá nhân. Tuy nhiên, nó không cho các chủ thể dữ liệu bất kỳ sự kiểm soát nào đối với sự tiết lộ những dữ liệu cá nhân như thế.

Đạo luật bảo vệ tính riêng tư năm 1974 chỉ liên quan tới dữ liệu cá nhân do các cơ quan liên bang xử lý. Nó đòi hỏi các cơ quan này phải thông báo về việc sử dụng mới đề xuất đối với dữ liệu cá nhân, sao cho các bên có liên quan có thể lập các bản đệ trình. Tuy nhiên, các cá nhân bị ảnh hưởng như vậy có thể gặp khó khăn trong việc truy nhập tới những thông báo đó.

Đạo luật bảo vệ tính riêng tư quy định thành lập Ủy ban nghiên cứu bảo vệ tính riêng tư nhưng đó không phải là cơ quan thường trực. Ủy ban báo cáo những phát hiện của nó, kể cả khuyến nghị rằng, Đạo luật về tính riêng tư không nên mở rộng sang khu vực tư nhân, vào năm 1977. CIA và những cơ quan thi hành pháp luật được miễn trừ theo Đạo luật về tính riêng tư, nhưng Đạo luật kiểm soát tội phạm, 1973 lại đòi hỏi các hệ thống thông tin tư pháp hình sự nhà nước do Quỹ liên bang thành lập, phải thực hiện những biện pháp để đảm bảo tính riêng tư và an ninh.

Đạo luật quyền giáo dục gia đình và tính riêng tư năm 1974 quy định bảo vệ dữ liệu đối với dữ liệu cá nhân do các trường phổ thông và các đại học lưu giữ. Đạo luật này đảm bảo cho các bậc cha mẹ và sinh viên truy nhập được các hồ sơ sinh viên, quyền không thừa nhận dữ liệu không đúng và quy định những hạn chế tiết lộ những dữ liệu cá nhân như thế.

Đạo luật tự do thông tin năm 1978, theo nghĩa nào đó có mục đích ngược với

Đạo luật về tính riêng tư vì nó cho phép tiết lộ thông tin của chính phủ. Bởi thế, có khả năng dữ liệu cá nhân có thể bị phát ra do Đạo luật tự do thông tin trái với Đạo luật về tính riêng tư.

Pháp chế về bảo vệ dữ liệu liên quan tới những lĩnh vực ứng dụng đặc thù đã được quy định bởi Đạo luật Quyền giữ kín tài chính năm 1978, Đạo luật giữ kín các nạn nhân bị cưỡng dâm năm 1978, Đạo luật chuyển tiền điện tử năm 1978, Đạo luật tính riêng tư năm 1990, Đạo luật giảm bớt công việc giấy tờ năm 1980, Đạo luật đòi nợ năm 1982, Đạo luật chính sách truyền thông cáp năm 1984, Đạo luật bảo mật videơ năm 1988 và Đạo luật toàn vẹn tài chính của các nhà quản lý Liên Bang.

Ở Hoa Kỳ người ta đã quan tâm tới hệ quả của các phương pháp so khớp máy tính trên những cơ sở dữ liệu lớn đối với việc bảo vệ dữ liệu cá nhân. Đạo luật so khớp máy tính và bảo vệ tính riêng tư năm 1988 quy định những thủ tục cơ bản cho các cơ quan Liên bang tiến hành những sự so khớp như thế. Đạo luật an toàn máy tính năm 1987 có những hệ quả đối với bảo vệ dữ liệu, ví nó liên quan tới cấp an toàn dữ liệu của các hệ máy tính thuộc Liên bang. Đạo luật tiếp nối là Đạo luật an toàn máy tính năm 1988 quy định thành lập Ban an toàn hệ máy tính và tính riêng tư. Ba bang Minnesota, New York và Haoai đã thực hiện các luật bảo vệ dữ liệu gần tương tự với những luật ở Châu Âu. *Xem* computer matching, data protection.

data rate *tốc độ dữ liệu* (1) Trong truyền thông dữ liệu, lượng dữ liệu truyền trong một đơn vị thời gian trên một liên kết dữ liệu, thường biểu thị theo bit trên giây. (2) Trong các thiết bị ngoại vi, tốc độ dữ liệu thường biểu thị theo byte hoặc từ trên giây, được truyền giữa các thiết bị của hệ máy tính. *Xem* bit, byte, word.

data reduction *rút gọn dữ liệu* Trong tin học, quá trình biến đổi dữ liệu thô thành dạng hữu dụng đơn giản hơn. Quá trình này thường liên quan tới các thao tác như điều chỉnh, định tỷ lệ, làm nhẵn, nén và soạn thảo dữ liệu. *So sánh với* data compression.

data retrieval *truy lục dữ liệu, truy tìm dữ liệu* *Xem* information retrieval.

Data Seal *thuật toán Data Seal* Trong xác thực, thuật toán xác thực không công bố, có sở hữu.

data security *an toàn dữ liệu* (1) Sự bảo vệ dữ liệu khỏi bị sửa đổi, phá hủy hoặc tiết lộ ngẫu nhiên hoặc cố ý. (2) Môn khoa học và nghiên cứu các phương pháp bảo vệ dữ liệu trong các hệ máy tính và các hệ truyền thông chống lại sự tiết lộ, chuyển, sửa đổi hoặc phá hủy không được phép cho dù là ngẫu nhiên hay cố ý. Nó liên quan tới bốn kiểu kiểm soát: kiểm soát mật mã, kiểm soát truy nhập, kiểm soát luồng thông tin và kiểm soát suy luận. *Xem* access control, computer security, cryptographic control, inference control, information flow control. *Đồng nghĩa với* information asset security, information security.

data security architecture *kiến trúc an toàn dữ liệu* Trong an toàn dữ

liệu, cấu trúc của hệ an toàn dữ liệu tích hợp, nhằm tạo ra mức bảo đảm an toàn thích hợp. Mức cao nhất của kiến trúc có thể bao gồm chính sách an toàn của tổ chức, mức tiếp theo là an toàn thủ tục mà lần lượt được hỗ trợ bởi các cơ chế an toàn vật lý và logic. Các khía cạnh của kiến trúc ở mỗi mức không chỉ tương thích và bổ sung cho nhau mà còn phải tạo ra sự bảo vệ theo chiều sâu. Phải đặc biệt chú ý tới các giao diện của hệ thống để đảm bảo chúng duy trì tính toàn vẹn an toàn. Kiến trúc phát triển tốt sẽ tạo ra sự quản lý với sự khái quát toàn diện toàn bộ tập hợp các biện pháp đối phó an toàn bên trong tổ chức. Biên chế kỹ thuật sẽ có một cơ sở hạ tầng xác định tốt trong đó, các hệ thống hiện thời có thể hoạt động và các hệ thống mới có thể được thực hiện một cách an toàn. Các giao diện được xác định tốt sẽ xác định rõ ràng các trách nhiệm an toàn. *Xem* digital distributed system security architecture, security policy.

data security officer ***nhân viên an toàn dữ liệu*** Trong an toàn máy tính, người có trách nhiệm bảo vệ các hệ thống tin học và dữ liệu của chúng chống lại sự lạm dụng.

data security package ***bộ chương trình an toàn dữ liệu, gói chương trình an toàn dữ liệu*** Trong an toàn máy tính, bộ chương trình phần mềm kiểm soát sự truy nhập vào các dữ liệu được lưu giữ. *Xem* ACF2, RACF, SMF, UCCL

dat set ***tập dữ liệu; thiết bị dữ liệu*** (1) Trong các cơ sở dữ liệu, tập dữ liệu là tập hợp đã đặt tên của các mục dữ liệu, có quan hệ logic với nhau và được sắp theo thứ tự định trước, nó cũng có thể chứa dữ liệu để truy nhập dữ liệu, ví dụ như các chỉ số. (2) Trong truyền thông dữ liệu, thiết bị dữ liệu là một modem. *Đồng nghĩa với* MODEM.

data set ready ***tín hiệu báo thiết bị dữ liệu sẵn sàng*** Trong truyền thông dữ liệu, tín hiệu dùng ở các modem để chỉ báo rằng nguồn đã bật và modem đang sẵn sàng nhận dữ liệu để truyền. Nó cũng được sử dụng cho kiểm soát luồng; ví dụ, nếu một máy in được nối với một máy tính thì máy in phải đảm bảo rằng máy tính không gửi các ký tự nhanh hơn việc chúng có thể được in ra. *Xem* data set, MODEM, RS-232C.

data-signalling rate ***tốc độ báo hiệu dữ liệu*** Trong truyền thông dữ liệu, tốc độ gộp để truyền các chữ số nhị phân đi qua một mạch, biểu thị theo bit trên giây. *So sánh với* data transfer rate. *Xem* bit.

data-signalling rate selector ***(tín hiệu) chọn tốc độ báo hiệu dữ liệu*** Trong truyền thông dữ liệu, tín hiệu được dùng khi modem cho phép chuyển mạch giữa hai tốc độ truyền. Nếu modem ở đầu gọi thiết lập tốc độ cho nối thì máy tính gọi sử dụng tín hiệu chọn tốc độ báo hiệu dữ liệu (nguồn thiết bị đầu cuối dữ liệu) để xác định tốc độ đường truyền. Modem gọi báo tốc độ cho modem đáp, và modem đáp thông báo cho máy tính được gọi bằng cách thiết lập tín hiệu chọn tốc độ báo hiệu dữ liệu (nguồn thiết bị kết thúc mạch dữ liệu) ở giá trị thích hợp. *Xem* data circuit terminating equiment, MODEM, RS-232C.

data sink ***nơi gom dữ liệu, bộ góp dữ liệu*** Trong truyền thông dữ liệu, phần thiết bị đầu cuối dữ liệu nhận dữ liệu. *So sánh với* data source.

Datasolve ***hãng Datasolve*** Trong truy tìm thông tin trực tuyến, người bán cơ sở dữ liệu chuyên về các cơ sở dữ liệu toàn văn bản. *Xem* database vendor, full-text database.

data source ***nguồn dữ liệu*** Trong truyền thông dữ liệu, phần thiết bị đầu cuối dữ liệu đưa dữ liệu vào liên kết. *So sánh với* data sink.

Data-Star ***dịch vụ Data-Star*** Trong truy tìm thông tin trực tuyến, dịch vụ truy tìm thông tin trực tuyến của Thụy Sĩ.

data station ***trạm dữ liệu*** Trong truyền thông dữ liệu, cụm thiết bị bao gồm thiết bị đầu cuối dữ liệu và thiết bị kết thúc mạch dữ liệu. *Xem* data circuit terminating equipment, data terminal equipment.

data stream ***dòng dữ liệu, luồng dữ liệu*** (1) Trong an toàn dữ liệu, bản gốc hoặc bản mật mã được xem như dãy các ký tự mã trong mã dòng. *Xem* ciphertext, plaintext. (2) Trong truyền thông dữ liệu, dòng liên tục các dữ liệu nối tiếp được truyền ở dạng ký tự hoặc dạng chữ số nhị phân qua một kênh. Dòng dữ liệu có thể chứa thông tin điều khiển và khuôn thức.

data structure ***cấu trúc dữ liệu*** Hệ thống các quan hệ giữa các mục dữ liệu. Các ngôn ngữ bậc cao thiết kế tốt sẽ cho phép người lập trình xác định và xử lý các cấu trúc dữ liệu thích hợp, làm giảm hẳn tính phức tạp của các chương trình. *Xem* array, high-level language, list, queue, stack.

data subject ***chủ thể dữ liệu*** Trong lập pháp, theo định nghĩa của Luật bảo vệ dữ liệu năm 1984 của Anh, cá nhân là đối tượng của dữ liệu cá nhân. *Xem* data protection, personal data.

data-switching exchange ***tổng đài chuyển mạch dữ liệu*** Trong truyền thông dữ liệu, thiết bị lắp đặt ở một vị trí duy nhất dùng để chuyển mạch lưu lượng dữ liệu. *Xem* circuit switching, message switching, packet switching.

data tablet ***bảng dữ liệu*** *Xem* digitizing tablet.

data terminal equipment ***thiết bị đầu cuối dữ liệu, DTE*** Trong truyền thông dữ liệu, bộ phận thiết bị bất kỳ mà tại đó đường truyền thông bắt đầu hoặc kết thúc (ví dụ, thiết bị hiển thị). *So sánh với* data circuit terminating equipment

data terminal ready ***(tín hiệu) terminal dữ liệu sẵn sàng, (tín hiệu) đầu cuối dữ liệu sẵn sàng, DTR*** Trong truyền thông dữ liệu, tín hiệu dùng cùng với modem tự đáp để báo rằng, nó sẵn sàng nhận một cuộc gọi. *Xem* automatic answering, RS-232C.

data transfer rate ***tốc độ chuyển dữ liệu*** Trong truyền thông dữ liệu, số trung bình các bit hoặc byte chuyển qua giữa các thiết bị trong một đơn vị thời gian. Tốc độ chuyển đĩa trung bình từ một thiết bị (ví dụ, ổ đĩa từ) sẽ phụ thuộc vào các tính chất điện và cơ của thiết bị đó, nhưng giới hạn trên của tốc độ tức thời có thể phụ thuộc vào giao diện hoặc đường truyền. *So sánh với*

data-signalling rate. *Xem* magnetic disk.

data transmission ***truyền dữ liệu*** *Xem* data communications.

data transparency ***thông suốt dữ liệu*** Trong truyền thông dữ liệu, kỹ thuật nhờ đó mẫu bit bất kỳ gồm cả những bit thường được dự trữ cho các mục đích kiểm tra có thể được truyền như một khối. *Xem* block, transparent.

data transport system ***hệ chuyển tải dữ liệu*** *Xem* wide area network.

data type ***kiểu dữ liệu*** *Xem* abstract data type, type.

data under voice ***hệ dữ liệu (bên) dưới tiếng nói, DUV*** Trong truyền thông dữ liệu, hệ truyền thông mang dữ liệu số nằm trong phần phổ vô tuyến dưới tần số dùng cho truyền tiếng nói. *So sánh với* data above voice, data in voice.

data user ***người sử dụng dữ liệu, người dùng dữ liệu*** Trong lập pháp, theo Luật bảo vệ dữ liệu năm 1984 của Anh, người nắm giữ dữ liệu. Một người nắm giữ dữ liệu nếu:

(*a*) dữ liệu tạo thành một phần của tập hợp dữ liệu được xử lý hoặc được định để xử lý bởi, hoặc nhân danh người đó;

(*b*) là người (hoặc một mình hoặc liên kết, hoặc cùng với những người khác) kiểm soát nội dung và sử dụng dữ liệu chứa trong tập hợp; và

(*c*) dữ liệu ở dạng trong đó nó được xử lý, hoặc dự định để được xử lý như đã nói ở trên hoặc (mặc dù hiện không phải ở dạng đó) ở dạng mà nó phải được biến đổi thành sau khi được xử lý như vậy và nhằm được xử lý tiếp như thế trong một trường hợp sau đó. *Xem* data protection, personal data.

data validation ***phê chuẩn dữ liệu, xác nhận tính hợp lệ dữ liệu*** Trong tin học, hành động kiểm tra để dữ liệu phù hợp với một số tiêu chuẩn xác định.

data word ***từ dữ liệu*** Trong lập trình, mục dữ liệu được lưu giữ như một từ đơn. *Xem* word. *Đồng nghĩa với* information word.

data word size ***cỡ từ dữ liệu, kích thước từ dữ liệu*** Trong cấu trúc dữ liệu, độ dài một từ dữ liệu, tính theo bit, mà một bộ xử lý trung tâm riêng được thiết kế để xử lý. *Xem* central processing unit, data word.

date of message origination ***ngày thiết lập thông báo*** Trong xác thực, ngày mà người gửi thông báo tính toán MAC (mã xác thực thông báo). Ngày này được dùng để đồng bộ hóa quá trình xác thực thông qua lựa chọn khóa đúng. *Xem* MAC, sender.

date/time stamp ***tem ngày/giờ*** Trong xác thực, một trường trong một thông báo cho biết thời gian và ngày tháng phát xuất của thông báo. Nó được dùng để bảo vệ chống lại các cuộc tấn công phát lại. *Xem* replay.

datum ***mục dữ liệu*** *Xem* data item.

Day-Night switch ***chuyển mạch ngày-đêm*** *Đồng nghĩa với* authorized access control switch.

db ***dB*** *Xem* decibel.

DBA *Xem* database administrator.

Dbase ***virut Dbase*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây

nhiễm các tệp COM, làm sai lạc các tệp dữ liệu, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

DBMS *Xem* database management system.

DC1 ***mã DC1*** Trong mã hóa, mã điều khiển ASCII tương ứng với XON. *So sánh với* DC4. *Xem* ASCII, XON-XOFF protocol.

DC4 ***mã DC4*** Trong mã hóa, mã điều khiển ASCII tương ứng với XOFF. *So sánh với* DC1. *Xem* ASCII, XON XOFF protocol.

DCD *Xem* data carrier detect.

DCE *Xem* data circuit terminating equipment.

DCID ***DCID*** Viết tắt của U.S. Director of Central Intelligence Directive (chỉ thị của giám đốc Cục tình báo trung ương Hoa Kỳ).

DDL ***DDL*** (1) Viết tắt của Data Description Language (ngôn ngữ mô tả dữ liệu). *Xem* data description language. (2) Viết tắt của Document Description Language (ngôn ngữ mô tả tài liệu).

DDN ***DDN*** Trong truyền thông dữ liệu, viết tắt của Defense Data Network (mạng dữ liệu quốc phòng). *Xem* APRPANET.

DDP ***DDP*** Trong tin học, viết tắt của distributed data processing (xử lý dữ liệu phân tán).

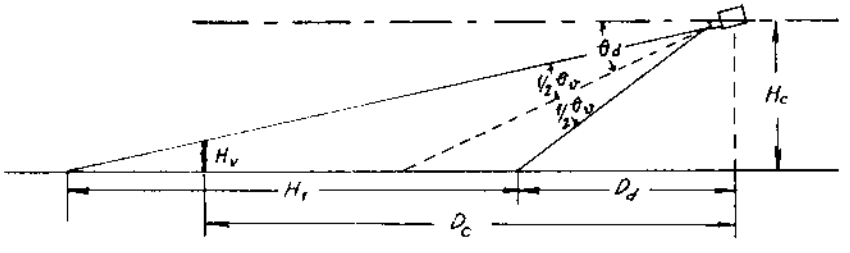
DDS ***DDS*** Trong truyền thông dữ liệu, viết tắt của Direct Digital Service (dịch vụ số trực tiếp). *Xem* ISDN.

DEA *Xem* data encryption algorithm.

DEA 1 ***chuẩn DEA 1*** Trong an toàn dữ liệu, thuật ngữ của Tổ chức tiêu chuẩn hóa quốc tế (ISO) để chỉ tiêu chuẩn mã dữ liệu. *So sánh với* DEA 2. *Xem* data encryption algorithm, data encryption standard.

DEA 2 ***DEA 2*** Trong an toàn dữ liệu, thuật ngữ của Tổ chức tiêu chuẩn hoá quốc tế (ISO) để chỉ RSA. *So sánh với* DEA 1. *Xem* RSA.

DEA device ***thiết bị DEA*** Trong lập mã, một phần hoặc cụm con phần cứng điện tử chỉ thực hiện DEA như đặc tả trong ANSI.92 - 1981 và được Viện tiêu chuẩn quốc gia phê chuẩn. *Xem* ANSI X3.92 - 1981, data encryption standard.



dead zone: *vùng không nhạy.* D_c = khoảng cách từ camera tới vật; H_v = trường nhìn dọc; Θ_d = góc chúi; D_d = vùng không nhạy; H_c = độ cao camera; Θ_v = góc đứng của thấu kính; tất cả các khoảng cách đều đo theo mét.

deadlock ***tắc nghẽn*** (1) Trong truyền thông dữ liệu, tình huống mà trong đó một giao thức không thể tiến triển tiếp được do không có sự chuyển tiếp khả dĩ, hoặc không có sự chuyển tiếp khả dĩ nào để tiến triển tiếp. *Xem* protocol. (2) Trong các hoạt động, điều kiện lỗi trong đó, xử lý không thể tiếp tục vì mỗi trong hai phần tử của quá trình đang chờ tác động từ phần tử kia.

dead zone ***vùng không nhạy, vùng chết*** Trong kiểm soát truy nhập, vùng bên trong một mẫu hình bảo vệ mà trong đó bộ cảm biến không có hiệu lực.

deal ***thỏa thuận mua bán*** Trong hoạt động ngân hàng, một giao dịch dùng trong phạm vi những sản phẩm riêng. *Xem* product.

debit advice ***giấy báo nợ*** Trong hoạt động ngân hàng, giấy báo của ngân hàng phục vụ tài khoản về một khoản nợ đối với tài khoản của người nhận (chủ tài khoản). *Xem* account servicing bank.

debit card ***thẻ ghi nợ*** Trong hoạt động ngân hàng, thẻ cho phép thuê bao mua các loại hàng hóa và dịch vụ từ nhiều loại cửa hàng và cho phép ghi nợ vào tài khoản ngân hàng mà thuê bao đứng tên. *So sánh với* credit card.

debit party ***bên nợ*** Trong hoạt động ngân hàng, nguồn tiền trên sổ sách ngân hàng nhận. *So sánh với* beneficiary, credit party.

debit transfer ***chuyển nợ*** Trong hoạt động ngân hàng, lệnh mà ở đó người gửi được phép chỉ rõ bên nợ chứ không phải bản thân người đó. *Xem* debt party. *Đồng nghĩa với* direct debit.

debug ***gỡ rối; tìm rệp*** (1) Trong tin học, gỡ rối là phát hiện, cách ly và hiệu chỉnh sai sót trong một chương trình máy tính hoặc bản thân hệ máy tính. *Xem* bug, debugger. (2) Trong điện tử học, tìm rệp là dò tìm và loại bỏ các thiết bị nghe lén lắp bí mật mà thường được gọi là con rệp (bug).

debugger ***bộ gỡ rối*** Trong lập trình, chương trình tham gia thử và tìm dấu vết lỗi ở một chương trình ứng dụng. Bộ gỡ rối cho phép người dùng dò từng lệnh một trong suốt chương trình ngôn ngữ bậc thấp, cung cấp các chi tiết về nội dung thanh ghi v.v. sau mỗi lần thực hiện. *Xem* instruction, low-level language.

decentralized computer network ***mạng máy tính phi tập trung*** Trong truyền thông dữ liệu, mạng máy tính trong đó một số các chức năng điều khiển mạng được phân tán trên nhiều nút mạng. *Xem* node.

decibel ***đexiben, dB*** Trong điện tử học và truyền thông, một phần mười của ben, số đo cường độ tín hiệu so với mức chuẩn nào đó. Đexiben bằng mười lần loga thập phân của tỷ số đó. *Xem* bel, logarithm.

decimalization table ***bảng thập phân hóa*** Trong hoạt động ngân hàng, bảng dùng để dịch các ký tự thập lục phân (hệ cơ số 16) sang các ký tự thập phân. Nếu cần rút ra các số thập phân từ một xâu các chữ số nhị phân thì có thể chia xâu thành một loạt các nhóm nửa byte bốn bit. Mỗi nhóm nửa byte biểu thị một giá trị thập lục phân 0-9, A-F. Bảng thập phân hóa cho phép liên kết một

cách tùy ý một số thập phân với mỗi giá trị thập lục phân. Có thể sử dụng quy trình này để rút ra một giá trị xác minh PIN từ bản mã nhận được từ phép mã dữ liệu về tài khoản định danh v.v.. *Xem* ciphertext, hexadecimal, PIN, verification value.

decipher ***giải mật mã, đọc mật mã*** Trong mật mã học, biến đổi bản đã mã hóa thành bản gốc tương đương với nó bằng cách sử dụng một khóa thích hợp. *So sánh với* encipher. *Xem* decrypt, key, plaintext.

decipherment ***(sự) giải mật mã, (sự) đọc mật mã*** Trong lập mã, sự đảo ngược quá trình mã hóa có thể đảo được tương ứng. *So sánh với* encipherment. *Xem* reversible encryption.

decision support system ***hệ hỗ trợ quyết định*** Trong các ứng dụng, hệ xử lý thông tin dùng để hỗ trợ việc ra quyết định, thường trong phạm vi một tổ chức nào đó. *Xem* database, knowledge base.

declarative language ***ngôn ngữ khai báo*** *Đồng nghĩa với* nonprocedural language.

declassification of magnetic storage media ***khử phân loại các phương tiện nhớ từ tính*** Trong an toàn dữ liệu, thủ tục loại bỏ hoàn toàn thông tin đã phân loại hoặc nhạy cảm lưu giữ trên các phương tiện từ tính tiếp nối bằng việc xem xét lại thủ tục đã thực hiện. Sau đó có thể đưa ra một quyết định để (hoặc chống lại) loại bỏ thực tế mức phân loại của phương tiện. Việc khử phân loại cho phép giải phóng phương tiện khỏi môi trường có kiểm soát nếu được những cơ quan cấp phép thích hợp chấp thuận.

decode ***giải mã*** Dịch hoặc xác định ý nghĩa của thông tin đã mã hóa. *So sánh với* decipher, encode. *Xem* decoder.

decoder ***bộ giải mã*** (1) Trong tin học, thiết bị logic nhằm biến đổi dữ liệu từ hệ đếm này sang hệ đếm khác (ví dụ, từ hệ nhị phân sang hệ thập phân). (2) Trong kỹ thuật videotex, thiết bị dùng để giải mã các tín hiệu videotex và hiển thị chúng trên màn hình. (3) Trong truyền hình, hệ mạch máy thu giữa bộ tách sóng tín hiệu và màn hình vốn giải mã các tín hiệu phát hình.

decoupling key ***khóa khử ghép, khóa tách riêng*** (1) Trong hoạt động ngân hàng, khóa dùng cùng với nội dung hiện thời của thanh ghi khóa để tạo dựng khóa giao dịch hiện thời. Ở chế độ hoạt động dựa trên thẻ, các khóa khử ghép được dẫn xuất từ thông tin lưu giữ trên thẻ của người giữ thẻ. Cần có những phương pháp sinh tham số khác cho các chế độ hoạt động không dựa trên thẻ. Về cơ bản, ít nhất một trong các khóa khử ghép trong một giao dịch là hàm của một thông tin nào đó. Thông tin này có thể dẫn xuất từ hoặc cơ sở nhận hoặc cơ sở phát hành thẻ và thiết bị đầu cuối và dù thế nào đi nữa cũng không được truyền đi. *Xem* acquirer, card based mode, card holder, card issuer, key management key system. (2) Trong quản lý khóa, một mục thông tin mà máy chủ và thiết bị đầu cuối trong một mạng EFTPOS biết được, nhưng không được truyền giữa chúng và được dùng trong việc hình thành tham số uỷ quyền. *Xem* transaction key system.

decrypt ***giải mật mã, mở khóa*** Trong mật mã học, biến đổi văn bản đã cải mã (mã hóa hoặc tạo mật mã) thành văn bản gốc tương đương của nó nhờ sử dụng khóa thích hợp. *So sánh với* decipher, encrypt. *Xem* decipher, encode key, plaintext.

decryption ***(sự) giải mật mã*** *Đồng nghĩa với* decipherment.

dedicated ***dành riêng, chuyên dụng*** Thuật ngữ chỉ thiết bị được dành cho một người sử dụng hoặc một kiểu ứng dụng. Ví dụ, bộ xử lý văn bản dành riêng có thể dự trữ cho sự sử dụng của những cá nhân riêng hoặc các báo cáo xử lý văn bản riêng.

dedicated access ***truy nhập dành riêng*** Trong truyền thông dữ liệu, sự nối thường xuyên giữa một terminal và mạng dịch vụ hoặc máy tính dịch vụ.

dedicated channel ***kênh chuyên dụng*** Trong truyền thông dữ liệu, mạch hoặc kênh để dành hoặc được ủy nhiệm cho một sử dụng hoặc một ứng dụng định rõ (ví dụ, cho các mục đích khẩn cấp).

dedicated mode ***chế độ dành riêng, chế độ chuyên dụng*** Trong an toàn máy tính, hoạt động của một hệ ADP sao cho phương tiện máy tính trung tâm, các thiết bị ngoại vi được nối, các phương tiện truyền thông và tất cả các đầu cuối ở xa đều được sử dụng và kiểm soát độc quyền bởi những người sử dụng hoặc những nhóm người sử dụng cụ thể để xử lý những loại và những phạm trù thông tin đặc thù. *Xem* dedicated security mode.

dedicated security mode ***chế độ an toàn dành riêng*** (1) Trong an toàn máy tính, chế độ hoạt động trong đó, mọi người sử dụng đều có mức thông (mức truy nhập) thích hợp và mức cần biết thích hợp đối với mọi dữ liệu trong hệ thống. Hệ được dành riêng đặc biệt và độc quyền và được kiểm soát để xử lý một kiểu hoặc một phân loại thông tin đặc thù hoặc trong hoạt động toàn thời gian hay trong một khoảng thời gian xác định. *So sánh với* multilevel security mode, system high security mode. *Xem* classification, need to know. (2) Trong an toàn máy tính, chế độ hoạt động trong đó, mọi người sử dụng đều có mức truy nhập, sự phê duyệt truy nhập, hình thức và nhu cầu cần biết đối với mọi dữ liệu xử lý bởi AIS. Ở chế độ dành riêng, AIS có thể xử lý một mức phân loại đơn và hoặc một nhóm thông tin hoặc một khoảng các mức phân loại và/hoặc các nhóm thông tin. *Xem* AIS, classification, need to know. (3) Trong an toàn máy tính, hoạt động của một hệ ADP sao cho phương tiện máy tính trung tâm, các thiết bị ngoại vi được nối, các phương tiện truyền thông và tất cả những thiết bị đầu cuối ở xa đều được sử dụng và được kiểm soát một cách độc quyền bởi những người sử dụng hoặc nhóm người sử dụng riêng để xử lý những kiểu và nhóm thông tin đặc biệt.

DEE ***DEE*** Viết tắt của Data Encryption Equipment (thiết bị mã hóa dữ liệu).

default ***ngầm định, ngầm hiểu*** Trong tin học và các hệ điều hành, chỉ một mục chọn sẽ được lấy khi không có những lệnh chỉ rõ của người sử dụng. Các mật khẩu ngầm định thường được hacko khai thác.

default classification ***phân loại ngầm định*** Trong an toàn dữ liệu, sự phân loại tạm thời phản ánh mức phân loại cao nhất đang được xử lý trong một hệ thống tự động hóa. Sự phân loại ngầm định được bao hàm trong câu lệnh bảo vệ gắn với sản phẩm. *Xem* classification.

default to denial of access ***ngầm định từ chối truy nhập*** Trong kiểm soát truy nhập, chỉ thiết kế một hệ trong đó, các cấp phép truy nhập là bắt buộc và các đối tượng không có những sự cho phép đó bị khóa không cho truy nhập. *Xem* access authorization.

defeat ***tránh trót lọt, khắc phục trót lọt*** Trong an toàn vật lý, chỉ sự tránh thành công một hệ báo động hoặc một bộ cảm biến khiến cho một kẻ đột nhập xâm nhập không bị phát hiện.

Defense Data Network ***mạng dữ liệu quốc phòng*** *Xem* ARPANET.

defense industry information ***thông tin công nghiệp quốc phòng*** Thông tin về việc lập kế hoạch kỹ thuật, các yêu cầu và tiếp nhận dự phòng ngành công nghiệp thông qua những chương trình khác nhau cho phép ngành công nghiệp đáp ứng được những nhu cầu về vũ khí và các hệ thống hỗ trợ. Các chương trình bao gồm các IAC của Bộ quốc phòng Hoa Kỳ, các chương trình thầu khoán tiềm tàng của các bộ phận của Bộ quốc phòng Hoa Kỳ, các bản tóm tắt quy hoạch tiền tiến cho công nghiệp, các hội thảo kỹ thuật về những chủ đề đặc biệt và những dịch vụ do Văn phòng thứ trưởng bộ quốc phòng về nghiên cứu và kỹ thuật và những bộ phận khác của Bộ quốc phòng Hoa Kỳ khởi xướng. *Xem* IAC, OUSDR&E.

defensive depth ***độ sâu phòng thủ*** Trong an toàn máy tính, nguyên tắc thiết kế để kẻ tấn công bị buộc phải khắc phục được một loạt các biện pháp an toàn để đạt tới mục tiêu của hắn (ví dụ truy nhập vùng rất nhạy cảm đòi hỏi phải thông qua số tối đa các vùng có kiểm soát và vi phạm một điểm điều khiển sẽ gây báo động và buộc phải tuân thủ lại tất cả các điểm kiểm soát lân cận).

degauss ***khử từ; xóa hẳn*** (1) Trong an toàn máy tính khử từ là tác dụng trường dòng xoay chiều (AC) biến đổi nhằm khử từ phương tiện ghi từ tính, thường là băng từ. Quá trình liên quan tới làm tăng trường AC dần dần từ zero tới giá trị cực đại và làm giảm nó dần trở lại giá trị zero, nó để lại độ cảm ứng từ dư rất thấp trên phương tiện. *Đồng nghĩa với* deperm. (2) Theo nghĩa rộng, xóa hẳn là loại bỏ thông tin khỏi phương tiện lưu giữ từ tính.

degausser ***bộ khử từ*** Trong điện tử học, thiết bị điện (AC hoặc DC) hoặc một cụm nam châm cầm tay có thể sinh ra lực kháng từ nhằm khử từ các phương tiện nhớ từ tính hoặc vật liệu từ khác. *Xem* coercive force, degauss.

degradation ***giảm mức, xuống cấp*** Trong truyền thông dữ liệu, sự giảm phẩm chất trong các đặc trưng của tín hiệu vì lý do bất kỳ.

degree of trust ***mức tin cậy*** Mức độ tin cậy có thể đặt vào các cơ chế an toàn nhằm làm cho chính sách an toàn trở nên có hiệu lực một cách đúng đắn. *Xem* security policy.

DEK *Xem* data-encrypting key.

DEL *Xem* delete character.

delay circuit ***mạch trễ*** Trong an toàn vật lý, mạch trong hệ thống báo động cho phép đi vào hoặc đi ra trong một khoảng thời gian nào đó, và do đó cho phép cá nhân được phép đủ thời gian để vào hoặc ra trước khi hệ thống báo động hoặc thôi báo động.

delay/denial of service ***trì hoãn/từ chối phục vụ*** Trong an toàn truyền thông, những cuộc tấn công nhằm ngăn không cho các thông báo đạt tới đích của chúng trong khoảng thời gian chấp nhận được. Tác dụng này có thể đạt được bằng nối lén chủ động, chương trình con ngựa thành Tơroa, truyền thông báo hoạc định tuyến sai các thông báo. Nối lén chủ động có thể dùng để loại bỏ hoặc làm trễ các thông báo trong mạng. Chương trình con ngựa thành Tơroa có thể nhận các tín hiệu mã hóa từ kẻ tấn công để khởi phát làm rối loạn hệ thống. Những cuộc truyền thông báo không được phép có thể được dùng để gây tràn mạng và do đó làm giảm thiểu hiệu năng của mạng, trong khi đó định tuyến sai các thông báo có thể ngăn không cho chúng tới được địa chỉ đã định hoặc tới vào thời khoảng chấp nhận được.

Sự phát hiện các cuộc tấn công trì hoãn/từ chối phục vụ sẽ phức tạp nếu sự tấn công được khởi phát ở trạng thái lưu lượng tĩnh. Sau đó máy phát cố thiết lập truyền thông sẽ phát hiện được rằng, dịch vụ bị từ chối hoặc bị trễ bởi thiếu hoặc trễ tín hiệu báo nhận từ máy thu. Mặt khác, máy thu sẽ không biết được về sự tấn công. Cơ chế đáp lại yêu cầu sẽ đưa ra sự cảnh báo về các cuộc tấn công trì hoãn/từ chối với cái giá phải trả là dải thông hiệu dụng của mạng bị giảm. *Xem* active wiretapping, bandwidth, banking networks, denial of service, request response, Trojan Horse.

delay distortion ***méo do trễ*** Trong truyền thông dữ liệu, méo gây ra bởi tốc độ lan truyền khác nhau của các tín hiệu trong môi trường truyền dẫn nảy sinh do các chênh lệch tần số của chúng. Loại méo này không ảnh hưởng tới tiếng nói nhưng có thể có ảnh hưởng nghiêm trọng tới sự truyền dữ liệu nào đó.

delay equalizer ***bộ bù trễ pha*** Trong truyền thông, mạng hiệu chỉnh dùng để bù lại độ trễ pha hoặc tốc độ thay đổi độ lệch pha theo tần số, của một hệ thống, về cơ bản không đổi trong dải tần cần thiết. *Xem* phase delay. *Đồng nghĩa với* phase equalizer.

delay line ***đường trễ*** Trong điện tử học, thiết bị gây ra độ trễ thời gian khi truyền một xung.

delay vector ***vectơ trễ*** Trong truyền thông dữ liệu, danh sách các thời gian chuyển tiếp ước lượng được đối với gói tin từ một nút tới mọi nút khác trong mạng chuyển mạch gói. Nó được dùng trong các hệ định tuyến thích ứng. *Xem* adaptive routing, packet switching.

delegate ***ủy nhiệm*** Trong kiểm soát truy nhập, cho quyền một chủ thể thực hiện một quyền nào đó của chủ thể khác. *Xem* subject.

delete ***xóa, bỏ*** (1) Ở các hệ thống

nhớ, loại bỏ một tệp khỏi băng hoặc đĩa từ. *Xem* magnetic disk, magnetic tape. (2) Trong xử lý văn bản, chức năng cho phép xóa các đoạn văn bản lưu giữ trong bộ nhớ.

delete character ***xóa ký tự, ký tự DEL, DEL*** Trong mã hóa, ký tự điều khiển dùng để xóa ký tự lỗi hoặc không mong muốn (ví dụ, ký tự truyền theo mạch truyền thông).

deliberate threat ***hiểm họa có chủ tâm*** Trong an toàn máy tính, hiểm họa từ một người hoặc nhiều người phá hỏng một cách có ý thức và sẵn sàng đối với hệ máy tính. *So sánh với* accidental, threat, active threat, logical threat, passive threat, physical threat. *Xem* threat.

delimeter ***dấu tách, dấu phân tách*** Trong tin học, một ký tự xác định dùng để chỉ kết thúc của một trường. *Xem* field.

deliverable ***có thể chuyển giao*** Trong an toàn thông tin, một mục hoặc tài nguyên được tạo ra hoặc được sử dụng trong quá trình phát triển một mục tiêu đánh giá mà cần phải làm cho những người đánh giá có thể sử dụng được cho mục tiêu đánh giá. *Xem* information technology security evaluation criteria, information technology security evaluation manual.

delivery assurance ***bảo đảm cung cấp, bảo đảm phân phát*** Trong an toàn dữ liệu, chỉ mức hư hỏng gắn liền với sự trì hoãn hoặc từ chối các thông báo. Bảo đảm phân phát liên quan không chỉ tới sự mất mát các thông báo mà cả tới sự ngăn ngừa bổ sung hoặc xem lại các thông báo. *Xem* delay/denial of service, end-to-end assurance, replay.

delta modulation ***điều biến denta*** Trong truyền thông dữ liệu, dạng điều chế PCM vi sai trong đó, chỉ một bit cho mỗi mẫu được sử dụng. *Xem* differential PCM.

delta routing ***định tuyến denta*** Trong truyền thông dữ liệu, phương pháp định tuyến trong mạng chuyển mạch gói mà trong đó, bộ điều khiển định tuyến trung tâm nhận thông tin từ các nút và phát ra các lệnh định tuyến, song vẫn để cho các nút riêng lẻ có một mức tự do. *So sánh với* adaptive routing, centralized adaptive routing, directory routing, fixed routing, hot potato routing. *Xem* node, packet switching network, routing.

demand multiplexing ***dồn kênh theo nhu cầu*** Trong truyền thông dữ liệu, dạng dồn kênh phân thời trong đó các khe thời gian được phân phối theo nhu cầu. *Xem* time division multiplexing. *Đồng nghĩa với* dynamic multiplexing.

demarcation strip ***dải ranh giới, tấm mạch ranh giới*** Trong truyền thông dữ liệu, bo mạch đầu cuối tác động như giao diện vật lý giữa một máy kinh doanh và hãng truyền thông công cộng. *Xem* common carrier.

democratic network ***mạng dân chủ*** Trong truyền thông dữ liệu, mạng đồng bộ hóa trong đó không một nhịp đồng hồ nào có quyền ưu tiên so với nhịp đồng hồ khác. *So sánh với* despotic network, hierarchical network.

demodulation ***giải điều (chế)*** Trong truyền thông, quá trình khôi phục lại

tín hiệu điều biến ban đầu từ tín hiệu đã điều biến. Các phương pháp điều biến được dùng cả ở máy thu vô tuyến (thu thanh) lẫn máy thu hình và ở thiết bị truyền thông dữ liệu. *So sánh với* modulation.

demodulator ***bộ giải điều (chế)*** (1) Trong truyền thông, thiết bị thực hiện chức năng giải điều chế trong các máy thu thanh hoặc thu hình. *Xem* demodulation. (2) Trong truyền thông dữ liệu, thiết bị thực hiện chức năng giải điều chế ở mạch truyền dữ liệu. Nó thường nằm chung với thiết bị thực hiện điều biến, cùng nhau tạo thành modem. *Xem* MODEM.

demon ***quá trình đemon; (chương trình) demon*** (1) Trong lập trình, quá trình đemon là quá trình tạm treo chờ xảy ra một loại biến cố nào đó. Khi đó nó được tự động kích hoạt, thực hiện tiếp công việc của nó và hoặc kết thúc hoặc tự treo chờ biến cố tiếp theo. Nó được dùng trong các ứng dụng trí tuệ nhân tạo. *Xem* artificial intelligence, coroutine. (2) Trong bảo vệ phần mềm, chương trình dùng để phá vỡ một số sơ đồ bảo vệ phần mềm. Chương trình đemon (con quỷ) ban đầu dùng để chặn và giám sát tất cả các yêu cầu đĩa do chương trình được bảo vệ thực hiện. Nếu một bản sao chương trình được bảo vệ được lập, chẳng hạn bằng bộ sao chụp bit thì demon sẽ mô phỏng "dấu tay" mà chương trình nguồn sử dụng và do đó, có khả năng bỏ qua (tránh được) sơ đồ bảo vệ phần mềm. Đemon không có hiệu quả đối với các chương trình lập địa chỉ điều khiển đĩa trực tiếp chứ không phải thông qua hệ điều hành hoặc BIOS. *So sánh với* daemon. *Xem* BIOS, bit copier, execute protection, fingerprint, operating system.

demultiplexing ***phân kênh, tháo dồn kênh*** Trong truyền thông dữ liệu, sự phân chia một hoặc nhiều dòng thông tin thành một số dòng lớn hơn. *So sánh với* multiplexing.

denial ***từ chối, không nhận*** Trong truyền thông, điều kiện xuất hiện trong mạng điện thoại khi không có mạch nào sẵn sàng và âm bận được trả về bên gọi.

denial of message service ***từ chối dịch vụ thông báo*** Trong an toàn truyền thông, một cuộc tấn công vào PDU trong một luồng thông báo vốn hoặc loại bỏ PDU trong quá trình chuyển tiếp hoặc trì hoãn PDU đi theo một hoặc cả hai hướng. *So sánh với* message stream modification, spurious association initiation. *Xem* denial of service, PDU.

denial of service ***từ chối dịch vụ*** (1) Trong an toàn dữ liệu, sự ngăn cản truy nhập được phép vào các tài sản hoặc dịch vụ của hệ thống, hoặc làm trễ thời gian của các hoạt động quan trọng. *Xem* denial of massage service. (2) Trong an toàn máy tính, hoạt động hoặc các hoạt động ngăn ngừa một phần bất kỳ của một AIS hoạt động phù hợp với mục đích chủ đích của nó. Điều này cũng bao gồm hoạt động bất kỳ gây ra sự phá hủy, sự sửa đổi trái phép hoặc sự trì hoãn dịch vụ. *Xem* delay/denial of service.

dense index ***chỉ mục trù mật, danh mục trù mật*** Trong các cơ sở dữ liệu, chỉ mục chứa một mục nhập cho mỗi

bản ghi cần tìm kiếm. *So sánh với* non-dense index. *Xem* index, record.

Den Zuk ***virut Den Zuk*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động của đĩa mềm, ảnh hưởng tới hoạt động thời gian chạy và làm sai lạc cung khởi động. *Xem* virus names.

dependability ***độ tin cậy, tính đáng tin cậy*** Trong kỹ thuật tin cậy, chỉ độ chắc chắn mà một hệ thống sẽ hoạt động đúng.

dependence ***(sự) phụ thuộc*** Sự tồn tại một quan hệ trong đó, chủ thể có thể không hoạt động đúng trừ phi đối tượng (có thể là chủ thể khác) có hành vi đúng.

deperm ***khử từ*** *Xem* degauss.

derived PIN ***số nhận dạng cá nhân dẫn xuất, PIN dẫn xuất*** Trong công tác ngân hàng, số nhận dạng cá nhân (PIN) được tạo ra từ thông tin nào đó liên quan tới số tài khoản hoặc danh tính khách hàng. PIN nhận được nhờ thuật toán có chứa một khóa bí mật. Những PIN như thế có thể được kiểm chứng ở vị trí bất kỳ, bằng việc truy nhập khóa mật dùng trong thuật toán, mà không đòi hỏi nhớ PIN ở tại vị trí. *Xem* PIN, PIN management and security, PIN offset.

DES *Xem* data encryption standard.

descriptive top-level specification ***đặc tả mô tả mức cao nhất*** Một đặc tả mức cao nhất được viết bằng ngôn ngữ tự nhiên (ví dụ tiếng Anh), một biểu diễn thiết kế chương trình không chính thức, hoặc tổ hợp cả hai. *So sánh với* formal top-level specification. *Xem* top-level specification.

descriptor ***bộ mô tả*** Trong lập trình, thông tin chứa các chi tiết cho biết cách nhớ thông tin khác. Do đó chương trình có thể tham khảo bộ mô tả, chẳng hạn của một tệp và sau đó thông dịch đúng dữ liệu được tham chiếu. *Xem* file descriptor.

designated approving authority ***người có thẩm quyền phê duyệt chỉ định*** (1) Trong an toàn máy tính, một quan chức được chỉ định phê duyệt hoạt động của các hệ thống tự động hóa ở các phương tiện máy tính trong phạm vi quyền hạn của người đó về xử lý thông tin hoặc về xử lý tới hạn. *Xem* critical processing. (2) Trong an toàn máy tính, quan chức cao cấp tinh thông có quyền và trách nhiệm ra quyết định quản lý về việc chấp nhận hay bác bỏ các biện pháp bảo vệ an toàn quy định cho một AIS; quan chức có thể chịu trách nhiệm đưa ra lệnh công nhận ghi lại quyết định chấp nhận những biện pháp bảo vệ đó. *Xem* AIS, accreditation. (3) Trong an toàn máy tính, quan chức được quy định trách nhiệm công nhận các bộ phận, các hoạt động và các mạng ADP trong phạm vi thẩm quyền của quan chức đó.

design standard ***tiêu chuẩn thiết kế*** Các chuẩn cứ thiết kế đặc biệt xác định cả kết quả lẫn phương pháp thực hiện mỗi tiêu chuẩn. *So sánh với* performance standard.

design verification ***(sự) kiểm chứng thiết kế*** Trong an toàn máy tính, việc sử dụng các kỹ thuật kiểm chứng,

thường có máy tính trợ giúp, để chứng minh sự tương ứng toán học giữa mô hình (an toàn) trừu tượng và đặc tả hệ thống hình thức. *Xem* security model, verification.

desk checking ***kiểm tra tại bàn*** Trong lập trình, quá trình thủ công trong đó dữ liệu mẫu được lần theo dấu vết suốt logic chương trình để xác định xem xử lý logic có như mong muốn không.

despotic network ***mạng "chuyên chế"*** Trong truyền thông dữ liệu, mạng đồng bộ hóa trong đó một đồng hồ chủ duy nhất điều khiển tất cả các đồng hồ khác trong mạng. *So sánh với* democratic network. *Xem* hierarchical network.

destruction ***(sự) phá hỏng, (sự) phá hủy*** Trong an toàn máy tính, sự thay đổi vật lý các phương tiện của hệ ADP hoặc các thành phần của hệ ADP khiến cho chúng không còn dùng được nữa để lưu giữ hoặc truy lục thông tin. *Xem* ADP.

destructive readout ***đọc có xóa, đọc phá hủy*** Trong các hệ thống nhớ, một thuộc tính của một số hệ thống nhớ. Khi đọc phá hủy một vị trí nhớ, dữ liệu được chuyển sang bộ xử lý song bản sao trong bộ nhớ bị hủy do quá trình đọc. Các hệ thống nhớ đọc hủy đòi hỏi logic đặc biệt để ghi lại dữ liệu sao khi nó được đọc. *So sánh với* nondestructive readout.

Destructor ***virut Destructor*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

detector ***máy dò, thiết bị phát hiện*** Trong an toàn vật lý, thiết bị dùng để phát hiện một điều kiện báo động đòi hỏi tác động ngay lập tức, ví dụ sự xâm nhập, hỏa hoạn, khói, vận hành thiết bị không an toàn, trục trặc thiết bị.

deterrent ***bộ cản*** Trong an toàn máy tính, thiết bị ngăn cấm tác động không được phép. Cửa bị khóa là ví dụ về bộ cản vật lý, trong khi đó camera giám sát có thể thực hiện chức năng bộ cản tâm lý.

development center ***trung tâm phát triển*** Trong tin học, cơ sở thực hiện phần cứng và phần mềm cần thiết cho phát triển ứng dụng. *Xem* information centre.

device assignment ***gán thiết bị*** Trong các hệ điều hành, chỉ phương tiện logic cho các chỉ định vật lý cho phép các thiết bị ngoại vi hoạt động khi một chương trình ứng dụng yêu cầu mà không cần ngắt hoặc nối vật lý. *Xem* logical.

device control ***(ký tự) điều khiển thiết bị*** Trong truyền thông dữ liệu, ký tự trong mã truyền dữ liệu có thể dùng để điều khiển một thiết bị, ví dụ bật hoặc tắt thiết bị.

Devil's Dance ***virut Devil's Dance*** Trong an toàn máy tính, virut máy tính kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

DFT scrambler ***bộ xáo trộn DFT*** *Xem* discrete Fourier transform scrambler.

DGP ***DGP*** (1) Trong an toàn vật lý, viết tắt của Data Gathering Panel (bảng thu thập dữ liệu), thiết bị điều khiển để nhận, hiển thị và nhớ thông tin di động. (2) Trong an toàn vật lý, hệ thống nhận và phát lại tín hiệu (bộ phát đáp) nhận một số tín hiệu báo động để giao tiếp với bộ xử lý báo động.

DGT ***DGT*** Viết tắt của Director Generale des Telecommunications (tổng giám đốc hãng viễn thông).

DG XIII ***ban DG XIII*** Ban XIII thuộc tổng giám đốc ủy ban Cộng đồng Châu Âu, nghiên cứu thị trường thông tin và sự đổi mới.

diagnostic code ***mã chẩn đoán*** Trong an toàn vật lý, sự hiển thị chữ số mô tả một điều kiện hệ thống, chẳng hạn một trục trặc. Mã có thể tự giải thích hoặc có thể liên quan tới một điều kiện được giải thích chi tiết trong sổ tay hoặc sổ hướng dẫn thao tác.

diagnostics ***hệ chẩn đoán*** Trong tin học, các chương trình và phương pháp dùng để phát triển và cách ly các lỗi trong một hệ thống, thành phần hoặc chương trình. Chương trình chẩn đoán sẽ thường tạo ra một bản in phân tích hoạt động đang được kiểm tra để giúp tìm và hiệu chỉnh lỗi. *So sánh với* debugger. *Đồng nghĩa với* service software.

dial access ***truy nhập qua quay số*** Trong truyền thông dữ liệu, sự nối tới một mạng, một dịch vụ hay một máy tính thông qua mạng điện thoại chuyển mạch công cộng, từ một thiết bị đầu cuối.

dial back ***quay số ngược*** *Xem* call back.

dialer ***bộ quay số*** *Đồng nghĩa với* telephone dialer.

dial-up control ***kiểm soát quay số*** Trong an toàn máy tính, hệ an toàn được dùng để xử lý sự lạm dụng các hệ thống máy tính bởi các hackơ. Sự lạm dụng đó có thể gây ra các vấn đề từ truy nhập bất hợp pháp và làm sai lạc các tệp đến đơn giản là cản trở tuyến điện thoại. Một số hệ thống quay số đòi hỏi nhận dạng người dùng và kiểm chứng trước khi truyền âm modem; quá trình này ngăn cản hackơ quay số điện thoại theo trình tự cho tới khi nhận được âm modem. Những biện pháp phòng ngừa an toàn khác bao gồm các phản ứng đối với việc người sử dụng liên tiếp không nhập được mật khẩu đúng, trong một số hệ thống, những cuộc gọi như vậy được tự động rẽ mạch tới một nhân viên an toàn, một người không biết về người gọi, để khởi phát tìm vết của số điện thoại đang gọi. Các hệ thống gọi ngược đòi hỏi người sử dụng tự định danh và sau đó treo máy. Số điện thoại được phép đối với người sử dụng đó sau đấy được gọi ngược và sau khi người sử dụng hợp pháp đưa một mã nhận dạng thì đường nối được lập. *Xem* call back, MODEM, telephone intrusion.

DIANE ***mạng DIANE*** Viết tắt của Direct Information Access Network for Europe (mạng truy nhập thông tin trực tiếp cho châu Âu); các dịch vụ thông

tin được cung cấp qua hệ Euronet. *Xem* Euronet.

dibit ***dibit, bit đôi*** Trong truyền thông dữ liệu, nhóm hai bit. Bốn trạng thái có thể của bit đôi là 00, 01, 10, 11. *So sánh với.* tribit. *Xem* bit.

dictionary attack ***tấn công dùng từ điển*** Trong kiểm soát truy nhập phương pháp thu được hiểu biết về các mật khẩu. Một từ điển lớn các mật khẩu tiềm tàng được dùng để đoán nhận các mật khẩu. Những cuộc tấn công như vậy có thể bị phát hiện bởi việc giám sát trực tuyến các mục nhập mật khẩu. Ở một số hệ thống, các mật khẩu được mã hóa không đảo được và được lưu giữ trong một tệp mật khẩu. Kỹ thuật mã hóa có thể không bao gồm khóa bí mật, ví dụ mật khẩu tự nó có thể được dùng như khóa để mã một khối dữ liệu cố định. Trong trường hợp này, tấn công dùng từ điển có thể được thực hiện ngoại tuyến nếu kẻ tấn công có thể truy tìm được tệp mật khẩu. Kẻ tấn công mã hóa từng mục trong từ điển và kiểm tra kết quả so với danh sách các mật khẩu mã hóa đã lưu. *Xem* Hanover hacker, Morris worm, password.

differential PCM ***điều biến mã xung vi sai, điều chế mã xung vi sai, DPCM*** Trong truyền thông dữ liệu, một biến thể của điều biến mã xung (PCM) trong đó, hiệu giá trị giữa một mẫu và mẫu trước đó được mã hóa. Vì số bit cần truyền đi ít hơn so với ở PCM nên phương pháp này được dùng trong liên lạc vệ tinh. *Xem* pulse code modulation, sampling.

Diffie-Hellman technique ***phương pháp Diffie-Hellman*** Trong lập mã, phương pháp khóa công khai để phân phối khóa. Hai bên Alice và Bob trao đổi thông tin, cho phép mỗi người trong họ xác định cùng khóa mật, nhưng một kẻ nghe lén không thể thực hiện được về mặt tính toán trong việc xác định khóa trên cơ sở thông tin trao đổi.

Alice và Bob thỏa thuận về hai số nguyên α và số nguyên tố p. Alice chọn một số nguyên a và tính y_a:

$$y_a = \alpha^a \bmod p$$

tương tự, Bob chọn số nguyên b và tính y_b:

$$y_b = \alpha^b \bmod p$$

Alice và Bob trao đổi các giá trị tính được y_a và y_b; sau đó họ sử dụng chúng để tính khóa mật K:

$$K = (\alpha)^{ab} \bmod p$$

Tương tự, máy tính của Bob sử dụng giá trị nhận được y_a và số bí mật b để tính:

$$K = (y_a)^b \bmod p$$

Nỗ lực tính toán đối với mỗi bên là tương đương với chừng $2\log_e(p)$ phép nhân mod p. Tuy nhiên, một kẻ nghe lén cần tính hoặc a hoặc b để xác định K, trong đó:

$$a = \log_\alpha y_b \bmod p.$$

Việc tính toán số nguyên a đòi hỏi xấp xỉ $p^{1/2}$ phép tính. Nếu p là nhỏ hơn 2^{200} một chút thì các bên truyền thông thực hiện 400 phép nhân mod p, nhưng một kẻ tấn công phải thực hiện 2^{100}, tức là xấp xỉ 10^{30} phép tính để xác định K. Tuy nhiên, một kẻ đánh lừa có thể khai thác phương pháp này nếu có thể chặn các cuộc liên lạc giữa các bên truyền thông. Kẻ đánh lừa tạo ra một số nguyên c và tính:

$y_c = \alpha^c \bmod p$

y_a đã truyền bị chặn từ Alice và kẻ đánh lừa truyền y_c vào chỗ của nó cho Bob. Tương tự, y_b từ Bob bị chặn và lại được thay thế bởi y_c và gửi tiếp cho Alice. Alice tính toán một khóa dựa trên y_c và số nguyên a, trong khi đó Bob tính toán một khóa dựa trên y_c và b. Kẻ tấn công cũng tính toán giống như thế cả hai khóa. Sau đó Alice và Bob truyền dữ liệu đã mã hóa mà có thể được kẻ đánh lừa giải mã và tái mã hóa để truyền tiếp.

Phương pháp Diffie-Hellman được bảo vệ bằng các bằng sáng chế. *So sánh với* keyless cryptography. *Xem* cryptographic key, ElGamal cipher.

diffuse risk from adversarial source ***rủi ro lan truyền từ các nguồn bất lợi*** Trong quản lý rủi ro, một tình huống thông thường trong an toàn máy tính, trong đó bản chất của rủi ro và các đối tượng của rủi ro là lan truyền và nguồn rủi ro có thể là kẻ thù có ảnh hưởng xấu. *Xem* risk analysis, risk assessment.

diffusion ***phân tán, phát tán*** (1) Trong lập mã, phương pháp tăng sức mạnh của một hệ mật mã bằng cách trải rộng các thống kê của không gian thông báo thành một cấu trúc thống kê gồm các tổ hợp dài các ký tự trong bản mã. Điều đó làm tăng có hiệu quả độ dài của bản mật mã cần thiết cho mọi phép phân tích thống kê của nhà phân tích mật mã (nhà mã thám). *So sánh với* confusion. *Xem* ciphertext, cryptanalysis, strength. (2) Trong lập mã, đặc tính của các thuật toán mật mã vốn che dấu các tính chất thống kê của bản gốc bằng cách pha loãng chúng trong bản mật mã.

digital ***(thuộc) số, digital, dạng số*** Chỉ các chữ số hoặc biểu diễn dữ liệu hoặc các đại lượng vật lý bằng các chữ số. *So sánh với* analog.

digital bit pipe ***ống bit số*** Trong truyền thông dữ liệu, một kênh quan niệm giữa một người sử dụng đầu cuối và một hãng truyền thông để truyền dữ liệu nhị phân.

digital communicator ***bộ truyền tin số*** Trong an toàn vật lý, thiết bị tự động quay số một trạm trung tâm khi nhận một tín hiệu báo động, và truyền thông báo đã mã chứa các chi tiết về danh tính thuê bao và bản chất của báo động. Thông thường bộ truyền tin số chờ tín hiệu báo nhận từ trạm trung tâm trước khi tắt. *Xem* central station. *Đồng nghĩa với* digital dialer.

digital dialer ***bộ quay số bằng số*** *Đồng nghĩa với* digital communicator.

digital distributed system security architecture ***kiến trúc an toàn hệ thống số phân tán*** Trong an toàn máy tính, kiến trúc an toàn phát triển cho các hệ máy tính phân tán của hãng DEC (Digital Equipment Corporation).

Tổng quan

Kiến trúc tạo ra một khuôn khổ chung cho một môi trường tính toán đa dụng có các hệ không đồng nhất, trong đó không có các cơ quan ủy quyền hoặc các kiểm soát trung tâm và không có sự tín nhiệm trên toàn cầu. Kiến trúc bao quát các vấn đề xác thực người sử dụng và hệ thống, kiểm soát truy nhập bắt buộc và tùy ý, khởi tạo và nạp an

toàn, và ủy quyền.

Hệ thống phân tán sẽ không có bộ giám kiểm tham chiếu đơn lẻ ép tuân thủ một chính sách an toàn duy nhất. Mỗi hệ thống bên trong hệ phân tán sẽ có bộ giám kiểm tham chiếu riêng buộc tuân thủ theo chính sách riêng của nó. Khi nhận được một yêu cầu truy nhập đối với một đối tượng vùng từ một nguồn ở xa, bộ giám sát tham chiếu cục bộ phải đảm bảo rằng: sự xác thực chủ thể thích hợp đã xảy ra, hệ ở xa đã được chủ thể cấp phép để thực hiện yêu cầu đó và có sự tương thích giữa chính sách an toàn của chủ thể ở xa và đối tượng vùng, để có thể đánh giá được các quyền truy nhập. Cũng phải có một mức tin cậy lẫn nhau nào đó giữa các bộ giám kiểm tham chiếu.

Kiến trúc tạo điều kiện sử dụng rộng rãi các MAC (mã xác thực thông báo) để đảm bảo tính toàn vẹn của các thông báo. Kiến trúc cũng sử dụng các MAC phi mật mã sao cho người sử dụng có thể kiểm tra MAC của một thông báo, mà không cần truy nhập khóa mật mã, song không có khả năng tạo ra một thông báo sinh ra MAC xác định trước. Các MAC phi mật mã như thế phải được phân tán với tính toàn vẹn được đảm bảo, ví dụ như được công bố bởi nguồn đáng tin cậy. Ví dụ, các MAC như thế có thể được dùng để đánh giá tính toàn vẹn của phần mềm dùng rộng rãi.

Có thể tạo ra một kênh an toàn hoặc bằng một đường vật lý có bảo vệ, ví dụ như dây dẫn, hoặc đường logic được khóa mã. Một kênh an toàn như thế sẽ tạo ra hoặc sự xác thực hoặc tính bí mật hoặc cả hai, trong khi kênh không an toàn chẳng cho gì cả. Một kênh vật lý an toàn được nhận dạng bởi một địa chỉ phần cứng, ví dụ như một số hiệu cổng I/O ở một máy tính, trong khi mà kênh mã hóa được nhận dạng bằng khóa mật mã. Các mật mã đối xứng được sử dụng để giữ bí mật các kênh mã hóa, còn mật mã khóa công khai, với việc sử dụng các thông báo chứng nhận, được dùng cho các kênh an toàn sẽ cung cấp sự xác thực.

Các kênh vật lý có thể được xử lý như các đối tượng và được bảo vệ bởi kiểm soát truy nhập, nhưng sự kiểm soát truy nhập như thế không thích hợp cho một đường logic mã hóa vì việc sử dụng kênh phụ thuộc vào sự hiểu biết các khóa mật mã thích hợp.

Tính toàn vẹn của phần mềm đã nạp

Sự an toàn của hệ thống máy tính phụ thuộc rất quan trọng vào tính toàn vẹn của phần mềm đã nạp. Tuy nhiên, thực sự có những tầng phần mềm trong một hệ máy tính. Phần mềm khởi động, thường trú trong phần cứng hoặc phần sun, sẽ nạp hệ điều hành. Sau đó hệ điều hành có thể nạp một hệ như một DBMS, hệ này đến lượt nó lại nạp một chương trình ứng dụng riêng. Hơn nữa, các quá trình máy tính mà biểu thị hiệu quả phần mềm đang hoạt động sẽ liên lạc ngày càng tăng với những quá trình khác qua mạng, và những quá trình như thế phải có khả năng tiến hành xác thực lẫn nhau.

Tính toàn vẹn của phần mềm có thể được kiểm tra theo cách tương tự với cách dùng cho các thông báo đã truyền, tức là với các MAC. Tuy nhiên, thông

D

thường MAC được sử dụng giữa một cặp máy gửi/máy nhận nào đó giữ một khóa mã đối xứng bí mật. Trong trường hợp tính toàn vẹn phần mềm được kiểm tra bởi một tập hợp các hệ nhận thì sử dụng các chứng chỉ (thông báo chứng thực).

Một bản sao phần mềm khởi động được cung cấp với cặp khoá mật/công khai và một thông báo chứng nhận (chứng chỉ) chứa MAC của hệ điều hành. Khi hệ điều hành được nạp vào thì bản sao khởi động sẽ kiểm tra MAC của phần mềm đã nạp với MAC chứa trong thông báo chứng nhận. Trong trường hợp kiểm tra thành công, bản sao khởi động tạo ra một cặp khóa mật/khóa công khai cho phần mềm đã nạp, ký một thông báo chứng nhận cho MAC và khóa công khai được tạo ra, cùng với khóa mật của bản sao khởi động, xóa thông tin mật khởi động khỏi mọi vị trí nhớ mà hệ điều hành có thể truy nhập và sau đó thực hiện hệ điều hành. Hệ điều hành có thể tự xác thực trước những quá trình khác, bằng khóa mật và thông báo chứng nhận do bản sao khởi động cung cấp. Toàn bộ quá trình này có thể được lặp lại khi nạp mức tiếp theo của phần mềm; như vậy tạo ra một sự đảm bảo đối với tính toàn vẹn của phần mềm đã nạp và một biện pháp cho các quá trình để xác thực lẫn nhau trong một hệ phân tán.

Kiểm soát truy nhập

Quy ước đặt tên nhất quán là điều căn bản đối với kiến trúc an toàn phân tán, các chủ thể ở xa phải có khả năng tự nhận dạng các đối tượng. Các đối tượng phải có khả năng đặt tương quan một chủ thể với các quyền truy nhập đã lưu của nó. Trong DSSA, một hệ thống thư mục phân cấp và các chủ thể, cung cấp một phương tiện đưa ra tên đường dẫn cho các chủ thể. Một ID người dùng duy nhất được lưu ở mục nhập thư mục được định vị bởi tên đường dẫn của nó.

Các quyền kiểm soát truy nhập được lưu trong các danh sách kiểm soát truy nhập, ACL, của các đối tượng, tức là tên một chủ thể và các quyền truy nhập được lưu trong ACL tương ứng của đối tượng. ACL có thể chứa các tên chủ thể, các nhóm chủ thể và các tên chủ thể hoặc các nhóm chủ thể bị từ chối truy nhập. Một chủ thể hoặc nhóm có thể được gộp trong một danh sách bị từ chối truy nhập, ngay cả khi chủ thể nằm trong một nhóm được cấp quyền truy nhập, hoặc nhóm là nhóm con của một nhóm được cấp quyền truy nhập như thế.

Mỗi ACL trên thực tế là một tệp mà tự nó là chủ thể kiểm soát truy nhập và như vậy có ACL riêng của mình. Danh sách tiềm tàng vô hạn các ACL có thể được kết thúc bởi ACL, tác động như ACL riêng của nó.

Xác thực

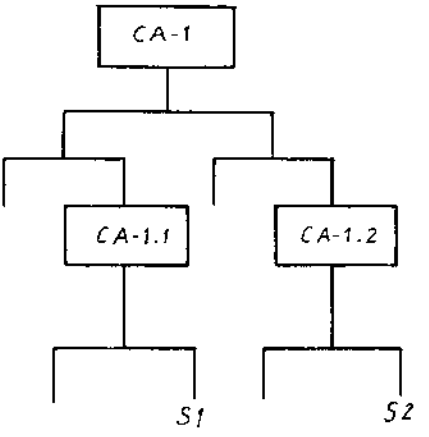
Các chủ thể và các hệ thống có thể xác thực lẫn nhau nhờ sử dụng mật mã khóa công khai và các phương pháp đòi hỏi/đáp ứng. Chủ thể tự định danh đối với hệ thống bằng cách trước hết khai ID người dùng và hệ thống đáp lại bằng một số ngẫu nhiên. Chủ thể mã hóa số ngẫu nhiên bằng khóa mật của nó và trả kết quả về cho hệ thống, hệ thống tìm khóa công khai ứng với ID người

dùng đã khai báo và sử dụng nó để giải mã bản mã trả lời từ chủ thể. Nếu bản đáp ứng đã giải mã tương ứng với số ngẫu nhiên ban đầu thì chủ thể tự nó đã xác thực thành công với hệ thống. Tương tự, người sử dụng có thể nhập vào một hội thoại đòi hỏi/đáp ứng (hỏi/đáp) để xác thực hệ thống. Các thẻ thông minh gài sẵn thuật toán mật mã khóa công khai và các khóa mật đã lưu, cung cấp cho người sử dụng một cơ chế thuận tiện để thực hiện các thủ tục đòi/đáp như vậy.

Khi người sử dụng và hệ thống đã xác thực lẫn nhau, một bên có thể tạo ra một khóa mật mã đối xứng bí mật, mã nó theo khóa công khai của bên kia và gửi nó để sử dụng trong xác thực sau đó, ví dụ cho MAC đã mã.

Có thể đạt được xác thực mà không cần sử dụng mật mã khóa công khai, nếu sử dụng một trung tâm phân phối khóa tin cậy. Mỗi bên đều tin vào trung tâm để phát triển thông tin cho xác thực.

Các cơ quan có quyền chứng nhận (CA) (cơ quan cấp chứng chỉ trong kiến trúc là những hệ thống được tín nhiệm để chứng nhận các khóa công khai, các MAC được dùng để kiểm chứng tính toàn vẹn của phần mềm và một bản sao phần mềm có thể được nạp vào một hệ máy tính riêng. Các thông báo chứng nhận do CA cung cấp giúp cho mỗi hệ thống khỏi phải ghi khóa công khai của tất cả các chủ thể mà dựa vào đó chủ thể định danh. Do đó các CA được ủy thác đảm bảo rằng, một chủ thể tự định danh đúng trước CA khi nó cung cấp khóa công khai của nó. Thông báo chứng thực liên kết ID người dùng và khóa công khai được ký bởi khóa mật của CA.



digital distributed system security architecture: *kiến trúc an toàn hệ thống số phân tán.* Phân cấp của các CA.

Các hệ phân tán có lẽ có một số CA vì không chắc rằng tất cả các chủ thể đều có thể có khả năng kiểm chứng danh tính của chúng và khóa công khai đối với một CA duy nhất. Trong những tình huống đó, sự phân cấp của các CA sẽ tồn tại và thông báo chứng nhận do một CA phát ra có thể kèm theo bởi một thông báo chứng nhận khác chứng nhận khóa công khai của bản thân CA. Quy ước đặt tên nhắc đến ở trên sử dụng sự phân cấp của các thư mục và các chủ thể và các CA có thể gắn với một thư mục riêng. Một CA nằm ở một thư mục riêng sẽ chứng nhận những CA khác nằm sát trên và sát dưới nó trong hệ thống phân cấp. Khi một hệ thống nhận một thông báo chứng nhận từ một hệ thống khác thì đó sẽ là một tập các

D

thông báo chứng nhận kết hợp biểu diễn một đường dẫn ngược lên theo hệ thống phân cấp cho đến tận CA cha chung và sau đó xuôi xuống về phía kia của hệ thống phân cấp tới CA của bên thứ hai.

Ví dụ như, trong hệ thống phân cấp minh họa ở hình minh họa, S1 có thể cung cấp các thông báo chứng nhận do CA-1.1 phát ra cho S1, do CA-1 phát ra cho CA-1.1 và do CA-1.2 phát ra cho CA-1. S2 có thể tin vào những thông báo chứng nhận như vậy bởi vì chúng bao gồm một thông báo chứng nhận từ CA-1.2 được S2 tín nhiệm và một chuỗi thông báo chứng nhận dẫn tới S1.

Các quyền truy nhập được ủy nhiệm

Các chủ thể không truy nhập các đối tượng trực tiếp trong một hệ phân tán, đúng hơn chúng sử dụng các đối tượng trung gian mà chúng tín nhiệm để nhân danh chúng. Tuy nhiên, hệ đối tượng phải tự đảm bảo rằng bên trung gian có sự ủy quyền đại diện cần thiết từ chủ thể khởi đầu và quả thực, bản thân trung gian phải tự đảm bảo về tính xác thực của chủ thể. Sự đảm bảo đó được đưa ra trong cấu trúc bởi các thông báo chứng nhận ủy nhiệm. Ví dụ, những người sử dụng tự xác thực với một trạm làm việc và sau đó, phát ra một thông báo chứng nhận cho trạm làm việc đó. Đến lượt nó trạm làm việc lại có thể tự xác thực đối với máy chủ và sau đó tạo ra thông báo chứng nhận ủy quyền với cùng một yêu cầu truy nhập. Máy chủ kiểm tra yêu cầu truy nhập so với tên người sử dụng trong ACL của tệp cần được truy nhập.

Không có sự đảm bảo rằng, trạm làm việc sẽ không phát ra những yêu cầu sau đó mà không được người sử dụng ủy quyền. Do đó, phải có một cơ chế nào đó để kết thúc thời khoảng ủy quyền. Người sử dụng có thể xóa khóa bí mật đã dùng để ký thông báo chứng nhận ủy quyền, thông tin cho mọi hệ thống rằng, các thông báo chứng nhận được ký bằng khóa đó không còn hiệu lực nữa. Trong bất kỳ trường hợp nào, các thông báo chứng nhận ủy quyền đều phải có một thời hạn nhất định, được xác định bởi một thời gian/ngày tháng kết thúc, nhằm giảm tới tối thiểu mọi thất thoát nảy sinh từ trục trặc hoặc thất thoát của hệ thống.

Một người sử dụng có thể muốn chỉ ủy quyền một tập giới hạn các quyền, ví dụ như truy nhập vào một tập hợp tệp riêng. Một sự hạn chế như thế có thể đạt được tốt nhất bởi những người sử dụng chấp nhận một loạt các ID người sử dụng. Các ID này tương ứng với một tập hợp các quyền cần ủy quyền ở bất kỳ một thời điểm nào. Sau đó, hệ thống đối tượng sẽ kiểm tra đơn giản truy nhập được yêu cầu so với ID người dùng riêng chứa trong thông báo chứng nhận ủy quyền.

Hủy bỏ các quyền truy nhập

Phần lớn các hệ an toàn đều tập trung vào các cơ chế giải quyết việc cấp phát ban đầu hoặc từ chối truy nhập, nhưng sự đảm bảo nào tồn tại với các cơ chế thu hồi những quyền đó? Như vậy, bằng cách nào hệ thống đáp ứng lại các tình huống: rút tên ra khỏi một danh sách truy nhập, một người sử dụng rút ra khỏi một nhóm, một thông báo chứng nhận xác thực hoặc ủy quyền cần rút

ra, hoặc một phiên xác thực không còn hiệu lực nữa.

Hủy bỏ ngay lập tức các quyền là một vấn đề khó khăn vì các hệ giữ các quyền hiện thời trong một bộ nhớ cục bộ và sẽ không thực tiễn nếu thông báo tin cậy và ngay lập tức cho tất cả các hệ rằng, thông tin kiểm soát truy nhập đã thay đổi. Như vậy, một hệ có thể phân tích cú pháp một danh sách kiểm soát truy nhập, mở rộng tất cả các nhóm thành các ID người sử dụng. Nếu một ID người sử dụng được rút ra khỏi một nhóm thì thông tin đó sẽ không ảnh hưởng tới các truy nhập đang trong tiến trình.

Kiến trúc cho phép hủy bỏ chậm chứ không phải ngay lập tức. Các ứng dụng sẽ quyết định khi nào các quyết định hủy bỏ sẽ được thực hiện, ví dụ khi một tệp mở. Tuy nhiên, cần phải thận trọng để đảm bảo rằng các ứng dụng không hoạt động trong những khoảng thời gian dài mà không kiểm tra về những quyết định hủy bỏ (thu hồi). Các thông báo chứng nhận có thể được rút về trước thời điểm hết hạn, do nghi bị thất thoát khóa bí mật, điều quan trọng là, các thông báo chứng nhận chỉ có thể được truy lục từ những kho lưu trữ đáng tin cậy mà sẽ báo cáo về những quyết định thu hồi như vậy.

Sự xác thực không thể thu hồi được; một khi một cặp hệ thống đã xác thực lẫn nhau cho một phiên làm việc thì không có cơ chế nào để rút lại sự xác thực đó. Do vậy, điều quan trọng là các phiên làm việc phải có thời khoảng giới hạn, với những phiên xác thực mới ở những khoảng tương xứng với các quá trình để kiểm tra các nguồn tin cậy đối với thông báo chứng nhận.

Kiểm soát truy nhập bắt buộc

Kiến trúc cho phép kiểm soát truy nhập bắt buộc cũng như tùy ý. Dù cho các hệ thống thương mại sẽ có xu hướng không ép buộc kiểm soát truy nhập bắt buộc, song chúng phải tương thích với các hệ thống chấp nhận những phương pháp đó. Một yêu cầu truy nhập phát đi từ một hệ thống ở xa, buộc tuân theo kiểm soát truy nhập bắt buộc, sẽ được kèm theo một nhãn mà bộ kiểm soát tham chiếu từ xa chỉ ra. Nhãn này tương ứng với lớp truy nhập của chủ thể khởi phát yêu cầu. Ngoài ra, các thông báo chứng nhận chỉ rõ lĩnh vực chính sách và tập hợp các lớp truy nhập của bộ kiểm soát tham chiếu từ xa sẽ được cung cấp. Bộ giám soát cục bộ sẽ chỉ cho phép truy nhập trên cơ sở thông tin được cung cấp. Thông tin này có thể bao gồm những chi tiết liên quan tới mức đảm bảo của bộ kiểm soát tham chiếu từ xa, và lớp truy nhập của đối tượng. Vấn đề hủy bỏ sẽ chặt chẽ hơn trong trường hợp kiểm soát truy nhập bắt buộc vì mọi sự thay đổi ở các thuộc tính kiểm soát truy nhập bắt buộc đều phải có ảnh hưởng ngay lập tức. *Xem* access control list, certificate, certification authority, challenge/response, directory, discretionary access control, key distribution center, label, mandatory access control, message authentication code, object, public key cryptography reference monitor, secure channel, subject, symmetric cipher.

digital enveloping ***bọc gói số*** Trong mật mã, phương pháp trong đó mọi

người đều có thể niêm phong một thông báo theo một cách sao cho chỉ có người nhận nhằm tới mới có thể mở thông báo đã niêm phong. Thông thường, người gửi chọn một khóa đối xứng bí mật ngẫu nhiên và sử dụng nó để khóa mã thông báo. Sau đó bản thân khóa đối xứng được mã hóa bằng khóa công khai của người nhận, khóa đã mã hóa và thông báo đã mã hóa sau đó được truyền đi. *Xem* public key, symmetric key system.

digital keyad ***vùng phím số*** Trong an toàn vật lý, vùng phím với các phím bấm số dùng để nhập thông tin kiểm soát truy nhập đối với đối tượng vào hoặc ra khỏi một vùng được kiểm soát. Các thủ tục kiểm soát truy nhập có thể đòi hỏi nhập một mã thích hợp trong một khoảng thời gian xác định sau khi nhấn phím đầu tiên. Hệ thống có thể bao gồm những tín hiệu bắt buộc và hệ thống sẽ khóa nếu nhập các mã không đúng. Vùng phím số cũng có thể được dùng cùng với một bộ đọc thẻ. *Xem* card reader, duress alarm.

digital multiplex switching system ***hệ chuyển mạch dồn kênh số, DMS*** Ở truyền thông dữ liệu, sự sử dụng các hệ điều biến mã xung và dồn kênh phân thời qua các tuyến chuyển mạch. *Xem* circuit switching, PCM, TDM.

digital signal ***tín hiệu số*** Tín hiệu điện rời rạc hoặc không liên tục, mà những trạng thái khác nhau của nó đều ở những khoảng gián đoạn nhau. *So sánh với* analog signal.

digital signalling ***báo hiệu số*** Trong truyền thông dữ liệu, sự sử dụng kênh truyền số để thiết lập, điều khiển và hủy các cuộc gọi. *Xem* signalling.

digital signature ***chữ ký số*** (1) Trong xác thực, dữ liệu gắn vào, hoặc là một phép biến đổi mật mã của đơn vị dữ liệu mà cho phép nơi nhận đơn vị dữ liệu chứng minh nguồn và tính toàn vẹn của đơn vị dữ liệu và bảo vệ chống lại sự làm giả, ví dụ bởi nơi nhận. (2) Trong xác thực, khối dữ liệu gắn vào một thông báo, hoặc thông báo mã đầy đủ, sao cho người nhận có thể xác nhận nội dung thông báo và/hoặc chứng minh rằng, nó chỉ có thể bắt nguồn từ người gửi có chủ đích.

Tổng quan

Chữ ký số là hàm số của

- thông báo, giao dịch hoặc tài liệu cần ký;
- thông tin bí mật chỉ người gửi biết được;
- thông tin công khai dùng trong quá trình phê chuẩn;
- các mã xác thực thông báo cho phép người nhận thông báo đảm bảo rằng, nội dung không thể bị thay đổi ngẫu nhiên hoặc có suy tính bởi bên thứ ba. Tuy nhiên, vì cả người gửi lẫn người nhận đều dùng chung cùng thông tin bí mật nên không có phương pháp giải quyết các tranh chấp. Người nhận có thể tính toán dấu xác thực và do đó có thể thay đổi thông báo hoặc giả mạo thông báo mới, phát triển dấu xác thực và quả quyết rằng nó đã được truyền đi bởi người gửi dùng chung cùng khóa bí mật để xác thực. Ngược lại, người gửi có thể từ chối thông báo đã xác thực và quả quyết rằng người nhận đã tạo

ra thông báo giả mạo bằng cách sử dụng khóa bí mật chung.

Thực chất của chữ ký số là để người nhận phải có khả năng chứng minh rằng thông báo khởi phát từ người gửi nào đó, nhưng lại không có khả năng xây dựng thông báo có chữ ký. Như vậy, người gửi cần thông tin bí mật để xây dựng thông báo có chữ ký, còn người nhận phải có khả năng truy nhập thông tin công khai để dùng trong phê chuẩn tính hợp lệ của thông báo. Trong trường hợp tranh chấp, người nhận phải có khả năng cung cấp thông tin không bí mật cho trọng tài (tức là thông báo có chữ ký và thông tin sẵn có công khai) để chứng minh sự xác thực và nguồn gốc thông báo.

Các chữ ký số có thể được phân loại rộng rãi như chữ ký số đa năng và chữ ký số trọng tài. Các chữ ký số đa năng có thể được phê chuẩn bởi bất kỳ người nào có truy nhập tới các tham số phê chuẩn có sẵn công khai, trong khi các chữ ký trọng tài đòi hỏi các dịch vụ của một trọng tài được tín nhiệm, người ký thông báo cho nơi gửi và phê chuẩn nó cho nơi nhận.

Chữ ký đa năng - mật mã không đối xứng

Các chữ ký đa năng có thể được cung cấp cùng với:

- mật mã khóa công khai;
- các thuật toán thông thường và các mã pháp đối xứng hoạt động theo cách cung cấp có hiệu quả các phương tiện mật mã khóa công khai.

RSA cung cấp một phương pháp cực kỳ tao nhã và hiệu quả để tạo ra các chữ ký số. Các đặc điểm cơ bản của phương pháp này là thông báo ban đầu được mã hóa bằng khóa riêng của người gửi và người nhận thu được thông báo ban đầu bằng cách giải mã thông báo đã ký bằng khóa công khai của người gửi. Như vậy

Người gửi khai triển

$C = ek_S(M)$

Người nhận tạo ra

$M^R = dk_P(C)$

$= dk_P\ (ek_S(M)) = M$

Trong đó k_P là khóa công khai của người gửi, còn k_S là khoá riêng của người gửi.

Trong cách sử dụng RSA thông thường, thông báo rõ (thông báo gốc) được mở ra bằng phép giải mã bằng khóa riêng đối với bản mã được mã trước đó bằng khóa công khai của người nhận, tức là:

$M = dk_s(ek_P(M))$

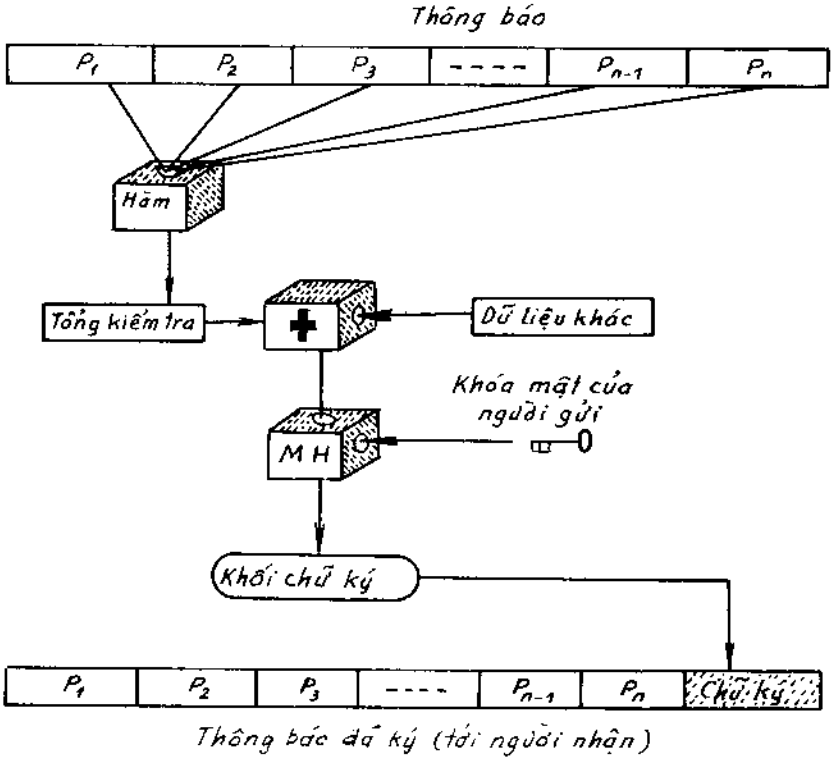
Bản chất của RSA cho phép hai phép mã hóa và giải mã được đảo ngược, theo các khóa đã dùng và vẫn tạo ra thông báo ban đầu. Sở dĩ như vậy là vì cả hai thao tác đều liên quan tới phép mã hóa. Nơi nhận thông báo đã ký được đảm bảo rằng, thông báo được bắt nguồn từ người gửi chủ định và chỉ có người gửi mới truy nhập được khóa bí mật k_S.

Tuy nhiên, cần có một số biện pháp phòng ngừa bổ sung trong thực hiện phương pháp chữ ký số đó. Trước hết, thông báo phải có độ dư thừa, thứ hai, nó phải bảo vệ chống lại sự sắp xếp lại dãy các khối thông báo và thứ ba, cần có mã hóa bổ sung để đảm bảo độ mật. Thực chất vấn đề của người nhận là chỉ có người gửi có thể khởi phát một

thông báo, nghĩa là không có bên thứ ba có thể tạo ra bản mã (mà có thể được biến đổi thành thông báo có nghĩa nhờ phép giải mã bằng khóa công khai của người gửi).

ký, hoặc được ký riêng rẽ và gắn thêm vào như một chữ ký.

Nếu một thông báo đầy đủ được ký, thì một sự tấn công vẫn có thể xảy ra bằng



digital signature: *chữ ký số.*

Việc yêu cầu bản gốc nhận được phải có nghĩa ngụ ý là nó chứa một độ dư thừa cao. Nếu trạng thái tự nhiên của thông báo chứa một mức dư thừa thấp, ví dụ như một tập hợp ngẫu nhiên của các bit tạo ra bởi một công cụ giám sát, thì phải sử dụng một dấu xác thực. Dấu xác thực có thể được gộp vào như một phần không tách rời của thông báo đã

cách sắp thứ tự lại các khối RSA thành phần. Sự sắp xếp lại như vậy vẫn có thể tạo ra một thông báo có ý nghĩa có vẻ như được ký bởi người gửi. Một sự tấn công như vậy có thể được ngăn cản bằng cách gộp thêm một số thứ tự trong mỗi khối, hoặc nhờ sử dụng một dấu xác thực nhạy với thứ tự các thành phần thông báo.

Một phương pháp thay thế là tạo ra "khối chữ ký" ngắn hơn nhờ sử dụng hàm băm, hoặc hàm tóm lược thông báo. Nó có tính chất là không thể thực hiện được về mặt tính toán để xác định một thông báo thứ hai có cùng bản tóm lược thông báo như của thông báo gốc. Bản tóm lược thông báo cần có độ dài để có thể được tính toán như một khối đơn trong RSA. Sau đó bản tóm lược thông báo được ký bởi khóa mật của người gửi và gắn vào thông báo gốc để truyền đi.

Trong trường hợp này Alice:

- đặt hàm tóm lược thông báo H lên thông báo ban đầu M, tạo ra bản tóm lược thông báo $H(M)$;
- mã hóa $H(M)$ bằng khóa RSA bí mật để tạo ra khối chữ ký $ek_s(H(M))$;
- truyền M, $ek_s(H(M))$ và thông tin định danh của Alice để máy thu chọn khóa công khai của Alice, Alice có thể lần lượt gắn một thông báo chứng nhận của khóa công khai;
- Bob đầu tiên tính toán bản tóm lược thông báo của thông báo nhận được M^k, tức là $H(M^k)$;
- Sau đó Bob truy lục khóa công khai k_p của Alice, tính toán $dk_p(ek_s(H(M)))$ và so sánh kết quả với $H(M^k)$;
- nếu chúng bằng nhau thì Bob chấp nhận thông báo nhưng vẫn giữ lại nó cùng với khối chữ ký và thông tin định danh của Alice, hoặc thông báo chứng nhận, trong trường hợp cần sự phán xét để phân xử tranh chấp về sau.

Thông báo được ký bằng khóa RSA mật có thể được biến đổi thành bản gốc với khóa công khai tương ứng. Do đó, những thông báo như thế có thể phát hiện bởi một kẻ tấn công. Nếu cần sự bí mật của thông báo đã ký thì phải có hai thao tác mật mã ở cả đầu gửi lẫn đầu thu. Nếu thông báo (M) được Alice ký và được mã hóa để truyền an toàn cho Bob, thì thông báo truyền đi (C) được tạo ra bởi:

$C = ek_{pB}(ek_{sA}(M))$,

Trong đó k_{pB} là khóa công khai của Bob còn k_{sA} là khóa riêng của Alice.

Như vậy thông báo được mã hóa bằng khóa bí mật của Alice và sau đó mã hóa lại bằng khóa công khai của Bob. Các thao tác đảo ngược được thực hiện bởi Bob.

Như vậy

$M = dk_{pA}(dk_{sB}(ek_{pB}(ek_{sA}(M))))$

Thông báo mật mã đã ký đầu tiên được tạo ra nhờ phép mã hóa bằng khóa mật của Alice và sau đó mã hóa bằng khóa công khai của Bob; thông báo gốc ban đầu sau đó được mở ra nhờ giải mã bằng khóa công khai của Alice và giải mã bằng khóa mật của Bob. Kỹ thuật này có thể dẫn tới những phức tạp vì phép lấy modun tương ứng với hai tập khóa sẽ khác nhau. Nếu thông báo đầu tiên được mã hóa theo modun cao hơn thì sẽ phải nhóm lại khối bản mật mã cho phép mã thứ hai sau đó. Nếu quá trình ký và mã hóa được đảo ngược để tránh vấn đề này thì việc đánh giá phải đương đầu với một thủ tục phức tạp hơn trong kiểm tra chữ ký.

Nếu khối chữ ký được gắn thêm vào bản gốc thì thông báo gốc này có thể được mã hóa bằng khóa công khai của

người nhận để bảo vệ tính bí mật của nó.

Một phương pháp thay thế cho việc sử dụng thuật toán RSA đã được đề xuất và trong trường hợp này là thuật toán ElGamal.

Các mã pháp ba lô (knapsack) không cung cấp cùng các phương tiện cho chữ ký số như RSA vì chúng làm mở rộng thông báo trong quá trình mã. Điều này có nghĩa là sự mã hóa bằng các mã pháp ba lô không phải là một song ánh và như vậy phép mã và giải mã không thể đảo ngược được đối với các thao tác ký. Một dạng mật mã ba lô đã sửa đổi dành cho những ứng dụng chữ ký số đã được Shamir đề xuất. Cả Rabin lẫn Lamport-Diffie đều đã đề xuất các phương pháp chữ ký số liên quan tới các khóa công khai bằng các thuật toán thông thường, nhưng những phương pháp này làm giãn thông báo đáng kể, một số lớn khóa công khai và cả các khóa phải được thay đổi với mỗi chữ ký. Bởi thế chúng liên quan tới các tổng phí chủ yếu ở các phương tiện đăng ký công khai và truyền thông.

Tính xác thực của một đăng ký khóa công khai là thiết yếu trong các ứng dụng chữ ký số. Nếu một kẻ tấn công có thể thay thế khóa công khai của Alice bằng một khóa của riêng anh ta thì Bob có thể bị thuyết phục chấp nhận các thông báo do kẻ tấn công tạo ra mà dường như do Alice ký. Tương tự, Alice có thể không thừa nhận các thông báo bằng cách cho là khóa của Alice đã bị đánh cắp và được sử dụng để làm giả thông báo. Các thông bảo chứng nhận có thể được sử dụng để khắc phục vấn đề này, nhưng vẫn cần có một hệ thống nào đó thông báo cho người sử dụng về việc thu hồi các thông báo chứng nhận và sự thất thoát có thể khóa bí mật dùng để ký các thông báo chứng nhận.

Chữ ký vạn năng - mật mã đối xứng

Mật mã đối xứng không thích hợp cho các chữ ký số vì người gửi và người nhận dùng cùng một khóa. Tuy nhiên, có thể thực hiện các mã pháp đối xứng để tạo ra các khóa chỉ mã hóa và khóa chỉ giải mã. Thực chất của phương pháp này là phương tiện mật mã trong đó, một khóa chủ, hoặc một khóa trao đổi, được lưu giữ trong một bộ nhớ modun chống làm giả. Các thông báo giữa người gửi và người nhận được mã hóa bằng một khóa dữ liệu, nhưng những người sử dụng chỉ truy nhập vào khóa dữ liệu khi nó được mã hóa bằng khóa mã hóa khóa. Nếu sử dụng các kỹ thuật tương tự với công chứng khóa, có thể đảm bảo rằng, người gửi được cung cấp một phương tiện mã hóa duy nhất, đối với một người nhận riêng, trong khi người nhận có thể giải mã nhưng không mã hóa được những thông báo nhận được như thế. Điều này tương tự với một hệ thống các khóa công khai và khóa riêng; tuy nhiên, những người sử dụng hệ thống này bị hạn chế chỉ truy nhập vào phương tiện mật mã cần thiết chứa các khóa trao đổi đối với những cặp người sử dụng riêng.

Chữ ký trọng tài

Các chữ ký trọng tài có thể được thực hiện bằng các mã pháp đối xứng, như DES, và bao hàm có hiệu quả một thông báo xác thực từ một người gửi cho

trọng tài, và thông báo xác thực riêng từ trọng tài tới người nhận. Mỗi người sử dụng dùng chung một khóa mật riêng với trọng tài nhưng người nhận và người gửi không biết về những khóa mật của nhau. Trong một hệ chữ ký trọng tài điển hình, người gửi, Alice, dùng chung một khóa mật (k_A) với trọng tài. Người gửi muốn gửi một thông báo đã ký của văn bản (I) cho Bob và đó sẽ là thông báo thứ i trong dãy. Người gửi lập một thông báo (ID_A, ID_B, i, I) mã hóa nó theo k_A và gắn dấu xác thực (AC), là hàm của k_A lên nó.

Thông báo tổng đó, kèm theo ký hiệu nhận dạng ID_A của Alice ở dạng rõ, được gửi tiếp cho trọng tài. Ký hiệu nhận dạng ID_A cho phép trọng tài lựa chọn khóa k_A từ một bộ nhớ an toàn; sau đó thông báo được giải mã bằng khóa này, ký hiệu nhận dạng ID_A được trích từ thông báo đã mã hóa và được so sánh với giá trị ở dạng rõ nhắc đến ở trên. Nếu chúng không bằng nhau thì người gửi chủ định được thông báo và thủ tục dừng lại. Nếu không thì dấu xác thực được kiểm tra và trọng tài lập một tử mã cho xác thực hoặc không xác thực tùy thuộc vào kết quả. Trọng tài sau đó khai triển một thông báo gồm (ID_A, ID_B, i, T, AC) cộng với từ mã để "xác thực" hoặc "không xác thực". Ký hiệu nhận dạng ID_B của Bob sau đó được trọng tài dùng để chọn khóa bí mật k_B của Bob từ bộ nhớ. Trọng tài mã hóa thông báo theo khóa này, gắn thêm một dấu xác nhận cũng được tạo thành nhờ sử dụng k_B và thông báo kết quả được chuyển tiếp cho Bob.

Bob giải mã thông báo, kiểm tra xem nó có chứa từ mã để "xác thực" và dấu xác thực của trọng tài có phù hợp với thông báo và thuật toán xác thực không. Bob cũng giữ lại dấu xác thực (AC) và bản thông báo nhận được để làm bằng chứng trong tranh chấp. Việc xét đoán có thể đòi hỏi trọng tài phải tính toán dấu xác thực của thông báo bằng khóa k_A và so sánh kết quả với AC. Bob không thể tính được AC vì nó liên quan tới sự hiểu biết khóa bí mật k_A.

Phương pháp chữ ký trọng tài có thể được dùng với các mã pháp đối xứng truyền thống và không đòi hỏi một phương tiện mật mã đặc biệt với các khóa chủ đã lưu. Mặt khác, nó không yêu cầu các dịch vụ về trọng tài được tín nhiệm; vì thế nó thích hợp hơn cho những người sử dụng trong một hiệp hội có liên kết chặt chẽ.

Hệ thống mật khẩu động cũng có thể được dùng để ký một thông báo. Ở đây, thông báo đầu tiên được xử lý thành một tổng kiểm tra mà có thể là MAC. Tổng kiểm tra này được đưa vào như một yêu cầu bảy chữ số vào một thiết bị cầm tay đặc biệt để tạo ra một đáp ứng; điều này tương đương với chữ ký và được gửi đi cùng với thông báo. Thiết bị cầm tay chứa khóa bí mật chỉ được biết bên trong một mạng máy tính cụ thể; do đó mạng có khả năng khẳng định tính xác thực của chữ ký. Việc sử dụng các chữ ký điện tử tự động trong các sơ đồ quản lý tiền mặt ở ngân hàng có thể có tiềm năng tiết kiệm được khá nhiều tổng phí văn phòng gián tiếp trong việc kiểm tra các chữ ký viết tay

ở văn phòng. *Xem* arbitrated signature, authenticator, back office, certificate, DES, DSS, dynamic password, electronic signature, ElGamal digital signature, interchange key, key encrypting key, key notarization, knapsack cipher, Lamport-Diffie signature, MAC, message authentication, modulo arithmetic, public key cryptography, Rabin signature, RSA, tamper resistant module, universal signature.

digital signature standard ***chuẩn chữ ký số*** Trong mật mã, chuẩn về chữ ký số do NIST đề xuất.

Trong chuẩn này một số tham số được định nghĩa:

- p = một modun nguyên tố sao cho $2^{511} < p < 2^{512}$;
- q = ước nguyên tố của $p - 1$; trong đó $2^{159} < q < 2^{160}$;
- $g = h^{(p-1)/q} \bmod p$, trong đó h là một số nguyên bất kỳ với $0 < h < p$ sao cho $h^{(p-1)/q} \bmod p > 1$;
- x = một số nguyên sao cho $0 < x < q$;
- $y = g^x \bmod p$;
- m = thông báo cần ký và truyền đi;
- k = số nguyên ngẫu nhiên sao cho $0 < k < q$;
- H = hàm băm một chiều

Các tham số có thể được nhóm lại:

- p, q và g được biết công khai và chung cho một nhóm người sử dụng;
- x và k là bí mật đối với người ký thông báo và k phải được thay đổi đối với mỗi thông báo;
- y là khóa công khai của người ký;
- H không được định nghĩa trong tiêu chuẩn nhưng nó phải không thể tính được về mặt tính toán để tạo ra một thông báo tương ứng với một hàm băm đã cho, hoặc để tìm hai thông báo với cùng hàm băm.

Khi người gửi muốn ký thông báo m thì một số ngẫu nhiên k được chọn và người gửi tính:

- $r = (g^k \bmod p) \bmod q$;
- $s = (k^{-1} (H(m)) + xr)) \bmod q$.

Chữ ký bao gồm r và s, được truyền theo thông báo m.

Người nhận thông báo sẽ nhận được m', s' và r' và muốn xác nhận rằng, s' và r' biểu diễn một chữ ký hợp lệ cho thông báo đã nhận m'. Các kiểm tra được tiến hành là:

- $0 < r' < q$ và $0 < s' < q$, nếu một trong những phép thử đó không đúng thì chữ ký không hợp lệ và thông báo bị loại bỏ, nếu không thì những kiểm tra sau đây được thực hiện:
- $w = (s')^{-1} \bmod q$ được tính toán;
- $u1 = ((H(m'))w) \bmod q$ được tính toán;
- $u2 = ((r')w) \bmod q$ được tính toán;
- $v = (((g)^{u1} (y)^{u2}) \bmod q) \bmod q$ được tính toán;
- nếu $v = r'$ thì khối chữ ký có thể được chấp nhận với một mức tin cậy cao.

Xem digital signature, ElGamal digital signature.

digital switching ***chuyển mạch số*** Trong truyền thông, quá trình thiết lập các đường nối bằng các thao tác trên các tín hiệu số mà không cần đầu tiên biến đổi chúng thành các tín hiệu tương tự. *Xem* digital signal.

digital transmission system ***hệ truyền số*** Trong truyền thông dữ liệu, mạng trong đó thông tin tương tự được

số hóa thông qua kỹ thuật điều biến và truyền dưới dạng rời rạc như một chuỗi xung. Ở trạm thu, dữ liệu tương tự được khôi phục từ các tín hiệu đã số hóa. Các hệ truyền số hỗ trợ tốc độ dữ liệu cao, phát hiện lỗi và giảm đến tối thiểu các hiệu ứng do tiếng ồn.

DIN ***tiêu chuẩn DIN*** Viết tắt của Deutsch Industrie Norm (tiêu chuẩn công nghiệp Đức); tổ chức tiêu chuẩn hóa của Đức. *Xem* Association Française de Normalisation, British Standards Institution.

diplex operation ***vận hành song tín, vận hành song lộ*** Trong truyền thông, việc sử dụng một mạch đơn, sóng mang hoặc anten để truyền đồng thời hoặc thu đồng thời hai tín hiệu. *So sánh với* full duplex. *Xem* carrier.

direct access ***truy nhập trực tiếp*** Trong an toàn cơ sở dữ liệu, một dạng hiểm họa trong đó người sử dụng yêu cầu thông tin ở một mức phân loại an toàn cao hơn so với mức của người sử dụng và hệ thống cung cấp thông tin đó. *So sánh với* indirect access, Trojan Horse direct release, Trojan Horse leakage.

direct data access arrangement ***thiết bị truy nhập dữ liệu trực tiếp*** Trong truyền thông dữ liệu, thiết bị gồm biến áp cách ly để nối thông thiết bị người dùng với mạng điện thoại. Nó được thiết kế để ngăn ngừa các điện áp hoặc tín hiệu có hại đi vào mạng.

direct debit ***ghi nợ trực tiếp*** *Đồng nghĩa với* debit transfer.

directly connected transaction ***giao dịch nối trực tiếp, giao tác nối trực tiếp*** Trong hoạt động ngân hàng, giao tác được đặc trưng bằng điều kiện là nơi phát hành thẻ (hoặc đại lý của nơi đó) mà nơi nhận thẻ liên lạc với có sự hiểu biết đầy đủ về thẻ của người giữ thẻ và do đó có khả năng tạo dựng khóa thẻ. *So sánh với* indirectly connected transaction. *Xem* acquirer, card holder, card issuer, card key, key management.

direct memory access ***truy nhập bộ nhớ trực tiếp, kỹ thuật DMA*** Ở các hệ thống nhớ, kỹ thuật cho phép thiết bị ngoại vi truy nhập trực tiếp bộ nhớ chính của máy tính. Khi thiết bị ngoại vi bắt đầu truy nhập bộ nhớ trực tiếp thì bộ xử lý bị buộc dừng toàn bộ hoạt động bus trong khi thiết bị ngoại vi chiếm dụng bus. Phương pháp này cho phép tốc độ chuyển dữ liệu cực kỳ cao. *So sánh với* cycle stealing. *Xem* bus, main memory, processor.

directory ***thư mục*** (1) Trong lập trình, bản ghi chứa các chi tiết về vị trí của tệp chứa trong bộ nhớ dự phòng, mà được truy nhập bởi hệ điều hành. *Xem* file, operating system, record. (2) Trong các cơ sở dữ liệu, tệp lưu giữ các quan hệ giữa các bản ghi ở những tệp khác. Thư mục chứa mô tả chung về dữ liệu đã lưu giữ và vì nó chiếm không gian nhớ ít hơn các tệp dữ liệu nên các tìm kiếm và thao tác thực hiện ở thư mục có hiệu quả hơn nhiều so với các tìm kiếm và thao tác thực hiện ở bản thân các tệp dữ liệu. *So sánh với* data dictionary, tree structured directory. (3) Trong truyền thông dữ liệu, bảng chứa thông tin định tuyến. *Xem* directory routing.

directory routing ***định tuyến theo thư mục*** Trong truyền thông dữ liệu, phương pháp định tuyến sử dụng một thư mục ở mỗi nút. Thư mục chứa các chỉ tiết về đường nối ra ưu tiên, và có thể ưu tiên thứ hai, cho mỗi nơi nhận. *So sánh với* adaptive routing, centralized adaptive routing, delta routing, fixed routing, hot patato routing. *Xem* routing.

Dir-Vir ***virut Dir-Vir*** Trong an toàn máy tính, virut lấy lén vốn kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

DIS ***tiêu chuẩn DIS*** Viết tắt của Draft International Standard (tiêu chuẩn dự thảo quốc tế của ISO). *Xem* ISO.

dissasembler ***bộ hợp dịch ngược*** (1) Trong lập trình, chương trình nhận chương trình mã máy như đầu vào và tạo ra một chương trình hợp ngữ tương ứng (ví dụ, với mọi mã phép toán được thay thế bằng những ký hiệu dễ nhớ của chúng). Điều này cung cấp cho người sử dụng danh sách tương đương của chương trình mã máy dễ đọc và dễ chẩn đoán hơn nhiều. *Xem* assembly language machine code, mnemonic, operation code. (2) Trong truyền thông dữ liệu, thiết bị trích ra nội dung thông báo từ các gói tin. *Xem* packet assembler/ disassembler, packet switching.

disaster plan ***kế hoạch phòng sự cố*** *Xem* contingency plans, disaster recovery plan.

disaster planning ***lập kế hoạch phòng sự cố*** Trong quản lý rủi ro, việc lập kế hoạch cho một biến cố bất kỳ gây đổ vỡ đáng kể đối với các hoạt động, do đó đe dọa sự sống còn của doanh nghiệp. *Xem* business resumption planning, disaster recovery plan.

disaster recovery manual ***sổ hướng dẫn khôi phục sau sự cố*** Trong an toàn máy tính, hệ tài liệu về kế hoạch khôi phục sau sự cố, bao gồm mô tả các hoạt động cần phải thực hiện, với các tài liệu hỗ trợ và danh sách kiểm tra. *Xem* disaster recovery plan.

disaster recovery plan ***kế hoạch khôi phục sau sự cố*** Trong an toàn máy tính, dãy các biến cố theo kế hoạch cho phép khôi phục một thiết bị máy tính và/hoặc những ứng dụng đã xử lý ở đó. *Xem* contingency plans.

disclosing ***tiết lộ*** Trong pháp lý, theo định nghĩa bởi Luật bảo hộ dữ liệu Anh năm 1984, chỉ sự tiết lộ đối với dữ liệu và bao hàm sự tiết lộ thông tin trích từ dữ liệu đó; và nơi mà danh tính của cá nhân là đối tượng của dữ liệu cá nhân, phụ thuộc một phần vào thông tin cấu thành dữ liệu và một phần vào thông tin khác thuộc quyền sở hữu của người dùng dữ liệu thì dữ liệu không được xem như bị tiết lộ hoặc chuyển giao, trừ phi thông tin kia cũng bị tiết lộ hoặc chuyển giao. *Xem* data, data protection, personal data.

disclosure ***(sự) để lộ, (sự) làm lộ*** Trong an toàn dữ liệu, sự thu nhận thông tin một cách không chính đáng. *Xem* masquerading.

disclosure risk ***rủi ro tiết lộ*** Trong an toàn dữ liệu, rủi ro làm cho thông

tin liên quan tới một cá thể có thể được suy ra bằng những câu truy vấn ở một cơ sở dữ liệu thống kê. *Xem* inference control, statistical database.

disconnect service message ***thông báo dịch vụ ngắt*** Trong quản lý khóa, thông báo tùy chọn để ngắt các khóa. *Xem* ANSI X9.17 - 1985.

discrepancy reports ***báo cáo về sai lệch, báo cáo về không nhất quán*** Trong xử lý dữ liệu, danh sách các mục mà đã vi phạm sự điều khiển thăm dò nào đó và cần nghiên cứu tiếp.

discrete Fourier transform scrambler ***bộ xáo trộn dùng phép biến đổi Fourier rời rạc*** Trong an toàn truyền thông, kỹ thuật xáo trộn tiếng nói trong đó tín hiệu tiếng nói được số hóa và tách thành các khung. Các tín hiệu đối với mỗi khung được biến đổi Fourier rời rạc và các thành phần miền tần số tạo thành được hoán vị. Tín hiệu nhận được sau đó được biến đổi Fourier ngược và được truyền đi. *So sánh với* two-dimensional scrambler. *Xem* voice scrambling. *Đồng nghĩa với* DFT scrambler.

discrete logarithm problem ***bài toán loga rời rạc*** Trong mật mã, bài toán phát biểu rằng, một cặp số nguyên g, s thuộc trường Galois $GF(N)$, trong đó N là số nguyên tố; cần xác định một số nguyên dương x $(0 \leq x \leq N)$ sao cho: $x = \log_g s \pmod N$. *Xem* Galois field.

discretionary access control ***kiểm soát truy nhập tùy ý, phương thức DAC*** Trong kiểm soát truy nhập, phương thức hạn chế truy nhập tới các đối tượng dựa trên mã định danh của các chủ thể và/hoặc các nhóm mà các chủ thể thuộc vào. Các kiểm soát là tùy ý theo nghĩa là một chủ thể với một sự cho phép truy nhập nào đó, có khả năng chuyển sự cho phép đó (có thể gián tiếp) cho một chủ thể khác nào đó. *So sánh với* mandatory access control. *Xem* object, subject.

discretionary processing ***xử lý tùy ý*** Trong an toàn máy tính, các hoạt động mà có thể bị ngắt trong một khoảng thời gian nào đó. Sự mất khả năng xử lý những ứng dụng như vậy trong một khoảng thời gian nào đó sẽ không ảnh hưởng nghiêm trọng tới trạng thái lành mạnh của tổ chức. *So sánh với* critical processing.

discretionary protection ***bảo vệ tùy ý*** Sự kiểm soát truy nhập nhận dạng những người sử dụng riêng lẻ và nhu cầu cần biết của họ và giới hạn những người sử dụng ở thông tin mà họ được phép xem. Sự kiểm soát này được dùng ở các hệ xử lý thông tin có cùng mức nhạy cảm. *So sánh với* discretionary security. *Xem* discretionary access control, need-to-know.

discretionary security ***an toàn tùy ý*** 1. Trong an toàn máy tính, các biện pháp an toàn khởi đầu bởi bản thân các thực thể. 2. Trong an toàn máy tính, các khía cạnh của chính sách an toàn bao gồm việc cung cấp các dịch vụ an toàn như kết quả của một yêu cầu của thực thể cần một nấc truyền thông. *So sánh với* mandatory security, non-discretionary security.

discretionary security policy ***chính sách an toàn tùy ý*** Trong kiểm soát

truy nhập, chính sách kiểm soát truy nhập trong đó người quản trị hệ thống, hoặc một người được ủy quyền nào đó khác, ví dụ như người sở hữu dữ liệu, có thể ra những quyết định tùy ý theo đó những người sử dụng có thể thực hiện những chế độ truy nhập riêng đối với một tập dữ liệu nào đó. *So sánh với* mandatory security policy. *Xem* data owner, discretionary security.

disgruntled employee ***nhân viên bất bình*** *Xem* security threats.

dishonest employee ***nhân viên không trung thực*** *Xem* security threats.

disjoint ***rời ra, tách ra*** không có các vùng chung.

disk crash ***sự cố đĩa*** (1). Ở các hệ thống nhớ, đầu đọc/ghi tạo ra tiếp xúc phá hủy bề mặt đĩa cứng. (2) Ở các hệ thống nhớ, trục trặc phần cứng hoặc phần mềm bất kỳ khiến không thể truy nhập dữ liệu đĩa. *Xem* hard disk, magnetic disk.

disk drive ***ổ đĩa*** Ở các hệ thống nhớ, cơ cấu để quay chồng đĩa hoặc đĩa từ và điều khiển chuyển động của chúng. *Xem* disk pack, hard disk.

diskette ***đĩa mềm*** *Đồng nghĩa với* floppy disk.

Disk killer ***virut Disk killer, virut kẻ phá đĩa*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động đĩa mềm và đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu, định dạng hoặc ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

disk pack ***bộ đĩa, chồng đĩa*** Ở các hệ thống nhớ, tập hợp các đĩa trên trục chung, được xử lý như một đơn vị duy nhất.

disk server ***hệ đĩa chủ, hệ đĩa secvơ*** Trong tin học, hệ đĩa cứng tạo ra bộ nhớ dự phòng cho một số người sử dụng máy vi tính trong mạng. *xem* file server.

dissemination ***phổ biến*** *Xem* special markings.

distortion ***méo*** Trong truyền thông dữ liệu, sự thay đổi không mong muốn bất kỳ trong tín hiệu. Các nguồn gây méo dạng sóng là quan hệ phi tuyến giữa đầu vào và đầu ra, sự truyền không đều ở những tần số khác nhau; và sự dịch pha không tỷ lệ với tần số. *Xem* intermodulation distortion.

distributed adaptive routing ***định tuyến thích ứng phân tán*** Trong truyền thông dữ liệu, phương pháp định tuyến trong đó các quyết định được đưa ra trên cơ sở trao đổi thông tin giữa các nút mạng. *Xem* adaptive routing.

distributed database ***cơ sở dữ liệu phân tán*** Trong các cơ sở dữ liệu, cơ sở dữ liệu được đặt trên một số máy tính khác nhau mà thường nằm ở các vị trí địa lý khác nhau. Cơ sở dữ liệu có thể được thiết kế như thực thể duy nhất (ví dụ để phục vụ các chi nhánh của một tổ chức lớn) hoặc nó có thể sinh ra do hợp nhất một số hệ riêng ban đầu.

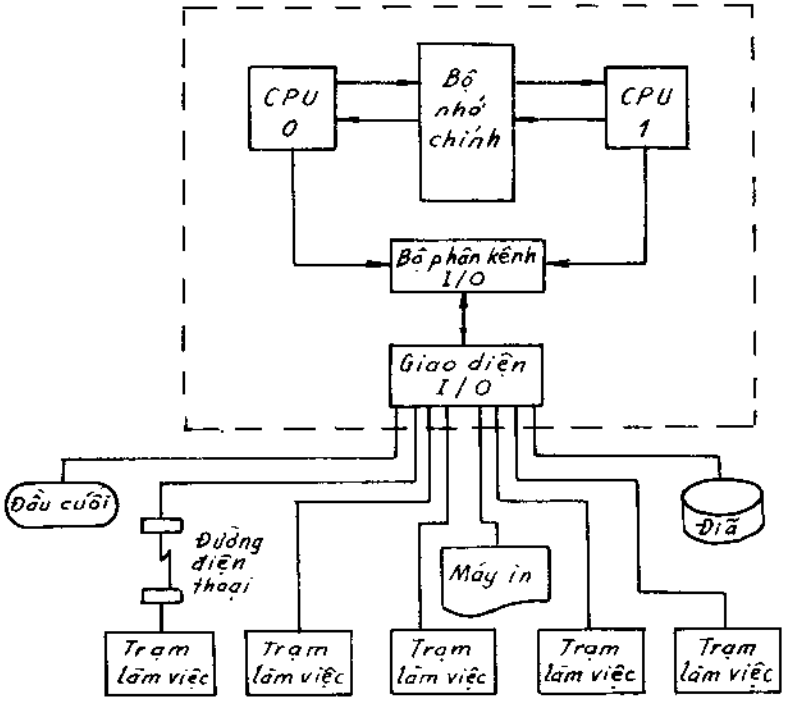
distributed data processing ***xử lý dữ liệu phân tán*** (1) Trong truyền thông dữ liệu, sự phân phối các chức năng xử

lý và dữ liệu, trong một tổ chức tới các vị trí cần chúng. *Xem* cooperative processing, end-user computing, System Network Architecture. *Đồng nghĩa với* distributed processing. (2) Trong tin học, tập hợp các quá trình nối thông với nhau để phân tán tài nguyên và tạo ra môi trường thực hiện các chương trình ứng dụng. *Xem* application program, distributed network, processor.

distributed function ***chức năng phân tán*** Trong truyền thông dữ liệu, việc sử dụng các terminal khả lập trình và những thiết bị khác để thực hiện các thao tác mà trước đó do bộ xử lý trung tâm thực hiện (ví dụ, quản lý mạng và tạo khuôn dữ liệu). *Xem* network management.

distributed logic ***hệ logic phân tán*** Trong tin học, hệ sử dụng các thiết bị liên kết với năng lực xử lý cục bộ (ví dụ, các terminal xử lý văn bản cục bộ dùng chung một số bộ nhớ và máy in chung). *Xem* shared logic.

distributed network ***mạng phân tán*** Trong tin học, tổ hợp bất kỳ của các hệ ghép lỏng và chặt. Cấu hình thông thường được minh họa trên sơ đồ. Máy chủ bao gồm một bộ đa xử lý ghép chặt với một bộ nhớ lớn dùng chung bởi hai bộ xử lý trung tâm (CPU). Bộ phân xử nhập/xuất cho phép cả hai bộ xử lý



distributed network: *mạng phân tán.*

truy nhập tất cả các thiết bị nhập/xuất. Nếu một CPU khai thác các vấn đề về phần cứng thì bộ xử lý còn lại có thể tiếp tục chạy tất cả các chương trình dẫu rằng với tốc độ chậm hơn. Các trạm làm việc có thể là những bộ xử lý đầy đủ với bộ nhớ, đĩa và các thiết bị nhập/xuất. Mỗi trạm có thể chạy ở chế độ độc lập; khi người sử dụng yêu cầu các dịch vụ không có sẵn cục bộ thì trạm làm việc có thể yêu cầu trợ giúp từ máy chủ.

Các mạng phân tán có thể có kiến trúc rất linh hoạt (ví dụ, mạng sao với tất cả các trạm nối trực tiếp với máy chủ hoặc mạng vòng với các cáp móc xích từ trạm này tới/trạm khác). *Xem* central processing unit, daisy chain, loosely coupled, multiprocessor, ring, star, tightly coupled, workstation.

distributed processing ***xử lý phân tán*** *Đồng nghĩa với* distributed data processing.

distributive law ***định luật phân phối*** Trong toán học, hai phép toán nhị phân thỏa mãn định luật phân phối nếu

$x + (y * z) = (x + y) * (x + z)$

$x * (y + z) = (x * y) + (x * z)$

trong đó x, y và z là các biến còn $*$ và $+$ biểu thị các phép toán nhị phân. *So sánh với* associative law, commutative law. *Xem* Galois field.

DIV *Xem* data in voice.

DIVA *Xem* data input voice answerback.

division ***phép chia*** Trong các cơ sở dữ liệu, phép toán trong các cơ sở dữ liệu quan hệ. Nếu quan hệ A có hai thuộc tính X, Y và quan hệ B có thuộc tính Z, với Y và Z được xác định trên cùng miền thì phép toán "Chia A cho B qua Y và Z" tạo ra thương số được xác định trên cùng miền như X. Thương chứa các tập giá trị có liên quan X; số bị chia (A) chứa các tập giá trị liên quan (X, Y) và số chia (B) chứa các tập giá trị có liên quan Z. Giá trị X chỉ xuất hiện nếu A chứa các cặp (X, Y) đối với tất cả các giá trị của Y trong B. *So sánh với* join, projection, selection. *Xem* attribute, domain, relational database, tuple.

Division A ***Phần A*** Trong an toàn thông tin, một phần trong các tiêu chuẩn TCSEC, các hệ thống ở phần này đã được đánh giá đối với toàn bộ hệ chức năng của Phần B, Lớp B3, nhưng cũng thỏa mãn các điều kiện chặt chẽ của kiểm chứng hình thức. Nó bao gồm một lớp: A1. *So sánh với* Division B, Division C, Division D. *Xem* formal verification, Orange Book, TCSEC.

Division B ***Phần B*** Trong an toàn thông tin, một phần trong các tiêu chuẩn TCSEC, các hệ thống ở phần này đã được đánh giá về kiểm soát truy nhập tùy ý. Nó bao gồm ba lớp: B1, B2 và B3, với B3 chỉ rõ những điều kiện chặt chẽ hơn B1. *So sánh với* Division A, Division C, Division D. *Xem* discretionary access control, mandatory access control, Orange Book, TCSEC.

Division C ***Phần C*** Trong an toàn thông tin, một phần trong các tiêu chuẩn TCSEC, các hệ thống ở phần này đã được đánh giá về kiểm soát truy nhập tùy ý. Nó bao gồm hai lớp: C1 và C2, với C2 đặc tả các điều kiện chặt chẽ hơn C1. *So sánh với* division A, Division B, Division D. *Xem* discretionary access

control, Orange Book, TCSEC.

Division D ***Phần D*** Trong an toàn thông tin, một phần trong các tiêu chuẩn TCSEC, các hệ thống ở phần này đã được đánh giá nhưng không thỏa mãn các chuẩn cứ của bất kỳ lớp cao hơn nào. *So sánh với* Division A, Division B, Division C. *Xem* Orange Book, TCSEC.

DMA *Xem* direct memory access.

DML *Xem* data manipulation language.

DMS *Xem* digital multiplex switching system.

document cycle ***chu trình chứng từ*** *Đồng nghĩa với* banking cycle.

DOD ***DOD*** Viết tắt của U.S. Department of Defense (Bộ quốc phòng Hoa Kỳ).

DODCSC ***DODCSC*** Viết tắt của Department of Defense Computer Security Center (Trung tâm an toàn máy tính của Bộ quốc phòng hoa Kỳ) . *Xem* National Computer Security Center.

DODD ***hướng dẫn DODD*** Viết tắt của U.S.Department of Defense Directive (hướng dẫn của Bộ quốc phòng Hoa Kỳ).

DOD Information Analysis Center ***Trung tâm phân tích thông tin Bộ quốc phòng Hoa Kỳ*** Hoạt động thu nhận, tóm tắt có hệ thống, phân tích, đánh giá, tổng hợp, lưu giữ, công bố và cung cấp các dịch vụ tư vấn và những dịch vụ khác cho người dùng liên quan tới thông tin khoa học và kỹ thuật toàn thế giới và các dữ liệu kỹ thuật trong một lĩnh vực hay một mảng vấn đề chuyên môn được xác định rõ ràng mà DOD đề cập tới hoặc quan tâm nhiều. Các IAC được phân biệt với các trung tâm thông tin kỹ thuật và các thư viện mà chức năng của chúng chủ yếu liên quan tới việc cung cấp tài liệu tham khảo hoặc truy nhập tới bản thân các tài liệu chứ không phải thông tin STI chứa trong các tài liệu.

DOD security criteria ***(các) tiêu chí an toàn của DOD*** *Xem* Orange Book.

DOD Technology Transfer ***chuyển giao công nghệ DOD*** Các chương trình khuyến khích sự chuyển giao công nghệ quân - dân sự và phát triển hợp tác trên cơ sở có hệ thống, bao gồm sự chuyển thích đáng công nghệ do DOD phát triển cho khu vực dân sự của Hoa Kỳ, nơi mà công nghệ như thế có thể được sử dụng sinh lợi và xác định những công nghệ mới đáng quan tâm cả về quân sự lẫn dân sự.

DOD 5200.28-STD ***tiêu chuẩn DOD 5200.28-STD*** Các chuẩn cứ đánh giá hệ máy tính tin cậy của Bộ quốc phòng Hoa Kỳ, tiêu chuẩn này được đưa ra tháng 12 năm 1985. *Xem* Orange Book, TCSEC.

DOE ***DOE*** Viết tắt của U.S. Department of Energy (Bộ năng lượng Hoa Kỳ).

domain ***miền, vùng, phạm vi*** (1) Trong an toàn máy tính, tập hợp các đối tượng mà một chủ thể có khả năng truy nhập. *Xem* access, object, subject. (2) Trong tin học, tài nguyên dưới sự kiểm soát của một hoặc nhiều bộ xử lý chủ có liên quan trên mạng. (3) Trong lập trình, tập hợp các giá trị gán cho các biến độc lập của một hàm.

dominate ***chi phối, trội hơn*** Trong an toàn máy tính, mức an toàn S_1 được coi là trội hơn mức an toàn S_2 nếu phân loại thứ bậc của S_1 là lớn hơn hoặc bằng phân loại thứ bậc của S_2 và các loại thứ bậc của S_1 bao gồm tất cả các loại không thứ bậc của S_2 như một tập hợp con. *Xem* Bell-La Padula model, security level.

DON ***DON*** Viết tắt của U.S.Department of the Navy (Bộ hải quân Hoa Kỳ).

dongle ***khóa phần cứng*** Trong bảo vệ phần mềm, dụng cụ phần cứng nhỏ, do người sản xuất phần mềm cung cấp và được chèn vào cổng nối tiếp của máy vi tính. Bộ chương trình sẽ không chạy trừ phi có mặt dụng cụ. Các khóa phần cứng không phải là phổ biến, một phần vì chúng trói buộc cổng máy vi tính và trong bất kỳ trường hợp nào cũng có những kỹ thuật phần mềm hiệu quả hơn cho các mục đích bảo vệ. *So sánh với* fingerprint. *Xem* execute protection.

Do-Nothing ***virut Do-Nothing*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Doom2 ***virut Doom2*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM và EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

Dot killer ***virut Dot killer*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

double circuiting ***mắc mạch kép*** Trong an toàn vật lý, chỉ việc dùng cách mắc dây dư ra giữa các bộ cảm biến và hệ thống báo động. *Xem* double crop.

double drop ***báo động kép*** (1) Trong an toàn vật lý, kỹ thuật truyền một tín hiệu báo động sử dụng cả báo động chéo lẫn báo động ngắt. *Xem* break alarm, cross alarm. (2) Trong an toàn vật lý, cách mắc dư dây trong mạch báo động nhờ sử dụng hai đường điện thoại đi vào tòa nhà ở những vị trí khác nhau. *Xem* double circuiting.

double-supervised system ***hệ giám sát kép*** Trong an toàn vật lý, hệ báo động khởi phát một tín hiệu cảnh báo trong trường hợp đầu vào nguồn trục trặc hoặc sự cố nguồn. *Xem* trouble condition.

down line load ***tải xuống, tải vào kênh*** Trong tin học, quá trình gửi các chương trình hoặc tệp từ máy tính chủ tới một máy tính ở xa.

download ***tải xuống*** *Đồng nghĩa với* down line load.

downtime ***thời gian ngừng*** Trong tin học, thời gian trong đó một thiết bị không hoạt động do sự cố. *So sánh với* idle time. *Xem* MTBF.

DP ***DP*** Trong các tiêu chuẩn, viết tắt của ISO Draft Proposal (đề xuất phác thảo của ISO). *Xem* ISO.

DQDB ***giao thức DQDB*** Trong truyền thông dữ liệu, viết tắt của distributed queue dual bus (bus kép

hàng đợi phân tán), một giao thức MAC được phát triển để sử dụng ở các mạng vùng thành phố. *Xem* MAC, municipal area network.

DR/AS *Xem* diffuse risk from adversarial sources.

draw down ***lệnh rút tiền*** Trong hoạt động ngân hàng, lệnh giảm số dư ở tài khoản người gửi (do người nhận phục vụ) một khoản tiền cho tài khoản người gửi tại một cơ sở tài chính khác.

drop ***phần cuối*** Trong truyền thông, phần trạm điện thoại bên ngoài mở rộng từ cáp phân phối điện thoại tới các địa điểm thuê bao.

DSA ***DSA*** (1) Trong hoạt động ngân hàng, viết tắt của Decimal Shift and Add (dịch chuyển thập phân và cộng), một phương pháp đã đề xuất để tính một dấu xác thực. Nó dùng hai khóa 10 chữ số thập phân bí mật và dựa trên số học thập phân. *Xem* authenticator. (2) Viết tắt của Digital Signature Algorithm (thuật toán chữ ký số). *Xem* digital signature standard.

DSE *Xem* data switching exchange.

DSM *Xem* ANSI X9.17 - 1985, disconnect service message.

DSO *Xem* data security officer.

DSR *Xem* data set ready.

DSS *Xem* decision support system, digital signature standard.

DSV *Xem* dynamic signature verification.

DTE *Xem* data terminal equipment.

DTI ***DTI*** Viết tắt của U. K. Department of Trade and Industry (Bộ thương mại và công nghiệp Anh).

DTLS *Xem* descriptive top-level specification.

dual control ***kiểm soát kép, kiểm soát đối ngẫu*** Trong quản lý khoá, quá trình sử dụng hai hoặc nhiều thực thể tách riêng (thường là người), hoạt động phối hợp, để bảo vệ những chức năng nhạy cảm hoặc thông tin. Cả hai thực thể đều có trách nhiệm như nhau đối với bảo vệ vật lý các tài liệu trong các chuyển tác dễ bị tổn hại. Không một người duy nhất nào có khả năng truy nhập hoặc sử dụng các tài liệu (ví dụ, khóa mật mã). Đối với việc sinh, vận chuyển, nạp, lưu giữ và truy lục khóa thủ công thì kiểm soát kép đòi hỏi sự phân chia hiểu biết về các khóa giữa các thực thể. *Xem* cryptographic key, split knowledge.

dual key ***khóa kép*** Trong mật mã, thuật ngữ bao hàm cả các khóa yếu lẫn các khóa bán yếu. *Xem* semiweak key, weak key.

dual redundancy ***dư thừa kép*** Trong lý thuyết độ tin cậy, dạng dư thừa modun nhờ dùng hai thiết bị giống nhau. Một thiết bị có thể là phần dự phòng để thay thế thiết bị hoạt động khi phát hiện được sự cố. Hoặc là hai thiết bị hoạt động đồng bộ và các đầu ra của chúng được so sánh. Khi xảy ra sự không ăn khớp sẽ có sự ngắt và chương trình nhận dạng sự cố được dùng để nhận dạng và cách ly modun có sự cố. *So sánh với* NMR, triple modular redundancy. *Xem* modular redundancy.

dual use system ***hệ công dụng kép*** Trong an toàn máy tính, hệ sử dụng cho mục đích cả quân sự lẫn dân sự.

dumb device ***thiết bị không thông minh*** Trong tin học, thiết bị, thường là một đầu cuối (terminal), mà chỉ có thể truyền hoặc nhận dữ liệu tới hoặt từ một máy tính chủ. *So sánh với* intelligent device, dumb terminal.

dumb terminal ***đầu cuối không thông minh*** Ở thiết bị ngoại vi, terminal (hoặc máy tính sử dụng phần mềm terminal không thông minh) mà cho phép truyền thông với các máy tính khác nhưng không tăng cường dữ liệu được trao đổi hoặc cung cấp những đặc điểm bổ sung như tải lên/tải xuống. *Xem* configurably dumb terminal, dumb device.

dump ***đưa ra, kết xuất*** (1) Trong tin học, chuyển khối dữ liệu từ phương tiện này sang phương tiện khác (ví dụ, sự chuyển nội dung của một phần bộ nhớ chính sang máy in dòng). *Xem* main memory. (2) Ở các cơ sở dữ liệu, chỉ sao dự phòng đều đặn cho các mục đích an toàn.

dumpster diving ***bới rác, kiểm tra thông tin từ giấy loại*** Trong an toàn máy tính, phương pháp rút ra thông tin tin cậy qua xem xét nội dung những thùng, những sọt rác của người dùng hợp pháp.

duplex ***song công*** *Đồng nghĩa với* full duplex.

duplex circuit ***mạch song công*** Trong truyền thông, mạch dùng để truyền các tín hiệu theo cả hai chiều đồng thời. *Xem* full-duplex, half-duplex.

duress alarm ***báo động bắt buộc*** Trong an toàn vật lý, hệ thống cho phép một cá nhân phát chỉ báo về một tình huống bắt buộc mà không gây nguy hiểm cho cá nhân. Báo động được vận hành bởi một bộ cảm biến đặt kín đáo. *Xem* ambush code.

DUV *Xem* data under voice.

dwell time ***thời gian dừng*** Trong an toàn vật lý, khoảng thời gian trong đó một cảnh duy nhất được hiện hình trên camera CCTV. *Xem* CCTV, video switcher.

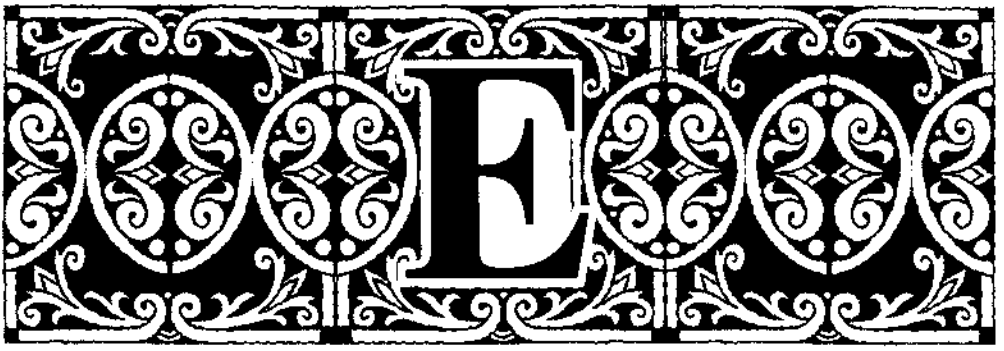
dynamic analysis ***phân tích động*** Trong an toàn máy tính, lớp các công cụ phần mềm để phân tích phần mềm. Những công cụ như thế phân tích mã đã biên dịch bằng cách tạo công cụ và thực hiện nó. *So sánh với* static analysis, dynamic testing. *Xem* software analysis, software tool.

dynamic password ***mật khẩu động*** Trong kiểm soát truy nhập, hệ tạo ra có hiệu quả một mật khẩu người dùng mới cho mỗi lần nhập mạng. Một số hệ thống sử dụng một thẻ bài với một đồng hồ cài sẵn, đồng bộ hóa với một đồng hồ ở máy tính chủ. Người sử dụng nhập mạng và mật khẩu động được chỉ ra trên màn hình LCD. Thiết bị có thể yêu cầu đưa vào PIN trước khi nó cung cấp mật khẩu động cần thiết. Các hệ thống đòi hỏi/đáp ứng cũng cung cấp có hiệu quả mật khẩu động. *Xem* challenge/response, DES, LCD, photosensor, PIN, replay, Watchword.

dynamic signature verification ***kiểm***

chứng chữ ký động Trong kiểm soát truy nhập, phương pháp kiểm chứng chữ ký dựa trên cách mà chữ ký được viết, chứ không phải ảnh hai chiều của chữ ký. *Xem* biometrics, signature analysis.

dynamic testing ***thử động*** Trong an toàn máy tính, việc thử nghiệm một hệ ứng dụng bằng cách thực hiện nó với các dữ liệu thử và so sánh các kết quả thực với kết quả chờ đợi hoặc đã biết. Các phương pháp thử động bao gồm: các bộ phân tích chương trình và phương pháp giả thiết sai. *So sánh với* static evaluation. *Xem* dynamic analysis, flaw hypothesis, program analyzer.



E0 ***E0*** Trong an toàn thông tin, mức đảm bảo thấp nhất trong ITSEC, tương ứng với Phần D trong TCSEC. *So sánh với* Division D, E1, E2, E3, E4, E5, E6. *Xem* ITSEC, TCSEC.

E1 ***E1*** Trong an toàn thông tin, một mức đảm bảo trong ITSEC. *So sánh với* E0, E2, E3, E4, E5, E6. *Xem* ITSEC.

E2 ***E2*** Trong an toàn thông tin, một mức đảm bảo trong ITSEC.

So sánh với E0, E2, E3, E4, E5, E6. *Xem* ITSEC.

E3 ***E3*** Trong an toàn thông tin, một mức đảm bảo trong ITSEC. *So sánh với* E0, E1, E2, E4, E5, E6. *Xem* ITSEC.

E^3 ***E^3*** *Xem* end-to-end encryption.

E4 ***E4*** Trong an toàn thông tin, một mức đảm bảo trong ITSEC. *So sánh với* E0, E1, E2, E3, E5, E6. *Xem* ITSEC.

E5 ***E5*** Trong an toàn thông tin, một mức đảm bảo trong ITSEC. *So sánh với* E0, E1, E2, E3, E4, E6. *Xem* ITSEC.

E6 ***E6*** Trong an toàn thông tin, mức đảm bảo cao nhất trong ITSEC. *So sánh với* E0, E1, E2, E3, E4, E5. *Xem* ITSEC.

EAPROM ***EAPROM*** Trong tin học, viết tắt của Electrically Alterable Programmable Read Only Memory (bộ nhớ chỉ đọc lập trình được có thể thay đổi được bằng điện). *Đồng nghĩa với* EPROM.

EAROM *Xem* electrically alterable ROM.

eavesdropping ***nghe lén, nghe trộm*** Trong an toàn dữ liệu, sự nghe trộm không được phép các bức xạ mang thông tin thông qua sử dụng các phương pháp chứ không phải nối dây trộm. *So sánh với* wiretapping. *Xem* compromising emanations, electronic countermeasures sweeping, passive attack.

EBCDIC code ***mã EBCDIC*** Trong mã hóa, viết tắt của Extended Binary-Coded Decimal Interchange Code (mã trao đổi thập phân mã hóa nhị phân mở rộng), một trong hai bộ mã dữ

liệu quốc tế dùng trong các thiết bị IBM. Mã tám bit cho 256 tổ hợp để biểu diễn sự lựa chọn các mã đồ họa (in) và phi đồ họa (điều khiển). Nó được IBM dùng để biểu diễn các ký tự và các giá trị điều khiển ở các máy tính lớn. *So sánh với* ASCII, ISO-7.

ECB *Xem* electronic codebook.

ECC *Xem* error correction code.

ECCM ***ECCM*** Viết tắt của electronic counter-countermeasures (các biện pháp chống phá rối bằng điện tử).

echocheck ***kiểm tra bằng tín hiệu dội*** *Xem* echoplex.

echoplex ***dò lỗi bằng tín hiệu dội*** Trong truyền thông dữ liệu, phương pháp sử dụng tín hiệu dội của dữ liệu đã thu để kiểm tra lỗi. Máy tính khi nhận dữ liệu từ một tuyến truyền thông hoạt động ở chế độ song công hoàn toàn sẽ trả dữ liệu nhận được về cho máy phát, do đó cho phép nó xác minh rằng dữ liệu đã được nhận đúng. *So sánh với* local echo. *Xem* full-duplex.

echo suppressor ***bộ triệt tín hiệu dội*** Trong truyền thông dữ liệu, các mạng thoại thông thường có các bộ triệt tín hiệu dội để ngăn chặn các tín hiệu dội phiền phức trong các cuộc đàm thoại. Những dụng cụ đó phát hiện sự có mặt của tín hiệu tiếng nói ở một chiều và ngăn chặn tín hiệu chạy theo chiều ngược lại. Những dụng cụ đó ngăn cản truyền thông dữ liệu song công hoàn toàn và vì thế phải được bỏ để chuyển dữ liệu. *Xem* full duplex.

ECM ***biện pháp ECM*** Trong an toàn dữ liệu, viết tắt của electronic countermeasures (biện pháp đối phó bằng điện tử).

ECMA ***tổ chức ECMA*** Viết tắt của European Computer Manufacturers Association (Hiệp hội các nhà sản xuất máy tính châu Âu).

ECOMA ***tổ chức ECOMA*** Viết tắt của European Computer Measurement Association (Hiệp hội đo máy tính châu Âu).

economic assessment ***đánh giá về mặt kinh tế*** Việc nghiên cứu chi tiết các biện pháp an toàn, tính khả thi về vận hành và về kỹ thuật của chúng, và chi phí và lợi ích của chúng. Đánh giá kinh tế trợ giúp cho việc lập kế hoạch và lựa chọn các biện pháp an toàn. *Xem* risk analysis.

economy of mechanism ***tiết kiệm cơ cấu*** Trong an toàn máy tính, nguyên tắc duy trì thiết kế an toàn càng đơn giản càng tốt. *Xem* principles of secure systems.

ECSA ***tổ chức ECSA*** Viết tắt của European Computer Services Association (Hiệp hội các dịch vụ máy tính châu Âu).

EDAC ***phương pháp EDAC*** Trong truyền thông dữ liệu, viết tắt của error detection and correction (phát hiện và sửa lỗi). *Xem* forward error correction.

EDI *Xem* electronic data interchange.

EDIFACT ***chuẩn EDIFACT*** Trong các tiêu chuẩn, viết tắt của EDI For Administration, Commerce and Transport (EDI cho quản trị, thương mại và vận tải), tiêu chuẩn của Liên Hợp Quốc cho các thông báo EDI. Các dữ liệu cần

truyền được lồng trong các đoạn bên trong các thông báo, vốn chứa thông tin về người nhận và tem thời gian. Các thông báo cùng kiểu cũng có thể được nhóm lại thành các nhóm chức năng, sự trao đổi là sự thu thập các thông báo hoặc các nhóm chức năng cho một người nhận cụ thể. *So sánh với* ANSI X.12. *Xem* electronic data interchange, EDI security.

EDI security ***an toàn EDI*** Trong an toàn dữ liệu, an toàn trong các hệ trao đổi dữ liệu điện tử phải cung cấp cho người sử dụng mức độ an toàn như của hệ thống hồ sơ và bưu điện truyền thống, mà nó thay thế, tức là xác thực người dùng, xác thực thông báo, chứng minh nguồn gốc, không từ chối và giữ bí mật. Ngoài ra, những dịch vụ này phải được cung cấp theo cách không liên quan tới sự phát triển của những giao thức riêng lẻ phức tạp được thiết lập giữa các bên buôn bán và chúng phải phù hợp với hệ thống luật pháp trong đó các bên buôn bán hoạt động.

Xác thực người sử dụng có nghĩa là, khi Alice thiết lập truyền thông với Bob thì cô ta phải có khả năng xác minh được rằng Bob là một người sử dụng hiện thời của hệ thống, được đăng ký bằng những dữ liệu ủy nhiệm xác định, ví dụ như ID người dùng, các đặc quyền người sử dụng v.v.. Các thông báo EDI thường không được trao đổi theo kiểu tương tác và do đó, các thủ tục xác thực người sử dụng đòi hỏi trao đổi thông tin giữa các bên ví dụ hỏi/đáp, thường là không thích hợp.

Xác thực thông báo có nghĩa là, khi Bob nhận một thông báo từ Alice thì anh ta phải có khả năng tự đảm bảo rằng thông báo xuất phát từ Alice, rằng thông báo không bị sửa đổi hoặc phát lại.

Bob sẽ yêu cầu một bằng chứng về nguồn gốc cùng với một thông báo EDI nhận được từ Alice để bất kỳ bên thứ ba nào cũng có thể kiểm chứng rằng, thông báo chỉ có thể được gửi đi từ Alice, tức là nó không được gửi đi bởi một bên khác và Bob không thể làm giả thông báo xác nhận rằng Alice là người gửi. Chứng minh nguồn gốc cũng phải ngăn ngừa khả năng thông báo chỉ là sự phát lại một thông báo trước đó, ví dụ như một ý đồ tạo ra một ủy quyền thanh toán kép.

Không từ chối trong các hệ EDI liên quan tới các hóa đơn của các thông báo sao cho nếu Alice đã gửi đi một biên lai thì một bên thứ ba có thể kiểm chứng rằng, biên lai chỉ có thể do Alice tạo ra. Biên lai phải chứa đủ thông tin để nhận dạng một cách duy nhất thông báo ban đầu đang xét. Tuy nhiên, biên lai phải được xác định rõ ràng và không thể bị nhầm với một thông báo ban đầu.

Giữ bí mật là một điều quan trọng, ít nhất đối với một số trường trong các thông báo EDI. Thông tin về những sắp xếp định giá đặc biệt, số lượng hoặc loại hàng hóa đã đặt thường có giá trị thương mại.

Các yêu cầu an toàn có thể được thỏa mãn bằng các hệ thống mật mã. Các hệ mật mã cả đối xứng lẫn không đối xứng đều đã được khuyến nghị cho các ứng dụng EDI, nhưng các hệ mã không đối xứng cung cấp những giải pháp trang

nhã hơn, đặc biệt cho những vấn đề liên quan tới chứng minh nguồn gốc.

Các điểm căn bản về an toàn được yêu cầu trong an toàn EDI bao gồm các mã xác thực thông báo, các mã phát hiện thông báo, các chữ ký số, mã hóa thông báo, lọc và quản lý khóa.

Các mã xác thực thông báo (MAC) được rút ra từ thông báo cần được xác thực, và một khóa mật chỉ bên gửi và bên nhận biết được. Chúng được gắn thêm vào thông báo sao cho bên nhận có thể được đảm bảo rằng, thông báo được gửi đi từ một bên gửi chủ định và sau đó không bị sửa đổi.

Các mã phát hiện thông báo (MDC) tương tự với các mã xác thực thông báo nhưng không sử dụng khóa mật. Những mã như thế có tính chất là không có khả năng xác định được hai thông báo cho ra cùng MDC.

Mật mã khóa công khai có thể được sử dụng để cung cấp chữ ký số của thông báo, và như vậy, đảm bảo về cả tính toàn vẹn của thông báo lẫn khả năng chứng minh nguồn gốc, để bên thứ ba sau đó có thể kiểm chứng rằng, chỉ có bên gửi chủ định mới có thể tạo ra thông báo. Thông thường, MDC của thông báo được mã bằng khóa mật của bên gửi. Bên nhận có thể được đảm bảo về tính xác thực của khóa công khai của bên gửi nhờ gộp chứng nhận của bên gửi với thông báo.

Một dạng chữ ký sử dụng các mã pháp đối xứng có thể thực hiện được nếu bên gửi và bên nhận đều được trang bị các hệ phần cứng đặc biệt, cả hai đều chứa cùng khóa mật. Hệ của bên gửi chỉ có phương tiện để khai triển MAC và hệ của bên nhận chỉ có phương tiện để kiểm chứng MAC. Theo cách này, bên nhận có thể được đảm bảo về tính xác thực của thông báo, về người gửi và nội dung của nó, nhưng không có phương tiện khai triển MAC và điều này sẽ đảm bảo rằng, bên thứ ba có thể kiểm chứng nguồn gốc khi có tranh chấp.

Việc mã hóa thông báo để đảm bảo tính bí mật liên quan tới cả một dạng quản lý khóa nào đó và phép lọc. Nếu cùng mật mã đối xứng ví dụ DES, thì dùng sơ đồ quản lý khóa, thường gồm các khóa phiên chính. Trong trường hợp mật mã công khai, thông báo có thể được mã hóa bằng khóa công khai của bên nhận. Tuy nhiên, thông thường hơn thì mật mã đối xứng được sử dụng để mã văn bản; khi đó khóa đối xứng được dùng được tự mã hóa bằng khóa công khai của bên nhận và khóa đã mã được gộp với thông báo đã mã hóa.

Các hệ EDI có những quy tắc chặt chẽ đối với các bộ ký tự cần sử dụng trong các thông báo. Tuy nhiên, bản mã được tạo ra bằng phép mã văn bản thông báo sẽ gồm những dòng bit ngẫu nhiên không tương thích với những quy tắc đó. Do vậy cần có một dạng lọc nào đó để bổ sung thông tin dư ra, cho phép truyền dòng bit dưới một dạng chỉ chứa các ký tự phù hợp. Khi đó, bên nhận áp dụng một dạng lọc ngược để tạo ra dòng bit bản mã ban đầu trước khi giải mã.

Các thông báo phải chứa đủ thông tin an toàn được nhúng bên trong để cho phép bên nhận áp dụng các quá trình thích hợp kiểm tra xác thực, giải mã

văn bản v.v.. Thông tin như vậy thường nằm dưới dạng các phần đầu (header) và phần đuôi an toàn ở những vị trí thích hợp trong thông báo.

Không giống như các hệ điểm tới điểm, liên lạc EDI sẽ liên quan tới một cộng đồng người sử dụng và điều căn bản là, bên nhận được trang bị một tập hợp các giao thức an toàn và dữ liệu an toàn có liên quan được lồng trong thông báo. Do vậy các chuẩn mô tả cách thức an toàn cần vận dụng là rất thiết yếu trong các hệ EDI. ANSI X.12 có một phần đề cập tới an toàn và chương trình TEDIS đã tính đến các nghiên cứu an toàn cho các hệ EDIFACT. *Xem* ANSI X.12 - 1983, asymmetric cipher, certificate, ciphertext, digital signature, filtering, DES, electronic data interchange, EDIFACT, key management, MAC, MDC, public key cryptography, symmetric cipher.

edit ***soạn thảo*** Trong tin học, soạn thảo là quy trình dùng để thay đổi hoặc sửa đổi dạng của dữ liệu đưa vào hệ thống. Quy trình này có thể gồm việc kiểm tra đầu vào để có định dạng đúng và thêm hoặc xóa các ký tự.

editing run ***chạy soạn thảo, chạy chương trình hiệu đính*** Trong tin học, sự chạy chương trình kiểm tra dữ liệu mới về tính hợp lệ theo một loạt các quy tắc xác định trước và nhận dạng mọi lỗi để sửa và đệ trình lại. Các phép thử thông thường gồm kiểm tra xem ngày tháng và các số có nằm trong các khoảng đã chờ đợi hay không, xác minh các chữ số kiểm tra v.v..

EDP ***EDP*** Viết tắt của Electronic Data Processing (xử lý dữ liệu điện tử). *Xem* data processing.

EDP auditor ***người kiểm toán EDP*** Trong hoạt động kiểm toán, người kiểm toán chịu trách nhiệm kiểm toán và kiểm chứng các kiểm soát phần mềm của một hệ máy tính, nhận dạng các lỗi tiềm ẩn và những chỗ dễ bị tổn thương về an toàn. *So sánh với* external auditor, internal auditor. *Xem* EDP controls.

EDP controls ***(các) kiểm soát EDP*** Trong hoạt động kiểm toán, các kiểm soát áp dụng trong một hệ EDP thường bao gồm:

- các kiểm soát ứng dụng;
- các kiểm soát cài đặt EDP;
- các kiểm soát phát triển và bảo trì hệ thống.

Các kiểm soát ứng dụng mà bao gồm các kiểm soát đầu vào, xử lý và các kiểm soát đầu ra đều được thiết kế để đảm bảo rằng các giao tác hợp lệ đã được xử lý và được ghi đầy đủ, chính xác, chỉ một lần và theo thang thời gian đúng. Các kiểm soát cài đặt EDP bao gồm phân tách các nhiệm vụ, giám sát và kiểm tra các hoạt động, kiểm soát truy nhập đối với các tòa nhà, phần cứng và phần mềm, các kiểm soát về các thư viện dữ liệu và chương trình v.v..

Các kiểm soát phát triển và bảo trì hệ thống được thiết kế để đảm bảo rằng, hệ thống đã cài đặt là được cấp phép đúng và an toàn, như vậy chúng bao gồm:

- một phương pháp luận về thực hiện và quản lý dự án;
- xem xét lại những cái có thể cung cấp

so với các mục tiêu đã thỏa thuận;
- các thủ tục đảm bảo chất lượng hình thức;
- thử nghiệm giai đoạn có kết quả;
- lập kế hoạch cài đặt chi tiết suốt dự án;
- các thủ tục kiểm soát sự thay đổi ứng dụng. *Xem* EDP auditor.

EDV ***virut EDV*** Trong an toàn máy tính, virut lấy lén kết thúc và lưu trú, lây nhiễm cung khởi động đĩa cứng và đĩa mềm, và bảng phân chia đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

EEFI *Xem* essential elements of friendly information.

EEPROM ***EEPROM*** Trong tin học, viết tắt của Electrically Erasable Programmable Read Only Memory (bộ nhớ chỉ đọc có thể lập trình xóa được bằng điện). *So sánh với* EPROM. *Xem* PROM.

EEPROM security ***an toàn EEPROM*** Trong an toàn máy tính, phần mềm lưu giữ trên các EEPROM (PROM xóa được bằng điện) tạo ra một độ an toàn cao hơn chống lại đọc không được phép, so với phần mềm lưu giữ trên ROM thông thường, vì không thể đọc dữ liệu đã nhớ bằng kính hiển vi quang học hoặc kính hiển vi điện tử quét. *Xem* EEPROM, PROM, ROM.

EEROM *Xem* electrically erasable ROM, KEEPROM.

EFF *Xem* electronic frontier foundation.

effectiveness ***hiệu quả*** Trong an toàn thông tin, phạm vi mà một hệ thống thỏa mãn các tiêu chuẩn của nó. *Xem* information technology security evaluation criteria.

E field ***trường E*** Trong an toàn vật lý, tên thương mại của bộ cảm biến trường tĩnh điện. *Xem* electrostatic field sensor.

EFT *Xem* electronic funds transfer.

EFTPOS *Xem* electronic funds transfer point of sale.

EFTS ***hệ EFTS*** Viết tắt của Electronic funds transfer system (hệ chuyển tiền điện tử). *Xem* electronic funds transfer.

EIA ***EIA*** Viết tắt của Electronic Industries Association (Hiệp hội công nghiệp điện tử).

EIN *Xem* European Informatics Network.

electrically alterable ROM ***bộ nhớ chỉ đọc thay đổi bằng điện, EAROM*** Trong các hệ thống nhớ, bộ nhớ chỉ đọc mà có thể được lập trình bằng cách tác dụng một điện áp vào các chân được chọn và nó được xóa hoặc bằng cách chiếu ánh sáng tử ngoại hoặc bằng cách đảo cực tính dùng khi ghi. *So sánh với* electrically programmable read-only memory (EPROM). *Xem* read-only memory (ROM). *Đồng nghĩa với* EEROM, electrically erasable ROM, EROM.

electrically erasable ROM ***ROM xóa được bằng điện*** *Đồng nghĩa với* electrically alterable ROM.

electrically programmable read only memory ***bộ nhớ chỉ đọc lập trình bằng điện, EPROM*** Trong các hệ thống nhớ, bộ nhớ chỉ đọc mà có thể lập trình bằng cách tác dụng một điện áp lên các chân chọn lọc. Thuật ngữ này

áp dụng cả cho các thiết bị mà có thể tái lập trình được cả cho các thiết bị không thể tái lập trình được. *Xem* electrically alterable ROM, PROM.

electrical metallic tubing ***ống kim loại bảo vệ*** Trong an toàn truyền thông, dạng ống tạo ra một sự bảo vệ vật lý và điện nào đó đối với các cáp.

electric field sensor ***bộ cảm biến điện trường*** Trong an toàn vật lý, bộ cảm biến gồm một dây có điện áp xoay chiều, một hoặc nhiều dây cảm biến song song, một bộ khuếch đại và một bộ xử lý tín hiệu. Sự có mặt một kẻ xâm nhập tạo ra các biến thiên điện trường và sự thay đổi này được phát hiện bởi các dây cảm biến, sẽ được bộ xử lý tín hiệu phân tích và kích hoạt báo động. *So sánh với* magnetic sensor. *Xem* electrostatic field sensor.

electromagnetic emanations ***phát xạ điện từ, phát tán điện từ*** Trong an toàn máy tính, các tín hiệu truyền như bức xạ qua không khí và qua các vật dẫn, nhất là qua các đường ra bộ nguồn và các cáp máy in. *Xem* compromising emanations, van Eck phenomenon. *Đồng nghĩa với* electromagnetic emissions, radio phát tán điện từ frequency emissions.

electromagnetic emissions ***phát xạ điện từ, phát tán điện từ*** *Đồng nghĩa với* electronmagnetic emanations.

electromagnetic interference ***nhiễu điện từ, EMI*** Trong an toàn máy tính, nguồn các điều kiện lỗi trong các máy tính do sự cảm biến bức xạ điện từ tạp tán gây ra. *So sánh với* electromagnetic emanations. *Đồng nghĩa với* radio frequency interference.

electronic blackboard ***bảng viết điện tử*** Trong truyền thông dữ liệu, hệ để gửi chữ viết tay và đồ họa vẽ bằng tay qua đường điện thoại. Người gửi có thể sử dụng hoặc bút quang hoặc bảng đồ họa và hình ảnh thích hợp xuất hiện trên màn máy thu hình ở vị trí ở xa.

electronic codebook ***sổ mã điện tử*** *Đồng nghĩa với* native mode.

electronic coin ***tiền điện tử*** Trong hoạt động ngân hàng, thẻ tiền mặt, kích thước tương tự với một đồng tiền kim loại, dưới dạng thẻ thông minh không tiếp xúc, được dùng như ví điện tử cho các máy bán hàng, điện thoại trả tiền v.v.. *So sánh với* electronic purse. *Xem* contactless smart card.

electronic countermeasures sweeping ***(các) biện pháp đối phó bằng quét điện tử, quét chống phá điện tử*** Trong an toàn truyền thông, quá trình nhận dạng và loại bỏ các dụng cụ nghe lén điện tử từ một vùng, hoặc một bộ phận thiết bị truyền thông. *Xem* electronic listenning device.

electronic data interchange ***trao đổi dữ liệu điện tử*** Trong tin học và truyền thông, sự truyền các tài liệu từ máy tính này tới máy tính khác qua một mạng. Nếu tất cả các bên kinh doanh đều có các hệ máy tính mà trong đó đã thỏa thuận một chuẩn cho trao đổi dữ liệu điện tử, như X.400, thì sẽ có những lợi ích lớn. Công việc giấy tờ được loại bỏ, những nhà cung ứng có thể đáp ứng nhanh hơn với những yêu cầu sản xuất và nhà sản xuất không phải đánh máy lại những chi tiết hóa

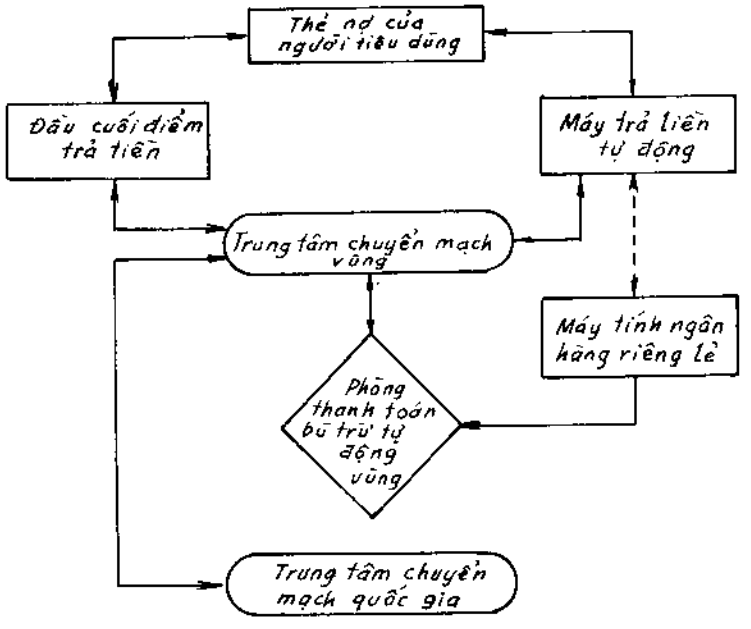
đơn cung ứng. Điều đó loại bỏ được các lỗi do sao chép và giảm được chi phí xử lý, nhất là nếu các bên tham gia là những tổ chức đa quốc gia sử dụng mạng toàn cầu. *Xem* EDIFACT, EDI security, ODETTE, X.400.

electronic data processing ***xử lý dữ liệu điện tử, EDP*** Trong tin học, sự xử lý dữ liệu thực hiện chủ yếu bởi các kỹ thuật điện tử so với các kỹ thuật thủ công hoặc cơ, thường bao gồm các giao tác toàn công ty.

electronic digital computer ***máy tính điện tử số*** Trong tin học, ở dạng đơn giản nhất là thiết bị với một bộ xử lý trung tâm (CPU) nhận tập hợp các lệnh và dữ liệu, thực hiện các tính toán và thao tác trên những dữ liệu đó theo các lệnh và đưa ra kết quả. Máy tính cơ bản bao gồm một thiết bị vào, bộ nhớ, một khối điều khiển và số học và một thiết bị ra.

electronic eavesdropping ***nghe trộm điện tử, nghe lén điện tử*** Trong an toàn dữ liệu, sự chặn bắt các buổi truyền vô tuyến (ví dụ, sóng phát thanh hoặc vi ba) hoặc năng lượng điện tử mang thông tin phát xạ từ các thiết bị điện tử. *So sánh với* acoustic eavesdropping. *Xem* compromising emanations, eavesdropping, Tempest, van Eck phenomenon.

electronic filing ***sắp xếp hồ sơ điện tử, sắp xếp lưu trữ điện tử*** Trong các ứng dụng, một hướng tự động hóa văn phòng liên quan tới sắp xếp lưu



electronic funds transfer: *chuyển tiền điện tử.* Các dịch vụ tài chính EFT và công nghệ hỗ trợ.

CÁC DỊCH VỤ TÀI CHÍNH	CÁC CÔNG NGHỆ EFT				
	POS	ATM	Ngân hàng qua điện thoại	Phòng thanh toán bù trừ	Các hệ chuyển tiền hữu tuyến
Các dịch vụ EFT hướng người sử dụng					
Các dịch vụ EFT tạo điều kiện chuyển thông tin					
Ủy quyền séc	x	-	-	-	-
Kiểm chứng séc	x	-	-	-	-
Bảo lãnh séc	x	-	-	-	-
Xem hồ sơ (hỏi số dư)	-	x	x	-	-
Các dịch vụ EFT lập hóa đơn chuyển tiền trực tiếp					
Gửi tiền	-	x	-	-	-
Rút tiền mặt	-	x	-	-	-
Thanh toán hóa đơn hoặc khoản vay	-	-	x	-	-
Mua hàng	x	-	x	-	-
Chuyển tiền cùng tài khoản	-	x	x	-	-
Nợ với đặc quyền chi trội	x	x	-	-	-
Mua chịu	x	-	-	-	-
Trả trước tiền mặt	-	x	-	-	-
Các dịch vụ EFT định hướng công ty					
Chuyển qua đường dây hữu tuyến	-	-	-	-	-
Gửi tiền lương trực tiếp	-	-	-	x	-
Các dịch vụ nợ ủy quyền trước	-	-	-	x	x
Quản lý tiền mặt công ty (bao gồm các chuyển tiền hữu tuyến giữa các ngân hàng và nội bộ ngân hàng)	-	-	-	x	x

electronic funds transfer: *chuyển tiền điện tử.* Các dịch vụ tài chính và công nghệ hỗ trợ EFT.

trữ các bản ghi văn phòng điển hình (ví dụ, các bản ghi nhớ, các báo cáo, các biểu đồ) trên băng từ hoặc đĩa. Trong một số trường hợp các kỹ thuật vi phim được dùng để lưu giữ những đối tượng đồ sộ và hệ thống thường cho phép ghi danh mục các đối tượng giấy tờ mà không thể đọc được thuận tiện vào hệ máy tính. *Xem* magnetic disk, magnetic tape.

electronic frontier foundation ***quỹ biên giới điện tử*** Trong lập pháp, quỹ của Hoa Kỳ được thành lập để bảo vệ các quyền công dân của những hacko

không can thiệp vào các hệ máy tính một cách bất hợp pháp. *Xem* hacker.

electronic funds transfer ***chuyển tiền điện tử, EFT*** Trong hoạt động ngân hàng dữ liệu, hệ tự động để chuyển tiền từ tài khoản ngân hàng này sang tài khoản ngân hàng khác nhờ sử dụng thiết bị điện tử và truyền thông dữ liệu chứ không phải phương tiện giấy tờ (ví dụ, séc) và hệ thống bưu điện. *So sánh với* EFTPOS. *Xem* banking networks, electronic funds transfer point of sale, key management, message authentication, PIN management and security.

electronic funds transfer point of sale ***điểm bán hàng chuyển tiền điện tử*** Trong hoạt động ngân hàng, điểm trả tiền qua thiết bị đầu cuối được nối qua đường truyền thông tới máy tính của cơ sở tài chính. Thiết bị đầu cuối thường đọc và truyền thông tin ghi trên sọc từ tính của thẻ tín dụng và chuẩn bị các chi tiết giao dịch thông qua bàn phím. *Xem* AS 2805, electronic funds transfer, point of sale.

Electronic Industries Association ***Hiệp hội công nghiệp điện tử, EIA*** Tổ chức tiêu chuẩn chuyên về các đặc trưng điện và chức năng của thiết bị giao diện.

electronic listening device ***thiết bị nghe lén điện tử*** Trong an toàn truyền thông, thiết bị dùng để thu thập và truyền thông tin tới một kẻ nghe lén. Những thiết bị như thế có thể được gài bí mật trong phòng hoặc nối với thiết bị điện thoại. Con bọ điện tử được dùng để nghe lén cuộc nói chuyện trong phòng và gồm có một micrô bé tí xíu, bộ khuếch đại, máy phát và nguồn nuôi. Nó có thể truyền cuộc nói chuyện dưới dạng tín hiệu tần số vô tuyến mà có thể thu được ở khoảng cách xa tới 10 kilomet, tùy thuộc vào tần số vô tuyến đã dùng, công suất máy phát và mật độ các tòa nhà trên đường truyền.

Những thiết bị như vậy cỡ bằng đồng xu nhỏ và dễ dàng nhét vào bút viết, gạt tàn thuốc lá, máy dập ghim, đồng gỗ, giá đèn v.v. Sự có mặt của các con bọ điện tử cũng có thể phát hiện được bởi máy thu vô tuyến dải tần rộng nối với một thiết bị âm thanh hoặc một máy hiện sóng.

Các máy nối trộm điện thoại tương tự với con bọ điện tử trừ một điều là chúng không chứa micrô hoặc nguồn nuôi và được nối nối tiếp hoặc song song với đường điện thoại. Vì chúng không cần nguồn nuôi nên chúng có thể hoạt động vô thời hạn và không cần gài vào vùng an toàn như một văn phòng. Máy nghe lén điện thoại có thể được nối với đường điện thoại thích hợp ở những điểm khác nhau (ví dụ ở các khung phân phối đặt cùng tầng, ở tầng hầm hoặc bên ngoài tòa nhà công sở). Những máy như vậy có thể dùng để nghe lén các cuộc nói chuyện, fax, telex hoặc dữ liệu máy tính. Sự có mặt của các máy nghe lén điện thoại có thể được phát hiện bằng cách chèn một tín hiệu lên đường dây và kiểm tra tín hiệu dội từ các điểm bị nghe lén, kiểm tra những thay đổi của điện áp hoặc điện trở đường dây so với giá trị bình thường, hoặc kiểm tra thực tế.

Việc bảo vệ chống các con bọ điện tử

trong phòng bao gồm việc sử dụng sự truyền sóng siêu âm đã điều chế, nó sẽ làm át các tín hiệu âm thanh ở máy thu. Việc chống lại các con rệp điện thoại bao gồm các thiết bị xáo trộn tiếng nói và các âm chấn đã truyền, nhưng những phương pháp như thế đòi hỏi có thiết bị ở cả đầu thu lẫn đầu phát. Ví dụ như cần có một bộ giải xáo trộn hoặc bộ lọc để loại bỏ những âm chấn ở máy thu. *Xem* voice scrambling, electronic countermeasures sweeping. *Đồng nghĩa với* bug.

electronic mail ***thư điện tử, EM***
Trong truyền thông dữ liệu, phương tiện cho phép người dùng trao đổi thông tin có địa chỉ cho một cá nhân riêng, hoặc một nhóm dùng các phương tiện truyền thông. Các tùy chọn có sẵn trong các hệ khác nhau có thể được phân thành Send (gửi), Receive (nhận), File Options (chọn tên) và Addressing Options (các mục chọn địa chỉ).

Các mục chọn Send bao gồm Carbon Copy (gửi thêm cho người khác), Blind copy (gửi thêm một bản cho người không quen). Reply Requested (yêu cầu trả lời), Expsers (gửi nhanh), Registered (đăng ký) và Delayed Delivery (phân phối trễ). Chọn Carbon Copy sẽ gửi thêm một thông báo tới tất cả những người sử dụng đã định, trong khi đó mục chọn Blind Copy thực hiện chức năng tương tự mà không chỉ rõ danh sách phân phối tới những người nhận riêng lẻ. Mục Reply Requested chỉ rằng thư tín phải được trả lời. Mục Express sẽ nhận một kiểu xử lý đặc biệt khi thu (ví dụ, cảnh báo trạm làm việc). Mục chọn Registered sẽ cho biết sự phân phát tới người nhận đã định còn Delayed delivery sắp xếp để thư được phân phát vào thời gian hoặc ngày tháng xác định.

Các mục chọn Receive bao gồm Forward (gửi tiếp), Reply (trả lời), Save (cất giữ), Delete (xóa) và Scan (quét). Mục Forward gửi thông báo tới người sử dụng khác với những ghi chú khi cần, không nằm trong danh sách địa chỉ ban đầu. Mục Reply cho phép trả lời thông báo ngay lập tức bất kể có được yêu cầu hay không. Mục Save giữ thông báo ở lại tệp hiện tại hoặc mới để biên tập, trộn, xem lại... về sau. Mục Delete hủy thông báo sau khi đọc và mục Scan cho phép duyệt nhanh thư tín đang chờ, chỉ xem những tên người gửi, các tiêu đề v.v..

Các mục chọn File gồm Editing (soạn thảo) và Merging (sắp trộn). Mục Editing cho phép đọc các thông báo đã chọn bởi khoảng ngày tháng, tìm kiếm bằng từ khóa, nơi gửi v.v., mục này cho khả năng soạn thảo trực tuyến hoặc ngoại tuyến, và mục Merging cho phép chèn thông tin định dạng trước vào thông báo trong khi chuẩn bị.

Các mục chọn Addressing bao gồm Group Addressing (lập địa chỉ nhóm), Standard Distribution (phân phối chuẩn), Hidden Distribution (phân phối ẩn) và Account Number/Name Association (kết hợp số hiệu/số tài khoản. Mục Group Addressing cho phép sử dụng nhiều số tài khoản người dùng trong danh sách địa chỉ. Mục Standard Distribution cho các danh sách phân phối nhớ sẵn, trong khi đó mục Hidden Distribution tương tự với Blind Copy (tức là không người nhận nào thấy danh sách phân phối).

Mục Account Number/Name Association cho phép lập địa chỉ theo tên chứ không phải theo số hiệu người dùng.

Các phương tiện hộp thư điện tử có thể được cung cấp trong phạm vi một tổ chức hoặc trên mạng quốc gia hoặc quốc tế (ví dụ, Telecom Gold hoặc Dialcom). *Xem* electronic mail security. *Đồng nghĩa với* computer based message system.

electronic mailbox ***hộp thư điện tử*** *Xem* electronic mail.

electronic mail security ***an toàn thư điện tử*** Trong an toàn truyền thông, an toàn ở các hệ thư điện tử có thể được đưa vào để đảm bảo giữ bí mật và/hoặc tính toàn vẹn của các thông báo thư điện tử hiện dạng được sử dụng rộng rãi trong các môi trường thương mại và nghiên cứu.

Các hệ thư điện tử thường liên quan tới những mạng phức tạp với rất nhiều hệ máy tính chủ và các trạm làm việc; nhiều bên tham gia có thể không cần các dịch vụ an toàn. Trong các tình huống đó, tốt nhất là cung cấp những dịch vụ an toàn như thế trên cơ sở điểm tới điểm, như vậy sẽ tránh được yêu cầu bổ sung các thành phần an toàn cho nhiều hệ khác nhau tạo nên toàn bộ mạng.

Các bên gửi phải có một cơ chế nào đó đảm bảo rằng, bên nhận có thể cam kết trao đổi an toàn trước khi truyền thông báo. Tuy nhiên, sự an toàn điểm tới điểm như thế có thể không cung cấp sự an toàn luồng thông tin.

Cần có sự mã hóa để đảm bảo giữ bí mật toàn bộ các thông báo, hoặc các thành phần nhạy cảm của các thông báo. Các mã toàn vẹn thông báo (MIC) có thể được sử dụng như một dạng tổng kiểm tra để cảnh báo sự sai lạc thông báo. Các hàm tạo ra các mã toàn vẹn thông báo có thể bao gồm các khóa mật mã, hoặc các MIC có thể được tạo thành mà không cần sử dụng các khóa mật. Bản thân các MIC có thể được mã hóa để chống lại sự sửa đổi ác ý đối với thông báo.

Thông báo thư điện tử an toàn hoàn toàn sẽ đòi hỏi ít nhất ba phần: các phần đầu (header) thông báo chuẩn, các phần đầu thông báo liên quan tới an toàn và văn bản thông báo. Các phần đầu thông báo chuẩn mà hệ thư điện tử đòi hỏi không thể được bảo vệ và sẽ cung cấp danh tính người gửi, người nhận, đầu mục chủ đề v.v.. Đầu mục chủ đề chứa trong đoạn đầu thông báo đó sẽ không được mã hóa; nếu nó bao gồm thông tin nhạy cảm thì nó phải được xử lý như một trường giả (ví dụ như Thông báo mã hóa số..), và đề mục chủ đề nhạy cảm được đặt trong phần được mã hóa của thông báo.

Các đoạn đầu thông báo liên quan tới an toàn sẽ chứa các chi tiết về các bên gửi và bên nhận, các thuật toán mã hóa (ví dụ như DES, RSA) và các chế độ (ví dụ như sổ mã điện tử, liên kết khối mã) đã sử dụng, các tham số mật mã, ví dụ như các vectơ khởi đầu, ký hiệu nhận dạng các khóa trao đổi, các khóa dữ liệu được mã hóa bằng các khóa trao đổi, MIC, các thông báo chứng nhận khóa công khai nếu dùng mật mã không đối xứng v.v..

Các hệ thư điện tử thường bao gồm rất

nhiều loại trạm làm việc của người sử dụng, mỗi loại sử dụng các hệ mã hóa riêng của nó đối với văn bản thông báo, ví dụ như EBCDIC, ASCII và các quy ước cục bộ cho xử lý các ký tự thoát, ký tự trở về đầu dòng, ký tự xuống dòng v.v.. Như vậy, các dòng bit biểu thị cùng văn bản thông báo tại các trạm làm việc gửi và các trạm làm việc nhận có thể khác nhau đáng kể. Những khác biệt như thế có thể gây ra các vấn đề trong tính toán các MIC, vì thế một thông báo sai lạc có thể tạo ra một MIC khác ở bên nhận so với MIC do bên gửi tạo ra và truyền đi. Vấn đề tương tự có thể này sinh với việc truyền bản mã. Văn bản mật mã do thuật toán mật mã tạo ra về cơ bản sẽ bao gồm một dòng bit tùy ý. Dòng bit này sẽ được mã hóa bởi trạm truyền và có thể là một số trong các ký tự được tạo ra sẽ có một ý nghĩa riêng đối với hệ thống truyền, ví dụ như một dãy ký tự nào đó có thể biểu thị kết thúc thông báo, các dãy điều khiển xuống dòng và về đầu dòng có thể bị biến đổi v.v..

Các vấn đề mã hóa nhắc đến ở trên đòi hỏi một sự mã hóa trước đặc biệt đối với bản thông báo được bảo vệ và đối với bản mật mã tương ứng. Dạng chính tắc của văn bản thông báo được tạo ra trước khi phát triển các MIC. Dòng bit biểu thị văn bản mã mật cũng phải được mã hóa trước khi truyền, theo cách để nó sẽ không bị biến đổi bởi mạng.

Nếu sử dụng mật mã đối xứng thì bên gửi và bên nhận phải có cùng khóa mật, thường gọi là khóa trao đổi (*IK*). Khóa này có thể được trao đổi qua một kênh an toàn, ví dụ như hệ thống bưu điện, hoặc nhờ một secvơ khóa cung cấp cho mỗi bên. Trong trường hợp sau, mỗi một bên có thể yêu cầu những khóa mật độc lập để liên lạc với secvơ khóa như vậy. Khóa trao đổi được dùng để mã hóa một khóa mã hóa dữ liệu (DEK) mà khóa này dùng để mã hóa văn bản của một thông báo riêng. DEK, được mã hóa bởi *IK*, có thể được gộp trong các đoạn đầu (header) liên quan tới an toàn của thông báo, cùng với thông tin đủ để bên nhận dạng *IK* mà người gửi dùng. Bên nhận sẽ giữ một số các *IK*, tương ứng với những người sử dụng thư điện tử mà bên nhận thực hiện truyền thông an toàn; hơn nữa, cặp bên gửi - bên nhận có thể lưu giữ một số các *IK* có các thời hạn khác nhau. DEK có thể được sử dụng trong tính toán MIC, còn bản thân MIC có thể được mã hóa bằng IK.

Nếu một thông báo được phân phối theo danh sách gửi thư, thì các *IK* có thể được nhận dạng riêng rẽ mỗi người nhận có trong danh sách, hoặc một *IK* đơn có thể được dùng cho mọi thành viên của danh sách. Các phần đầu (header) thông báo liên quan tới an toàn phải nhận dạng được từ *IK* riêng lẻ, đối với từng bên nhận riêng lẻ trong trường hợp đầu. Nếu dùng một *IK* chung cho tất cả các thành viên của danh sách thì những người sử dụng sẽ phụ thuộc vào các thủ tục an toàn mà mọi thành viên của danh gửi thư chấp nhận để bảo vệ *IK*. Hơn nữa, một kẻ tấn công là thành viên của danh sách gửi thư sẽ có thể có khả năng khai thác hệ thống và giả dạng như bất kỳ thành

viên nào khác.

Các mã pháp không đối xứng có những ưu điểm đáng kể đối với các hệ thư điện tử. Một mã không đối xứng sẽ được sử dụng để mã hóa các DEK, bản thân văn bản thông báo vẫn được mã hóa bằng một mật mã đối xứng. Trong trường hợp này, *IK* dùng để mã hóa DEK là khó., không đối xứng công khai của bên nhận. *IK* mã hóa MIC của thông báo là khóa bí mật của bên gửi, như vậy tạo ra một biện pháp chống từ chối, ngoài sự đảm bảo tính toàn vẹn của thông báo. Nếu dùng các mã pháp không đối xứng thì các thông báo chứng nhận (chứng chỉ) có thể được tạo ra, cung cấp cho người sử dụng một sự đảm bảo về tính xác thực của các khóa công khai nhận được.

Một thông báo, với một MIC được mã hóa bởi khóa mật mã không đối xứng mật của bên gửi, phải chứa thông báo chứng nhận đảm bảo tính xác thực của khóa công khai được sử dụng trong kiểm chứng chữ ký. Tương tự, khóa công khai dùng để mã hóa DEK phải được lấy từ một thông báo chứng nhận chứa trong một thông báo trước đó từ bên nhận chủ định.

Một cơ sở có quyền chứng nhận (cơ quan cấp chứng chỉ) duy nhất có thể không thích hợp trong một mạng thư điện tử lớn vì tất cả các thành viên của mạng, có sử dụng các dịch vụ an toàn, đều có thể yêu cầu liên lạc với cơ sở có quyền chứng nhận đó về mỗi khóa công khai được cung cấp. Sự phân cấp các cơ sở có quyền chứng nhận có thể thích hợp hơn cho các mạng lớn. Trong trường hợp này, khóa công khai của người sử dụng được cung cấp cùng với khóa công khai của cơ sở có quyền chứng nhận địa phương. Một thông báo chứng nhận mà khóa công khai của cơ sở có quyền chứng nhận địa phương được ký bởi một cơ sở chứng nhận cấp cao hơn sẽ được cả bên gửi và bên nhận tin cậy, cũng được gộp vào trong các đầu (header) thông báo của bên gửi. *Xem* ASCII, asymmetric cipher, certificate, checksum, cipher block chaining, DEK, DES, EBCDIC code, electronic codebook, end-to-end encryption, escape character, IK, initialization vector, MIC, privacy enhanced mail, public key, RSA, secret key, symmetric cipher, traffic flow security.

electronic messaging ***lập bảng thông báo điện tử*** *Xem* bulletin board.

electronic piggybacking ***(sự) gánh thêm điện tử, (sự) địu thêm điện tử*** Trong an toàn máy tính, sự chen không hợp lệ các thông báo thông qua một thiết bị đầu cuối hoạt động không được giám sát. *Xem* piggyback.

electronic publishing ***xuất bản điện tử*** Trong các ứng dụng, thuật ngữ chung để chỉ sự phân phối thông tin trên phương tiện điện tử, ví dụ như videotex. *Xem* videotex.

electronic purse ***ví điện tử*** Trong hoạt động ngân hàng, ứng dụng thẻ thông minh trong đó thẻ thông minh được nạp một giá trị tiền xác định. Người sử dụng có thể tiến hành các giao dịch và giá trị của giao dịch được trừ nợ từ thẻ. *So sánh với* electronic coin. *Xem* smart card. *Đồng nghĩa với*

electronic wallet.

electronic signature ***chữ ký điện tử*** *Đồng nghĩa với* digital signature.

electronic system for payments ***hệ thanh toán điện tử*** Trong hoạt động ngân hàng, hệ thống sắp xếp để chuyển giá trị và quản lý kèm theo của các tài khoản nhờ các phương tiện điện tử. *Xem* electronic funds transfer.

electronic token ***thẻ bài điện tử*** *Xem* smart card.

electronic vaulting ***nhảy điện tử, chuyển nhanh điện tử*** Trong an toàn máy tính, sự truyền thời gian thực dữ liệu từ một trung tâm dữ liệu tới một phương tiện nhảy.

electronic vibration detector ***bộ dò rung điện tử, bộ phát hiện dao động điện tử*** Trong an toàn vật lý, thiết bị dò nhạy sử dụng một micô tiếp xúc.

electronic wallet ***ví điện tử*** *Đồng nghĩa với* electronic purse.

electrostatic field sensor ***bộ cảm biến trường tĩnh điện*** Trong an toàn vật lý, một dạng bộ cảm biến trường thụ động dùng để phát hiện sự có mặt của một kẻ xâm nhập qua nhiễu loạn ở điện trường xung quanh. *Xem* electric field sensor.

element ***phần tử*** Trong toán học, một đối tượng, thực thể hoặc khái niệm có các tính chất xác định một tập hợp. *Xem* set.

ElGamal cipher ***mã pháp ElGamal, mã ElGamal*** Trong mật mã, một thuật toán mật mã khóa công khai dựa trên sơ đồ phân phối khóa Diffie-Hellman.

Alice và Bob, mỗi người đều thỏa thuận về một số nguyên tố lớn p sao cho $p - 1$ có ít nhất một thừa số lớn và một số nguyên α thứ hai nhỏ hơn p. Alice giữ một số nguyên bí mật a và tương tự, Bob có một số nguyên b. Alice tính:

$y_a = \alpha^a \bmod p$

và Bob tính:

$y_b = \alpha^b \bmod p$

Các số y_a và y_b có thể được xem như một dạng khóa công khai tương ứng đối với Alice và Bob và được đặt sẵn trong thư mục công khai cùng với α và p.

Alice muốn gửi thông báo được biểu diễn bằng số nguyên $m < p - 1$ cho Bob. Đầu tiên cô chọn một số k trong khoảng $0 \div (p - 1)$, thu được y_b từ thư mục công khai và tính:

$K = y_b^k \bmod p$

Thông báo mã bao gồm hai số c_1 và c_2 trong đó:

$c_1 = \alpha^k \bmod p$

$c_2 = Km \bmod p$.

Hãy chú ý rằng, bản mã dài gấp đôi độ dài bản gốc m.

Bob có thể giải mã thông báo bằng cách đầu tiên sử dụng số bí mật b để tính K từ c_1.

$K = y_b^k \bmod p$

$= (\alpha_k)^b \bmod p$

$= (c_1)^b \bmod p$

Giai đoạn thứ hai là chia $Km \bmod p$ cho K để khôi phục thông báo m. *So sánh với* ElGamal digital signature. *Xem* ciphertext, Diffie-Hellman technique, modulo aritometic, plaintext.

ElGamal digital signature ***chữ ký số***

ElGamal Trong mật mã, thuật toán để tạo ra chữ ký số.

Alice và Bob mỗi người đều thỏa thuận về một số nguyên tố lớn p, sao cho $p - 1$ có ít nhất một thừa số lớn và một số nguyên thứ hai α nhỏ hơn p. Alice giữ một số nguyên bí mật a, tương tự Bob giữ một số nguyên bí mật b. Alice tính:

$y_a = \alpha^a \bmod p$

và Bob tính

$y_b = \alpha^b \bmod p$

Các số y_a và y_b có thể được xem như một dạng khóa công khai tương ứng cho Alice và Bob, và đặt sẵn trong một thư mục công khai cùng với α và p.

Quá trình ký thông báo m, trong đó $0 < m < (p - 1)$ bởi Alice bao gồm ba giai đoạn.

- Alice chọn một số ngẫu nhiên k, đều giữa 0 và $p - 1$ sao cho k và $p - 1$ là nguyên tố cùng nhau.
- Alice tính:

$r = \alpha^k \bmod p$

- Alice xác định một giá trị s, $s < p - 1$, sao cho:

$m = (a.r + k.s) \bmod p - 1)$.

Cặp (r, a) chứa chữ ký cho thông báo m. Bên nhận kiểm tra chữ ký bằng cách tính:

- $\alpha^m \bmod p$ và $(y_a)^r . r^s \bmod p$
- và kiểm tra đề

$\alpha^m \bmod p = (y_a)^r . r^s \bmod p$

Hãy lưu ý rằng, Alice không giống Bob sẽ truy nhập vào các giá trị bí mật a và k, trong khi Bob truy nhập vào các giá trị y_a và r công khai và hoặc đã truyền. Bob do đó có thể kiểm chứng chữ ký nhưng không có phương tiện để tạo dựng nó. *So sánh với* ElGamal cipher *Xem* digital signature, coprime, Liffie-Hellman technique, modulo arithmetic.

emanation ***bức xạ rò*** Trong an toàn truyền thông, tín hiệu do một hệ phát ra mà theo chỉ tiêu kỹ thuật của hệ thì rõ ràng tín hiệu đó không được phép. *Xem* compromising emanstions, electromagnetic emanations, Tempest, van Eck phenomenon.

emanation security ***an toàn bức xạ; bảo vệ chống rò rỉ bức xạ*** Trong an toàn máy tính, sự bảo vệ bằng mọi biện pháp nhằm từ chối không cho những người không được phép nhận được thông tin có giá trị mà có thể rút ra từ nghe lén và phân tích tín hiệu bức xạ gây tác hại. *Xem* compromising emanations, Tempest, van Eck phenomenom.

embedded audit ***kiểm toán lồng trong, kiểm toán lồng sẵn*** Trong an toàn vật lý, việc sử dụng các sổ ghi an toàn cài sẵn trong một hệ máy tính để tạo ra sự giám sát liên tục.

embedded system ***hệ được nhúng, hệ lồng*** Hệ nhúng là hệ thực hiện hoặc điều khiển một chức năng, toàn bộ hoặc một phần, như một phần tử tích hợp của một hệ hoặc phân hệ lớn hơn. Ví dụ, thiết bị hỗ trợ mặt đất, các bộ mô phỏng bay, các giá thử động cơ hoặc các hệ kiểm soát phòng hỏa.

embezzlement ***biển thủ*** Trong lập pháp, một tội liên quan tới việc trộm cắp tài sản của chính người đã được giao tài sản đó.

embossed card ***thẻ dập nổi*** Trong kiểm soát truy nhập, dạng thẻ kiểm soát truy nhập trong đó thông tin đã mã hóa được dập nổi như mẫu hình trên bề mặt thẻ. *So sánh với* magnetic stripe card. *Xem* card reader.

emergency plan ***kế hoạch khẩn cấp*** *Xem* contingency plans.

emergency response ***đáp ứng khẩn cấp, phản ứng khẩn cấp*** Trong quản lý rủi ro, chỉ hành động cấp thời để bảo vệ phần cứng và phương tiện từ tính trong trường hợp có sự cố tự nhiên, hỏa hoạn, sự cố nguồn, trục trặc thiết bị, sự phá hoại, trộm cắp, làm giả v.v.. *Xem* contigency plans, emergency response plan.

emergency response plan ***kế hoạch đáp ứng khẩn cấp*** Trong quản lý rủi ro, kế hoạch đưa ra các quy trình để đáp ứng mau lẹ và có hiệu quả đối với một tình trạng hỗng hóc tiềm tàng để hạn chế thiệt hại. *Xem* contingency plans, emergency response.

EMI/RF radiation ***bức xạ EMI/RF*** Trong an toàn truyền thông, bức xạ nhiễu điện từ/tần số vô tuyến (viết tắt của electromagnetic interference/radio frequency radiation); các tín hiệu không mong muốn sinh ra từ các nguồn như động cơ, máy phát điện, bují ôtô và các đài phát thanh. *Xem* conductive shielding, EMI/RF shield.

EMI/RF shield ***màn chắn EMI/RF*** Trong sự toàn máy tính, màn chắn bằng kim loại được thiết kế đặc biệt để ngăn ngừa sự truyền không mong muốn các tín hiệu điện từ bức xạ và theo đường dẫn. *Xem* EMI/RF radiation, emission security, encapsulation, Tempest, van Eck phenomenon.

emission security ***an toàn phát xạ*** Trong an toàn máy tính, một thành phần của COMSEC vốn xuất phát từ mọi biện pháp từ chối cung cấp cho những người không được phép một thông tin có giá trị mà có thể được rút ra từ việc chặn nghe và phân tích các bức xạ gây hại từ các thiết bị và các hệ thống xử lý thông tin đã phân loại hoạt động bằng điện. *Xem* compromising emanations, Tempest, van Eck phenomenom.

Empire ***virut Empire*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trú, lây nhiễm cung khởi động của đĩa mềm hoặc đĩa cứng, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

employee monitoring ***giám sát nhân viên*** Trong lập pháp, chỉ các hệ vốn giám sát các tác động gõ phím, các lỗi, thời gian thiết bị đầu cuối rỗi, các động lực gõ phím v.v.. Thông tin như thế có thể được dùng để nhận xét về công việc của nhân viên.

empty slot ***khe trống, gói rỗng*** Trong truyền thông dữ liệu, gói dữ liệu liên tục luân chuyển quanh một mạng vòng. Mỗi khi một nút trong mạng muốn gửi thông tin thì nó chờ một khe trống và sau đó điền đầy dữ liệu và thông tin địa chỉ vào khe. *Xem* Cambridge Ring, packet switching.

EMS ***dịch vụ EMS*** Viết tắt của Electronic Mail Service (dịch vụ thư điện tử). *Xem* electronic mail.

EMT *Xem* electrical metallic tubing.

emulator ***bộ mô phỏng*** (1) Trong tin học, tổ hợp phần cứng và phần mềm cho phép viết các chương trình cho một máy tính chạy được trên một máy tính khác. Trong hệ thuật ngữ an toàn máy tính, hộ mô phỏng là phần của hệ thống chịu trách nhiệm tạo ra một môi trường tương thích hệ điều hành ngoài môi trường do nhân cung cấp. Trong KSOS, bộ mô phỏng ánh xạ môi trường nhân lên môi trường Unix. *Xem* KSOS, Unix. (2) Trong tin học, phần cứng hoặc phần mềm chuyên dụng cho phép một hệ tác động như thể nó là một hệ khác. Ví dụ, nó được sử dụng để giảm đến tối thiểu công sức tái lập trình khi một máy tính mới thay thế cho máy tính hiện thời.

encapsulation ***(sự) bọc gói, (sự) đóng kín*** Trong an toàn truyền thông, việc sử dụng các phương pháp lọc RF và sự chắn RF có tính toàn vẹn cao để chứa toàn bộ bức xạ bên trong hộp thiết bị. *So sánh với* source suppression. *Xem* compromising emanations, emission security, Tempest proofing, van Eck phenomenon.

encipher ***mã hóa, cài mã*** Trong lập mã, biến đổi văn bản gốc thành dạng không rõ ràng nhờ một hệ thống mật mã. *So sánh với* encode, decipher. *Xem* cipher system. *Đồng nghĩa với* encrypt.

encipherment ***phép mã hóa*** Trong lập mã, phép biến đổi dữ liệu để tạo ra văn bản mật mã. *So sánh với* decipherment. *Xem* ciphertext. *Đồng nghĩa với* encryption.

encode ***mã hóa*** (1) Trong mật mã, biến đổi văn bản gốc thành dạng không thể hiểu được nhờ một hệ mã. *So sánh với* encipher. *Xem* code system. (2) Trong truyền thông dữ liệu, biến đổi dữ liệu nhờ một mã (code) theo cách sao cho sau đó nó có thể được biến đổi lại thành dạng ban đầu. (3) Trong truyền thông dữ liệu, biến đổi từ hệ truyền thông này sang hệ truyền thông khác. *So sánh với* decode. *Xem* code.

encrypt ***mã hóa, cài mã*** Trong lập mã, biến đổi văn bản gốc thành dạng không rõ ràng nhờ một hệ thống mật mã. *So sánh với* decrypt. *Xem* cryptographic system. *Đồng nghĩa với* encipher.

encryption ***(sự) ghi mật mã, (sự) cài mã, (phép) mã hóa*** Trong lập mã, quá trình biến đổi dữ liệu thành dạng không thể hiểu được theo cách sao cho dữ liệu ban đầu hoặc không thể thu được (mã hóa một chiều) hoặc không thể thu được nếu không sử dụng quá trình giải mã ngược lại (mã hóa hai chiều). *Xem* encrypt, end-to-end encryption, link encryption. *Đồng nghĩa với* encipherment.

encryption algorithm ***thuật toán mã hóa*** (1) Trong lập mã, thuật toán được thực hiện trong hoặc phần sụn hoặc phần mềm và được sử dụng cùng với khóa bí mật để mã hóa bản gốc và giải mã bản mã. *Xem* algorithm, encryption. (2) Trong mật mã, tập hợp các quy tắc biểu thị bằng toán học làm thông tin trở nên không rõ ràng nhờ thực hiện một loạt các phép biến đổi thông qua sử dụng các phần tử có thể thay đổi (biến) được kiểm soát bởi sự áp dụng một khóa đối với biểu diễn bình thường

của thông tin. *Xem* key. *Đồng nghĩa với* privacy transformation.

encrypter board ***tấm mạch mã hóa, bo mạch mã*** Trong mật mã, một tấm mạch mở rộng cho máy tính cá nhân vốn cung cấp các dịch vụ mã hóa, thường là mã và giải mã dữ liệu, sinh và kiểm tra các MAC. Các tấm mạch thường dự phòng bộ nhớ an toàn các khóa mật mã và sử dụng một chip DES để mã hóa và giải mã an toàn, nhanh. *Xem* cryptographic key, DES, expansion board, MAC, personal computer security.

end of address ***kết thúc địa chỉ, EOA*** Trong truyền thông dữ liệu, ký tự điều khiển báo cho máy thu biết rằng ký tự cuối cùng của địa chỉ đã được truyền và các ký tự tiếp theo liên quan tới thông báo.

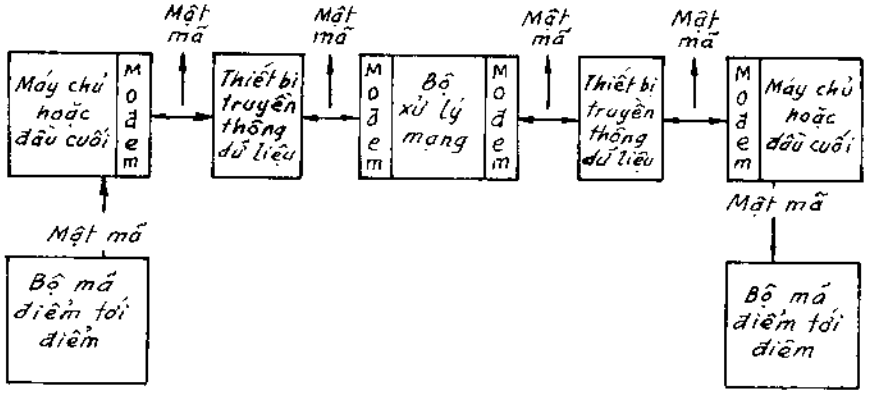
end of block ***kết thúc khối, EOB*** Trong truyền thông dữ liệu, ký tự điều khiển báo cho máy thu biết rằng ký tự cuối cùng của khối đã được truyền đi. *Xem* block.

end of file ***kết thúc tệp, EOF*** Trong các cấu trúc dữ liệu, ký tự cho biết rằng bản ghi cuối cùng của tệp đã được đọc. *Xem* file, record.

end-of-line resistor ***(cái) điện trở cuối đường*** Trong an toàn vật lý, linh kiện dùng để kết thúc một đường giám sát bằng điện. Nó làm cho tuyến liên tục về điện và cung cấp một dòng cố định và/hoặc điểm chuẩn điện trở để đo những thay đổi tạo ra những tín hiệu báo động. *Xem* supervised line.

end-of-line supervision ***giám sát cuối đường*** Trong an toàn vật lý, mạch báo động phát hiện các ý đồ nối một mạch phân dòng điện.

end of message ***kết thúc thông báo, EOM*** Trong truyền thông dữ liệu, ký tự điều khiển cho biết sự kết thúc thông báo; dùng để tách riêng các thông



end-to-end/encryption: *mã hóa điểm tới điểm.* Với mã hóa điểm tới điểm, chỉ có một nút hoặc gửi các thông báo đã mã hóa hoặc là địa chỉ cuối cùng cho các thông báo đã mã hóa, yêu cầu khả năng tạo mật mã. Thông tin định tuyến phải được làm cho khả dụng đối với mỗi nút trung gian mà qua đó thông báo được chuyển, do đó phương pháp này dễ bị phân tích lưu lượng.

báo trong luồng nhiều thông báo. *Xem* end of text.

end of text ***kết thúc văn bản, ETX*** Trong truyền thông dữ liệu, ký tự điều khiển báo cho máy thu biết ký tự trước đó là ký tự cuối cùng ở văn bản thông báo. *So sánh với* start of text.

end of transmission ***kết thúc truyền, EOT*** Trong truyền thông dữ liệu, ký tự điều khiển báo cho máy thu biết rằng đã hoàn thành sự truyền.

Endorsed Tempest Product List ***danh sách sản phẩm Tempest đã phê duyệt*** Trong an toàn máy tính, danh sách của Hoa Kỳ về các máy tính, các thành phần và thiết bị viễn thông tuân thủ các hướng dẫn hiện thời đối với các sản phẩm Tempest. *So sánh với* Evaluated Products List, Preferred Products List. *Xem* Tempest.

endorsement ***(sự) đóng dấu, (sự) phê duyệt*** Trong xử lý dữ liệu, sự đánh dấu một mẫu giấy mẫu hoặc tài liệu để hướng dẫn hoặc hạn chế việc sử dụng tiếp trong xử lý.

end-to-end assurance ***bảo đảm điểm tới điểm*** Trong an toàn dữ liệu, sự đảm bảo an toàn cho người gửi một thông báo đã hoặc sẽ được nhận đúng. *Xem* delivery assurance.

end-to-end control ***kiểm soát điểm tới điểm*** Trong truyền thông dữ liệu, kỹ thuật đảm bảo rằng thông tin được truyền giữa hai đầu cuối dữ liệu không bị mất hoặc bị sai lạc. *Xem* data terminal equipment, handshaking.

end-to-end encipherment ***phép mã điểm tới điểm*** Trong an toàn truyền thông, phép mã dữ liệu trong hoặc tại hệ thống đầu cuối nguồn, với sự giải mã tương ứng xuất hiện chỉ ở bên trong hoặc tại hệ thống đầu cuối nơi nhận. *So sánh với* link encryption. *Xem* decipherment, encipherment. *Đồng nghĩa với* end-to-end encryption.

end-to-end encryption ***mã hóa điểm tới điểm*** Trong an toàn truyền thông, sự mã hóa thông tin ở gốc trong mạng truyền thông và sự giải mã sau đó ở điểm nhận cuối cùng. *So sánh với* link encryption, node encryption. *Xem* encrypt, OSI socurity. *Đồng nghĩa với* end-to-end encipherment.

end user ***người sử dụng đầu cuối, người sử dụng trực tiếp*** Trong truyền thông, nguồn hoặc đích của luồng thông tin qua một hệ thống.

end user computing ***tính toán phía người sử dụng, xử lý phía người dùng*** Trong tin học, sự xử lý cá nhân thực hiện bởi người sử dụng đầu cuối, bao gồm phát triển chương trình, thông qua máy tính cá nhân hoặc terminal nối với máy tính chính. *Xem* fourth-generation language, information centre, personal computing.

end user device ***thiết bị người dùng đầu cuối*** Trong tin học, thiết bị (ví dụ như thiết bị hiển thị) cung cấp đầu ra cuối cùng của một thao tác mà không cần xử lý tiếp. *Xem* VDU.

enhanced services ***(các) dịch vụ cải tiến*** Trong truyền thông, dịch vụ sử dụng những phương tiện cơ bản do một hãng truyền thông công cộng cung cấp để đem lại những lợi ích bổ sung, khác hoặc lợi ích đã cơ cấu lại. Ở Mỹ các

dịch vụ cải tiến không bị điều chỉnh bởi Ủy ban truyền thông liên bang. *Xem* basic service, Computer Inquiry 1980, value-added network service.

Enigma ***virut Enigma*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trữ, lây nhiễm các tệp EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Enigma machine ***máy mã Enigma*** Trong mật mã, máy mã kiểu dùng nhiều roto do Đức và các đồng minh của Đức dùng trong Thế chiến hai.

ENQ *Xem* enquiry character.

enquiry character ***ký tự hỏi, ENQ*** Trong truyền thông dữ liệu, ký tự điều khiển dùng để yêu cầu sự đáp ứng từ một trạm ở xa. Đáp ứng có thể bao gồm nhận dạng trạm và kiểu thiết bị đang sử dụng.

enrolment ***lấy mẫu, nạp mẫu*** Trong kiểm soát truy nhập, thủ tục dùng trong các hệ kiểm soát truy nhập sinh trắc để lấy và nhập mẫu sinh trắc đối với người sử dụng mới vào hệ thống nhớ kiểm soát truy nhập. *Xem* biometrics.

entity ***thực thể*** Trong các cơ sở dữ liệu, đối tượng hoặc biến cố mà thông tin về nó được lưu giữ trong một cơ sở dữ liệu. *So sánh với* attribute, relationship.

entity identifier ***khóa nhận dạng thực thể*** Trong các cơ sở dữ liệu, khóa nhận dạng một cách duy nhất một thực thể. *Xem* key.

entrance delay ***độ trễ vào*** *Xem* delay circuit.

entrapment ***(sự) đặt bẫy, (sự) cài bẫy*** Trong an toàn máy tính, kỹ thuật gây sự chú ý tới các chỗ yếu đối với một kẻ tấn công tiềm tàng. Sau đó, bố trí dụng cụ tại những điểm yếu đó để phát hiện và ghi lại các cuộc tấn công. Kỹ thuật này có nhược điểm là những nỗ lực chú ý nhằm hấp dẫn người dùng thử tấn công có thể mang tính hợp pháp đáng ngờ. *Xem* pseudo-flaw, vulnerability.

entropy ***entropy*** Trong toán học, giá trị trung bình của số đo thông tin chuyển tải bởi lần xuất hiện một biến cố bất kỳ trong một số hữu hạn các biến cố loại trừ nhau. Entropy $H(x)$ đối với biến cố x với xác suất xuất hiện $p(x)$ được cho bởi

$H(x) = -p(x)\log p(x)$.

Xem information theory.

entry ***mục nhập*** *Xem* between-the-lines entry.

entry date ***ngày tháng nhập*** Trong hoạt động ngân hàng, ngày tháng mà các mục nhập được thực hiện ở các bản ghi của một tài khoản. *Đồng nghĩa với* posting date.

envelope ***đường bao; byte bao*** (1) Trong truyền thông dữ liệu, đường bao là đường nối các biến thiên biên độ của sóng mang điều biên. *Xem* amplitude modulation, envelope pattern. (2) Trong truyền thông dữ liệu, byte bọc là byte mà một số bit bổ sung được thêm vào cho các mục đích điều khiển và kiểm tra.

environment ***môi trường*** (1) Toàn bộ các tình huống, các điều kiện và các đối tượng bên ngoài ảnh hưởng tới sự phát

triển, sự vận hành và sự bảo trì của một hệ thống; (2) Trong an toàn máy tính, các yếu tố bên trong lẫn bên ngoài của một hệ ADP giúp xác định các rủi ro gắn liền với hoạt động của nó, ví dụ như các giao diện bên trong hệ ADP, phần mềm kết hợp, loại và mức độ thông tin chứa trong hệ ADP, các cơ cấu kiểm soát truy nhập dùng để hạn chế truy nhập và các đặc trưng vật lý của vùng hoạt động. *Xem* access control, ADP, physical, security.

EOA *Xem* end of address.

EOB *Xem* end of block.

EOF *Xem* end of file.

EOM *Xem* end of message.

EOT *Xem* end of transmission.

EPL *Xem* Evaluated Products List.

EPOS ***EPOS*** Viết tắt của Electronic point of sale (điểm bán hàng điện tử). *Xem* EFTPOS, point of sale.

EPROM ***EPROM*** (1) Trong tin học, viết tắt của Erasable Programmed Read Only Memory (bộ nhớ chỉ đọc được lập trình xóa được). (2) Trong tin học, viết tắt của Electrically Programmable Read Only Memory (bộ nhớ chỉ đọc lập trình) được bằng điện. *Xem* electrically programmable read only memory, erasable programmed read only memory. *Đồng nghĩa với* EAPROM.

equal error rate ***đồng suất lỗi*** Trong kiểm soát truy nhập, chỉ thiết bị sinh trắc với tỷ lệ loại bỏ giả và tỷ lệ chấp nhận giả bằng nhau. *Xem* biometrics, false acceptance rate, false rejection rate.

equalization ***bù, san bằng*** Trong truyền thông, thuật ngữ chung chỉ hệ thống được thiết kế để bù một dạng thiếu hụt nào đó trong đáp tuyến tần số. *Xem* loading.

equipment check ***kiểm tra thiết bị*** Trong an toàn máy tính, thiết bị cài trong ở một hệ máy tính để kiểm tra độ chính xác của dữ liệu đã xử lý, truyền đi hoặc được lưu giữ.

equivocation ***độ mập mờ, độ bất định*** Trong lý thuyết thông tin, entropy điều kiện. Nếu thông báo X là điều kiện đối với biến cố Y thì độ bất định của X khi cho trước Y được cho bởi:

$$H_y(X) = -\sum_y P(Y) \sum_y P_y(X) \log_2(P_y(X))$$

Trong đó $P(Y)$ = xác suất của biến cố Y và $P_y(X)$ = xác suất của biến cố X trong điều kiện xảy ra biến cố Y. *Xem* entropy, key equivocation.

erasable programmed read only memory ***bộ nhớ chỉ đọc được lập trình xóa được.*** *Xem* PROM.

erasable storage ***bộ nhớ xóa được*** (1) Trong tin học, thiết bị nhớ mà dữ liệu của nó có thể thay đổi trong quá trình tính toán. (2) Trong các hệ thống nhớ, vùng bộ nhớ dùng cho các mục đích tạm thời. (3) Trong các hệ thống nhớ, phương tiện nhớ có thể xóa được và sử dụng lặp lại (ví dụ, bộ nhớ đĩa từ).

erasure ***(sự) xóa, (sự) tẩy*** (1) Trong an toàn máy tính, một quy tắc mô hình an toàn nói rằng, các đối tượng phải được làm sạch trước khi được kích hoạt hoặc gán lại. Điều đó đảm bảo rằng không thông tin nào còn được giữ lại

bên trong đối tượng khi nó được gán lại cho một chủ thể ở một mức an toàn khác. *Xem* object, object reuse, subject. (2) Trong an toàn máy tính, quá trình nhờ đó một tín hiệu được ghi trên phương tiện từ tính được loại bỏ (tức là được khử từ). Xóa có thể được thực hiện theo hai cách: trong cách xóa bằng AC, phương tiện được khử từ bằng cách tác dụng một trường dòng xoay chiều mà biên độ giảm từ một giá trị cao ban đầu (tức là được cấp nguồn AC); trong cách xóa bằng DC, phương tiện được làm bão hòa bằng cách tác dụng trường dòng một chiều (tức là được cấp nguồn DC hoặc bằng cách sử dụng một nam châm vĩnh cửu). *Xem* degauss.

EROM ***EROM*** Trong tin học, viết tắt của Erasable Read Only Memory (bộ nhớ chỉ đọc xóa được). *Đồng nghĩa với* electrically alterable ROM.

error ***sai số; lỗi*** (1) Trong toán học, sai số chênh lệch giữa giá trị tính toán hoặc đo được và một giá trị chuẩn khách quan nào đó. *Xem* error condition. (2) Trong an toàn thông tin, lỗi là một vi phạm đối với sự xử lý tinh tế đúng. *Xem* correct refinement.

error burst ***chùm lỗi*** Trong truyền thông dữ liệu, chuỗi các lỗi liên tiếp. Các lỗi xuất hiện thành các nhóm hoặc chùm không phải điều bất thường.

error condition ***điều kiện lỗi*** Trong tin học, trạng thái nảy sinh từ nỗ lực thực hiện các lệnh không hợp lệ hoặc thao tác trên các dữ liệu không hợp lệ. *Xem* instruction.

error correction code ***mã sửa lỗi, ECC*** Trong các mã, mã được thiết kế để phát hiện lỗi, ở một từ hoặc ký tự, nhận dạng bit hoặc các bit không đúng và thay thế chúng bằng bit hoặc những bit đúng. Số bit không đúng có thể được sửa phụ thuộc vào số bit dư dùng trong mã. *So sánh với* error-detection code. *Xem* Hamming code, redundancy. *Đồng nghĩa với* selfcorrecting code.

error detection code ***mã phát hiện lỗi, EDC*** Trong các mã, mã được thiết kế để phát hiện nhưng không sửa lỗi trong một từ hoặc ký tự. Số bit không đúng mà có thể được phát hiện phụ thuộc vào số bit dư trong mã. *So sánh với* errorcorrection code. *Xem* parity checking.

error extension ***mở rộng lỗi*** Trong mật mã, hiệu ứng nảy sinh khi các kênh truyền thông tạp nhiễu gây ra các lỗi, hoặc một kẻ tấn công đưa vào những thay đổi trong bản mật mã đã truyền, và những lỗi đó dẫn đến những lỗi thậm chí dài hơn ở văn bản gốc thu được sau đó. Ví dụ, trong chế độ liên kết khối mật mã, một lỗi bit đơn ở bản mã sẽ tạo ra một khối bản gốc 64 bit bị bóp méo và lỗi một bit đơn ở khối bản gốc kế tiếp. *Xem* cipher block chaining, cipher feedback. *Đồng nghĩa với* error propagation, garble extension.

error message ***thông báo lỗi*** Trong tin học, thông báo cho biết rằng máy tính đã phát hiện lỗi trong pha dịch hoặc thực hiện một chương trình.

error propagation ***lan truyền lỗi*** *Đồng nghĩa với* error extension, garble extension.

error rate ***tần suất lỗi, tỷ lệ lỗi*** Trong truyền thông dữ liệu, tần số xuất

hiện các lỗi, được định nghĩa như tỷ số số bit thu được không đúng trên tổng số bit thu được.

error recovery service message ***thông báo dịch vụ khôi phục lỗi*** *Xem* ANSI X9.17 - 1985.

error service message ***thông báo dịch vụ lỗi*** Trong quản lý khóa, thông báo được gửi đi để báo cáo một lỗi trong thông báo dịch vụ mật mã. *Xem* ANSI X9.17 - 1985, cryptographic service message.

error source statistics ***thống kê nguồn lỗi*** Trong kiểm toán, sự tích lũy thông tin về kiểu và nguồn gốc của các lỗi, dùng để xây dựng các biện pháp sửa chữa nhằm giảm các lỗi như thế.

ERS *Xem* error recovery service message.

ESC *Xem* escape code.

escape character ***ký tự thoát*** *Xem* escape code.

escape code ***mã thoát, ESC*** Trong các mã, tổ hợp mã khiến cho một thiết bị nhận ra tất cả các tổ hợp mã sau đó như là có nghĩa khác so với biểu diễn bình thường của chúng. Các mã thoát dùng để chỉ báo dãy các thông báo điều khiển ở dạng mã ASCII. *Xem* ASCII. *Đồng nghĩa với* flag code.

escorts ***đội dẫn đường, đội hộ tống*** Trong an toàn vật lý, nhân sự được chỉ định đúng đắn có các mức thông (truy nhập) và các mức ủy quyền truy nhập thích hợp đối với các tư liệu chứa trong hệ thống và đủ thông thạo để hiểu được những hệ quả an toàn của việc kiểm soát và kiểm soát các hoạt động và sự truy nhập của cá nhân đang được hộ tống.

escow agent ***người được ủy nhiệm lưu giữ, đại diện lưu giữ*** Trong bảo vệ phần mềm, người môi giới trung thực được sử dụng để giải quyết các bất hòa giữa người cung cấp phần mềm và người có môn bài. Người cung cấp ký thác mã nguồn cho người đại diện để giữ an toàn, và người có môn bài (được chuyển nhượng) sẽ có quyền sử dụng nó trong trường hợp vỡ nợ của người cung cấp hoặc không trợ giúp thích hợp. *Xem* source code.

EMS ***EMS*** *Xem* ANSI X9.17 - 1985, error service message.

escrow cryptography ***mật mã ủy nhiệm*** Một vài năm trở lại đây, việc sử dụng rộng rãi mạng thông tin Internet đã tạo nên việc sử dụng mật mã tràn lan, dẫn tới việc các chính phủ không thể kiểm soát nổi thông tin, thu thập hồ sơ, kiểm soát sự nghe trộm, chỉnh đốn kinh tế và thậm chí thu thuế...

Một mô hình mật mã mới - mật mã khóa ủy nhiệm - được đưa ra như một biện pháp hữu hiệu nhằm giúp chính phủ kiểm soát tình trạng nêu trên. Đó là sự kết hợp mật mã mạnh với khả năng giải mã trong trường hợp khẩn cấp. Nó có một khóa khôi phục dữ liệu để thuận tiện cho việc giải mã trong trường hợp khẩn cấp. Khóa này không cần là khóa được dùng để giải mã thông thường mà có thể chỉ cung cấp cách truy nhập đến khóa đó. Khóa khôi phục dữ liệu được người được ủy quyền có tín nhiệm giữ, thường là một tổ chức của chính phủ, tòa án hoặc một

tổ chức tư nhân được tín nhiệm. Khóa có thể được chia nhỏ cho vài cơ quan như vậy giữ. Các tổ chức đã đăng ký với cơ quan ủy nhiệm có thể yêu cầu các khóa riêng cho họ để giải mã trong những trường hợp khẩn cấp. Các cơ quan điều tra hay cơ quan tình báo sẽ truy nhập đến các tệp lưu trữ hay lưu chuyển trên mạng bằng các ứng dụng thông qua các thủ tục thích hợp và làm đúng các yêu cầu đề ra về khóa. Những yêu cầu chính đáng về tính riêng tư sẽ được bảo vệ qua các giao thức truy nhập, kiểm toán và các biện pháp bảo vệ khác.

Tháng 4/1993, để đáp lại những nhu cầu đang tăng lên về sử dụng các sản phẩm mật mã, chính quyền Clinton đã thông báo một luật mới cho phép các cơ quan điều tra được ủy quyền dùng cách giải mã hợp pháp để chặn bắt hay tìm kiếm các tệp (file) lưu trên máy tính hay truyền trên kênh. Các cơ quan chính phủ đã triển khai một chính sách mật mã toàn diện, điều tiết giữa nhu cầu đảm bảo giữ bí mật cá nhân cho các công dân và doanh nghiệp với khả năng cho các cơ quan được ủy quyền của chính phủ truy nhập đến thông tin và dữ liệu theo trật tự luật pháp và tòa án. Một phần trong sự khởi xướng này là việc chính phủ triển khai một chip mã ủy nhiệm được gọi là chip Clipper. Mỗi chip Clipper là một khóa duy nhất được lập trình sẵn trên chip và được dùng để khôi phục dữ liệu đã mã bằng chính chip đó. Khóa này được chặt nhỏ thành hai phần, mỗi phần được một cơ quan chính phủ giữ một cách độc lập. Thuật toán mã dữ liệu của chip Clipper là Skipjack - một thuật toán được giữ bí mật do Cục An ninh Quốc gia thiết kế. Nó có kích thước khóa 80 bit. Những chi tiêu kỹ thuật chung của chip Clipper đã được thông qua và chấp nhận vào 2/1994 và được gọi là Chuẩn Mã Ủy nhiệm (EES) được dùng cho cả liên lạc điện thoại, fax và dữ liệu. Việc thực hiện EES đòi hỏi dùng mạch cứng chống giả mạo để bảo vệ các thuật toán mật. Chip và hệ thống ủy nhiệm khóa kèm theo được thiết kế với bộ phận an toàn mở rộng gồm hai pháp nhân kiểm soát và kiểm toán nhằm chống lại việc sử dụng trái phép các khóa.

Cục An ninh Quốc gia cũng thiết kế một chip cải tiến hơn gọi là Capston như một phần của sự khởi đầu hệ thống thông tin an toàn nhiều mức (MISSI). Nó được nhúng trong một tấm thẻ Fortezza (cạc PCMPCI) được dùng để cung cấp các dịch vụ mật mã cho việc giữ bí mật các tệp lưu và lưu chuyển. Các khóa mật được dùng cho thiết lập khóa và chữ ký số được lưu trên thẻ Fortezza nhưng không được lưu trong hệ thống ủy nhiệm khóa Clipper. Tuy nhiên, chúng được ủy nhiệm cùng với người có thẩm quyền xác nhận khóa công khai (của người sử dụng) để có thể khôi phục lại trong trường hợp thẻ bị hỏng hay bị sửa đổi. Điều này cho phép đọc lại được các tệp mã và các thông báo điện tử nhận được trước đó. Ngoài khả năng cung cấp bí mật và giải mã khẩn cấp, mật mã ủy nhiệm được xem như một cách khắc phục những hạn chế xuất khẩu, phổ biến đối với nhiều nước bị hạn chế về mật mã mạnh trong việc bảo vệ các bí mật quốc gia

của mình. Với khóa ủy nhiệm, mật mã mạnh có khả năng xuất khẩu có thể được chuẩn hóa và có mang tính quốc tế để hỗ trợ các nhu cầu bảo mật thông tin trong thương mại quốc tế. Mật mã ủy nhiệm khóa là một biện pháp đáp ứng được các yêu cầu giữ bí mật và khôi phục dữ liệu của các tổ chức, trong khi vẫn cho phép chính phủ truy nhập hợp pháp để chống tội phạm và khủng bố. Nó có thể tạo điều kiện dễ dàng phổ biến các chuẩn và các sản phẩm hỗ trợ các nhu cầu an toàn thông tin của cơ sở hạ tầng thông tin toàn cầu. *Xem* PKI, public key cryptography.

espionage ***hoạt động tình báo*** Trong lập pháp, sự thu thập bất hợp pháp thông tin độc quyền hoặc bí mật bằng bất kỳ phương tiện nào.

essential elements of friendly information ***thông tin cốt lõi*** Thông tin liên quan tới một kế hoạch, đề án hoặc hoạt động mà nếu đối phương thu được bằng bất kỳ cách nào cũng có thể gây nguy hiểm cho sự thực hiện thành công một hoạt động.

essentiality ***mức cốt yếu, dữ liệu chủ chốt*** Trong quản lý rủi ro, chỉ dữ liệu có tầm quan trọng cao đối với người sử dụng, mà nếu nó bị mất đi do sửa đổi cố ý hoặc đánh cắp thì phải rất tốn kém mới khôi phục được.

Estelle State Transition Language ***ngôn ngữ chuyển tiếp trạng thái Estelle*** Trong truyền thông dữ liệu, ngôn ngữ đặc tả giao thức. *Xem* protocol.

Ethernet ***mạng Ethernet*** Trong truyền thông dữ liệu, nhãn thương mại của một sản phẩm đặc biệt thực hiện theo tiêu chuẩn IEEE 802.3 dành cho mạng cục bộ sử dụng chế độ truyền dải cơ sở ở 10 megabit trên giây, cáp đồng trục, topo bus và giao thức đa truy nhập cảm biến sóng mang có dò xung đột. Ban đầu nó được Xerox phát triển. *So sánh với* Cambridge Ring. *Xem* IEEE 802.3, local area network.

ETPL *Xem* Endorsed Tempest Products List.

ETR *Xem* evaluation technical report.

ETX *Xem* end of text.

Euclid's algorithm ***thuật toán Euclid*** Trong lý thuyết số, phương pháp xác định ước số chung lớn nhất của hai số nguyên. Hãy xét hai số 42 và 27, phương pháp được minh họa như sau:

$42/27 = 1 + 15/27$

$27/15 = 1 + 12/15$

$15/12 = 1 + 3/12$

$12/3 = 4 + 0$

Ước số chung lớn nhất là mẫu số của thương không có dư, tức là 3. Thuật toán có những ứng dụng trong mật mã khóa công khai trong đó cần xác định một nghịch đảo trong số học modulo, tức là $w.w^{-1} = 1 \pmod{n}$, trong đó w là nguyên tố cùng nhau với n và cần xác định w^{-1}. Bài toán là tương đương với xác định hai số nguyên w^{-1} và k sao cho $w.w^{-1} = k.n + 1$. *Xem* coprime, greatest common divisor, knapsack cipher.

Euler's Generalization ***suy rộng Euler*** Trong lý thuyết số, với mỗi số nguyên b và n sao cho ước số chung lớn nhất của b và n là 1 thì:

$b^{\phi(n)} \pmod{n} \equiv 1$.

Trong đó $\phi(n)$ là hàm Euler. *Xem* coprime, Euler totient function, Fermat's Theorem, greatest common divisor, knapsack cipher, mod n.

Euler totient function ***hàm Euler*** Trong lý thuyết số, số các phần tử trong một tập rút gọn của các phần dư với một số nguyên n cho trước, thường được ký hiệu là $\phi(n)$. Nó bằng số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. *Xem* relatively prime, reduced set of residues, RSA.

Euronet ***mạng Euro, Euronet*** Trong truyền thông dữ liệu, mạng truyền dữ liệu do các chuyên viên viễn thông của các nước thành viên EEC chuẩn bị cho EEC. Những người sử dụng Euronet có khả năng truy nhập thông tin chuyên ngành khoa học, kỹ thuật và kinh tế thông qua mạng chuyển mạch gói mạng này lại được nối với hệ thống điện thoại công cộng của các nước thành viên. *Xem* DIANE, packet switching.

European Information Network ***Mạng tin học Châu Âu*** Trong truyền thông dữ liệu, dự án của Châu Âu được thiết lập để phối hợp nghiên cứu đối với các mạng và thúc đẩy sự thỏa thuận về các chuẩn. Nhiệm vụ đầu tiên của nó là xây dựng một phân mạng chuyển mạch gói, mạng vòng bắt đầu hoạt động vào năm 1976. *Xem* packet switching.

Evaluated Products List ***danh sách sản phẩm đã đánh giá*** Danh sách kiểm kê đã lập hồ sơ về phần cứng và phần mềm máy tính tin cậy khả dụng trong thương mại vốn đã được Trung tâm an toàn máy tính quốc gia đánh giá dựa vào các tiêu chuẩn đánh giá hệ thống máy tính tin cậy của Bộ quốc phòng Hoa Kỳ. *So sánh với* Endorsed Tempest Products List, Preferred Products List.

evaluation ***(sự) đánh giá, (sự) ước lượng*** Trong an toàn máy tính, báo cáo của người đánh giá gửi cho Cơ quan phê duyệt được chỉ định, mô tả các thủ tục nghiên cứu và thử nghiệm dùng trong phân tích các đặc điểm an toàn hệ thống ADP, nó có một bản mô tả và các kết quả thử nghiệm dùng để hỗ trợ hoặc bác bỏ những điểm yếu hệ thống riêng mà qua đó, có thể thu được tư liệu đã phân loại nhận dạng được từ các tệp dữ liệu an toàn hoặc được bảo vệ. *Xem* ADP, designated approving authority.

evaluation technical report ***báo cáo đánh giá kỹ thuật*** Trong an toàn thông tin, báo cáo do một phương tiện đánh giá an toàn công nghệ thông tin và được đệ trình lên cơ quan cấp chứng nhận. Báo cáo ghi chi tiết các kết quả đánh giá và trở thành cơ sở của giai đoạn chứng nhận việc đánh giá một mục tiêu. *Xem* certification body, information technology security evaluation criteria, information technology security evaluation facility, target of evaluation.

evaluator ***người đánh giá*** Trong an toàn máy tính, người được chỉ định đặc biệt để tham gia duyệt đội thử nghiệm, phân tích, thử nghiệm và đánh giá các đặc điểm an toàn của hệ thống tự động hóa. *Xem* evaluation.

EVD *Xem* electronic vibration detector.

even parity ***tính chẵn*** *Xem* parity.

event code ***mã biến cố*** Trong an toàn vật lý, tín hiệu do một bộ truyền thông số sinh ra cho biết loại báo động. *Xem* digital communicator.

event sequence analysis ***phân tích dãy biến cố*** *Xem* static analysis.

exchangeable disk storage ***bộ nhớ đĩa thay đổi được*** Trong tin học, một hoặc nhiều bộ đĩa với các chồng đĩa mà người vận hành có thể thay thế được. *Xem* disk pack.

EXCLUSIVE OR ***phép loại trừ - hoặc, phép tuyển loại, EXCLUSIVE OR, XOR*** Phép toán logic, *A* EXCLUSIVE OR *B* là đúng nếu hoặc *A*, hoặc *B*, chứ không phải cả hai, là đúng. Bảng chân lý tương ứng là:

A	*B*	*A* EXCLUSIVE OR *B*
0	0	0
1	0	1
0	1	1
1	1	0

Xem data encryption standard.

execute protection ***bảo vệ chạy chương trình, bảo vệ chống sao chép*** Trong bảo vệ phần mềm, sử dụng các biện pháp bảo vệ để ngăn ngừa không cho chương trình được thực hiện sau khi nó đã bị sao chép.

Phần lớn các sơ đồ bảo vệ đều phụ thuộc đĩa nguồn được xác định duy nhất bởi "dấu tay", không thể sao được qua đĩa mềm khác. Khi chương trình được bảo vệ bắt đầu thực hiện, nó kiểm tra xem có dấu tay, như dấu đốt hoặc các bit yếu không. Nếu có thì quá trình thực hiện sẽ tiếp tục, nếu không thì kết thúc.

Dấu tay phải có ba thuộc tính: nó phải là duy nhất, không sao chép được và không thể dò ra được. Nhược điểm của các sơ đồ bảo vệ như vậy là chúng ngăn cản việc lấy hợp pháp các bản sao dự phòng của phần mềm và chương trình được bảo vệ thường không thể làm việc trên đĩa cứng.

Nói chung, vì phần lớn các sơ đồ chống sao chép đều đòi hỏi kiểm tra sự có mặt của dấu tay nên chúng đều có thể bị bỏ qua bởi một đoạn mã sửa tạm. Với thế hệ các công cụ gỡ rối hiện nay, nhiệm vụ này không quá khó đối với một chuyên gia.

Chương trình sao chép đủ tinh ranh có thể sao được hầu như mọi đặc tính. Cái gì không thể sao được bằng một chương trình sao chép thì thường có thể làm cho làm việc được với những công cụ khác. *Xem* bit copier, burn mark, debugger, demon, diskette, dongle, fingerprint, install-deinstall, patch, weak bits.

executive state ***trạng thái thi hành, trạng thái điều hành*** Trong an toàn máy tính, một trong hai trạng thái khả dĩ chung trong đó một hệ ADP có thể hoạt động và chỉ có một số lệnh đặc quyền có thể được thực hiện; những lệnh đặc quyền như thế có thể không được thực hiện khi hệ hoạt động trong một trạng thái khác, trạng thái của người sử dụng. *Xem* ADP. *Đồng nghĩa với* supervisor state.

exhaustive attack ***tấn công toàn diện, tấn công vét cạn*** (1) Trong an toàn dữ liệu, sự tấn công nhằm khám

phá các dữ liệu bí mật bằng cách cố thử mọi khả năng và kiểm tra tính đúng đắn. (2) Trong phân tích mật mã, kỹ thuật trong đó các ý đồ được thực hiện để thu được bản gốc hoặc khóa mật mã bằng các phương pháp dò tìm trực tiếp. *So sánh với* analytical attack. *Xem* cryptographic key, key exhaustion, message exhaustion, plaintext.

exit button ***núm thoát*** (1) Trong an toàn vật lý, núm bấm dùng để thoát khỏi một vùng bị kiểm soát khi bộ đọc thẻ chỉ được sử dụng để vào. *Xem* card reader. (2) Trong an toàn vật lý, phương pháp tạm thời bỏ qua một mạch báo động để cho phép thoát ra ngoài.

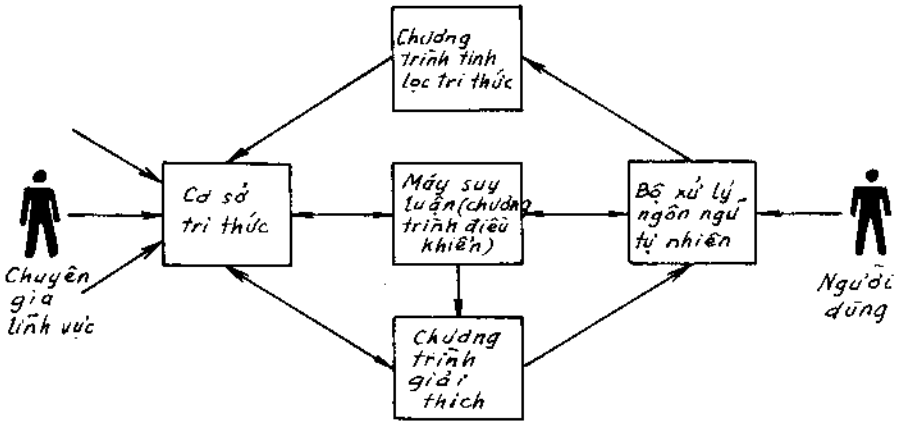
expander board ***bo mạch mở rộng*** *Đồng nghĩa với* expansion card.

expansion board ***tấm mạch mở rộng*** *Đồng nghĩa với* expansion card.

expansion card ***bìa mở rộng, tấm mạch mở rộng, cạc mở rộng, bo mạch mở rộng*** Trong tin học, bo mạch bổ sung vào hệ thống để lắp các chip hoặc mạch bổ sung nhằm tăng cường khả năng của hệ thống (ví dụ, modem, bộ nhớ chỉ đọc bổ sung). Ở máy vi tính, bo mạch mở rộng thường nối trực tiếp với bus hệ thống. *Xem* add-in, bus, encryptor board, microcomputer, MODEM, RAM.

expert systems ***(các) hệ chuyên gia*** Trong các ứng dụng, hệ máy tính phản ánh các quá trình ra quyết định của một chuyên gia. Nó biểu hiện tri thức có tổ chức liên quan tới một lĩnh vực chuyên môn xác định và nhằm hoạt động như cố vấn tài tình, hiệu quả trong chi phí. *Xem* artificial intelligence.

expired password ***mật khẩu quá hạn, mật khẩu hết hiệu lực*** Trong an toàn máy tính, mật khẩu mà phải được người sử dụng thay đổi trước khi có thể hoàn thành đăng nhập vào hệ thống. *Xem* log in, password.



expert systems: *(các) hệ chuyên gia.*

exploitable channel ***kênh khai thác được*** Trong an toàn máy tính, kênh bất kỳ mà có thể dùng được hoặc phát hiện được bởi các chủ thể bên ngoài Cơ sở tính toán tin cậy. *Xem* subject, trusted computing base.

exploitable vulnerability ***điểm yếu có thể khai thác, điểm dễ tổn thương có thể khai thác được*** Trong an toàn thông tin, một điểm dễ tổn thương mà có thể khai thác được trong thực tiễn để làm tiêu tan cái đích an toàn của một mục tiêu đánh giá. *So sánh với* construction vulnerability, operational vulnerability, potential vulnerability. *Xem* information technology security evaluation criteria, target of evaluation, vulnerability.

exponent ***số mũ*** Trong toán học, số cho biết số lần mà một số khác, cơ số, phải lặp lại như thừa số. Các số mũ dương chỉ phép nhân, các số mũ âm chỉ phép chia và số mũ phân số chỉ căn số. *Xem* base.

exponentiation ***(sự) mũ hóa*** Trong toán học, phép toán nâng một số lên một lũy thừa: x lũy thừa n thực hiện phép nhân x với chính nó n lần hoặc bằng phép mũ hóa x với số mũ n. *Xem* exponent.

exponentiation cipher ***phép mã lũy thừa, phép mã mũ hóa*** Trong mật mã, mã pháp trong đó các quá trình mã hóa/giải mã liên quan tới nâng các thông báo gốc/bản mã lên các lũy thừa xác định (tức là mũ hóa) theo số học modulo. *Xem* Diffie-Hellman technique, exponentiation, mental poker, modulo arithmetic, Pohlig-Hellman cipher, RSA.

Export Administration Act of 1979 ***đạo luật Quản lý xuất khẩu 1979*** Trong lập pháp, luật của Hoa Kỳ hạn chế việc bán thiết bị liên quan tới an ninh quốc gia, ví dụ các vi chip, phần cứng và phần mềm máy tính cho Liên Xô cũ và các nước thuộc khối Xô viết cũ.

exportation ***xuất*** Trong truyền thông dữ liệu, quá trình khiến cho dữ liệu chảy từ thành phần mạng này sang thành phần mạng lân cận.

exposure ***mức lộ, mức phơi bày*** Trong an toàn máy tính, mức độ khả dụng tương đối của dữ liệu trong môi trường nó được sử dụng. Mức lộ là khía cạnh chính về tính dễ tổn thương của một hệ thống. *Xem* access, usage, vulnerability.

expression ***biểu thức*** (1) Trong toán học, đồng nhất thức hoặc quan hệ toán học. (2) Trong lập trình, tổ hợp ngôn ngữ nguồn của một hoặc nhiều phép tính. (3) Trong lập trình, ký hiệu trong một chương trình biểu diễn một giá trị.

extension ***phần mở rộng*** Trong tin học, một phần trong mô tả tệp. Thông thường, một mô tả tệp có dạng - ổ đĩa: tên tệp: phần mở rộng - và phần mở rộng được dùng để chỉ loại của tệp; loại tệp văn bản, loại tệp chương trình v.v.

external auditor ***người kiểm toán ngoài, người kiểm tra ngoài*** Trong hoạt động kiểm toán, đại diện của một hãng kế toán công được thuê để cho ý kiến khách quan, công bằng về các báo cáo tài chính của một tổ chức. *So sánh với* EDP auditor, internal auditor.

external data file ***tệp dữ liệu ngoài*** Trong các cấu trúc dữ liệu, tệp chứa dữ liệu được lựa tách riêng khỏi chương trình xử lý nó.

external interrupt ***ngắt ngoài*** Trong tính toán, ngắt không phải do một biến cố gây ngắt trong chương trình tạo nên mà do một thiết bị bên ngoài bộ xử lý, ví dụ thiết bị ngoại vi. *Xem* interrupt, peripheral.

external label ***nhãn ngoài*** Trong các hệ thống nhớ, nhãn nhận dạng gắn ngoài phần chứa môi trường tệp (ví dụ, nhãn dính gắn với hộp đĩa từ).

external schema ***sơ đồ ngoài*** *Đồng nghĩa với* subschema.

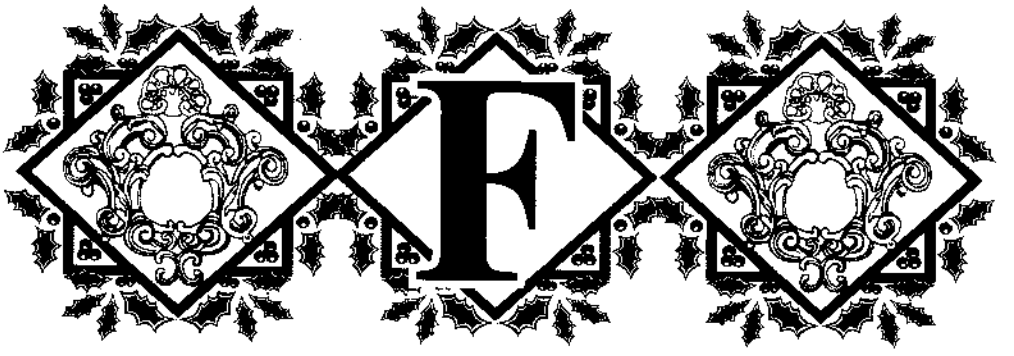
external security audit ***kiểm toán an toàn ngoài*** Trong an toàn máy tính, sự kiểm toán an toàn do một tổ chức độc lập với tổ chức đang được kiểm toán tiến hành. *So sánh với* internal security audit. *Xem* audit, security audit.

external timing ***định thời bên ngoài, đồng bộ bên ngoài*** Trong truyền thông dữ liệu, mục chọn ở một số modem trong đó đồng hồ hoặc các bit đồng bộ hóa được tạo ra từ bên ngoài, thường bằng đầu cuối dữ liệu mà modem được nối. *Xem* MODEM.

eye retina analysis ***phân tích võng mạc mắt*** Trong kiểm soát truy nhập, kỹ thuật sinh trắc dựa trên tính chất là các mẫu mạch máu của mắt là duy nhất đối với những người sử dụng, như tiến sĩ Robert Hill khám phá ra vào năm 1953.

Ở giai đoạn đăng nhập, người sử dụng đặt đầu của mình thẳng trên thiết bị, giữ cho mắt cách thấu kính chừng nửa insơ và tập trung vào mẫu nhìn giống thẳng. Sau đó người sử dụng nhấn núm khởi động quét võng mạc mắt; một nguồn sáng cường độ thấp quét một vùng tròn của võng mạc theo một cung 45 độ, chừng 320 số đọc điểm dữ liệu được lấy. Mẫu 40 byte được tạo ra nhờ thao tác đó dành cho các yêu cầu truy nhập về sau. Giai đoạn đăng nhập mất xấp xỉ một phút.

Khi yêu cầu truy nhập, người sử dụng chỉ đơn giản đặt mắt vào thị kính và thời gian nhận dạng là dưới 2 giây. Đó là một hệ sinh trắc đơn giản, thuận tiện và an toàn mà dường như ngày càng được chuộng trong lĩnh vực kiểm soát truy nhập. Các nhược điểm tiềm tàng duy nhất có thể này sinh đối với những người sử dụng bị khuyết tật, ví dụ những người phải ngồi xe đẩy không thể với tới được bộ quét. Một số người trong cộng đồng cũng có thể quan tâm tới việc các tia quét có thể gây hư hại cho mắt họ, mặc dù người ta cho rằng mọi lo lắng như thế là không có cơ sở. *Xem* biometrics.



facilities management ***quản lý phương tiện, FM*** Trong tin học, việc sử dụng một tổ chức dịch vụ độc lập để quản lý và vận hành cài đặt máy tính.

facility ***phương tiện*** Trong truyền thông dữ liệu, đường truyền giữa hai hoặc nhiều vị trí mà không có thiết bị chấm dứt hoặc báo hiệu.

facility code ***mã phương tiện*** Trong kiểm soát truy nhập, mã nhận dạng khách hàng hoặc vị trí của thiết bị trong kiểm soát truy nhập hoặc hệ báo động.

facility line ***đường thiết bị, kênh phương tiện*** Trong hoạt động ngân hàng, phương tiện riêng lẻ mở rộng tới một khách hàng, thuộc một loại phương tiện xác định trước. *Xem* facility type.

facility type ***loại phương tiện*** Trong hoạt động ngân hàng, tên đặt cho một thiết bị, ví dụ như bảo hiểm cho vay, ô bảo vệ. *Xem* facility line. *Đồng nghĩa với* product type, service type.

facsimile ***fax*** Trong truyền thông, chỉ sự truyền hình ảnh qua các tuyến truyền thông vốn có dải thông thấp hơn dải thông cần thiết cho các tín hiệu video. Hình ảnh được quét bởi chùm sáng và một tín hiệu thể hiện độ chói của phần ảnh dưới chùm quét được truyền qua tuyến dưới dạng tín hiệu tương tự hoặc số đã điều biến. Ở trạm thu, tín hiệu kích một nguồn năng lượng để tái tạo hình ảnh nhờ các kỹ thuật chụp ảnh, nhiệt hoặc in xero.

factor ***thừa số, nhân tử*** Trong toán học, một trong những số hoặc đại lượng bất kỳ là toán hạng trong phép nhân. *Xem* operand.

factoring ***rửa tiền; phân tích ra thừa số*** (1) Trong hoạt động ngân hàng, rửa tiền là việc gửi những số lượng lớn các khoản tiền rút doanh thu viết tay gian lận thông qua những lái buôn thông đồng, kim ngạch thấp ở

biên giới. (2) Trong an toàn dữ liệu, an toàn của hệ mật mã RSA phụ thuộc vào việc không có khả năng thực hiện bằng tính toán phép phân tích ra thừa số một tích lớn của hai số nguyên tố, mỗi số chừng 100 chữ số. Những cuộc tấn công như thế đã được thử bằng cách sử dụng năng lực máy tính dư thừa trên các mạng. *Xem* cryptography, prime number, RSA.

fail mafe ***tự an toàn, an toàn khi có sự cố*** (1) Trong an toàn máy tính, kết thúc và bảo vệ tự động các chương trình và/hoặc các hệ thống xử lý khi sự cố phần cứng hoặc phần mềm được phát hiện trong hệ thống tin tự động hóa. *Xem* principles of secure systems. (2) Trong an toàn vật lý, điều kiện trong đó, một sự cố hệ thống khiến thiết bị khóa lại để trở lại điều kiện mở, ví dụ cho phép cá nhân bỏ vùng bảo vệ. *So sánh với* fail secure. (3) Trong an toàn vật lý, hệ khởi đầu một báo động trong trường hợp sự cố nguồn hoặc hệ thống. *So sánh với* fail secure.

fail secure ***tự khóa*** Trong an toàn vật lý, chỉ điều kiện trong đó sự cố hệ thống khiến cho thiết bị khóa trở về điều kiện bị khóa. *So sánh với* fail safe.

fail soft ***gần tự an toàn, an toàn mềm*** (1) Trong an toàn máy tính, kết thúc có chọn lọc quá trình xử lý không cần bàn bị ảnh hưởng khi sự cố phần cứng hoặc phần mềm được phát hiện trong một hệ thống tự động hóa. *So sánh với* fail safe. (2) Trong kỹ thuật an toàn, chỉ hệ vẫn tiếp tục hoạt động mặc dù theo cách kém hơn, ngay cả khi một phần của hệ thống bị sự cố.

failure access ***truy nhập do sự cố*** Trong an toàn máy tính, sự truy nhập không được phép và thường thiếu thận trọng vào dữ liệu do sự cố phần cứng hoặc phần mềm trong hệ ADP. *Xem* access control, ADP.

failure control ***kiểm soát sự cố*** Trong an toàn máy tính, phương pháp luận dùng để phát hiện và khôi phục khả năng an toàn khi có sự cố hoặc an toàn mềm từ các sự cố phần cứng và phần mềm trong hệ ADP. *Xem* ADP, fail safa, fail soft.

fall back ***thủ tục dự phòng*** Trong tin học, các thủ tục dự trữ để dùng trong trường hợp có sự cố các dịch vụ hoặc máy. Những thủ tục đó có thể là thủ công hoặc liên quan tới sử dụng những máy tính và cơ sở dữ liệu khác.

false acceptance rate ***suất nghiệm thu sai*** Trong kiểm soát truy nhập, xác suất để lỗi loại 2 xuất hiện. *So sánh với* false rejection rate. *Xem* Type 2 error.

false rejection rate ***suất loại bỏ sai*** Trong kiểm soát truy nhập, xác suất để lỗi loại 1 xuất hiện. *So sánh với* false acceptance rate. *Xem* Type 1 error.

false solution ***nghiệm sai*** *Đồng nghĩa với* spurious key decipherment.

family ***họ*** Trong tin học, loạt các bộ xử lý của nhà sản xuất được bán để cho phép khách hàng nâng cấp thiết bị bằng thiết bị mạnh hơn mà không phải thay đổi phần còn lại của thiết bị hoặc các chương trình.

FAR *Xem* false acceptance rate.

fast connect circuit switching ***chuyển mạch nối nhanh*** Trong

truyền thông dữ liệu, dạng chuyển mạch trong đó một thiết bị đầu cuối quay số máy tính chủ, khi một dòng được nhập ở bàn phím thì dữ liệu được truyền đi và thiết bị đầu cuối ngắt cuộc gọi. *So sánh với* circuit switching.

fast data encipherment algorithm ***thuật toán mã dữ liệu nhanh*** Trong mật mã, thuật toán mật mã khối được các nhà nghiên cứu ở Công ty điện báo và điện thoại Nippon thiết kế để thay thế thuật toán mã hóa dữ liệu.

Mật mã sử dụng khóa 64 bit và khối bản gốc 64 bit; các phép mã thành phần tên là FEAL-*N*, trong đó *N* là số các vòng lặp.

- FEAL-4 cần sử dụng cho xác thực thông báo, liên lạc mật sử dụng chế độ CBC và các hàm băm 64 bit;
- FEAL-8 cần sử dụng cho liên lạc mật với chế độ CBC;
- FEAL-16 cần sử dụng cho xác thực thực thể ngang hàng, liên lạc mật với chế độ ECB;
- FEAL-32 cần sử dụng cho các ứng dụng cần an toàn cao trong môi trường không thân thiện bị rất nhiều những cuộc tấn công thám mã.

Các cuộc tấn công bản gốc đã chọn trên FEAL-4 và FEAL-8 đã được báo. *Xem* block cipher, CBC, chosen plaintext, data encryption standard, ECB.

Father Christmas ***virut Father Christmas*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND. COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

father file ***tập bố, file bố*** Trong tin học, phương pháp dùng trong cập nhật các tệp đĩa hoặc băng từ sao cho, trong trường hợp sai lạc nghiêm trọng hoặc mất dữ liệu thì có thể thiết lập lại tệp chủ. Khi tạo ra tệp mới là kết quả của việc cập nhật tệp hiện thời thì tệp chủ cũ được gọi là "tệp bố". Tệp mới đã cập nhật được gọi là "tệp con", trong khi đó tệp được dùng ban đầu để tạo ra tệp bố trở thành "tệp ông". *Xem* file.

fault ***sai sót, sự cố*** Trong quản lý rủi ro, điều kiện khiến cho thiết bị, thành phần hoặc linh kiện không thực hiện được theo cách cần thiết. Sự cố có thể là hoặc vật lý hoặc logic. *Đồng nghĩa với* loophole.

fault diagnosis ***chẩn đoán sự cố*** Trong kỹ thuật tin cậy, hoạt động nỗ lực định vị sự cố và giới hạn tác hại của nó.

fault tolerance ***khả năng kháng lỗi*** Trong kỹ thuật tin cậy, khả năng của hệ thống hoạt động đúng theo các chi tiết kỹ thuật của bản thiết kế của nó bất chấp những sai sót nhất thời hay thường trực.

fault trace ***vết sự cố*** Trong tin học, bản ghi các sự cố và các tình huống xuất hiện của chúng như xác định được nhờ một hệ giám sát được thiết kế đặc biệt.

fault tree ***cây sự cố*** Trong tin học, giản đồ cây cho các kỹ sư bảo trì đã hướng họ tới những quan sát cần thực hiện, những di chuyển cần thực hiện sau đó tùy thuộc vào những quan sát đó và những hoạt động sửa chữa cuối cùng. *Xem* tree.

F-AV ***lớp F-AV*** Trong an toàn thông

tin, lớp chức năng được định nghĩa trong ITSEC, xác định đối với các hệ thống đặt ra những yêu cầu cao đối với tính sẵn sàng của một hệ thống đầy đủ hoặc các chức năng đặc biệt của một hệ thống. Những yêu cầu cao như vậy rất quan trọng trong những lĩnh vực ứng dụng, ví dụ các hệ thống điều khiển quá trình. *Xem* ITSEC, TCSEC.

F-B1 ***lớp F-B1*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC chỉ rõ sự kiểm soát truy nhập bắt buộc, dẫn xuất từ lớp B1 của TCSEC. *So sánh với* B1. *Xem* mandatory access control, ITSEC, TCSEC.

F-B2 ***lớp F-B2*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, chỉ rõ sự kiểm soát truy nhập bắt buộc, dẫn xuất từ lớp B2 của TCSEC. *So sánh với* B2. *Xem* mandatory access control, ITSEC, TCSEC.

F-B3 ***lớp F-B3*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC chỉ rõ sự kiểm soát truy nhập bắt buộc, dẫn xuất từ lớp B3 của TCSEC. *So sánh với* B3. *Xem* mandatory access control, ITSEC, TCSEC.

FC ***FC*** *Xem* FC FIPS.

F-C1 ***lớp F-C1*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, định rõ sự kiểm soát truy nhập tùy ý, dẫn xuất từ lớp C1 của TCSEC. *So sánh với* C1. *Xem* discretionary access control, ITSEC, TCSEC.

F-C2 ***lớp F-C2*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, xác định kiểm soát truy nhập tùy ý, dẫn xuất từ lớp C2 của TCSEC. *So sánh với* C2. *Xem* discretionary access control, ITSEC, TCSEC.

FCAP *Xem* Fortran Complexity Analysis Program.

FCC *Xem* Federal Communications Commission.

FC-FIPS ***dự án FC-FIPS*** Trong an toàn máy tính, dự án liên doanh của Viện tiêu chuẩn quốc gia và Cơ quan an ninh quốc gia (Hoa Kỳ) nhằm tạo ra tiêu chuẩn xử lý thông tin liên bang để thay thế cho TCSEC.

Dự án đó sẽ phát triển một loạt các FIP và những tài liệu khác cung cấp các chuẩn cứ và sự hướng dẫn về an toàn trong các hệ điều hành và những lĩnh vực công nghệ thông tin khác như các mạng, các cơ sở dữ liệu và các ứng dụng. Các FC-FIPS nhằm mục đích hữu dụng cho một nền tảng rộng rãi những người sử dụng bao gồm các cộng đồng tư nhân, chính phủ dân sự và quốc phòng.

Dự án đầu tiên nghiên cứu các yêu cầu chức năng an toàn cho các hệ điều hành đa dụng nhiều người dùng. *Xem* information technology security evaluation criteria, MFSR, Orange Book, TCSEC.

FD *Xem* full duplex.

F-DC ***lớp F-DC*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, xác định cho các hệ với các nhu cầu cao về độ tin cậy của dữ liệu trong trao đổi dữ liệu. Ví dụ dự tuyển cho lớp này là thiết bị mật mã. *Xem* cryptography, ITSEC, TCSEC.

FDDI *Xem* fiber distributed data interface.

F-DI *lớp F-DI* Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, xác định cho các hệ có những yêu cầu cao đối với việc bảo vệ tính toàn vẹn dữ liệu trong quá trình trao đổi dữ liệu. *Xem* ITSEC, TCSEC.

FDM *Xem* frequency division multiplexing.

FDX *Xem* full duplex.

F-DX *lớp F-DX* Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, xác định cho các mạng có những nhu cầu cao về tính bí mật và tính toàn vẹn của thông tin cần trao đổi. Ví dụ, điều này có thể là trường hợp khi phải trao đổi thông tin nhạy cảm thông qua mạng không an toàn. *Xem* ITSEC, TCSEC.

FEAL *Xem* fast data encipherment algorithm.

FEC *Xem* foward error correction.

Federal Communications Commission *Ủy ban truyền thông liên bang, FCC* Tổ chức quy chế độc lập do Quốc hội Mỹ lập ra theo Luật truyền thông năm 1934 và được Luật trao quyền để điều hành các dịch vụ truyền thông vô tuyến và hữu tuyến trong nước và nước ngoài bắt nguồn từ Hoa Kỳ.

Federal Criteria *(các) tiêu chuẩn liên bang* *Xem* FC-FIPS.

federal funds *tiền liên bang, quỹ liên bang* Trong hoạt động ngân hàng, đôla của Hoa Kỳ gửi một ngân hàng dự trữ liên bang ở Hoa Kỳ.

Federal State Joint Board *Ban phối hợp bang của Liên bang* Trong truyền thông, ban do Ủy ban truyền thông liên bang Hoa Kỳ lập ra và gồm các ủy viên đại diện pháp quyền bang và liên bang. *Xem* Federal Communications Commission.

FedWire *hệ thống FedWire* Trong hoạt động ngân hàng, dịch vụ thanh toán do Hệ thống dự trữ liên bang Hoa Kỳ vận hành như một mạng hữu tuyến riêng dành cho các cuộc chuyển dữ liệu giữa các cơ sở tài chính có các tài khoản ở Ngân hàng dự trữ liên bang. *Xem* banking networks.

Feistel cipher *mã pháp Feistel* Trong mật mã, lớp các phép mã khối có các tính chất:

- kích thước khối m là chẵn, tức là $m = 2L_0$, từ đó khối bản gốc gồm hai phần mỗi phần có độ dài L_0, như vậy $P = (x_0, x_1)$;
- mỗi khóa xác định một tập hợp các khóa con $k_1, k_2, \ldots k_n$;
- Với mỗi khóa con k_i, có tương ứng một phép biến đổi F_i được xác định trên các khối độ dài L_0;
- khối bản gốc P được mã hóa trong h bước như sau:

  Bước 1: $(x_0, x_1) \rightarrow (x_1, x_2)$

  Bước i: $(x_{i-1}, x_i) \rightarrow (x_i, x_{i+1})$

  Bước h: $(x_{h-1}, x_h) \rightarrow (x_h, x_{h+1})$;

  Trong đó $x_{i+1} = x_{i-1} +_2 F_i(x_i)$
- khối bản mã C được cho bởi (x_h, x_{h+1});
- trước khi giải mã, hai nửa của C được đảo ngược và các khóa được cung cấp theo trình tự đảo ngược:

  Bước 1: $(x_{h+1}, x_h) \rightarrow (x_h, x_{h-1})$

  Bước h: $(x_2, x_1) \rightarrow (x_1, x_0)$;

  Trong đó $x_{i-1} = x_{i+1} +_2 F_i(x_i)$

Xem block cipher, data encryption standard.

Fellowship ***virut Fellowship*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

FEP *Xem* front end processor.

Fermat prime ***số nguyên tố Fermat*** Trong toán học, số nguyên tố dạng

$F_n = 2^m + 1$

trong đó $m = 2^n$

F_0, F_1, F_2, F_3 và F_4 là các số nguyên tố nhưng $F_5 = 4294967297$ lại không phải số nguyên tố. *So sánh với* Mersenne prime.

Fermat's Theorem ***định lý Fermat*** Trong toán học, nếu p là một số nguyên tố thì với mỗi số nguyên b mà mẫu số chung lớn nhất của b và p là 1 thì

$b^{p-1} \pmod p \equiv 1$

Xem Euler's Generalization, greatest common divisor, mod n.

fetch protection ***bảo vệ tìm nạp*** Trong an toàn máy tính, sự hạn chế do hệ thống dự phòng để ngăn ngừa chương trình truy nhập dữ liệu ở đoạn bộ nhớ của người sử dụng khác. *Xem* access, bounds checking.

Fiat Shamir algorithm ***thuật toán Fiat Shamir*** Trong mật mã, thuật toán chứng minh không để lộ thông tin có thể được Alice sử dụng để chứng minh danh tính của Alice cho Bob mà không để lộ đủ thông tin để Bob sau đó có thể dùng để giả mạo Alice. Một dạng thực hiện thuật toán được mô tả như sau.

- Một dịch vụ xác thực khai triển hai số nguyên tố lớn, p và q và công bố tích $n = p.q$, trong khi vẫn giữ bí mật của p và q. Tất cả những phép toán sau đó đều được thực hiện theo modulo n.
- Alice nhận được từ trung tâm dịch vụ số hiệu nhận dạng người dùng (ID) dựa trên (chẳng hạn) tên, địa chỉ v.v.. Một số QR sau đó được khai triển là hàm của ID và biến V. Với hiểu biết về p và q, ta có thể rút ra V và QR sao cho, QR có một căn bậc hai modulo n và tính căn bậc hai đó.
- Alice có nhiệm vụ chứng minh cho Bob rằng, mình biết căn bậc hai của QR mà không để lộ giá trị của nó.
- Alice gửi ID và V cho Bob;
- Bob biết thủ tục để tính QR từ ID và V;
- Bob tạo ra một dãy ngẫu nhiên gồm các số 1 và 0 và thực hiện các bước sau đây cho đến khi Bob bị thuyết phục rằng Alice biết căn bậc hai của QR.
- Alice chọn một số x, tính $t = x^2 \bmod n$ và gửi giá trị của t cho Bob;
- Bob chọn 1 hoặc 0 tiếp theo trong dãy ngẫu nhiên và gửi nó cho Alice;
- Nếu Alice nhận được 1 thì cô gửi tiếp tích $x.\sqrt{(QR)} \bmod n$ (tức là $x.\sqrt{(t.QR)} \bmod n$) cho Bob, nếu không Alice gửi x.
- Bob lấy bình phương số nhận được từ Alice và kiểm tra nó so với $t.QR \bmod n$ (nếu 1 được gửi cho Alice) hoặc so với t (nếu ngược lại).

Theo quan điểm của Bob, nếu Alice biết

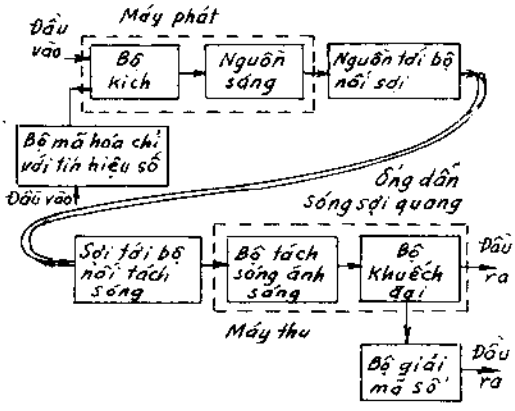
được dãy các số 0 và 1 cần gửi thì Alice có thể phát triển câu trả lời cần thiết mà không cần biết căn bậc hai của *QR*, tức là Alice có thể giả dạng như chủ thực sự của danh tính *ID*. Nếu Alice được yêu cầu gửi cả hai câu trả lời thì cô ta không thể lừa được nhưng Bob lại có thể có đủ thông tin để tính căn bậc hai của *QR*. *Xem* modulo arithmetic, zero knowledge proof.

fiber cross-talk ***xuyên âm sợi quang*** Trong quang điện tử học, sự trao đổi năng lượng sóng ánh sáng giữa lõi và lớp bọc của cáp sợi quang, lớp bọc và môi trường xung quanh hoặc giữa các lớp chỉ số khác nhau. Xuyên âm được giảm thận trọng bằng cách làm cho lớp bọc suy giảm. *Xem* core, fiber optics.

fiber distributed data interface ***giao dịch dữ liệu phân tán bằng sợi quang*** Trong truyền thông dữ liệu, kiến trúc vòng thẻ bài tính năng cao sử dụng sợi quang, hoạt động qua khoảng cách tới 200 kilomet ở tốc độ 100 Mbps. Mạng cáp bao gồm hai vòng, một truyền theo chiều kim đồng hồ và vòng kia ngược chiều kim đồng hồ. Nếu cáp bị ngắt, các role rẽ mạch ở các trạm lân cận kích hoạt, nối hai vòng ở mỗi phía của chỗ ngắt và tạo ra một vòng đơn dài gấp đôi các vòng riêng lẻ ban đầu. *Xem* token ring.

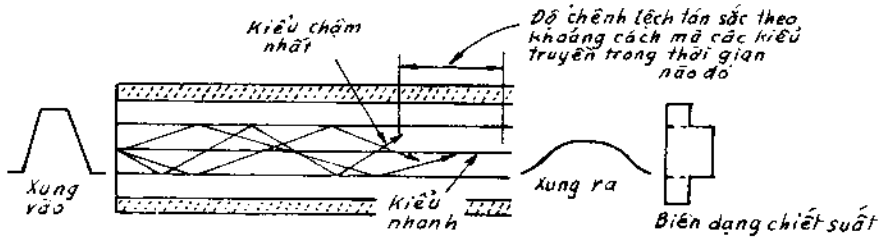
fiber optics ***quang sợi*** Trong truyền thông, kỹ thuật nghiên cứu sự truyền thông các tín hiệu bằng cách truyền ánh sáng qua những sợi thủy tinh hoặc chất dẻo cực kỳ tinh khiết.

Cáp sợi quang bao gồm lõi chất dẻo hoặc thủy tinh được bao quanh bằng lớp vỏ bọc chất dẻo hoặc thủy tinh, mà bên ngoài lại được bao bằng vỏ chất dẻo để bảo vệ lõi khỏi bị ẩm và mài mòn. Đường kính của lõi thay đổi theo loại sợi từ 2 tới 200 micromet. Các tín hiệu sáng được chèn vào từ các điot phát quang (LED) hoặc các laze phun, được truyền nhờ khúc xạ hoặc phản xạ trong và được gom lại bằng các bộ tách sóng ánh sáng ở đầu thu.



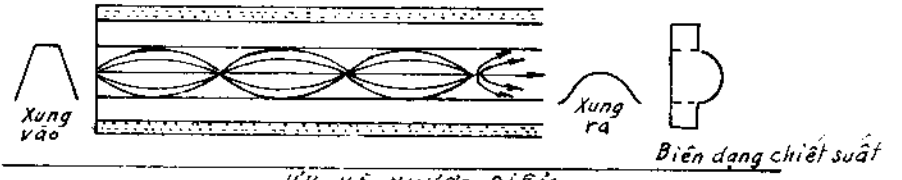
fiber optics: *quang sợi.* Hình 1. Các bộ phận cơ bản của hệ truyền sợi quang.

Sự lan truyền dọc theo cáp theo kiểu phản xạ hoặc khúc xạ là tùy thuộc vào loại cáp - đơn kiểu chỉ số bậc thang, đa kiểu chỉ số bậc thang hoặc đã kiểu chỉ số phân cấp. Ở đây thuật ngữ chỉ số là chỉ chiết suất (chỉ số khúc xạ) và như các tên gọi cho thấy, chiết suất của các sợi quang chỉ số bậc thang là không đổi trong suốt lõi và thay đổi đột ngột ở mặt phân cách lõi - lớp bọc, trong khi trong trường hợp sợi chỉ số phân cấp đa kiểu, chiết suất giảm từ từ từ tâm lõi tới biên ngoài của nó. Ở cáp đơn kiểu đường kính lõi rất nhỏ (2-10



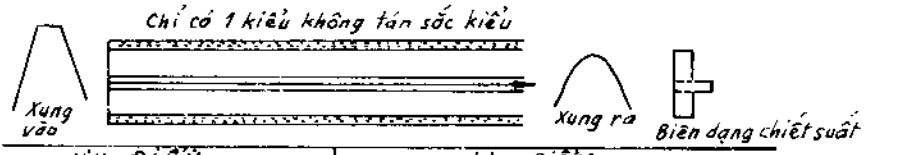
a)

ƯU ĐIỂM	NHƯỢC ĐIỂM
Rẻ, khẩu số lớn: gom ánh sáng tốt Dễ gánh cuối	Độ tán sắc lớn, dải thông tối thiểu: tốc độ vận hành thấp



b)

ƯU VÀ NHƯỢC ĐIỂM
Sợi đa kiểu chỉ số phân cấp là trung gian giữa hai loại sợi khác, các ưu điểm và nhược điểm nằm giữa hai loại sợi đó



c)

ƯU ĐIỂM	NHƯỢC ĐIỂM
Tán sắc tối thiểu, dải thông lớn: tốc độ làm việc cao, rất Hiệu quả	Khẩu số nhỏ: đòi hỏi nguồn sáng laze, Khó gánh cuối, Đắt

fiber optics: *quang sợi.* Hình 2.(*a*) sợi đa kiểu chỉ số bậc thang; (*b*) sợi đa kiểu chỉ số phân cấp; (*c*) sợi kiểu đơn chỉ số bậc thang.

micromet) và chỉ có một đường - dọc theo tâm của lõi - dành cho các tín hiệu ánh sáng. Với các sợi đa kiểu chỉ số bậc thang, tia sáng truyền dưới những góc khác nhau tới trục và phản xạ bên trong tại mặt phân cách lõi - lớp bọc. Trong trường hợp này, các tia sáng sẽ truyền theo các đường độ dài khác nhau và do vậy, các xung tín hiệu trải rộng và bị méo. Ở sợi chỉ số phân cấp các tia sáng truyền gần biên ngoài của lõi nhanh hơn so với dọc trục, bởi vì chiết suất thấp hơn. Hiệu ứng này có xu hướng làm giảm độ tán sắc vì các tia sáng truyền dọc theo các quãng đường dài hơn có xu hướng truyền nhanh hơn.

Các tín hiệu ánh sáng được tạo ra hoặc bởi các LED hoặc bởi laze phun. Các ưu điểm tương đối của laze phun so với LED là công suất ra cao hơn và chùm hẹp, nhưng chúng có xu hướng đắt hơn và có thời hạn làm việc ngắn hơn. Ánh sáng truyền đi thường ở dải hồng ngoại, sự suy giảm tín hiệu là rất nhạy với bước sóng, có xu hướng giảm khi

bước sóng tăng. Các ưu điểm của cáp sợi quang so với cáp đồng trục thông thường là tính chống nhiễu điện từ, dung lượng mang dữ liệu cao, độ suy giảm tín hiệu thấp tính an toàn, giá nguyên liệu, độ ổn định hóa học và không có nhiễu đồng kênh. Theo quan điểm an toàn dữ liệu thì cáp sợi quang có ưu điểm là chúng không phát ra tín hiệu tỏa tia và tương đối khó nối trộm, mặc dù chúng có thể bị nối trộm chủ động bởi loại sợi tinh quái. *Xem* compromising emanations, rogue fiber, Tempest proofing, wiretap.

field *trường* (1) Trong toán học, tập hợp các số nguyên mà các phép cộng, phép trừ, phép nhân, phép chia (trừ chia cho 0) trên chúng được định nghĩa và tuân theo các luật giao hoán, kết hợp và phân phối. Hệ phần dư đầy đủ, nghĩa là modulo một số nguyên tố, tạo thành một trường. Khái niệm trường liên quan chặt chẽ với số học modulo. Hãy xét một trường gồm các chữ số 1, 2, 3... 7, phép cộng và phép nhân có thể được định nghĩa để các kết quả là những phần tử của trường, ví dụ như:

4 + 6 = 3

3 x 5 = 1 v.v..

Hoặc là điều đó có thể được biểu thị theo số học modulo 7 (4 + 6) ≡ 3 (mod 7), (3 x 5) ≡ 1 (mod 7). *Xem* associative law, commutative law, complete set of residues, distributive law, Galois field, modulo arithmetic. (2) Trong xử lý dữ liệu, không gian vật lý ở một phương tiện ghi dữ liệu được dành cho một hoặc nhiều phần tử dữ liệu có liên quan. (3) Trong tin học, một phần tử của một bản ghi. *Xem* record.

field data code *mã dữ liệu quân sự* Trong mã hóa, mã truyền dữ liệu quân sự tiêu chuẩn hóa gồm bảy bit dữ liệu cộng với một bit chẵn lẻ. *Xem* bit, parity.

field separator *dấu tách trường, FS* Trong mã hóa, ký tự dùng để tách các trường hoặc những mục dữ liệu khác trong bộ nhớ, sự chuyển hoặc truyền dữ liệu. *Xem* field.

field tag *nhãn trường* Trong xác thực, xâu ký tự duy nhất dùng trong các thông báo đã định dạng nhằm xác định ý nghĩa và vị trí của trường dữ liệu kết hợp. *Xem* field.

FIFC *Xem* first in first out.

file *tệp* Trong các cấu trúc dữ liệu, tập hợp các bản ghi có liên quan về mặt logic với nhau và được xử lý như một đơn vị, ví dụ, gán cho chúng một cái tên duy nhất. Tệp có thể tồn tại trên băng từ, đĩa từ v.v.. *Xem* magnetic disk, magnetic tape, record.

file access *truy nhập tệp* Trong an toàn dữ liệu, các thủ tục kiểm soát truy nhập xác định các tệp có thể truy nhập được bởi một người dùng máy tính được phép và các thao tác mà có thể được thực hiện khi sử dụng những tệp đó.

Các tệp máy tính được phân phối cho các thư mục và những thư mục đó có thể được tổ chức theo cấu trúc cây. Do đó, một người sử dụng tệp tiềm ẩn nào đó phải có tên tệp, tên thư mục và có thể, các tên những thư mục gốc. Khi đó truy nhập vào tệp có thể được kiểm soát bởi các mật khẩu tệp và/hoặc các bảng truy nhập. Các mật khẩu tệp bảo

F

vệ tương tự các mật khẩu máy tính.

Sơ đồ bắp xếp liên hệ một người sử dụng, tệp và đặc quyền tệp được lưu giữ trong các bảng truy nhập; hoặc là, các tệp có thể được phân chia thành những đoạn rời rạc và một ma trận truy nhập sẽ liên kết các đặc quyền cấp cho những người sử dụng, từ một đoạn, khi truy nhập các tệp từ những tệp khác. Ví dụ, các tệp của một trường đại học có thể được chia thành hành chính, giảng dạy và nghiên cứu; khi đó ma trận phân chia cho biết các đặc quyền tệp cấp cho nhân sự nghiên cứu khi truy nhập các tệp hành chính.

Các loại đặc quyền tệp thông thường là: đọc, sửa đổi, cấp phát, ghi, gắn thêm và thi hành. Đọc cho phép người sử dụng xem nội dung của tệp nhưng không sửa đổi hoặc sử dụng được nó, ví dụ, thực hiện một tệp chương trình. Sửa đổi là một thuật ngữ bao hàm mọi hành động thay đổi có thể thực hiện đối với một tệp. Cấp phát cho phép người sử dụng cấp những đặc quyền truy nhập cho người sử dụng khác nhưng những đặc quyền đó phải không được vượt quá những đặc quyền của chính người cấp phát. Các đặc quyền ghi bao gồm cất giữ, xóa, thay thế, tạo ra một tệp, thay đổi nội dung tệp và có thể tạo ra hoặc xóa một thư mục con. Gắn thêm cho phép người sử dụng bổ sung tiếp thông tin vào một tệp mà không sửa đổi dữ liệu hiện hành, ví dụ như một số người sử dụng có thể nhập dữ liệu từ một cuộc khảo sát thống kê nhưng không thay đổi dữ liệu đã nhập bởi người khác, và thi hành cho phép tệp được chạy như một chương trình. Các đặc quyền tệp có thể được cấp cho các nhóm người sử dụng cũng như các cá nhân. *Xem* access control, database security, directory, file protection, lockword, tree structured directory.

file authentication code ***mã xác thực tệp*** Trong an toàn cơ sở dữ liệu, mã được tạo ra theo cách tương tự với MAC mà có thể được sử dụng để đảm bảo rằng, dữ liệu chứa trong một tệp không bị xóa hoặc sửa đổi. *Xem* MAC.

file cleanup ***xóa tệp, dọn tệp*** Trong tin học, loại bỏ những dữ liệu không cần thiết khỏi tệp. *Đồng nghĩa với* file tidying.

file conversion ***biến đổi tệp*** Trong tin học, quá trình thay đổi phương tiện hoặc cấu trúc tệp, thường do các yêu cầu của chương trình mới hoặc sự thay đổi phần cứng. *Xem* file, hardware.

file descriptor ***số liệu nhận dạng tệp tin, bộ mô tả tệp*** Trong tin học, thông tin thường được nhớ như bản ghi tiêu đề trên đĩa từ hoặc băng từ, cho biết các chi tiết về tên tệp, số hiệu thế hệ, ngày hết hạn, ngày truy nhập cuối cùng và cấu trúc các bản ghi. *Xem* descriptor.

file layout ***sơ đồ tệp, cách bố trí tệp, bố cục tệp*** Trong tin học, sự bố trí và cấu trúc của dữ liệu trong một tệp, bao gồm trình tự và kích thước trường của mỗi phần tử. *Xem* field, file. *Đồng nghĩa với* file organization.

file lock ***khóa tệp*** Trong tin học, phương tiện từ chối truy nhập vào một tệp. Nó được dùng trong các hệ nhiều người sử dụng để ngăn ngừa hai người sử dụng ghi đồng thời vào cùng một

tệp. *So sánh với* record lock.

file maintenance ***bảo trì tệp*** Trong tin học, hoạt động giữ cho tệp được cập nhật bằng cách bổ sung, thay đổi hoặc xóa dữ liệu (ví dụ, thêm các chương trình mới vào thư viện chương trình trên các đĩa từ). *Xem* file management, file organization.

file management ***quản lý tệp*** Trong tin học, thủ tục hoặc tập hợp các quá trình để tạo ra và bảo trì các tệp. *Xem* file, file maintenance, file organization.

file name ***tên tệp*** Trong tin học, xâu ký tự nhận dạng duy nhất một tệp. Các tệp có thể được nhận dạng bởi hai tên, tên ngoài và tên trong. Tên tệp ngoài được hệ điều hành dùng và chứa tất cả các chủ nhân bậc cao hơn của tệp trong thư mục cấu trúc cây, cộng với phần mở rộng. Tên tệp trong có thể được cấp cho tệp bên trong một chương trình, lệnh mở tệp sẽ liên hệ các tên tệp trong và ngoài, sau đó mới dùng các lệnh đọc hoặc ghi các tên tệp trong. *Xem* extension, file, open, operating system, path, tree-structured directory.

file processing ***xử lý tệp*** Trong tin học, cập nhật định kỳ các tệp chủ để phản ánh các ảnh hưởng của dữ liệu hiện thời (ví dụ, mở kho hàng tháng cập nhật tệp kho chủ).

file protection ***bảo vệ tệp*** (1) Trong an toàn máy tính, toàn bộ các quá trình và thủ tục thiếp lập trong hệ ADP và được thiết kế để ngăn cản truy nhập không được phép, sự ô nhiễm hoặc loại bỏ một tệp. *Xem* file access, data contamination, key management. (2) Trong tin học, phương pháp bảo vệ các tệp trước sự truy nhập không được phép của người sử dụng khác. Nếu thư mục chung được dùng thì các mục vào thư mục sẽ chứa nhãn cho biết chủ nhân và kiểu bảo vệ cần thiết. Có thể dự phòng một số mức bảo vệ (ví dụ, cho phép ghi, cho phép đọc, cho phép thực hiện và cho phép gắn thêm). Mức bảo vệ cuối cùng cho phép những người sử dụng ghi các bản ghi vào cuối tệp nhưng không đọc hoặc sửa đổi những bản ghi hiện thời, một phương tiện hữu ích để thu thập thống kê từ rất nhiều người sử dụng. *So sánh với* memory protection. *Xem* directory, file, file access, record.

file protect ring ***vòng bảo vệ tệp*** Ở các hệ thống nhớ, vòng mà khi loại bỏ khỏi cuộn băng từ sẽ ngăn không cho dữ liệu được ghi vào băng. *Xem* file protection.

file restructuring ***tái cấu trúc tệp*** Trong tin học, kỹ thuật dùng để tối ưu hóa vị trí dữ liệu trên đĩa từ. Trong các thao tác tệp, việc lưu các mục dữ liệu tùy thuộc vào trình tự nhận được chúng; trong một thời hạn dài điều này có thể dẫn tới sự xuống cấp tính năng của hệ thống. Tái cấu trúc tệp đôi khi được thực hiện trong các hoạt động sao chép dự phòng có hệ thống.

file security ***an toàn tệp*** Trong an toàn dữ liệu, các cách sắp xếp để đảm bảo tính bí mật hoặc để những người không được phép không thể truy nhập vào các tệp. *xem* data security, file access, file protection.

file server ***bộ phục vụ tệp, secvơ tệp, trình dịch vụ tệp*** Trong tin học, dạng

phức tạp của trình phục vụ đĩa vốn duy trì một hệ tệp logic đầy đủ. Những người sử dụng máy vi tính nối mạng có thể truy nhập thông tin trong cùng những vùng thư mục và các cơ cấu phục vụ tệp sẽ giải quyết các vấn đề truy nhập không được phép, truy nhập tương tranh v.v.. Tập hợp không đồng nhất của các máy vi tính cũng có thể được điều hợp bằng phần mềm nằm trong các máy vi tính và chuyển các yêu cầu của hệ điều hành thành các yêu cầu của trình phục vụ tệp tương đương. *Xem* disk server, file, server.

file storage ***bộ nhớ tệp*** Trong tin học, thiết bị ngoại vi có thể nhớ khối lượng lớn dữ liệu. Những thiết bị đó gồm các thiết bị đĩa từ, thiết bị băng từ và thiết bị bia từ tính.

file system check ***kiểm tra hệ thống tệp*** Trong tin học, lệnh trong Unix để kiểm tra tính toàn vẹn của hệ tệp. Nếu một tệp bị hỏng được phát hiện thì thao tác viên sẽ xin phép để sửa nó nhưng tác động như thế có thể dẫn tới mất dữ liệu. *Xem* file, Unix.

file tidying ***dọn dẹp tệp*** *Đồng nghĩa với* file cleanup.

file transfer, access and management ***chuyển, truy nhập và quản lý tệp*** Trong truyền thông dữ liệu, các quá trình cần thiết khi các tệp được xử lý từ xa hoặc được chuyển qua mạng.

file updating ***cập nhật tệp*** Trong tin học, một trong những thao tác thông thường nhất trong xử lý dữ liệu và giao tác. Nội dung của tệp được thay đổi mà không làm thay đổi cấu trúc cơ bản. Trong các hệ xử lý theo lô những thay đổi phải được thực hiện đối với tệp được sắp theo dãy, tương ứng với dãy các bản ghi lưu giữ trong tệp, và các bản ghi của tệp được chèn, sửa đổi hoặc xóa tùy theo dữ liệu nhập vào trong một lần chạy chương trình. Sự xuất hiện thiết bị nhớ trực tiếp đã cho phép truy nhập ngẫu nhiên có hiệu quả vào bản ghi tệp, do đó các chuyển tác riêng lẻ có thể được xử lý một cách tương tác.

fill character ***ký tự điền, ký tự lấp đầy*** Trong các cấu trúc dữ liệu, ký tự, thường là dấu cách, được bổ sung vào tập hợp các ký tự để tạo ra tập có độ dài đã cho.

filter ***bộ lọc*** Trong an toàn cơ sở dữ liệu, nhân an toàn chịu trách nhiệm áp đặt những yêu cầu của an toàn nhiều mức. *Đồng nghĩa với* guard.

filtering ***(phép) lọc*** trong mật mã, kỹ thuật dùng để biến đổi bản mã thường là một dòng bit ngẫu nhiên thành một dòng các ký tự mà một giao thức truyền nào đó cho phép. Ví dụ, dòng bit có thể được chia thành 4 nhóm bit và mỗi nhóm biểu diễn như một ký tự thập lục phân 1 - 9 , A - F, sau đó, có thể biến đổi những ký tự ấy thành các ký tự ASCII 1 byte và truyền đi. Kỹ thuật như thế bổ sung độ dư cho dòng truyền đi và do đó làm tăng số các bit trong dòng ký tự được truyền đi. *Xem* ANSI - X.12.

FIMAS ***FIMAS*** Trong hoạt động ngân hàng, viết tắt của Financial Institution Message Authentication Standard (tiêu chuẩn xác thực thông báo của cơ sở tài chính). *Đồng nghĩa với* ANSI X9.9 - 1986.

F-IN ***lớp F-IN*** Trong an toàn thông tin, lớp chức năng định nghĩa trong ITSEC, xác định cho các hệ thống với tính toàn vẹn cao đối với các dữ liệu và chương trình. Những yêu cầu như thế rất quan trọng đối với các hệ thống cơ sở dữ liệu. *Xem* integrity, ITSEC, TCSEC.

financial institution ***cơ sở tài chính*** Trong hoạt động ngân hàng, cơ sở chịu trách nhiệm lưu, cho vay, trao đổi hoặc phát hành tiền; mở rộng tín dụng; và để tạo điều kiện chuyển tiền.

financial message ***thông báo tài chính*** Trong hoạt động ngân hàng, thông báo chứa các lệnh kéo theo các tác động tài chính.

fingerprint ***ký dấu, dấu vân tay*** (1) Trong bảo vệ phần mềm, phương pháp gán dấu hiệu duy nhất hoặc chữ ký cho một đĩa mềm, vốn không thể sao được. Thường trình thử đặc biệt đó xem chữ ký có mặt hay không và nếu không tìm được thì chương trình bảo vệ sẽ bị vô hiệu hóa. *So sánh với* dongle. *Xem* burn mark, execute protection, weak bits. *Đồng nghĩa với* signature, unique identification. (2) Trong kiểm soát truy nhập thuộc tính nhận dạng duy nhất của một cá nhân. *Xem* fingerprint analysis.

fingerprint analysis ***phân tích dấu vân tay*** Trong kiểm soát truy nhập, kỹ thuật sinh trắc dựa trên phép đo dấu vân tay của người sử dụng. Năm 1897, chánh Sở cảnh sát thủ đô, ngài Edward Henry, đã nghĩ ra phương pháp phân loại các dấu vân tay mà về sau các lực lượng cảnh sát dùng rộng rãi.

Dấu vân tay là mẫu các đường vân trên da các đầu ngón tay và mẫu đó thể hiện ba đặc điểm chính: các vân xoáy, vân vòng và vân dạng cung, cộng với những đặc trưng chi tiết hơn gọi là những chi tiết vân tay chính xác. Các vân xoáy là những mẫu lằn gợn với những đặc trưng xoáy ốc, các vân vòng là những mẫu lằn gợn khép kín, trong khi các vân cung là những đường cong trong mẫu không khép kín. Vị trí và hướng của những chi tiết vân tay chính xác đóng một vai trò quan trọng trong nhận dạng dấu vân tay; những chi tiết chính xác như thế ngoài những cái khác ra, bao gồm những nhánh lằn gợn mà ở đó hai lằn gợn hòa vào thành một lằn gợn đơn lẻ và các đầu lằn gợn, tại đó một lằn gợn riêng kết thúc.

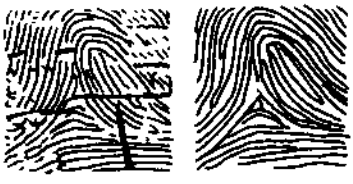
Các thiết bị quét dấu vân tay thường ghi hai dấu vân tay để phòng tránh từ chối truy nhập do sự tổn thương một ngón tay. Ngón tay được đặt trên một tấm kính nhỏ, thường với người hướng dẫn giúp đặt ngón tay theo hướng thích hợp. Các suất lỗi loại 1 và loại 2 thường gặp là suất loại bỏ sai 2% và xác suất nhận sai 0,0001%.

Các ảnh dấu vân tay thường được đọc nhờ sự phản xạ trong toàn phần của hình ảnh trên tấm kính. Hình ảnh bị ảnh hưởng bởi rất nhiều các yếu tố bao gồm cặn dầu ở da, sự định hướng và sức ép của ngón tay v.v.. Một số hệ thống cung cấp cho người sử dụng thông tin hồi tiếp như một hình ảnh về vân tay, hoặc số đo sức ép ngón tay để giúp phát triển những hình ảnh thích hợp cho việc quét.

Trong một số hệ thống, người quản lý

có thể có khả năng tia gọt những tham số kiểm soát truy nhập bằng cách đặt các tham số, với mức độ phù hợp chấp nhận được ở giai đoạn đăng nhập và mức độ khớp chấp nhận được đối với một ý đồ truy nhập. Mức độ phù hợp cao hơn ở giai đoạn đăng nhập ngụ ý rằng, chỉ có những lần quét mẫu chấp nhận được cho đăng nhập là có một mức độ khớp cao với nhau, do đó đảm bảo mẫu vân tay được lưu có chất lượng cao. Nếu dùng một mẫu chất lượng thấp thì xác suất để một người sử dụng sau đó bị bác bỏ sai sẽ lớn hơn. Tham số so khớp kiểm soát mức độ khớp giữa mẫu được đưa ra và mẫu lưu sẽ được coi như thích hợp cho nhận dạng khẳng định. Nếu tham số đó được đặt ở giá trị thấp thì nó sẽ giảm các lỗi loại 1 nhưng có nguy cơ kèm theo về khả năng tăng đăng ký một chấp nhận sai.

Các bộ quét dấu vân tay có nhiều ưu điểm kỹ thuật cho các ứng dụng kiểm soát truy nhập, và giá của những hệ thống như thế có thể tỏ ra hấp dẫn trong tương lai.



fingerprint analysis: *phân tích dấu vân tay.* Vì không có hai cá thể có cùng chi tiết dấu vân tay nên phương pháp kiểm soát truy nhập này dựa trên một "cái gì đó có chữ" như biện pháp chủ yếu để thiết lập nhận dạng cá nhân.

Nhược điểm của những bộ quét đó có thể là ở độ nhạy cảm của công chúng, bởi vì những kỹ thuật như thế thường gắn liền với công việc pháp lý. *Xem* biometrics, Type 1 error, Type 2 error.

FINS ***FINS*** Trong hoạt động ngân hàng, viết tắt của Financial Institution Numbering System (hệ thống đánh số cơ sở tài chính). *Xem* ANSI X9.5 - 1988.

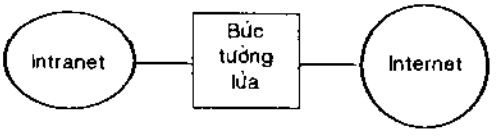
FIPS ***FIPS*** Viết tắt của Federal Information Processing Standard (tiêu chuẩn xử lý thông tin Liên bang).

FIPS PUB ***ấn phẩm FIPS*** Viết tắt của Federal Information Processing Standard Publication (ấn phẩm tiêu chuẩn xử lý thông tin Liên bang).

FIPS Pub 65 ***ấn phẩm FIPS 65*** Một ấn phẩm FIPS nghiên cứu phân tích rủi ro. *Xem* FIPS Pub, quantifield analysis.

fire walls ***bức tường chống lửa; bức tường lửa*** (1) Trong an toàn vật lý, bức tường chống lửa là bức tường có sức chịu lửa đủ để ngăn không cho lửa lan rộng. (2) Trong mạng thông tin, bức tường lửa là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy nhập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập không mong muốn từ bên ngoài vào hệ thống nội bộ. Cũng có thể xem bức tường lửa là một cơ chế bảo vệ mạng tin cậy khỏi các mạng không tin cậy... Thông thường bức tường lửa được đặt giữa Internet (bên ngoài) và intranet (mạng nội bộ của công ty hay quốc gia - bên trong) để kiểm soát sự lưu thông và truy nhập giữa chúng với nhau. Nó sẽ quyết định

những dịch vụ bên trong nào được phép truy nhập ra ngoài, những cá nhân từ bên ngoài được truy nhập tới các dịch vụ từ bên trong và cả những dịch vụ bên ngoài nào được phép truy nhập bởi những người bên trong. Hình 1 là sơ đồ hệ thống chức năng của bức tường lửa:



Fire wall: *bức tường lửa.* Hình 1. Hệ thống chức năng.

Cấu trúc của bức tường lửa gồm:

- Một hoặc nhiều hệ thống máy chủ kết nối với bộ định tuyến hoặc có chức năng định tuyến.
- Một phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực, cấp quyền và kiểm toán.

Một bức tường lửa chuẩn bao gồm một hoặc nhiều các thành phần sau:

- Bộ lọc gói;
- Cổng ứng dụng hoặc cổng ủy nhiệm;
- Cổng vòng.

Bộ lọc gói

Dùng để cho phép hoặc từ chối mỗi gói tin mà nó nhận được. Nó sẽ kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các quy định của lọc gói hay không. Các quy tắc lọc gói này dựa trên các thông tin ở đầu mỗi gói (phần tiêu đề) bao gồm:

- Địa chỉ IP chỉ nơi xuất phát (địa chỉ nguồn);
- Địa chỉ IP đích;
- Các thủ tục truyền tin (TCP, UDP, ICMP, IP);
- Cổng nguồn TCP/UDP;
- Cổng đích TCP/UDP;
- Kiểu thông báo ICMP;
- Giao diện gói đến;
- Giao diện gói đi.

Nếu các quy tắc lọc gói được thỏa mãn, gói sẽ được chuyển qua bức tường lửa. Nếu không, nó sẽ bị loại ra.

Cổng ứng dụng

Đây là kiểu bức tường lửa được thiết kế nhằm tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được phép truy nhập mạng. Cơ chế hoạt động của nó dựa trên dịch vụ đại diện hay ủy nhiệm (proxy service). Dịch vụ ủy nhiệm là các bộ mã đặc biệt cài đặt trên các cổng cho từng ứng dụng. Nếu người quản trị mạng không cài đặt mã ủy nhiệm cho ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua bức tường lửa. Ngoài ra mã ủy nhiệm có thể định được cấu hình để hỗ trợ một số đặc điểm trong ứng dụng mà người quản trị thấy cần thiết, trong khi anh ta có thể từ chối các đặc điểm khác. Một cổng ứng dụng thường được coi là một pháo đài (bastion host) bởi vì nó được thiết kế đặc biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp bảo vệ an toàn cho một pháo đài là:

- Pháo đài luôn chạy các phiên bản an toàn của các phần mềm hệ thống. Các bản an toàn này được thiết kế chuyên chống lại sự tấn công vào hệ điều hành, cũng như bảo đảm sự tích hợp

F

bức tường lửa.

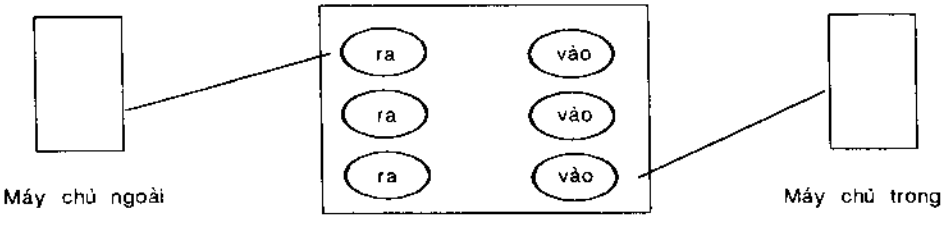
- Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên pháo đài, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng làm cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực người dùng là được cài trên pháo đài.
- Pháo đài có thể yêu cầu mức độ xác thực khác nhau, ví dụ như mật khẩu người dùng hay thẻ thông minh.
- Mỗi dịch vụ ủy nhiệm được đặt cấu hình để cho phép truy nhập chỉ một số máy chủ nhất định. Điều này có nghĩa là bộ lệnh và đặc điểm thiết lập cho mỗi ủy nhiệm chỉ đúng với một số máy chủ trên toàn hệ thống.
- Mỗi dịch vụ ủy nhiệm duy trì một sổ ghi nhật ký ghi chép lại toàn bộ chi tiết của dòng thông tin đi qua nó, thông tin về mỗi kết nối, về khoảng thời gian kết nối. Nhật ký này rất có ích trong việc theo dõi dấu vết hay ngăn chặn kẻ phá hoại.
- Mỗi cổng ủy nhiệm đều độc lập với các cổng ủy nhiệm khác trên pháo đài. Điều này cho phép cài đặt dễ dàng một cổng ủy nhiệm mới, hoặc tháo dỡ một cổng ủy nhiệm có vấn đề.

Cổng vòng (circuit level gateway)

Cổng vòng là một chức năng đặc biệt có thể thực hiện được bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc gói nào.

Hình 2 minh họa việc sử dụng nối Telnet vào cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối Telnet qua bức tường lửa mà không thực hiện sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào đó. Cổng làm việc như một sợi dây, sao chep các byte giữa các kết nối bên trong và các kết nối bên ngoài. Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống tường lửa nên nó che dấu thông tin về mạng nội bộ.

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một pháo đài có thể được cấu hình như một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến, và cổng vòng cho những kết nối đi. Điều này làm cho bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các



Fire wall: *bức tường lửa*. Hình 2. Cổng vòng.

dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ trước những tấn công từ bên ngoài. *Xem* Telnet, TCP/IP, gateway, UDP, authentication, authorization, LAN.

firmware ***phần sụn*** (1) Trong tin học, phần mềm thường xuyên lưu trong một thiết bị phần cứng, cho phép đọc phần mềm nhưng không cho ghi hoặc sửa đổi. Thiết bị thông dụng nhất đối với phần sụn là bộ nhớ chỉ đọc. *Xem* ROM. (2) Trong tin học, các chương trình máy tính được ghi ở một phương tiện vật lý thường xuyên hoặc bán thường xuyên gộp trong thiết bị máy tính. (3) Trong tin học, chương trình hoặc dữ liệu được nhớ thường xuyên trong bộ nhớ máy tính (tức là ROM, PROM, EROM hoặc EPROM). Phương pháp thực hiện phần mềm này tương phản với các chương trình lưu giữ trên các phương tiện từ tính và đầu tiên phải được nạp vào bộ nhớ RAM của máy tính trước khi chúng có thể được sử dụng. *Xem* EPROM, EROM, PROM, RAM, ROM.

first in first out ***vào trước ra trước, nhập trước xuất trước, FIFO*** Trong các cấu trúc dữ liệu, phương pháp lưu và truy tìm các mục từ cấu trúc sao cho phần tử đầu tiên được nhớ sẽ được tìm kiếm đầu tiên. *So sánh với* LIFO. *Xem* queue.

first normal form ***dạng chuẩn thứ nhất, FNF*** Trong các cơ sở dữ liệu, tính chất của một quan hệ trong cơ sở dữ liệu quan hệ. Quan hệ ở dạng chuẩn thứ nhất nếu nó không có bất kỳ nhóm lặp lại nào (tức là dữ liệu có thể được biểu diễn dưới dạng tệp phẳng). *So sánh với* second normal form, third normal form. *Xem* flat file, normal forms, relational database, repeating group.

Fish-6 ***virut Fish-6*** Trong an toàn máy tính, virut lấy lén vốn tự mã hóa, kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

FIU ***hiệp hội FIU*** Viết tắt của US Federation of Information Users (Hiệp hội người dùng thông tin Mỹ).

fixed and exchangeable disk storage ***bộ nhớ đĩa cố định và đổi được, FEDS*** Trong các hệ thống nhớ, thiết bị đĩa từ mà trong đó một số đĩa là cố định và những đĩa khác thao tác viên có thể đổi được. *Xem* exchangeable disk storage, fixed disk storage.

fixed disk storage ***bộ nhớ đĩa cố định, FDS*** Trong các hệ thống nhớ, bộ nhớ ở các đĩa từ không trao đổi được. *So sánh với* exchangeable disk storage.

fixed head disk ***đĩa đầu cố định*** Trong các hệ thống nhớ, hệ đĩa với đầu từ dành riêng cố định trên mỗi rãnh. Ở kiểu thiết bị đĩa thông thường hơn, đầu từ nằm trên một tay đòn và do đó có sự trễ trong khi đầu được định vị để tìm dữ liệu. Bằng cách loại bỏ trễ định vị đầu từ, phương pháp này cho phép truy nhập tốc độ rất cao. *So sánh với* movable-head disk. *Xem* hard disk, head, magnetic disk.

fixed length record ***bản ghi độ dài cố định*** Trong các cấu trúc dữ liệu, bản ghi mà luôn luôn có cùng độ dài như tất cả các bản ghi khác mà với

chúng, nó có liên quan logic hoặc vật lý. *So sánh với* variable-length record. *Xem* record. *So sánh với* adaptive routing, delta routing, directory routing, hot potato routing. *Xem* routing.

flag ***cờ, dấu hiệu*** (1) Trong truyền thông dữ liệu, một ký tự thường gồm tám bit, dùng để đánh dấu điểm khởi đầu một khung (frame) trong một gói tin. *Xem* frame, packet switching. (2) Trong tin học, tập hợp tín hiệu được thiết lập để chỉ báo rằng, một điều kiện riêng đã xảy ra. Ví dụ, khi bộ đệm đầy.

flag bit ***bit cờ*** *Xem* flag.

flag code ***mã cờ*** *Đồng nghĩa với* escape code.

flag sequence ***dãy cờ*** Trong truyền thông dữ liệu, dãy các bit dùng để nhận biết bắt đầu và kết thúc của khung. *Xem* flag, frame, packet switching.

Flash ***virut Flash*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM và EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lọc các tệp chương trình, OVL và dữ liêu và liên kết tệp. *Xem* virus names.

flat file ***tệp phẳng, tệp hai chiều*** Ở các cơ sở dữ liệu, tệp gồm tập hợp các bản ghi cùng kiểu không chứa các nhóm lặp lại. Tệp phẳng có thể được biểu diễn như mảng hai chiều của các mục dữ liệu. Cơ sở dữ liệu quan hệ gồm tập các tệp phẳng có cấu trúc rõ ràng. *Xem* record relational database, repeating group.

flaw ***kẽ hở, sai thủ tục*** Trong an toàn máy tính, lỗi do ủy thác, bỏ sót hoặc lơ là trong một hệ thống nhờ đó có thể tránh được các cơ chế bảo vệ. *Xem* pseudo-flaw. *Đồng nghĩa với* loophole.

flaw hypothesis ***giả thuyết về kẽ hở*** Trong an toàn máy tính, kỹ thuật thử động, trong đó các kẽ hở được giả thiết trên cơ sở các kẽ hở tương tự phát hiện được ở những hệ thống khác và sau đó được thử để xem có tồn tại ở hệ thống đang nghiên cứu không. *So sánh với* program analyzer. *Xem* dynamic testing, flaw hypothesis methodology.

flaw hypothesis methodology ***hệ phương pháp luận giả thuyết về kẽ hở*** Trong an toàn máy tính, sự phân tích hệ thống và kỹ thuật thâm nhập trong đó, những bản đặc tả và hồ sơ về hệ thống được phân tích và sau đó giả định về các kẽ hở trong hệ thống. Danh sách các kẽ hở giả định sau đó được đặt mức ưu tiên trên cơ sở xác suất ước lượng rằng một kẽ hở thực sự tồn tại và, giả sử kẽ hở tồn tại, theo khía cạnh dễ khai thác và theo mức độ kiểm soát hoặc dễ tổn thương. Danh sách đã đạt mức ưu tiên sẽ được dùng để định hướng việc kiểm định thực tế một hệ thống. *Xem* flaw.

flexibility ***mức linh hoạt*** Trong tin học, nỗ lực cần để sửa đổi một chương trình hoạt động.

Flip ***virut Flip*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

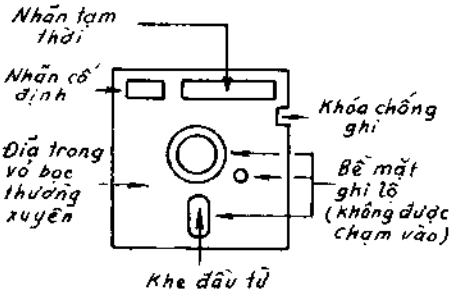
flooding ***truyền tới tấp, truyền tràn*** Trong truyền thông dữ liệu, phương

pháp định tuyến trong đó, mỗi nút sao chép lại các gói tin tới và gửi các bản sao tới các nút lân cận, do đó đảm bảo sẽ tới được nơi nhận thực sự một cách nhanh chóng và chắc chắn mặc dù khá tốn dung lượng truyền. *Xem* node, packet switching, routing.

flood testing ***thử tràn*** Trong truyền thông dữ liệu, phương pháp thử lưu lượng toàn bộ của hệ khi tất cả các đầu cuối trong mạng đều được sử dụng. *Xem* computer network.

floor sensor ***bộ cảm biến để sàn*** *Đồng nghĩa với* area mat.

floppy ***đĩa mềm, floppy*** Trong các hệ thống nhớ, viết tắt của floppy disk (đĩa mềm) hoặc floppy-disk drive (ổ đĩa mềm).



floppy disk: *đĩa mềm.*

floppy disk ***đĩa mềm*** Trong tin học, đĩa phủ từ tính dễ uốn, đặt trong vỏ bảo vệ cứng hoặc nửa cứng. Đĩa mềm cung cấp cho người sử dụng máy vi tính bộ nhớ dự phòng, truy nhập trực tiếp rẻ, dung lượng cao. Đĩa mềm nằm trong vỏ phủ kín để tránh bụi bẩn. Vỏ có một số lỗ cho trục ổ đĩa, lỗ đánh chỉ số để báo hiệu bắt đầu một cung từ và khe chống ghi. *Xem* personal computer security.

floppy disk drive ***ổ đĩa mềm*** Trong tin học, cơ cấu dẫn động đối với các đĩa mềm. Các thành phần cơ bản của ổ đĩa là môtơ điện và trục để quay đĩa, một hoặc nhiều đầu đọc/ghi, một hệ thống định vị đầu và, đối với nhiều hệ thống, một nguồn sáng cộng với bộ dò quang để phát hiện khởi đầu các cung. Tốc độ quay là thấp so với các ổ đĩa cứng bởi vì đầu đọc/ghi tiếp xúc với đĩa và tốc độ thường trong khoảng từ 300-600 vg/ph.

flops ***flops*** Trong tin học, viết tắt của floating point operations per second (số phép toán dấy phẩy động trên giây); số đo hiệu suất của máy tính. *So sánh với* LIPS, MIPS.

flow analysis ***phân tích luồng*** *Xem* information flow analysis, traffic analysis.

flow control ***kiểm soát luồng, điều khiển luồng*** (1) Trong an toàn máy tính, chiến lược để bảo vệ nội dung của các đối tượng thông tin khỏi bị chuyển tới các đối tượng ở các mức an toàn không đúng. Nó hẹp hơn nhiều so với kiểm soát truy nhập. *Xem* information flow control, object, subject. (2) Trong truyền thông dữ liệu, sự điều khiển luồng dữ liệu để ngăn ngừa quá đông hàng hoặc quá chật các bộ đệm hoặc mất dữ liệu do máy thu đã định không có khả năng nhận dữ liệu. *Xem* buffer.

flying dutchman ***mã tàu ma*** Trong an toàn máy tính, một dạng mã ác ý, thường được phát triển như một trò

F

chơi khăm của sinh viên. Nó ngủ im không hoạt động cho tới khi có những cố gắng của các nhà lập trình hệ thống nhằm đọc mã, khi đó chương trình có thể tự tái định vị và in một thông báo màn hình. Ví dụ "Ta đã ở đây, nhưng bây giờ ta đã biến". *Xem* malicious code.

flywheeling ***tạo đà*** Trong quản lý khóa, kỹ thuật để truyền các thông tin cập nhật khóa trong các hệ mật mã dòng. Các thông tin cập nhật khóa có thể được gửi cho bên nhận trong khi truyền thông báo, cho phép bên phát thay đổi dòng bit mật mã và duy trì tính đồng bộ. Thông tin cập nhật khóa được bên nhận giải mã và được dùng để thiết lập bộ tạo dòng bit mật mã về giá trị đặt đã cập nhật của nó. Tuy nhiên, nếu thông tin đồng bộ hóa bị mất do kênh ồn hoặc phá rối thì bên nhận không có khả năng tiếp tục giải mã. Kỹ thuật tạo đà khắc phục được vấn đề đó bằng cách phát triển các thông tin cập nhật khóa từ một bộ sinh số giả ngẫu nhiên. Trong trường hợp đó, nếu bên nhận bỏ lỡ một thông tin cập nhật khóa thì nó có thể thu được thông tin cập nhật đó từ bộ sinh số giả ngẫu nhiên và sử dụng nó để thiết lập lại bộ sinh dòng bit mật mã. *Xem* cryptographic bit stream, pseudorandom number, stream cipher.

FM *Xem* frequency modulation.

FNF *Xem* first normal form.

FNP *Xem* front end network processor.

FOI ***tự do thông tin, FOI*** Trong lập pháp, viết tắt của freedom of information (tự do thông tin); thông tin hoặc các hoạt động liên quan tới luật Tự do thông tin của Mỹ. *Xem* data protection.

foil ***lá an toàn*** Trong an toàn vật lý, băng dẫn điện dùng để phát hiện những kẻ xâm nhập mở cửa sổ v.v.. Nó được nối với một mạch điện và báo động được kích hoạt nếu bị làm đứt.

forbiden combination ***tổ hợp bị cấm, tổ hợp sai*** Trong tin học, tổ hợp các bit không hợp lệ theo các tiêu chuẩn mà người lập trình hoặc người thiết kế hệ thống thiết lập.

foreground program ***chương trình ưu tiên*** Trong tin học, chương trình có tính ưu tiên cao và lấy quyền ưu tiên so với những chương trình khác vốn chạy tương tranh trong môi trường đa nhiệm. *So sánh với* background program.

Foreign Government Information ***thông tin chính phủ nước ngoài*** Thông tin mà: (*a*) do một chính phủ hoặc các chính phủ nước ngoài, tổ chức quốc tế của các chính phủ, hoặc một bộ phận bất kỳ của tổ chức đó cung cấp cho Hoa Kỳ với kỳ vọng thông tin hoặc nguồn thông tin hoặc cả hai được giữ bí mật. (*b*) Do Hoa Kỳ đưa ra sau đó như kết quả sự kết hợp với chính phủ hoặc các chính phủ nước ngoài hoặc một tổ chức quốc tế của các chính phủ, hoặc một bộ phận bất kỳ của tổ chức đó, với đòi hỏi rằng, thông tin hoặc cấu trúc thông tin hoặc cả hai được giữ bí mật. Thông tin mô tả ở những mục nhỏ ở trên và thông tin thuộc sở hữu của bộ quốc phòng Hoa Kỳ là thông tin được phân loại phù hợp với 5200.1-R của bộ quốc phòng Hoa Kỳ.

forgery ***giả mạo*** Trong lập pháp, một bên liên lạc bịa thông tin rồi lại khẳng định thông tin đó nhận được từ bên kia. *Xem* digital signature.

Form ***virut Form*** Trong an toàn máy tính, virut kết thúc và lưu trữ, lây nhiễm cung khởi động đĩa mềm, lây nhiễm cung khởi động đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy và làm sai lạc các tệp dữ liệu. *Xem* virus names.

formal ***hình thức*** Chỉ khía cạnh chặt chẽ đối với hình thái là cơ sở toán học hoặc logic.

formal access approval ***(sự) phê duyệt truy nhập hình thức*** Trong an toàn dữ liệu, sự chấp thuận bằng văn bản của chủ dữ liệu cho phép truy nhập một loại hoặc hạng thông tin riêng. *Xem* data owner.

formal language ***ngôn ngữ hình thức*** Trong tin học, ngôn ngữ hình thức xác định một tập hợp các ký hiệu - bảng chữ cái - và một tập hợp các xâu của những ký hiệu đó. Ý nghĩa của ngôn ngữ hình thức trong lập trình là ở chỗ, một chương trình đã cho có thể được xem xét như một xâu của ngôn ngữ hình thức (tức là ngôn ngữ lập trình). Chương trình được tạo ra bằng cách ghi các biểu thức phù hợp với cú pháp của ngôn ngữ; điều này tương đương với sử dụng các sản phẩm của một ngữ pháp tương ứng. Chương trình dịch sẽ kiểm tra xem chương trình có phải là một trong các xâu của ngôn ngữ hay không và nếu không thì báo các lỗi cú pháp. *Xem* grammar.

formal proof ***chứng minh hình thức*** Trong an toàn máy tính, một lập luận toán học đầy đủ và có sức thuyết phục, đưa ra lý lẽ logic đầy đủ cho mỗi bước chứng minh, cho sự đúng đắn của một định lý hoặc tập hợp các định lý. Quá trình kiểm chứng hình thức sử dụng các chứng minh hình thức để chỉ ra sự đúng đắn của một số tính chất nào đó của phép đặc tả hình thức và để chỉ ra rằng, các chương trình máy tính thỏa mãn các bản đặc tả của chúng. *Xem* formal verification, proof of program correctness.

formal security policy model ***mô hình chính sách an toàn hình thức*** Trong an toàn máy tính, phát biểu chính xác về mặt toán học của một chính sách an toàn. Để đủ chính xác, một mô hình như thế phải trình bày trạng thái ban đầu của một hệ thống, cách mà hệ thống tiến triển từ trạng thái này tới trạng thái khác và định nghĩa về một trạng thái "an toàn" của hệ thống. Để có thể được chấp nhận như một cơ sở cho một TCB, mô hình phải được hỗ trợ bởi một chứng minh hình thức rằng, nếu trạng thái ban đầu của hệ thống thỏa mãn định nghĩa về trạng thái "an toàn", và nếu mọi giả thiết mà mô hình đòi hỏi đều giữ đúng, thì tất cả các trạng thái tương lai của hệ thống sẽ là an toàn. Một số kỹ thuật mô hình hóa hình thức bao gồm; các mô hình chuyển tiếp trạng thái, các mô hình logic tạm thời, các mô hình ngữ nghĩa ký hiệu, các mô hình đặc tả đại số. *Xem* Bell-La Padula model, security policy.

formal top-level specification ***đặc tả hình thức mức cao nhất*** Trong an toàn máy tính, đặc tả mức cao nhất

F

được viết theo ngôn ngữ toán học hình thức, cho phép giả định và chứng minh hình thức các định lý, thể hiện sự tương ứng của bản đặc tả hệ thống với các yêu cầu hình thức của nó. *So sánh với* descriptive top-level specification. *Xem* formal security policy model, top-level specification.

formal verification ***kiểm chứng hình thức, xác minh hình thức*** Trong an toàn máy tính, quá trình sử dụng các chứng minh hình thức để chứng minh tính nhất quán (kiểm chứng thiết kế) giữa đặc tả hình thức một hệ thống với mô hình chính sách an toàn hình thức hoặc (kiểm chứng cài đặt) giữa đặc tả hình thức và sự thực hiện chương trình của nó. *Xem* proof of program correctness, security policy.

formant ***thành tố, focman*** Trong an toàn truyền thông, chỉ một tần số cộng hưởng của đường thanh âm. *Xem* voice scrambling.

format ***khuôn, khuôn thức // tạo khuôn, định dạng, format*** (1) Trong tin học, khuôn là trình tự tổ chức hoặc vị trí bắt buộc xác định trước của các ký hiệu trong lệnh, dữ liệu hoặc từ máy tính, thông báo truyền dữ liệu v.v.. Trình tự là bắt buộc để máy tính có thể hiểu được và diễn dịch thông tin. *Xem* instruction, word, data transmission (2) Tạo khuôn là lệnh định dạng đĩa. *Xem* formatting.

formatted dump ***(sự) kết xuất đã định dạng*** Trong tin học, sự kết xuất trong đó một số vùng dữ liệu nhất định được cách ly và được định danh. *Xem* dump.

formatting ***(sự) tạo khuôn, (sự) định dạng*** Trong tin học, thao tác khởi tạo các đĩa trống; dữ liệu khởi tạo được ghi sao cho các rãnh được chia thành các cung (từ). Không có tệp nào có thể được ghi vào đĩa cho tới khi hoàn thành thao tác này.

form mode terminal ***đầu cuối chế độ khuôn dạng, đầu cuối chế độ mẫu biểu*** Trong truyền thông dữ liệu, một đầu cuối thông minh có thể tải xuống một khuôn dạng về đầu cuối. Mẫu biểu có thể chứa các trường chỉ đọc với thông tin về người thao tác cùng với những trường khác về nhận dữ liệu nhập thông qua gõ phím. *So sánh với* page mode terminal, scroll mode terminal. *Xem* field, intelligent terminal.

formulary ***quyết định động*** Trong an toàn máy tính, kỹ thuật cho phép ra quyết định cấp phép hoặc từ chối truy nhập động vào thời điểm truy nhập, chứ không phải trong thời gian tạo ra danh sách truy nhập. *Xem* access list.

For Official Use Only data ***dữ liệu chỉ dùng chính thức*** Trong an toàn dữ liệu, dữ liệu vốn là thông tin chính thức chưa phân loại có bản chất nhạy cảm, có sở hữu hoặc cá nhân, phải được bảo vệ khỏi sự phát hành công khai không được phép. *Xem* unclassified information.

FORTRAN ***ngôn ngữ FORTRAN*** Trong lập trình, viết tắt từ FORmula TRANslation (dịch công thức); ngôn ngữ biên dịch đa dạng cho phép thực hiện rất có hiệu quả, nhất là đối với các thao tác tốc hoạt số. Do đó nó khá phổ biến trong các cộng đồng khoa học

và kỹ thuật, nơi mà tốc độ thực hiện có tầm quan trọng hàng đầu. Nó được khởi sinh ở IBM vào cuối những năm 1950.

FORTRAN Complexity Analysis Program ***chương trình phân tích độ phức tạp FORTRAN*** Trong an toàn máy tính, chương trình phân tích độ phức tạp đối với các chương trình FORTRAN vốn xác định các số đo dựa trên số các đường điều khiển trong các modun và độ dài của các chương trình hoặc modun. *Xem* complexity analysis, FORTRAN.

forward channel ***kênh chuyển tiếp, kênh thuận, kênh xuôi*** Trong truyền thông dữ liệu, kênh truyền trong đó hướng truyền trùng với hướng trong đó thông tin người dùng đang được truyền đi. *So sánh với* backward channel.

forward error correction ***sửa lỗi tiến, hiệu chỉnh phòng lỗi, sửa lỗi trước, FEC*** Trong mã hóa, phương pháp sử dụng mã dư vừa cho phép phát hiện lỗi vừa sửa một số lỗi mà không phải truyền lại. *Xem* error-detecting code, Hamming code.

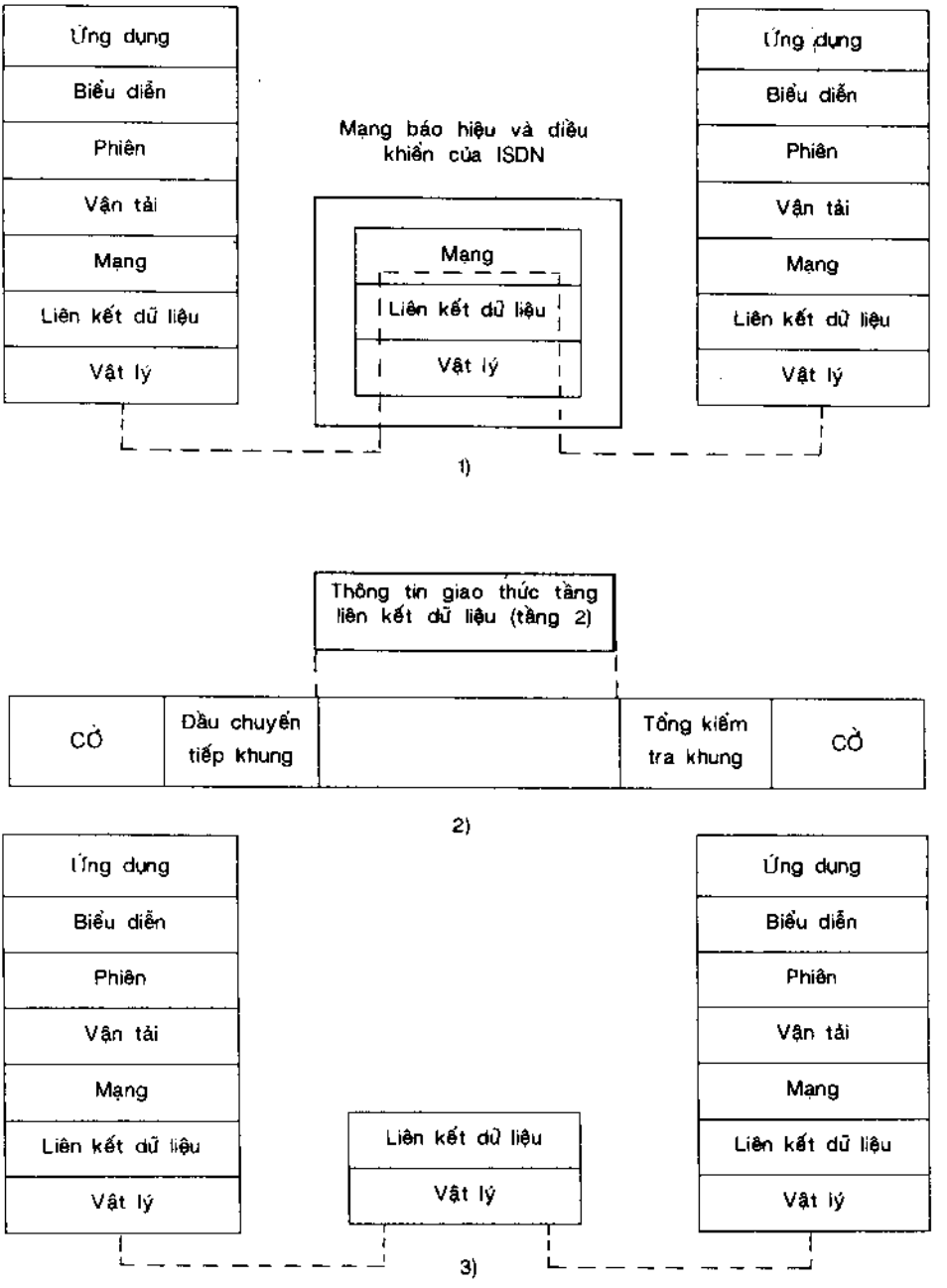
forward supervision ***giám sát xuôi, giám sát thuận, giám sát chuyển tiếp*** Trong truyền thông dữ liệu, việc sử dụng các dãy ký tự giám sát gửi từ trạm hoặc nút thứ nhất tới trạm hoặc nút thứ hai. *Xem* node, supervisory sequence, primary station, secondary station.

FOUO *Xem* For Official Use Only data.

four eyes ***bốn mắt*** Trong an toàn dữ liệu, chỉ các biện pháp an toàn đòi hỏi các chuyển tác phải được chấp thuận bởi nhân viên thứ hai.

fourth generation language ***ngôn ngữ thế hệ thứ tư*** Trong lập trình, ngôn ngữ thuận tiện cho người sử dụng, cho phép người ta thu được thông tin cần thiết với nỗ lực ít hơn so với nỗ lực gắn liền với những ngôn ngữ thủ tục truyền thống. Thuật ngữ ngôn ngữ thế hệ thứ tư được dùng rộng rãi và đã được áp dụng cho rất nhiều sản phẩm tới mức không một định nghĩa súc tích nào có thể bao quát thích đáng vô số những cách giải thích hiện thời. Những thuộc tính mong muốn của ngôn ngữ thế hệ thứ tư bao gồm: (*a*) chấp nhận lập trình phi thủ tục; (*b*) chấp nhận lập trình thủ tục; (*c*) một từ điển dữ liệu chủ động; (*d*) dự phòng quản lý cơ sở dữ liệu mạnh, thuận tiện và linh hoạt; (*e*) ngôn ngữ định hướng con người; và (*f*) dự phòng che chắn giữa người sử dụng và máy. *Xem* database management system, data dictionary, data processing, end user, nonprocedural language, procedural language, frelational database, syntax.

four-wire circuit ***mạch bốn dây*** Trong truyền thông, mạch hai chiều trong đó các tín hiệu đồng thời đi theo các tuyến tách riêng và phân biệt theo các hướng ngược nhau trong môi trường truyền. Mạch điện thoại mang các tín hiệu tiếng nói theo cả hai chiều và trong vòng nội hạt, điều đó đạt được qua hai dây vì các tín hiệu chạy trên mỗi hướng có thể phân biệt được. Ở mạng trung chuyển, nơi mà các bộ khuếch đại và các bộ dồn kênh được sử dụng thì hai hướng truyền phải tách riêng về mặt vật lý. Nó được gọi là



frame relay: *chuyển tiếp khung.* 1) Giao thức kênh D thiết lập cuộc gọi I.451 của ISDN. 2) Đường bao khung. 3) Sự chuyển khung LAP-D trên kênh B của ISDN.

mạch bốn dây vì ở dạng đơn giản, nó sử dụng một cặp dây cho mỗi hướng. *So sánh với* two-wire circuit. *Xem* trunk.

frame ***khung (bit)*** (1) Trong tin học, mảng các bit ngang chiều rộng băng từ. *Xem* bit. (2) Trong truyền thông dữ liệu, dãy đầy đủ của các bit được nhận dạng bởi một ký tự đồng bộ hóa mở và thường chứa một trường chứa dữ liệu người sử dụng.

frame relay ***chuyển tiếp khung*** Trong truyền thông dữ liệu, chuyển tiếp khung là một trong một tập hợp các giao thức truyền thông xác định bởi CCITT, như một phần của khái niệm chung về mạng dịch vụ số tích hợp (ISDN). Chuyển tiếp khung (các khuyến nghị I.122 và Q.922 của CCITT) được thiết kế để tạo ra một phương tiện chuyển thông tin tốc độ cao giữa hai ứng dụng mạng sử dụng ISDN.

Bước đầu tiên trong quá trình chuyển tiếp khung là phải thiết lập nối giữa các bên truyền thông nhờ sử dụng các thủ tục gọi kênh D của ISDN (khuyến nghị I.451 của CCITT) (hình 1). Một khi đã nối được, thông tin cần chuyển được phân đoạn với mỗi đoạn thông tin được đóng gói trong một bao gói với khung thích hợp (hình 2). Khi đó các khung được chuyển giữa các bên truyền thông nhờ sử dụng kênh B của ISDN (hoặc kênh ISDN khác tốc độ cao hơn, ví dụ như kênh H) (hình 3). Tốc độ chuyển dữ liệu cao đạt được chủ yếu nhờ giảm đến tối thiểu thời gian cần thiết qua mỗi nút mạng trong xử lý khung. *Xem* frame, integrated services digital network.

frame switching ***chuyển mạch khung*** *Xem* frame relay.

framing ***tạo khung, đóng khung*** (1) Trong truyền thông dữ liệu, quá trình nhờ đó các nhóm biểu diễn một hoặc nhiều ký tự được lựa chọn bên trong một luồng bit liên tục. *Xem* framing bit. (2) Trong truyền thông dữ liệu, phương pháp nhờ đó các khung bit riêng lẻ trong hệ dồn kênh phân thời được nhận biết để các khe thời gian có thể được xác định đúng: *Xem* time division multiplexing.

framing bits ***bit tạo khung*** Trong truyền thông dữ liệu, các bit được dùng để có thể tách các ký tự trong một luồng bit mà nếu không thì không mang thông tin. *Xem* bit stream.

framing pattern ***mẫu tạo khung*** Trong truyền thông dữ liệu, mẫu duy nhất của các bit tạo khung. *Xem* framing bits.

fraudulent retailer ***người bán lẻ gian lận*** Trong hoạt động ngân hàng, người tự cho mình là nhà buôn EFTPOS, nhờ sử dụng số hiệu nhà buôn thực, đánh cắp hoặc giả mạo và đưa một hoặc nhiều giao dịch không hợp lệ vào hệ thống. *Xem* EFTPOS.

FRC ***FRC*** Viết tắt của Federal Radio Commision (Ủy ban phát thanh liên bang hoa Kỳ).

FRD ***FRD*** Viết tắt của Formerly Restricted Data (dữ liệu trước đây bị hạn chế).

freedom of information ***tự do thông tin*** Trong lập pháp, chỉ quyền của các cá nhân được truy nhập tới thông tin

chính thức. *So sánh với* data protection.

French roundoff ***làm tròn kiểu Pháp*** *Đồng nghĩa với* salami technique.

frequency agility ***linh động tần*** Trong an toàn truyền thông, kỹ thuật chống nhiễu trong đó, tần số truyền đi được thay đổi theo một dãy nào đó mà chỉ máy phát và máy thu hợp pháp biết được trong khi truyền. *Xem* jamming.

frequency division multiple access ***đa truy nhập phân tần, FDMA*** Trong truyền thông, kỹ thuật mà nhờ nó các nhóm người sử dụng (ví dụ, một số trạm mặt đất trong hệ truyền thông vệ tinh) được phân phối các tần số để sử dụng một kênh chung dùng các kỹ thuật dồn kênh phân tần. Sự phân phối các tần số có thể được thực hiện trên cơ sở cố định hoặc theo nhu cầu. *So sánh với* time division multiple access. *Xem* frequency division multiplexing.

frequency division multiplexing ***dồn kênh phân tần, FDM*** Trong truyền thông, quá trình mà nhờ nó hai hoặc nhiều tín hiệu có thể được truyền đi qua một đường dải rộng chung, nhờ sử dụng các phần khác nhau của dải tần đối với mỗi tín hiệu. Ở đầu kia của đường dây các tín hiệu được tách riêng và nhận dạng bởi các bộ lọc chọn lọc vốn phân kênh chúng. *So sánh với* time division multiplexing. *Xem* filter.

frequency modulation ***điều tần, điều biến tần số, FM*** (1) Trong truyền thông, dạng điều biến mà trong đó tần số tức thời của sóng mang bị lệch khỏi tần số mang bình thường một lượng tỷ lệ với biên độ tức thời của đường bao điều biến. *So sánh với* amplitude modulation, phase modulation, pulse modulation. *Xem* modulation. (2) Trong các hệ thống nhớ, phương pháp ghi dữ liệu lên các bề mặt từ hóa. Chiều của dòng điện trong cuộn ghi được đảo ngược ở những khoảng được xác định bởi trình tự định thời. Nếu bit 1 phải được ghi thì dòng cũng đảo chiều ở điểm giữa giữa các xung đồng hồ. Những thay đổi dòng đó tạo ra những thay đổi tương ứng trong định hướng của các hạt từ tính trên bề mặt đĩa.

frequency multiplexing ***dồn kênh phân tần*** *Xem* frequency division multiplexing.

frequency shift keying ***đánh tín hiệu dịch tần, bấm manip dịch tần, FSK*** Trong truyền thông dữ liệu, phương pháp báo hiệu trong đó sóng mang được điều tần bởi tín hiệu mà có một số cố định các giá trị rời rạc. *Xem* frequency modulation.

frequent buyer ***người mua thường xuyên*** Trong lập pháp, kế hoạch chiết khấu do các siêu thị vận hành, trong đó các khách hàng cung cấp các chi tiết cá nhân trong một mẫu điền sẵn. Các siêu thị ghi những khoản mua riêng lẻ nhờ các mã sọc ở hàng hóa và do đó có thể phát triển thông tin tiếp thị có giá trị liên hệ lượng hàng bán được với các đặc trưng của khách hàng. *Xem* data protection.

Frere Jacques ***virut Frere Jacques*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy và làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Friday 13th ***virut Thứ sáu ngày 13*** Trong an toàn máy tính, virut lây nhiễm các tệp COM, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Frogs ***virut Frogs*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

front end network processor ***bộ xử lý ngoại vi mạng, bộ tiền xử lý mạng, FNP*** Trong tin học, bộ xử lý trước xử lý các chức năng giao diện giữa máy tính và mạng dữ liệu. *Xem* front end processor.

front end processor ***bộ xử lý trước, bộ tiền xử lý, FEP*** Trong tin học, máy tính nhỏ dùng để xử lý giao diện truyền thông (ví dụ, hỏi vòng, dồn kênh, dò lỗi) cho máy tính khác. *Xem* multiplexing, polling.

front end security filter ***bộ lọc an toàn trước, bộ lọc ngoại vi*** Trong an toàn máy tính, quá trình được gọi ra để xử lý dữ liệu theo một chính sách an toàn xác định trước khi giải phóng dữ liệu ra ngoài môi trường xử lý hoặc nhận dữ liệu từ một nguồn ngoài.

front office ***văn phòng trực tiếp*** Trong hoạt động ngân hàng, địa điểm tại đó tiến hành xử lý trực tiếp các hoạt động. *So sánh với* back office.

FRR ***FRR*** *Xem* false rejection rate.

FS *Xem* field separator.

fsck *Xem* file system check.

FSK *Xem* frequency shift keying.

FTAM *Xem* file transfer, access and management.

FTLS *Xem* formal top-level specification.

FTP ***FTP*** Viết tắt của File Transfer Program (chương trình chuyển tệp). *Xem* file transfer.

full duplex ***song công (hoàn toàn); sao hoàn toàn, FD, FDX*** (1) Trong truyền thông dữ liệu, song công hoàn toàn là chế độ truyền thông tin mà trong đó dữ liệu được truyền theo cả hai hướng đồng thời. *So sánh với* haff-duplex, simplex. *Đồng nghĩa với* duplex. (2) Trong tin học, sao hoàn toàn là sự sao chép đầy đủ một phương tiện xử lý dữ liệu bất kỳ.

fully connected network ***mạng nối đầy đủ, mạng nối hoàn toàn*** Trong truyền thông dữ liệu, mạng trong đó mỗi nút đều được nối trực tiếp với mọi nút khác. *Xem* node.

fully distributed costs ***chi phí phân phối hoàn toàn*** Trong truyền thông, hệ thống xác định các chi phí của những dịch vụ khác nhau do một hãng truyền thông công cộng cung cấp. Ở Mỹ tổng các chi phí hoạt động chấp nhận được và cơ sở cước phí được phân chia giữa những dịch vụ khác nhau phù hợp với các quy trình cố định do FCC thiết lập. *Xem* FCC.

fully functional dependent ***phụ thuộc hàm hoàn toàn*** Trong các cơ sở dữ liệu, tập hợp các thuộc tính A của quan hệ R là phụ thuộc hàm hoàn toàn vào tập hợp khác của các thuộc tính, B, của quan hệ R nếu A phụ thuộc hàm vào toàn bộ B chứ không phải vào tập con bất kỳ của B. Giả sử quan hệ chứa tên

nhân viên, số hiệu nhân viên và ban, và mỗi nhân biên trong một ban riêng đều có một số hiệu duy nhất. Khi đó tên nhân viên phụ thuộc hàm hoàn toàn vào số hiệu nhân viên và ban, bởi vì hai nhân viên ở các ban khác nhau có thể có cùng số hiệu. *Xem* attribute, functional dependence, normal forms, relation.

Fu Manchu ***virut Fu Manchu*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

functional dependence ***(sự) phụ thuộc hàm*** Trong các cơ sở dữ liệu, sự chỉ ra các mối quan hệ qua lại của các thuộc tính trong một quan hệ. Thuộc tính A của quan hệ R là phụ thuộc hàm vào thuộc tính B của quan hệ R nếu trong mọi thời điểm, mỗi giá trị của B đều có nhiều hơn một giá trị của A gắn với nó. Giả sử quan hệ chứa tên nhân viên, số hiệu nhân viên và ban, nếu mỗi nhân viên có một số hiệu duy nhất thì tên nhân viên là phụ thuộc hàm vào số hiệu nhân viên. Hãy lưu ý rằng số hiệu nhân viên không phụ thuộc hàm vào tên nhân viên vì hai nhân viên có thể có các tên giống nhau. *Xem* attribute, fully functional dependent, normal forma, relation.

functional group ***nhóm chức năng*** *Xem* ANSI - X.12, EDIFACT.

functional testing ***thử chức năng*** Trong an toàn máy tính, phần thử an toàn trong đó các đặc điểm của hệ thống đã quảng cáo được thử xem có hoạt động đúng không.

funds transfer ***(sự) chuyển tiền*** Trong hoạt động ngân hàng, sự chuyển trọn vẹn tiền trực tiếp giữa người gửi và người được hưởng. Sự chuyển tiền có thể gồm một hoặc nhiều giao dịch chuyển tiền. *Xem* funds transfer transaction. *Đồng nghĩa với* transfer.

funds transfer transaction ***giao dịch chuyển tiền, chuyển tác chuyển tiền*** Trong hoạt động ngân hàng, sự chuyển tiền trực tiếp giữa hai bên không liên quan tới bên trung gian nào ngoài dịch vụ thanh toán hoặc truyền thông. *Đồng nghĩa với* transfer.

funds type ***kiểu tiền*** Trong hoạt động ngân hàng, các đặc trưng của tiền bên trong một loại tiền tệ nào đó, liên quan tới khả năng sẵn có và tính cơ động, sự điều chỉnh mức sử dụng hoặc hối đoái, ví dụ ở Hoa Kỳ, "tiền cùng ngày" và "tiền ngày hôm sau"; ở Bỉ, "frăng chuyển đổi và "frăng tài chính".

fuzzy sector technique ***kỹ thuật cung mờ*** *Đồng nghĩa với* weak bits.

F-Word ***virut F-Word*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND, COM và COM, ảnh hưởng hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.



G *G Xem* giga.

galactic *có phạm vi rộng lớn, galactic* Trong các cơ sở dữ liệu, chỉ các dữ liệu có phạm vi rộng lớn và khả truy từ nhiều nơi và bởi nhiều ứng dụng.

Galois field *trường Galois* Trong mật mã, trường Galois $GF(p)$, trong đó p là số nguyên tố, là một hệ toán học với một tập hợp hữu hạn các phần tử và hai phép toán: phép cộng và phép nhân theo modulo p, mỗi phép toán có một phần tử đơn vị, 0 đối với phép cộng và 1 đối với phép nhân. Tồn tại các phép đảo đơn trị đối với mỗi phần tử và có thể áp dụng các luật kết hợp, phân phối và giao hoán.

Trong mật mã, $GF(2^n)$ được sử dụng. Một đa thức nhị thức $f(x)$ bậc n, tức là

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$$

trong đó các hệ số a_{n-1} v.v. là các chữ số nhị phân, được sử dụng để định nghĩa một số z sao cho $f(z) = 0$. Trường Galois $GF(2^n)$ là một tập các đa thức nhị thức $\{a_{n-1}z^{n-1} + \ldots a_1 z + a_0\}$. Ví dụ, với $GF(2^3)$, đa thức nhị thức $f(z) = z^3 + z + 1 = 0$, sẽ xác định một số z, và $GF(2^3)$ chứa các phần tử $\{0, 1, z, 1 + z, z^2, 1 + z^2, z + z^2, 1 + z + z^2\}$. Các phép toán được phép là phép cộng và phép nhân các đa thức nhị phân. Do đó

$(z^2 + 1) + z^3 = 1.$

Vì các hệ số được cộng theo modulo 2, nên cần chú ý rằng $z^3 + z + 1 = 0$,

$(z^2 + 1)z^2 = z^4 + z^2$

$= z.(z^3 + z + 1) + z$

$= z$

Các phần tử của trường Galois có thể được viết theo ký pháp nhị phân, do đó $a_{n-1}z^{n-1} + \ldots a_1 z + a_0$ có thể được biểu diễn bằng số nhị phân:

$a_{n-1}a_{n-2}\ldots a_1 a_0$

Do đó $z^2 + 1$ có thể được biểu diễn bằng 101. *Xem* field.

GAO *GAO* Viết tắt của U.S. General

Accounting Office (cơ quan kế toán chung của Hoa Kỳ).

garbage *rác liệu, rác* Trong tin học, dữ liệu và chương trình trong bộ nhớ không còn cần thiết nữa.

garbage collection *thu gom rác, thu gom dữ liệu hỏng, dọn rác liệu, dọn rác* (1) Trong tin học, cách nói để chỉ sự làm sạch các bản ghi không cần nữa khỏi tệp. (2) Trong tin học, loại bỏ các mục đã đánh dấu xóa (deleted) khỏi bộ nhớ chính để tạo không gian cho các chương trình hoặc dữ liệu mới. *Xem* file, main memory.

garbage in garbage out *vào rác ra rác, GIGO* Trong tin học, cách nói để phản ánh sự kiện là chất lượng đầu ra của máy tính phụ thuộc vào chất lượng đầu vào.

garble extension *mở rộng sai lệch* *Đồng nghĩa với* error extension, error propagation.

gateway *cổng nối, cổng vào* (1) Trong truyền thông dữ liệu, thiết bị để ghép nối các mạng sao cho một thiết bị đầu cuối có thể liên lạc với một thiết bị đầu cuối hoặc máy tính ở mạng khác. *So sánh với* bridge. *Đồng nghĩa với* communication server. (2) Trong hoạt động ngân hàng, mạng EFTPOS trong đó đó một người bán lẻ được nối trực tiếp với một nhà cung cấp truy nhập mà sau đó định hướng lại các giao dịch tới các cơ sở tài chính của khách hàng và người bán lẻ. *So sánh với* open system.

Gaussian distribution *phân bố Gauss* Trong toán học, phân bố xác suất do Gauss rút ra đối với phân bố sai số ở phép đo thực nghiệm. Nó được dùng trong truyền thông nhằm xác định xác suất để một tín hiệu mang thông tin sẽ vượt quá biến độ tạp nhiễu trên kênh. *So sánh với* Poisson distribution.

GCD *ƯSCLN* *Xem* greatest common divisor.

general purpose *đa dụng, đa năng* Chỉ hệ thống mà có thể áp dụng cho rất nhiều nhiệm vụ mà không có sự sửa đổi cơ bản. *So sánh với* special purpose.

general purpose computer *máy tính đa năng, máy tính đa dụng* Trong tin học, máy tính số được thiết kế để hoạt động trong rất nhiều ứng dụng. Nó có thể tương phản với máy tính chuyên dụng có phần cứng chuyên dụng và/hoặc phần mềm cho một mục đích riêng. Ví dụ điều khiển một quá trình công nghiệp. *So sánh với* special purpose.

General Services Administration *Quản trị dịch vụ chung* Cơ quan điều tiết của chính phủ liên bang Hoa Kỳ có trách nhiệm kiểm soát việc mua thiết bị, các cung ứng và dịch vụ bởi cán bộ và văn phòng thuộc chính phủ liên bang.

generation *thế hệ* (1) Trong tin học, số đo mức xa cách của một tệp so với tệp gốc. *Xem* father file. (2) Trong tin học, chỉ công nghệ dùng để chế tạo các thành phần của một máy tính. (3) Trong lập trình, chỉ lớp các phương tiện được cung cấp trong các ngôn ngữ lập trình. *Xem* fourth-generation language.

genuine *mật mã thực* Trong mật mã, một mã pháp không phải mã đồng nhất, tức là bản gốc không đồng nhất với bản mã. *So sánh với* identity.

geophone ***máy thu địa chấn*** Trong an toàn vật lý, dạng máy dò địa chấn, dùng để chôn ngầm dưới đất, nó cảm biến các tần số truyền trong đất do hoạt động ở sâu dưới đất hoặc trên bề mặt đất. *Xem* seismic sensor.

GF(p) ***GF(p)*** *Xem* Galois field.

Ghost Boot ***virut Ghost Boot*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm cung khởi động của đĩa mềm và đĩa cứng, làm sai lạc cung khởi động, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

Ghost COM ***virut Ghost COM*** Trong an toàn máy tính, virut lây nhiễm các tệp COM, làm sai lạc cung khởi động, các tệp chương trình và OVL. *Xem* virus names.

GHz ***GHz*** Ký hiệu của gigahec. *Xem* giga.

GIDEP ***chương trình GIDEP*** Viết tắt của U.S. Government Industry Data Exchange Program (chương trình trao đổi dữ liệu công nghiệp của Hoa Kỳ).

giga ***giga*** Một tỷ, tức là 10^9.

GIGO *Xem* garbage in garbage out.

GISA ***GISA*** Viết tắt của German Information Security Agency (cơ quan an toàn thông tin Đức). *Xem* ZSI.

global ***biến toàn cục*** Trong lập trình, một biến có thể truy nhập giá trị của nó suốt toàn bộ chương trình. *So sánh với* local.

GMT ***GMT*** *Xem* Greenwich mean time. *Đồng nghĩa với* coordinated universal time. *So sánh với* local.

go back n ***trở lại n bước*** Trong truyền thông dữ liệu, giao thức dùng trong hệ xử lý liên hợp. Khi một khung dữ liệu bị sai lạc tới, máy thu vứt bỏ tất cả các khung sau đó cho tới khi khung sai lạc hoặc mất được truyền lại và nhận lại đúng đắn. *So sánh với* selective repeat. *Xem* frame, pipelining.

good value ***giá trị đúng*** Trong hoạt động ngân hàng, cách diễn đạt để yêu cầu áp dụng một ngày có giá trị hồi cố xác định đối với một giao dịch.

GOSIP ***lược tả GOSIP*** Trong các tiêu chuẩn, viết tắt của Government OSI Profile (lược tả OSI của chính phủ), đặc tả các tiêu chuẩn và các mục chọn bên trong các tiêu chuẩn vốn thích hợp cho việc sử dụng của chính phủ Hoa Kỳ. GOSIP cung cấp các hướng dẫn cài đặt chi tiết cho các hệ OSI để đảm bảo khả năng vận hành qua lại giữa các sản phẩm từ những người bán khác nhau. *Xem* open systems interconnection.

graceful degradation ***xuống cấp nhẹ*** *Xem* fail soft.

grade A central station ***trạm trung tâm cấp A*** Trong an toàn vật lý, một trong các cấp phòng thí nghiệm được bảo hiểm của các trạm chính. Sự phân loại phụ thuộc vào mức độ bảo vệ đã đề ra và các tiêu chuẩn về thiết bị, nhân sự, các thủ tục, các hồ sơ và việc bảo trì. *So sánh với* grade AA central station, grade B central station. *Xem* central station, Underwriter's Laboratory.

grade AA central station ***trạm trung tâm cấp AA*** Trong an toàn vật lý, một trong các cấp phòng thí nghiệm được bảo hiểm của các trạm trung tâm. Sự phân loại phụ thuộc vào mức độ bảo

vệ đã đề ra và các tiêu chuẩn về thiết bị, nhân sự, các thủ tục, các hồ sơ và bảo trì. *So sánh với* grade A central station, grade B central station. *Xem* central station, Underwriter's Laboratory.

grade B central station ***trạm trung tâm cấp B*** Trong an toàn vật lý, một trong những cấp phòng thí nghiệm được bảo hiểm của trạm trung tâm. Sự phân loại phụ thuộc vào mức độ bảo vệ đã đề ra và các chuẩn cứ về thiết bị, nhân sự, các thủ tục, các hồ sơ và sự bảo trì. *So sánh với* grade A central station, grade AA central station. *Xem* central station, Underwriter's Laboratory.

grade of service ***cấp dịch vụ*** Trong truyền thông, số đo chất lượng của dịch vụ theo mức khả dụng của các mạch khi thực hiện các cuộc gọi. Cấp dịch vụ được đo trong giờ bận nhất của ngày và thường được biểu thị như tỷ lệ các cuộc gọi có thể không thành công trong lần quay số đầu tiên do những hạn chế của thiết bị.

Graham-Shamir knapsack cipher ***mã pháp ba lô Graham-Shamir*** Trong mật mã khóa công khai, dạng mật mã ba lô được coi là an toàn hơn, nhanh hơn và dễ cài đặt hơn so với mật mã ba lô Merkle-Hellman ban đầu. Vectơ ba lô "dễ" được biểu thị như một ma trận các chữ số nhị phân. Mỗi hàng của ma trận biểu diễn một trong các số nguyên của vectơ ba lô $(a_1, a_2, ..., a_n)$. Một hàng riêng lẻ a_j được biểu thị bằng một hàng chữ số nhị phân (R_j, I_j, O_j, S_j) trong đó:

R_j = dòng bit ngẫu nhiên dài.

I_j = n bit mà tất cả đều là bằng 0 trừ bit thứ j.

O_j = xâu các bit 0.

S_j = dòng bit ngẫu nhiên thứ hai.

Ví dụ:

	R	I	O	S
a_1 =	0101	1000	000	1010
a_2 =	1110	0100	000	1110
a_3 =	1011	0010	000	0110
a_4 =	1101	0001	000	0010

Nếu bản gốc 1100 được mã bằng vectơ này thì các xâu bit a_1 và a_2 có thể được thêm vào để tạo thành thông báo

	R	I	O	S
C =	10011	1100	001	1000

Thông báo này không che dấu bản gốc ban đầu vì:

- khối I tương ứng với thông báo ban đầu;
- tổng các chữ số trong khối S bị chặn trước không làm ảnh hưởng tới khối I vì mọi số mang sang từ khối S đều bị giữ trong phạm vi khối O mà để đạt được mục đích này, khối này phải đủ dài.

Vectơ ba lô dễ có thể được biến đổi thành một ba lô khó, để mã hóa, theo cách tương tự với phương pháp mã ba lô Merkle-Hellman. Như vậy, hai số nguyên w và m được chọn và các hàng của ma trận được nhân với w theo (mod m). Ma trận là khóa mã hóa công khai và thông báo được mã hóa như trong mã pháp Merkle-Hellman, các hàng của ma trận tương ứng với vectơ ba lô $(a_1, a_2, ..., a_n)$. Ở đầu thu thông báo đã mã được nhân với w^{-1} (mod m) và các bit biểu diễn bản gốc ban đầu được trích ra từ khối I. *So sánh với* RSA. *Xem* knapsack cipher, Merkle-Hellman knapsack cipher, modulo arithmetic.

superincreasing series.

grammar ***ngữ pháp, văn phạm*** Trong tin học, phương pháp đặc tả một ngôn ngữ hình thức. Ngữ pháp bao gồm tập hợp các quy tắc, hoặc các sản phẩm, tập các ký hiệu kết thúc, tập các ký hiệu không kết thúc và ký hiệu khởi đầu. Các quy tắc dự phòng tạo ra xâu ký hiệu này từ xâu ký hiệu khác; các ký hiệu không kết thúc có thể được biến đổi thành các xâu chứa các ký hiệu kết thúc và/hoặc không kết thúc. Xâu khởi đầu phải là ký hiệu khởi đầu xác định cho ngữ pháp và các sản phẩm có thể áp dụng có thể được áp dụng thành công cho tới khi xâu kết quả chỉ chứa các ký hiệu kết thúc. Sau đó xâu cuối cùng này có thể là xâu khả chấp trong ngôn ngữ tương ứng. *Xem* formal language.

grandfather file ***tệp ông*** *Xem* father file.

granularity ***độ kết hạt, độ chi tiết*** (1) Trong an toàn máy tính, độ mịn hoặc độ thô tương đối mà một cơ chế có thể điều chỉnh được. Câu nói "độ kết hạt một người sử dụng đơn lẻ" có nghĩa là cơ chế kiểm soát truy nhập có thể được điều chỉnh để tính đến hoặc loại trừ một người sử dụng đơn lẻ bất kỳ. (2) Trong an toàn máy tính, mức độ cách ly mà một cấp dịch vụ hoặc cơ chế an toàn riêng nào đó được gọi ra. *Xem* isolation.

graphic annunciator ***hệ biểu đồ chỉ báo*** Trong an toàn vật lý, bảng mô phỏng bản đồ phương tiện và các vị trí của các bộ cảm biến hoặc các vùng báo động. Trạng thái của các bộ cảm biến và các báo động được đưa ra một cách trực quan. *Xem* annunciator.

Gray code ***mã Gray*** Trong mã hóa, mã nhị phân trong đó các số tuần tự được biểu thị bằng các biểu thức nhị phân, mỗi biểu thức nhị phân khác với biểu thức trước đó ở một vị trí duy nhất:

Thập phân	Nhị phân	Gray
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111

greatest common divisor ***ước số chung lớn nhất*** Trong toán học, số nguyên lớn nhất là ước của hai số nguyên xác định, ví dụ như ước số chung lớn nhất của 8 và 12 là 4. *So sánh với* least common multiple. *Xem* relatively prime.

Greenwich Mean Time ***giờ Greenwich trung bình*** *Đồng nghĩa với* coordinated universal time.

grid sensor ***lưới cảm biến*** *Đồng nghĩa với* burglar alarm pad.

group ***nhóm*** (1) Trong truyền thông, cụm 12 kênh điện thoại tạo thành dải tần 48 kHz của hệ truyền sóng mang. *Xem* channel. (2) Trong các cấu trúc dữ liệu, tập hợp các bản ghi có liên quan có cùng giá trị đối với một trường cụ thể trong tất cả các bản ghi. *Xem* field, record.

grouping ***kết nhóm*** Trong an toàn dữ liệu, dạng giới hạn ô trong đó, các nhóm giá trị thuộc tính được kết hợp lại sao

cho không có ô nào chứa dữ liệu lấy từ một số hạn chế các bản ghi. Ví dụ, nếu các khoảng lương 10.000 - 11.000 và các khoảng tuổi 64 - 65 đưa ra các thống kê nhạy cảm thì có thể dùng khoảng lương từ 10.000 tới 12.000 và tuổi khoảng 63 - 65. *So sánh với* audit expert, cell suppression, implied queries control, overlap control, query set size control. *Xem* cell restriction. *Đồng nghĩa với* rolling up.

GSA *Xem* General Services Administration.

GSIS ***nhóm GSIS*** Viết tắt của US Group for the Standardization of Information Services (Nhóm tiêu chuẩn hóa các dịch vụ thông tin của Mỹ).

guard ***bảo vệ*** Trong an toàn cơ sở dữ liệu, *đồng nghĩa với* filter.

guard band ***dải bảo vệ*** (1) Trong tin học, phần băng từ trống tách bạch hai vệt thông tin, nhờ đó ngăn được nhiễu tín hiệu. (2) Trong truyền thông, dải hẹp tần số không sử dụng giữa các kênh được phân phối, nhằm giảm đến tối thiểu khả năng nhiễu lẫn nhau. Ví dụ, phần lớn các kênh truyền hình đều có dải bảo vệ 0,5 MHz ở mỗi bên kênh.

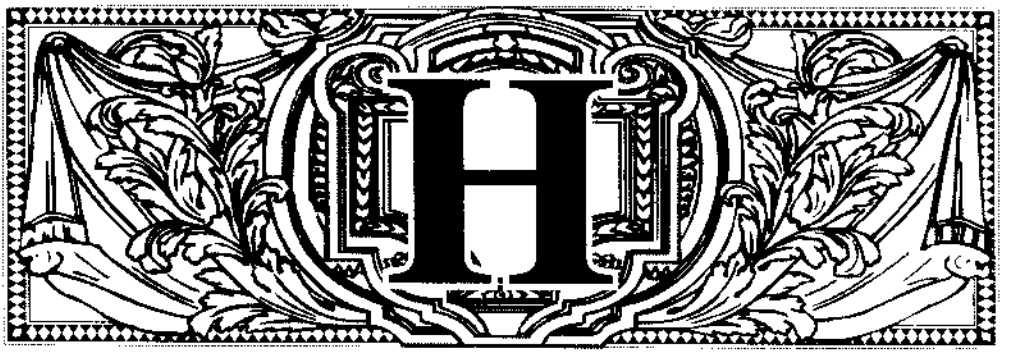
guarding ***phòng sai*** Chức năng ngăn ngừa hoạt động sai của một thiết bị.

Guardwire ***hệ Guardwire*** Trong an toàn vật lý, tên thương mại cho một hệ phát hiện xâm nhập. Guardwire là cáp kết thành hàng rào an toàn và nó phát hiện các rung động do những kẻ xâm nhập trèo rào gây ra v.v.. Cáp cấu tạo từ hai sợi vật liệu dựa trên ferit, tác dụng như các cực của một nam châm vĩnh cửu; giữa những cực đó là một cặp dây dẫn, cùng với hai dây cảm ứng di chuyển tự do trong một khe không khí. Khi cáp di chuyển, một dòng điện tạo ra trong các dây cảm ứng. Hệ thống này rất nhạy và các tín hiệu tạo ra bởi chuyển động của cáp có thể được xử lý để giảm đến tối thiểu các báo động giả.

Guillou-Quisquater ***thuật toán Guillou-Quisquater*** Trong mật mã, thuật toán dùng để tạo ra các chữ ký số. *Xem* digital signature.

Guppy ***virut Guppy*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND. COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Gypsy ***ngôn ngữ Gypsy*** Trong an toàn máy tính, ngôn ngữ đặc tả chương trình hình thức kết hợp và ngôn ngữ bậc cao có thể kiểm chứng được, phát triển ở Đại học Texas và dùng kết hợp với một hệ kiểm chứng đầy đủ. *Xem* Affirm, Hierarchical Development Methodology, Ina Jo Formal Methodology.



hacker ***tin tặc, hacker*** (1) Trong tin học, người mê tin học. Thuật ngữ này thường chỉ người tìm thấy thích thú trong thực nghiệm các hệ phần cứng hệ thống, phần mềm và truyền thông. *Xem* cracker. (2) Trong an toàn dữ liệu, người sử dụng không được phép cố nhập vào một mạng máy tính bằng cách vô hiệu hóa các hệ kiểm soát truy nhập của hệ thống. *Xem* access control, crasher, phracker, telephone intrusion. *Đồng nghĩa với* terminal thief.

hack hack ***quét*** *Đồng nghĩa với* scanning.

half duplex ***bán song công, HD, HDX*** Trong truyền thông dữ liệu, sự truyền diễn ra trên một đường tại một thời điểm trong mạch hai đường. *So sánh với* full-duplex. *Xem* duplex.

halon system ***hệ halon*** Trong an toàn vật lý, hệ thống chữa cháy, so với các hệ phun nước nó có ưu điểm là không làm hư hại thiết bị cũng không gây hại cho con người. Tuy nhiên việc sử dụng nó bị hạn chế bởi những thỏa thuận khác nhau do tác động đến môi trường của nó. *Xem* bromochlorodifluoromethane.

Hamming code ***mã Hamming*** Trong mã hóa, mã phát hiện lỗi trước có khả năng phát hiện và sửa các lỗi một bit nhưng không sửa được phần lớn các lỗi nhiều bit. *Xem* forward error correction.

hand geometry analysis ***phân tích hình học tay*** Trong kiểm soát truy nhập, kỹ thuật sinh trắc dựa trên các phép đo về tay của người sử dụng. Kỹ thuật này đặc biệt thích hợp đối với truy nhập có kiểm soát ở điểm nhập, nơi tốc độ lưu lượng cao. Thiết bị có thể quét dữ liệu liên quan tới kích thước tay, cấu trúc xương, gang tay và/hoặc mẫu các đường trên lòng bàn tay. Có thể thu được ảnh ba chiều nhờ camera video. Các suất lỗi loại 1 và loại 2 bằng nhau điển hình 1% đã được báo cáo. *Xem* biometrics, Type 1 error, Type 2 error.

handled by ***nắm bắt*** Trong an toàn máy tính, các hoạt động được thực hiện trên dữ liệu trong một hệ thống thông tin tự động hóa, như thu thập, xử lý, vận chuyển, lưu trữ, truy tìm, phân loại, truyền, phân phối và kiểm tra. *Xem* AIS.

handler ***bộ điều khiển, mục quản, bộ quản*** Trong tin học, chương trình chịu sự điều khiển của hệ điều hành, nó điều khiển một thiết bị ngoại vi riêng, như đĩa hoặc máy in, và cũng xử lý các ngắt. *Xem* interrupt.

handling caveats ***dấu báo trước xử lý*** *Xem* special markings.

handling restrictions ***giới hạn xử lý*** *Xem* special markings.

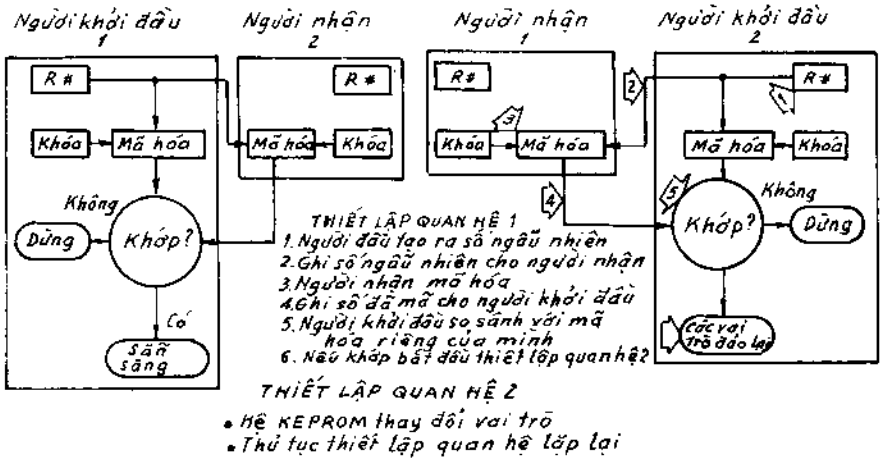
handshaking ***thiết lập quan hệ, xác định đặt quan hệ*** (1) Trong truyền thông dữ liệu, sự trao đổi các tín hiệu định trước khi cuộc nối lần đầu tiên được tiến hành qua một giao diện, để xác nhận nó làm việc thỏa đáng và ngăn ngừa thất thoát dữ liệu. *Xem* interface, protocol. (2) Trong xác thực, thủ tục đảm bảo rằng cuộc liên lạc đã được thiết lập giữa hai nút thực sự trong một mạng truyền thông. Các thủ tục thiết lập quan hệ đảm bảo rằng, một kẻ tấn công không thể giả dạng như một nút giả thực thụ. Một phương pháp thiết lập quan hệ dựa vào hai nút thực sự dùng chung một khóa mật. Khi nút A thiết lập liên lạc với nút B thì nút A tạo ra một số ngẫu nhiên (RN), mã hóa nó bằng khóa mật dùng chung với nút B, và truyền thông báo đã mã cho B. Tại nút B, số ngẫu nhiên được tìm ra bằng cách giải mã. Số ngẫu nhiên này chịu tác dụng của một thuật toán không bí mật, kết quả $(f(RN))$ được mã hóa bằng cùng khóa dùng chung và được truyền ngược về nút A. Ở nút A, thông báo được giải mã và được so sánh với giá trị $f(RN)$ tạo ra bằng cách cho số ngẫu nhiên ban đầu chịu tác dụng của thuật toán f. *Xem* cryptographic key, handshaking procedure, masquerading, midnight attack.

handshaking procedure ***thủ tục móc nối quan hệ, thủ tục thiết lập quan hệ*** Trong an toàn máy tính, đối thoại giữa người sử dụng và một máy tính, giữa máy tính này với máy tính khác, giữa chương trình với một chương trình khác nhằm định danh một người sử dụng và xác thực danh tính của người đó, thông qua một loạt các câu hỏi và câu trả lời dựa trên thông tin đã lưu trước đó trong máy tính, hoặc do bên khởi phát đối thoại cung cấp vào máy tính. *Xem* handshaking. *Đồng nghĩa với* password dialogue.

Hanover Hacker ***hacko Hanover*** Trong an toàn máy tính, Markus Hess, một hacko thâm nhập các mạng Arpanet và Milnet từ Đức và được Clifford Stoll lần ra dấu vết như báo cáo trong cuốn sách của ông nhan đề "Tổ chim cúc cu". *Xem* Chaos Club.

Happy Day ***virut Happy Day*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Happy New Year ***virut Chúc mừng năm mới*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các



handshaking: *thiết lập quan hệ.* Trình tự thiết lập quan hệ xác thực bao gồm việc tạo ra và mã hóa (theo một khóa mật) các số ngẫu nhiên bởi hai EPROM Intel 27916 được khóa mã giống hệt nhau. Hai EPROM so sánh các số đã được mã hóa, sau đó trao đổi các vai trò và lặp lại trình tự. Sự không phù hợp dẫn đến không có khả năng truy nhập được vào hệ máy tính hoặc nội dung của EPROM.

tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

hard disk ***đĩa cứng*** Trong tin học, thiết bị nhớ truy nhập trực tiếp với đĩa từ cứng. Mật độ nén cao và tốc độ dữ liệu cao đòi hỏi đĩa quay với tốc độ cao với các đầu đọc/ghi cách mặt đĩa cỡ 1 micromet. Những yêu cầu đó đòi hỏi kỹ thuật chính xác và môi trường vận hành cực kỳ tinh khiết. Các hệ đĩa cứng máy chính thông thường cung cấp các chồng đĩa cả cố định lẫn tháo lắp được, nhưng công nghệ như thế là quá đắt đối với thị trường máy vi tính. Công nghệ đĩa Winchester, sử dụng bộ thiết bị hàn kín để tránh bụi hoặc khói có thể gây sự cố đầu từ, là tương đối rẻ và chiếm lĩnh thị trường thiết bị nhớ dự phòng hiệu năng cao đối với máy vi tính. *So sánh với* floppy disk.

hard error ***lỗi cứng*** Trong tin học, lỗi trong đọc dữ liệu từ một đĩa từ mà không thể sửa được. Sự mất dữ liệu được coi là không thể khôi phục được. *So sánh với* soft error. *Xem* magnetic disk.

hardware ***phần cứng*** Trong tin học, thiết bị vật lý như ổ đĩa, bộ xử lý hoặc máy in, đối lập các chương trình, thủ tục, quy tắc và hệ tài liệu có liên quan (tức phần mềm). *So sánh với* firmware, software.

hardware handshaking ***kỹ thuật liên kết phần cứng, móc nối quan hệ phần cứng*** Trong truyền thông dữ liệu, sự chuyển các ký tự điều khiển (ví dụ, ACK, NAK, XON, XOFF) giữa hai thiết bị, để điều khiển luồng thông tin

giữa các thiết bị. *Xem* ACK, handshaking, XON/XOFF protocol.

hardware interrupt ***ngắt phần cứng*** Trong tin học, một ngắt kích hoạt bởi một thiết bị ngoại vi hoặc một thiết bị bên ngoài khác nào đó. Trong một thao tác ngắt phần cứng điển hình, thiết bị bên ngoài gửi đi một tín hiệu, trên tuyến yêu cầu ngắt, tới CPU. Nếu CPU có thể đáp ứng ngắt, thì nó báo nhận yêu cầu và thiết bị bên ngoài đặt một byte lên bus dữ liệu chỉ báo kiểu tác động ngắt đã yêu cầu. CPU lưu cất các chi tiết về những trạng thái hiện thời của nó, các thanh ghi, các cờ, con trỏ địa chỉ trở về v.v. lên một ngăn xếp. Byte trên bus dữ liệu từ thiết bị bên ngoài được dùng để lựa chọn một vị trí, bên trong vị trí nhớ xác định trước, vốn chứa địa chỉ của thủ tục ngắt đã yêu cầu. CPU thực hiện thủ tục ngắt và sau đó khôi phục thao tác đã ngắt của nó. Các ngắt phần cứng là quan trọng trong các virut máy tính bởi vì ngắt đảm bảo gọi ra đoạn mã có thể chứa một virut. *So sánh với* software interrupt. *Xem* virus.

hardware redundancy ***dư thừa phần cứng, dự phòng phần cứng*** Trong biện pháp tin cậy, sự sử dụng hệ mạch bên ngoài hoặc thiết bị bên ngoài để dự phòng một mức độ kháng lỗi. *Xem* dual redundancy, hybrid redundancy, modular redundancy, NMR, self-checking circuit, structural redundancy, triple modular redundancy.

hardware security ***an toàn phần cứng*** Trong an toàn máy tính, các phương tiện riêng của thiết bị hoặc thiết bị máy tính dùng trong hệ xử lý dữ liệu để ngăn ngừa truy nhập bất hợp pháp tới các tài nguyên dữ liệu hoặc hệ thống.

hardwired ***nối cứng, cứng hóa*** Trong tin học, sự cài đặt phương tiện có sử dụng các mạch logic (phần cứng) chứ không sử dụng phần mềm. *Xem* hardware, logic circuit.

harmful event ***biến cố có hại*** Trong quản lý rủi ro, trường hợp đe dọa tác động tới chỗ yếu của hệ thống, gây bất lợi cho hệ thống. Điều này có thể bao gồm hư hại vật lý cho các phần tử của hệ thống hoặc có thể thể hiện ở: từ chối phục vụ, sử dụng không được phép các tài nguyên dữ liệu hoặc hệ thống, xử lý không được phép dữ liệu hoặc chương trình nhằm mục đích chiếm đoạt, hoặc tiết lộ không được phép thông tin. *Xem* threat, vulnerability.

harmonized criteria ***(các) tiêu chuẩn cân đối hóa*** *Xem* information technology security evaluation criteria.

hartley ***hartley, hatli*** Trong toán học, đơn vị thông tin dựa trên thang mười giá trị (tức là lượng thông tin có thể rút ra từ hiểu biết về sự xuất hiện của một biến cố ngẫu nhiên trong 10 biến cố đồng xác suất). *Xem* information content.

hash function ***hàm băm, hàm hash*** Trong toán học, hàm nhân một số đầu vào bất kỳ và tạo ra một đầu ra có độ dài cố định. Hàm nhận thực sự những số đầu vào từ một miền lớn và tạo ra một đầu ra trong một khoảng hạn chế. *Xem* hashing, one-way function.

hashing ***kỹ thuật băm*** Trong tin học, phương pháp cấp phát các vị trí nhớ

cho các bản ghi của một tệp. Một thuật toán được áp dụng cho khóa bản ghi để tạo ra địa chỉ vị trí. Với những thuật toán được thiết kế thích hợp, phương pháp này tạo ra một sự phân bố các vị trí nhớ đồng đều hơn so với nếu chỉ dùng một quan hệ tuyến tính đơn giản, nhất là khi phạm vi các khóa rộng và các bản ghi tụ nhóm thành một số dài nhất định. *Xem* file, key, record.

hash total ***tổng băm, tổng kiểm tra*** Trong tin học, con số thu được nhờ một số phép toán trên tất cả các mục trong một tập hợp dữ liệu và dùng cho các mục đích kiểm tra. Sự tính lại tổng băm và so sánh với giá trị đã tính trước đó cho phép kiểm tra sự mất mát hoặc sai lạc dữ liệu. *So sánh với* checksum, MAC.

hat box ***hộp nắp trong suốt*** *Đồng nghĩa với* shrink wrapped license.

Hayes ***chuẩn modem Hayes*** Trong truyền thông dữ liệu, chuẩn modem công nghiệp của Mỹ đối với các thủ tục thiết lập cuộc gọi và điều khiển luồng. Các lệnh modem Hayes có thể được bắt đầu bởi một chương trình trong máy tính cá nhân (ví dụ, để quay số tự động hoặc đáp tự động). Phần mềm truyền thông máy tính cá nhân không đồng bộ nhất tuân theo các giao thức Hayes. *Xem* auto dial, auto answer, asynchronous.

hazard ***nguy cơ sự cố*** Trong quản lý rủi ro, một phần tử hoặc điều kiện có khả năng gây thiệt hại. *Xem* threat.

HD *Xem* half duplex.

HDLC *Xem* high-level data link control.

HDM *Xem* hierarchical development methodology.

HDX *Xem* half duplex.

head crash ***sự cố đầu từ*** Trong tin học, sự cố ở ổ đĩa trong đó đầu từ chạm mặt đĩa cứng quay nhanh dẫn tới hư hại vật ký và sai lạc dữ liệu.

header ***tiêu đề, đoạn đầu; thông tin mở đầu; dòng đầu trang*** (1) Trong truyền thông dữ liệu, đoạn đầu là phần đầu tiên của thông báo hay gói tin chứa thông tin căn bản cho xử lý gói hoặc thông báo, nhưng không phải là một phần của văn bản thông báo (ví dụ, thông tin định tuyến, nơi nhận). *Xem* packet switching. (2) Trong tin học, thông tin mở đầu là thông tin đã mã hóa cho biết chi tiết về tập hợp dữ liệu (ví dụ, độ dài) nhưng không phải là một phần của bản thân dữ liệu. *Xem* header label.

header label ***nhãn đầu, nhãn tiêu đề*** Trong tin học, nhãn đứng trước các bản ghi dữ liệu của một tệp và chứa thông tin mô tả về tệp (ví dụ, tên tệp, số hiệu cuộn v.v.). *Xem* file, header.

heap ***khối xếp, vùng nhớ heap*** Trong tin học, vùng nhớ dùng để phân phối các cấu trúc dữ liệu; không giống như ngăn xếp, ở đây không có những hạn chế đối với các chế độ truy nhập vào dữ liệu đã nhớ. *So sánh với* stack.

heat detector ***bộ dò nhiệt*** Trong an toàn vật lý, thiết bị phát hiện hoặc một điều kiện đạt được một nhiệt độ cố định, hoặc phát hiện tốc độ thay đổi nhiệt độ vượt quá một giá trị xác định trước nào đó.

H

help *trợ giúp* Trong lập trình, phương tiện do một số bộ chương trình phần mềm tạo ra cho phép người dùng thu được thông tin ở một số phần mềm khía cạnh về bộ chương trình khi vận hành. Ở một số bộ chương trình, phương tiện trợ giúp được gọi ra bởi phím chức năng của chương trình, và nội dung của nó phụ thuộc vào giai đoạn gọi bộ chương trình. *Xem* software package.

hertz *hec* Trong truyền thông, đơn vị tần số, một chu kỳ mỗi giây, ký hiệu Hz.

heterogeneous computer network *mạng máy tính không đồng nhất* Trong truyền thông dữ liệu, mạng các máy tính chủ không giống nhau, vì chúng do các nhà sản xuất khác nhau đưa ra. *So sánh với* homogeneous computer network. *Xem* host computer.

heterogeneous multiplex *dồn kênh không đồng nhất* Trong truyền thông dữ liệu, cấu trúc dồn kênh trong đó các kênh mang thông tin không truyền ở cùng tốc độ báo hiệu dữ liệu. *So sánh với* homogeneous multiplex. *Xem* data signalling rate.

heuristic *thuật phỏng đoán, oristic* Trong toán học, cách tiếp cận thử sai gồm các ước lượng lần lượt ở mỗi bước thực hiện trong quá trình đạt tới kết quả cuối cùng. Trái lại, thuật toán biểu diễn cách tiếp cận nhất quán trong quá trình đi tới kết quả tối ưu. *So sánh với* algorithm.

hex *Xem* hexadecimal.

hexadecimal *thập lục phân* Trong toán học, hệ đếm với cơ số 16. Hệ đếm này được dùng do một byte gồm tám bit có thể được biểu diễn thuận tiện như hai chữ số thập lục phân. Các chữ số giữa 10 và 15 thập phân được biểu diễn tương ứng bởi các chữ cái A tới F (ví dụ, số thập phân 26 có thể được biểu diễn, như 1A thập lục phân). *Xem* byte, radix.

hico *độ kháng từ cao* *Đồng nghĩa với* high coercivity. *Xem* high coercivity card.

hidden files *(các) tệp ẩn* Trong tin học, tệp không phát hiện được bằng cách rà soát thư mục bình thường. Những tệp như thế thường là một phần của hệ điều hành và sẽ được báo cáo bởi một lệnh kiểm tra đĩa.

hidden object *đối tượng ẩn, đối tượng khuất* *Xem* persistent object.

hidden sections *(các) mục ẩn* Trong an toàn máy tính, các mục chọn thực đơn hoặc toàn bộ các thực đơn con mà người sử dụng không nhìn thấy hoặc truy nhập được do thiếu sự ủy quyền thích hợp.

hierarchical computer network *mạng máy tính phân cấp* Ở các mạng máy tính, mạng mà ở đó, các hoạt động liên quan tới điều khiển và xử lý được thực hiện ở nhiều mức bởi các máy tính thích hợp riêng với các nhiệm vụ mà chúng phải thi hành.

hierarchical database *cơ sở dữ liệu phân cấp* Cơ sở dữ liệu cho phép các bản ghi liên hệ với nhau theo ánh xạ một tới *n* (ví dụ, một bản ghi của nhân viên có thể trỏ tới một số bản ghi độc lập). Do đó các bản ghi liên quan với nhau theo cấu trúc cây. *So sánh với*

network database, relational database. *Xem* tree database, tree structure.

hierarchical decomposition ***phân tích theo thứ bậc*** Sự rút gọn có cấu trúc, có trật tự một hệ hoặc một thành phần thành các phần tử nguyên thủy.

hierarchical development methodology ***hệ phương pháp luận phát triển phân cấp*** Trong an toàn máy tính, phương pháp luận kiểm chứng và đặc tả hình thức được phát triển ở SRI quốc tế. HDM dựa trên một ngôn ngữ đặc tả chuyển trạng thái phi thủ tục, là ngôn ngữ Special và nó cung cấp công cụ phân tích luồng an toàn, MLS, để kiểm chứng các tính chất an toàn nhiều mức của đặc tả giao diện người dùng. *Xem* Affirm, Gypsy, Ina Jo Formal Development Methodology, MLS, security flow anslysis, Special.

hierarchical directory ***thư mục phân cấp*** *Đồng nghĩa với* tree structured directory.

hierarchical network ***mạng phân cấp*** Trong truyền thông dữ liệu, mạng được đồng bộ hóa thông qua việc sử dụng các nhịp đồng hồ, trong đó một số đồng hồ có điều khiển nhiều hơn những đồng hồ khác. Như vậy tốc độ hoạt động của mạng là trung bình theo trọng số của tốc độ của mọi đồng hồ. *So sánh với* democratic network.

high coercivity ***độ từ kháng cao*** Trong kiểm soát truy nhập, thuật ngữ dùng để chỉ các thẻ sọc từ, trong đó vật liệu từ có một độ từ kháng lớn hơn 2500 ơstet. *So sánh với* low coercivity card, oersted.

high coercivity card ***thẻ từ kháng cao*** Trong kiểm soát truy nhập, thẻ sọc từ sử dụng sọc từ bằng vật liệu từ kháng cao. Độ từ kháng của vật liệu sọc từ liên quan tới độ lớn của từ trường, cần thiết để xóa hoặc sửa đổi các dữ liệu đã ghi trên sọc. Ở các thẻ ngân hàng truyền thống, người ta dùng vật liệu có độ kháng từ thấp, cỡ 300 ơstet. Dữ liệu trên những thẻ như thế có thể xóa được bằng nam châm thông thường và sửa đổi được bằng những thiết bị đọc/ghi sọc từ tiêu chuẩn. Trong một số lĩnh vực ứng dụng, các thẻ với vật liệu từ kháng cao được sử dụng, tức là độ từ kháng quá 2500 ơstet. Những thẻ như vậy ít có xu hướng bị sai lạc ngẫu nhiên hơn và kẻ tấn công có thể phải có thiết bị chuyên dụng tốn kém hơn để sửa dữ liệu. Độ từ kháng của vật liệu liên quan tới lực từ cần thiết để thay đổi từ tính của thẻ. Tuy nhiên, vật liệu từ kháng thấp và cao có thể có cùng độ từ dư, do đó tín hiệu tạo ra bởi dữ liệu sọc từ ở bộ đọc có thể giống nhau đối với vật liệu từ kháng thấp và cao. Do đó một bộ đọc sọc từ có thể chấp nhận các thẻ từ kháng cả cao lẫn thấp. Nếu thiết bị chấp nhận một thiết bị cũng ghi lên thẻ, ví dụ một ATM mà có thể ghi một độ lệch, thì một thiết bị nhận các thẻ từ kháng thấp có thể đọc, nhưng không ghi vào thẻ từ kháng cao. *Xem* ATM, coercivity, magnetic stripe card, oersted, remanence.

high energy media ***phương tiện năng lượng cao*** *Đồng nghĩa với* Type 2 magnetic media.

high-level data link control ***điều khiển liên kết dữ liệu bậc cao, HDLC*** Trong truyền thông dữ liệu,

giao thức tầng liên kết dữ liệu chuẩn do Tổ chức tiêu chuẩn hóa thế giới xác định. Nó có khuôn thức dữ liệu thực sự đồng nhất với điều khiển liên kết dữ liệu đồng bộ, cho phép các thiết bị từ những nhà sản xuất khác nhau tương hợp với nhau và chuẩn hóa các bó thông tin giữa chúng. *Xem* ISO, protocol, synchronous data link control.

high-level language ***ngôn ngữ bậc cao*** Trong tin học, ngôn ngữ cho phép người lập trình định rõ một tập hợp các lệnh dưới dạng hướng tới bản chất của bài toán chứ không phải thao tác chi tiết hóa của máy tính. *So sánh với* low level language.

high-level protocol ***giao thức bậc cao*** Trong truyền thông dữ liệu, giao thức cho phép người sử dụng thực hiện các chức năng ở mức cao hơn là truyền đơn thuần các luồng hoặc các khối dữ liệu. *Xem* protocol.

high-speed ***tốc độ cao*** Trong truyền thông, chỉ các tốc độ truyền vượt quá những tốc độ thông thường qua các kênh cấp tiếng nói (tức là, quá 9600 bit mỗi giây). *Xem* medium speed, narrow band.

high-speed multiplex link ***liên kết dồn kênh tốc độ cao*** Trong truyền thông dữ liệu, liên kết tốc độ cao qua đó nhiều tín hiệu được kết hợp và sau đó được tách ra ở đầu xa của mạch. *Xem* multiplexing.

hit ***so khớp; nhiễu chạm đường truyền*** (1) Trong các cơ sở dữ liệu, so khớp là sự so sánh hai mục dữ liệu trong đó các điều kiện xác định được thỏa mãn. (2) Trong truyền thông dữ liệu, nhiễu chạm đường truyền là nhiễu loạn đường truyền tạm thời mà có thể dẫn tới sai lạc các ký tự đang truyền. *Xem* hit on the line.

hit on the line ***chạm đường, va đường truyền*** Trong truyền thông, thuật ngữ chung dùng để chỉ những nhiễu loạn ngắn gây ra bởi những nhiễu bên ngoài như tiếng ồn xung do sấm chớp hoặc nhiễu do con người tạo ra. *Xem* hit, noise.

Holocaust ***virut Holocaust*** Trong an toàn máy tính, virut lấy lên kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, dữ liệu và OVL và liên kết tệp. *Xem* virus names.

hologram ***ảnh toàn ký*** Trong kiểm soát truy nhập, hình ảnh ba chiều tạo ra nhờ sự kết hợp phương pháp chụp ảnh và các chùm laze. Ánh sáng laze nhiễu xạ từ một vật được dùng để bắt giữ hình giao thoa hai chiều trên phim ảnh. Những hình giao thoa đó khi được rọi sáng bằng laze tương tự sẽ tạo ra ảnh ba chiều của vật ban đầu. Các ảnh toàn ký được dùng ở các thẻ tín dụng vì chúng tương đối khó bị làm giả. *Xem* magnetic stripe card.

home banking ***ngân hàng tại nhà*** Trong hoạt động ngân hàng, việc sử dụng terminal truyền thông dân dụng, thường hiển thị dữ liệu để tiến hành các giao dịch trên tài khoản ngân hàng của người sử dụng. *So sánh với* self-banking. *Xem* home banking security, viewdata.

home banking security ***an toàn ngân***

hàng tại nhà Trong hoạt động ngân hàng, dịch vụ ngân hàng trong đó khách hàng tiến hành các giao dịch với một thiết bị đầu cuối đặt ở nhà và được nối với ngân hàng qua mạng điện thoại công cộng.

Các hệ an toàn dữ liệu chấp nhận cho hoạt động ngân hàng tại nhà bị ảnh hưởng bởi chi phí có thể chấp nhận được của thiết bị đầu cuối tại nhà, bởi việc sử dụng mạng điện thoại công cộng không an toàn và các hạn chế về tính chất phức tạp trong sử dụng mà các khách hàng của ngân hàng có thể chấp nhận được. Hơn nữa, khả năng tin cậy của hệ thống không được bị ảnh hưởng bất lợi bởi các sự cố vốn không thực sự gây nguy hiểm cho các giao dịch trong thực tế, nhưng lại có thể làm cho khách hàng mất niềm tin vào hệ thống, ví dụ, những đường điện thoại chéo nhau khiến cho trang màn hình các giao dịch của một khách hàng xuất hiện trên một thiết bị đầu cuối khác.

Một dạng tấn công nghiêm trọng có thể nảy sinh do nhiễu trực tiếp với cáp điện thoại. Một máy tính có nhân đặt xen có thể được dùng để giả dạng như ngân hàng đối với người sử dụng, và người sử dụng đối với ngân hàng; cho phép chuyển tiền từ tài khoản của khách hàng sang tài khoản của kẻ tấn công. *Xem* masquerading. VANS security.

homerun ***đường về riêng*** Trong an toàn vật lý, phương pháp nối dây trong đó mỗi bộ cảm biến được nối riêng rẽ với một hệ báo động hoặc hệ chỉ báo, tức là không sử dụng dồn kênh. *So sánh với* multiplex. *Xem* annunciator.

homing sequential switcher ***bộ chuyển mạch về tuần tự*** Trong an toàn vật lý, phương tiện chuyển mạch hình ảnh để tự động chuyển mạch một màn hình giám sát giữa các camera CCTV chuyên dụng. Các thời gian dừng có thể thay đổi và các camera được loại bỏ khỏi trình tự hoặc được chọn để xem mở rộng theo các lệnh thủ công. *Xem* CCTV, dwell time, sequential switcher, videc switcher.

homogeneous computer network ***mạng máy tính thuần nhất*** Trong truyền thông dữ liệu, mạng các máy tính chủ giống nhau, như thuộc một mẫu hoặc một hãng sản xuất. *So sánh với* heterogenous computer network.

homogeneous multiplex ***dồn kênh thuần nhất, dồn kênh đồng tính*** Trong truyền thông dữ liệu, cấu trúc dồn kênh trong đó các kênh mang thông tin được truyền với cùng tốc độ báo hiệu dữ liệu. *So sánh với* heterogenous multiplex. *Xem* data-signalling rate.

horizontal parity ***chẵn lẻ ngang*** *Xem* longitudinal redudancy check.

host ***máy chủ, máy chính*** Trong truyền thông dữ liệu, hệ dựa trên máy tính bất kỳ được nối với mạng và chứa phần mềm diễn dịch giao thức cần thiết để khởi động truy nhập mạng và thực hiện trao đổi thông tin qua mạng truyền thông. Định nghĩa này bao hàm các máy chủ lớn, các máy hỗ trợ đầu cuối chung (ví dụ ARPANET, TAC, DoDIIS, NTC) và các trạm làm việc nối trực tiếp với mạng con truyền thông và thực hiện các giao thức tạo mạng liên máy tính. Thiết bị đầu cuối (terminal) không phải là

máy chủ vì nó không chứa phần mềm giao thức cần để thực hiện trao đổi thông tin; một trạm làm việc là máy chủ vì nó có khả năng như thế.

host access control ***kiểm soát truy nhập máy chủ*** Trong an toàn truyền thông, cách để giới hạn các truy nhập ở mức 3 trong giao thức ISO dựa trên sự nhận dạng các máy chủ và/hoặc các nhóm mà chúng thuộc vào. *Xem* open systems interconnection.

host computer ***máy tính chủ*** *Xem* host.

hostile threat environment ***môi trường đe dọa thù địch*** Trong an toàn vật lý, một vùng chứa đựng những mối đe dọa đã biết và kiểm soát được ít hoặc không kiểm soát được đối với vùng xung quanh như một số phương tiện ngoại giao phải trải qua. *Xem* threat.

hot card list ***danh sách thẻ nóng*** Trong hoạt động ngân hàng, tệp trung tâm, chứa các chi tiết về các thẻ bị từ chối các đặc quyền thanh toán. Tệp được truy nhập khi có yêu cầu thanh toán thông qua một ATM. *Xem* ATM. *Đồng nghĩa với* blacklist, hot file, negative file.

hot file ***tệp nóng*** *Đồng nghĩa với* hot card list.

hot mode ***chế độ nóng*** Trong an toàn truyền thông, phương pháp theo đó mỗi terminal đều được yêu cầu phát liên tục các thông báo hoặc thông báo giả nếu cần; khi đó bất kỳ sự vắng thiếu truyền thông từ một terminal cũng đều cho biết có sự cố hệ thống. *Xem* banking networks, delay/denial of service.

hot potato routing ***định tuyến cấp thời*** Trong truyền thông dữ liệu, phương pháp định tuyến trong đó gói dữ liệu được truyền đi từ một nút càng sớm càng tốt, ngay cả khi đường đã chọn có thể không tối ưu theo quan điểm định tuyến. *So sánh với* adaptive routing, centralized adaptive routing, della routing, directory routing, fixed routing. *Xem* packet switching.

hot site ***(địa) điểm nóng, vị trí nóng*** Trong quản lý rủi ro, một trung tâm được trang bị đầy đủ cung cấp một năm lực tính toán thay thế trong trường hợp có tai họa đối với máy tính, ví dụ như lụt lội hoặc hỏa hoạn. Địa điểm nóng thường bao gồm các máy tính, các thiết bị điều khiển băng, thiết bị nhớ đĩa và những thiết bị ngoại vi khác. Các phương tiện máy tính sẽ tương thích với các phương tiện của trung tâm ban đầu để đảm bảo rằng, các vấn đề chuyển đổi là tối thiểu. Số thành viên của một tổ chức dự phòng cho địa điểm nóng sẽ bị giới hạn cũng như khoảng thời gian sử dụng những địa điểm đó. *So sánh với* cold site. *Xem* closed hot site, contingency plans, open hot site.

hot standby ***dự phòng nóng, dự phòng cấp một*** Trong các phương tiện tin cậy, phương pháp dự phòng phần cứng sẽ tự động chuyển sang hoạt động khi phát hiện được sự cố hệ thống. *So sánh với* cold standby, warm standby.

housekeeping ***hoạt động hỗ trợ, nội dịch*** Trong tin học, các hoạt động hỗ trợ là thứ yếu đối với những mục tiêu xử lý chính (ví dụ, khởi tạo, lập tên và

các hoạt động báo trì.

housekeeping information ***thông tin nội dịch*** Trong truyền thông dữ liệu, các tín hiệu được bổ sung vào những tín hiệu thông tin, nhưng chỉ nhằm để cho thiết bị thu có thể hoạt động đúng.

hub polling ***hỏi vòng trung tâm, kiểm tra tuần tự trung tâm*** Trong truyền thông dữ liệu, phương pháp hỏi vòng ở các tuyến đa điểm làm giảm tổn thất thời gian trong đổi chiều truyền. Bộ điều khiển đầu tiên hỏi vòng terminal cách xa nó nhất. Terminal đã lập địa chỉ đổi chiều đường truyền (tức là bố trí để tín hiệu được gửi theo hướng ngược lại): sự đảo chiều đường dây có thể mất hàng trăm milligiây trên mạng điện thoại với các bộ triệt tín dội. Nếu terminal có dữ liệu để truyền thì nó gửi dữ liệu đó tới bộ điều khiển; tuy nhiên, nếu nó không có dữ liệu thì nó chuyển tiếp thông báo hỏi vòng cho terminal lân cận gần nó nhất. Nếu terminal đó không có dữ liệu thì đến lượt nó lại gửi tiếp thông báo hỏi vòng tới lân cận gần nhất bên phía bộ điều khiển. Trong hỏi vòng thông thường, bộ điều khiển lập địa chỉ từng terminal một cách trực tiếp và mỗi terminal đều phải đảo chiều đường truyền để gửi đi thông báo "không dữ liệu". *So sánh với* roll call polling. *Xem* echo suppressor, multidrop circuit, polling.

Huffman code ***mã Huffman*** Trong mã hóa, mã trong đó các ký tự thường xuyên xuất hiện được gán ít ký hiệu hơn so với những ký tự xuất hiện kém thường xuyên hơn.

human interface functions ***(các) chức năng giao tiếp của con người*** Trong an toàn máy tính, các thao tác TCB đòi hỏi sự can thiệp hoặc phán xét của con người. Các quá trình không tin cậy có thể không có khả năng gọi chúng ra. *Xem* TCB.

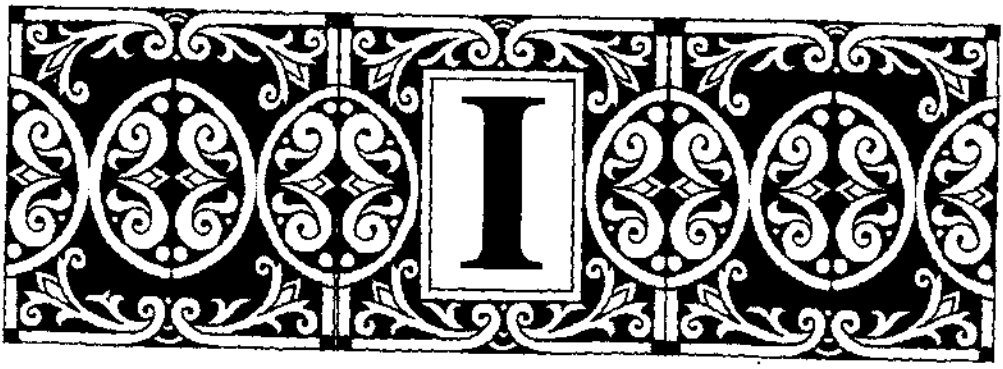
Hybrid ***virut Hybrid*** Trong an toàn máy tính, virut làm lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

hybrid redundancy ***dư thừa lai*** Trong các phương tiện tin cậy, dạng dư modun kết hợp các khái niệm NMR và dễ dành dự trữ. Khi hệ chọn lựa phát hiện thiết bị có sự cố thì thiết bị đó được chuyển mạch và thay thế bởi phần để dành dự trữ. Nếu có ba phần hoạt động và hai phần dành dự trữ được sử dụng thì hệ thống sẽ tiếp tục hoạt động sau khi ba modun bị hỏng. Hệ NMR với năm modun chỉ có thể kháng sự cố trong hai thiết bị. *Xem* modular redundancy, NMR.

Hymn ***virut Hymn*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

Hymn-2 ***virut Hymn-2*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

Hz *Xem* hertz.



I-4 ***I-4*** *Xem* International Information Integrity Institute.

I&A ***I&A*** Trong an toàn thông tin, viết tắt của Identification and Authentication (nhận dạng và xác thực). *Xem* information technology security evaluation criteria.

IA5 ***IA5*** *Xem* International Alphabet Number 5.

IAC ***IAC*** *Xem* DOD Information Analysis Center.

IBAC *Xem* identity based access control.

IC *Xem* integrated circuit.

Icelandic ***virut Icelandic*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

ICV *Xem* integrity check value.

ID ***ID*** *Xem* identification character.

IDA ***IDA*** Trong hoạt động ngân hàng, viết tắt của IDentity of key for Authentication (mã nhận dạng khóa để xác thực), sự nhận dạng khóa mật mã dùng trong thực hiện xác thực thông báo. *So sánh với* IDE, MID. *Đồng nghĩa với* key identifier.

IDE ***IDE*** Trong hoạt động ngân hàng, viết tắt của Identity of key for Encryption (mã nhận dạng khóa để mã hóa), sự nhận dạng khóa mật mã dùng trong thực hiện mã hóa thông báo. *So sánh với* IDA.

IDEA ***thuật toán mã dữ liệu quốc tế, chuẩn mã dữ liệu quốc tế*** Viết tắt của International Data Encryotion Algorithm. Đây là thuật toán mã các khối bản rõ 64 bit thành các khối bản mã 64 bit nhờ dùng khóa 128 bit. Dựa một phần trên sự tổng quát hóa cấu trúc Feistel, thuật toán gồm 8 vòng tính toán đồng nhất và sau đó là một phép biến đổi đầu ra. Vòng r dùng 6 khóa

con $K_i^{(r)}$ 16 bit, $1 \geq i \geq 6$ để biến đổi một đầu vào X 64 bit thành đầu ra có bốn khối 16 bit là đầu vào của vòng tiếp theo. Đầu ra vòng thứ 8 sẽ đưa vào phép biến đổi đầu ra nhờ dùng 4 khóa con bổ sung $K_i^{(9)}$, $1 \geq i \geq 4$ và tạo ra bản mã cuối cùng $Y = (Y_1, Y_2, Y_3, Y_4)$. Tất cả các khóa con đều nhận được từ K.

identification ***nhận dạng, định danh*** (1) Trong kiểm soát truy nhập, quá trình cho phép nói chung bằng cách sử dụng các tên duy nhất máy đọc được, thừa nhận những người sử dụng hoặc tài nguyên là đồng nhất với những người sử dụng hoặc tài nguyên trước đó đã mô tả đối với một hệ ADP. *Xem* access, ADP, resource. (2) Trong kiểm soát truy nhập, quá trình gắn một đặc trưng duy nhất vào một cá nhân. (3) Trong truyền thông dữ liệu, thủ tục do máy tính chủ thực hiện trong kiểm chứng mã định danh của một đường truyền, thiết bị, thuê bao riêng lẻ yêu cầu truy nhập. *Xem* host computer.

identification and authentication ***nhận dạng và xác thực*** Trong an toàn thông tin, các chức năng thiết lập và kiểm chứng mã định danh đã khai báo của người sử dụng. *Xem* information technology security evaluation criteria.

identification character ***ký tự định danh, ký tự nhận dạng, ID*** Trong truyền thông dữ liệu, ký tự định danh trạm dữ liệu ở xa với trạm trung tâm. *Xem* identification.

identification risk ***rủi ro nhận dạng*** *Xem* disclosure risk.

identifier ***ký hiệu nhận dạng, ký hiệu định danh*** (1) Trong tin học, ký tự hoặc nhóm các ký tự dùng để định danh, chỉ rõ hoặc gọi tên một khối dữ liệu. (2) Trong tin học, tên hoặc xâu ký tự dùng để định danh một biến, một thủ tục, cấu trúc dữ liệu hoặc một phần tử nào đó khác của một chương trình. *Xem* data structure, procedure.

identifier code ***mã nhận dạng*** Trong hoạt động ngân hàng, mã định danh rõ ràng một bên trước ngân hàng.

identity ***mã đồng nhất*** Trong mật mã, mã pháp trong đó bản gốc và bản mật mã giống hệt nhau. *So sánh với* genuine.

identity authentication ***xác thực danh tính*** Trong kiểm soát truy nhập, tập hợp các thủ tục thủ công hoặc tự động hóa nhằm xác minh rằng, những người sử dụng yêu cầu truy nhập chính là những người được phép.

identity based access control ***kiểm soát truy nhập dựa trên danh tính*** Trong kiểm soát truy nhập, cơ chế kiểm soát truy nhập chỉ dựa trên danh tính của chủ thể và đối tượng. *So sánh với* rule based access control. *Xem* discretionary access control, object, subject.

identity based security policy ***chính sách an toàn dựa trên danh tính*** Trong an toàn dữ liệu, chính sách an toàn dựa trên các danh tính và/hoặc các thuộc tính của người sử dụng, một nhóm người sử dụng, hoặc các thực thể hoạt động nhân danh những người sử dụng và các tài nguyên/đối tượng được truy nhập. *So sánh với* rule based security policy. *Xem* identity based

I

access control.

identity token ***thẻ nhận dạng*** Trong kiểm soát truy nhập, thẻ thông minh, khóa kim loại hoặc thẻ vật lý nào đó khác do người sử dụng hệ thống giữ, nó cho phép phê duyệt danh tính người sử dụng. *Xem* card reader, intelligent token, smart card.

identity validation ***phê chuẩn nhận dạng*** Trong kiểm soát truy nhập, sự thực hiện các phép thử, như kiểm tra mật khẩu, cho phép hệ thông tin thừa nhận nhưng người sử dụng hoặc các tài nguyên khi chúng đồng nhất với những người sử dụng hoặc tài nguyên đã mô tả trước đây cho hệ thống. *Xem* authentication.

IDES ***hệ IDES*** Trong kiểm soát truy nhập, viết tắt của Intrusion Detection Expert System (hệ chuyên gia phát hiện xâm nhập), phương pháp được đề xuất để phát hiện tự động sự xâm nhập vào các hệ máy tính nhờ phân tích các bản ghi kiểm toán. *Xem* audit data, intrusion detection.

idle character ***ký tự rỗi*** Trong truyền thông dữ liệu, ký tự điều khiển truyền trên đường viễn thông khi không có thông tin cần truyền. Ký tự sẽ không được hiển thị, in ra hoặc đục lỗ ra bởi terminal nhận.

idle time ***thời gian rỗi*** Trong tin học, thời gian có thể làm việc trong đó, một số hoặc toàn bộ hệ máy tính không được sử dụng. *So sánh với* operating time.

IDS *Xem* intruder detector system.

IDU *Xem* interface data unit.

IEC ***IEC*** Viết tắt của International Electrotechnical Commission (Ủy ban điện kỹ thuật quốc tế), cơ quan chịu trách nhiệm tiêu chuẩn hóa về điện, bao gồm các tiêu chuẩn về vật liệu, các linh kiện và các phương pháp đo lường. Một số công việc của IEC liên quan tới các ứng dụng viễn thông trong các lĩnh vực dây dẫn, cáp, ống dẫn sóng và các hệ CATV.

IEE ***IEE*** Viết tắt của Institution of Electrical Engineers (Hội kỹ sư điện của Anh).

IEEE ***IEEE*** Viết tắt của Institute of Electrical and Electronics Engineering (Viện công nghệ điện và điện tử Hoa Kỳ).

IEEE 802 ***chuẩn IEEE 802*** *Xem* IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.6.

IEEE 802.3 ***chuẩn IEEE 802.3*** Trong truyền thông dữ liệu, tiêu chuẩn đề cập tới các tầng vật lý và liên kết dữ liệu đối với các mạng vùng cục bộ CSMA-CD. *So sánh với* IEEE 802.4, IEEE 802.5, IEEE 802.6. *Xem* CSMA-CD, data link layer, Ethernet, local area network, physical layer.

IEEE 802.4 ***chuẩn IEEE 802.4*** Trong truyền thông dữ liệu, tiêu chuẩn đối với mạng cục bộ bus thẻ bài. *So sánh với* IEEE 802.3, IEEE 802.5, IEEE 802.6. *Xem* token bus.

IEEE 802.5 ***chuẩn IEEE 802.5*** Trong truyền thông dữ liệu, tiêu chuẩn đối với mạng vùng cục bộ vòng thẻ bài. *So sánh với* IEEE 802.3, IEEE 802.4, IEEE 802.6. *Xem* local area network, token ring.

IEEE 802.6 ***chuẩn IEEE 802.6*** Trong các tiêu chuẩn, tiêu chuẩn đối với các mạng vùng đô thị. *So sánh với* IEEE 802.3, IEEE 802.4, IEEE 802.5. *Xem* municipal area network.

IERE ***hội IERE*** Viết tắt của Institution of Electronic and Radio Engineers (Hội kỹ sư điện tử và vô tuyến Anh).

IFIP ***IFIP*** Viết tắt của International Federation for Information processing (Liên đoàn quốc tế về xử lý thông tin), liên đoàn của các hội chuyên môn và kỹ thuật có liên quan tới xử lý thông tin. Một hội được phép từ mỗi nước tham gia. IFIP có một số ủy ban kỹ thuật; IFIP TC 11 là ủy ban kỹ thuật liên quan tới an toàn và bảo vệ các hệ xử lý thông tin. *Xem* TC 11.

I Inf Sc ***viện IInfSc, IIS*** Viết tắt của Institute of Information Scientists (Viện các nhà khoa học thông tin Anh).

IIS *Xem* I InfSc.

IK *Xem* interchange key.

IKV528 ***virut IKV528*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

illegal character ***ký tự không hợp pháp, ký tự sai*** Trong các cấu trúc dữ liệu, ký tự hoặc tổ hợp các bit không đáp ứng một số tiêu chuẩn định trước (ví dụ, ký tự không phải là phần tử của một bảng chữ cái xác định nào đó). *So sánh với* forbidden combination.

immediate funds ***tiền trực tiếp, tiền tức thời*** Trong hoạt động ngân hàng, tiền cùng ngày trong đó, việc thanh toán đồng thời với việc thực hiện giao dịch.

IMP *Xem* interface message processor.

impact ***mức va chạm, mức ảnh hưởng*** Trong an toàn máy tính, thiệt hại đối với một tổ chức do một biến cố có hại. Nó thường được đo bằng số tiền mỗi lần xuất (biến cố). Trong những trường hợp phức tạp hơn, nó có thể được đo một cách định tính (ví dụ, thấp hoặc cao) hoặc bằng cách so sánh. *Xem* harmful event, loss, matrix methodology.

impact analysis ***phân tích mức ảnh hưởng*** Trong an toàn máy tính, số đo tổn thất từ một biến cố có hại. *Xem* harmful event, impact, loss.

impartiality ***(tính) công bằng*** Trong an toàn thông tin, yêu cầu rằng sự đánh giá an toàn không có khuynh hướng thiên vị đối với việc đạt bất kỳ kết quả cụ thể nào. *Xem* information technology security evaluation criteria.

impersonation ***mạo nhận, đóng giả*** Trong an toàn máy tính, ý đồ truy nhập một hệ thống nhờ đóng vai như người dùng được phép. *Xem* access. *Đồng nghĩa với* masquerading, mimicking.

implementation ***cài đặt, thực hiện*** Trong tin học, quá trình cài đặt một hệ máy tính hoặc nâng cao cho hệ hiện hành. Nó thể hiện giai đoạn cuối cùng của một loạt các bước trước khi hoạt động hằng ngày, bao gồm một số hoặc toàn bộ những vấn đề sau: nghiên cứu khả thi, định nghĩa phác họa về hệ thống, đặc tả hệ thống chi tiết, lập

trình, thử nghiệm tích hợp và thử nghiệm thu. Song song với những hoạt động đó, người sử dụng có thể được tính đến trong lựa chọn thiết bị, đào tạo nhân viên và xác lập các chính sách kiểm soát máy tính. Ở những dự án máy tính rất lớn, những khía cạnh quan hệ công nghiệp của việc đặt mua một hệ mới có thể phải được khảo sát rất tỷ mỉ và được nhất trí. *Xem* systems analysis.

implementation verification ***kiểm chứng cài đặt*** Trong an toàn máy tính, việc sử dụng các kỹ thuật kiểm chứng, thường có sự trợ giúp của máy tính, để chứng minh sự tương ứng về mặt toán học giữa một đặt tả hình thức và sự cài đặt nó trong mã chương trình. *Xem* formal verification.

implied queries control ***kiểm soát truy vấn ngầm định*** Trong an toàn cơ sở dữ liệu, một dạng kiểm soát hạn chế ô, nhằm ngăn ngừa những cuộc tấn công theo dõi. Trong thời câu truy vấn được đặt ra, cơ cấu kiểm soát cố xác định tất cả các tập câu hỏi có thể suy ra được từ câu truy vấn và những thống kê được phép khác. *So sánh với* audit expert, cell suppression, grouping, overlap control, query set size control. *Xem* cell restriction, inference control, query set, tracker.

impulsive noise ***tạp nhiễu xung, tiếng ồn xung*** Trong truyền thông, nhiễu đặc trưng bằng rối loạn thời gian ngắn, gián cách bởi những khoảng nghỉ (ví dụ, nhiễu thu vô tuyến do hệ đánh lửa ở ôtô gây ra).

inadvertent disclosure ***tiết lộ do sơ suất*** Trong an toàn dữ liệu, sự để lộ ngẫu nhiên thông tin phòng thủ nhạy cảm cho truy nhập không được phép của một cá nhân. Điều đó có thể dẫn tới sự làm lộ hoặc tới sự vi phạm nhu cầu cần biết. *Xem* need to know.

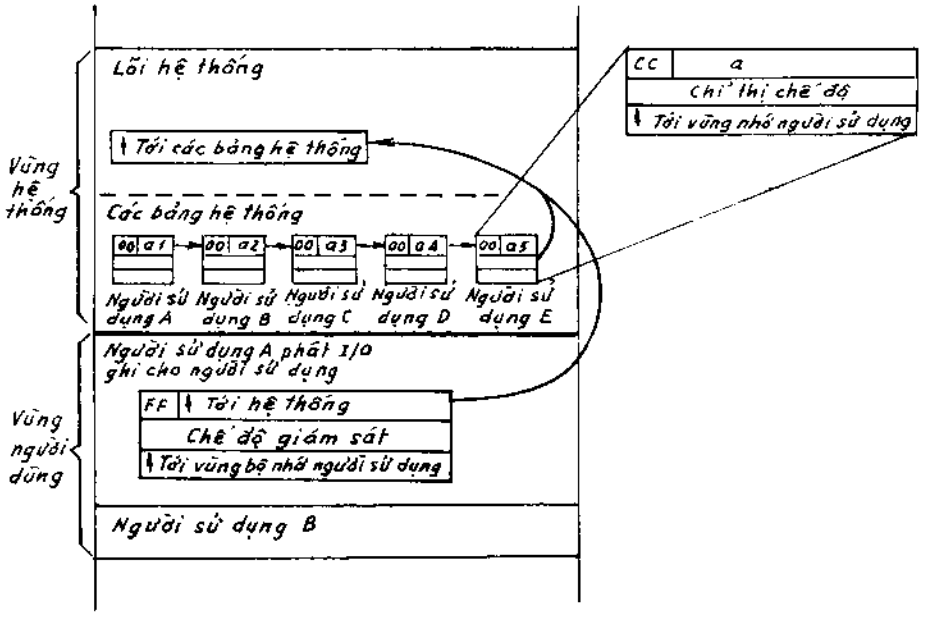
Ina Jo Formal Development Methodology ***hệ phương pháp luận phát triển hình thức Ina Jo*** Trong an toàn máy tính, hệ phương pháp luận đặc tả và kiểm chứng của Công ty phát triển hệ thống, dựa trên ngôn ngữ đặc tả chuyển tiếp trạng thái phi thủ tục Ina Jo. Hệ phương pháp luận Ina Jo bao hàm các bất biến do người dùng cung cấp để tạo ra sự chứng minh hình thức rằng, các tính chất an toàn đã được đáp ứng. *Xem* Affirm, Gypsy, HDM.

in band signalling ***báo hiệu trong dải*** Trong truyền thông, kỹ thuật dùng trong các hệ điện thoại truyền thống trong đó, một số tần số trong dải âm thanh được dùng để truyền thông tin báo hiệu. *Xem* signalling.

incoming message ***thông báo tới*** Trong truyền thông dữ liệu, thông báo truyền từ một trạm tới máy tính. *Xem* station.

incoming traffic ***lưu lượng tới*** Trong truyền thông dữ liệu, lưu lượng chuyển qua mạng và có nguồn gốc ở mạng khác. *Xem* traffic.

incomplete parameter checking ***kiểm tra tham số không đầy đủ*** Trong an toàn máy tính, sai sót hệ thống tồn tại khi tất cả các tham số chưa được hệ điều hành kiểm tra đầy đủ về sự chính xác và tính nhất quán khiến cho hệ thống dễ bị thâm nhập. *Xem* operating system, penetration.



incomplete parameter checking: *kiểm tra tham số không đầy đủ.* Những người sử dụng gọi các chức năng của hệ điều hành theo cách tương tự các gọi thủ tục con, có sử dụng nhiều tham số. Bằng cách cung cấp các địa chỉ bên ngoài khoảng được phân phối cho chương trình của người sử dụng đó, điều khiển có thể được trả lại cho những người sử dụng ở trạng thái giám sát.

Independent Verification and Validation ***thẩm tra và phê duyệt độc lập, IV&V*** Trong an toàn máy tính, quá trình xác định xem các sản phẩm ở một giai đoạn nào đó trong chu trình phát triển phần mềm có hoàn tất các yêu cầu đặt ra trong pha trước đó hay không, và quá trình đánh giá phần mềm ở cuối quá trình phát triển phần mềm để đảm bảo phù hợp với các yêu cầu phần mềm.

index ***chỉ số; danh mục, chỉ mục*** (1) Trong toán học, chỉ số của k modulo n là số nguyên nhỏ nhất t sao cho $g^t \equiv k \pmod{n}$, trong đó g là căn nguyên thuỷ của n. *Xem* modulo aritthmetic, primitive root. (2) Trong tin học, chỉ số treo dưới của một giá trị nguyên, chỉ ra vị trí của một mục dữ liệu so với một mục dữ liệu nào đó khác. (3) Trong các cơ sở dữ liệu, danh mục là danh sách các nội dung của một tệp, hoặc tài liệu, với các khóa hoặc tham chiếu để định vị nội dung.

index build ***xây dựng chỉ mục, lập chỉ mục, lập chỉ số*** Trong các cơ sở dữ liệu, quá trình tự động tạo ra chỉ mục luân phiên dựa trên các kết quả thu được từ việc sử dụng các phương pháp truy nhập hiện thời.

indexed file ***tệp được lập danh mục, tệp có đánh chỉ số*** Trong các cấu trúc dữ liệu, tệp với chỉ mục có liên quan chứa các con trỏ tới các bản ghi hoặc nhóm bản ghi trong tệp. *Xem* file, index, pointer.

indirect access ***truy nhập gián tiếp*** Trong an toàn cơ sở dữ liệu, dạng hiểm họa trong đó, người sử dụng yêu cầu dữ liệu được phép nhưng dữ liệu trả về lại phụ thuộc dữ liệu không được phép, tức là có cấp phân loại an toàn cao hơn và trong những tình huống đó, một kẻ tấn công có thể suy ra thông tin không được phép từ thông tin đã cung cấp. *So sánh với* direct access, Trojan horse direct release, Trojan horse leakage. *Xem* inference control.

indirectly connected transaction ***giao dịch nối gián tiếp*** Trong hoạt động ngân hàng, giao dịch được đặc trưng bằng điều kiện mà cả bên nhận lẫn bên phát hành thẻ (hoặc đại lý của bên phát hành thẻ) mà bên nhận liên lạc với đều không biết về thẻ của người giữ thẻ. *So sánh với* directly connected transaction. *Xem* acquirer, card holder, card issuer, key management.

individual accountability ***phân định trách nhiệm cá nhân*** Trong an toàn máy tính, chỉ các biện pháp liên kết danh tính đúng của những người sử dụng với sự truy nhập của họ tới các máy, tài liệu, dữ liệu v.v. và thời gian, phương pháp và mức độ truy nhập.

induced interference ***nhiễu cảm ứng*** Trong truyền thông, tạp nhiễu cảm ứng trong mạch do ghép điện từ với nguồn bên ngoài. *Xem* noise.

inertia sensor ***bộ cảm biến quán tính, bộ cảm biến kháng lại sự thay đổi*** Trong an toàn vật lý, bộ cảm biến kích hoạt một báo động khi nó bị thay đổi chuyển động.

inference ***suy luận*** Trong an toàn dữ liệu, sự diễn dịch thông tin bí mật liên quan tới một cá nhân nhờ mối tương quan của chúng có thống kê liên quan tới một nhóm các cá nhân. *Xem* inference control.

inference control ***kiểm soát suy luận, khống chế suy luận*** Trong an toàn cơ sở dữ liệu, sự kiểm soát dùng để ngăn ngừa người hỏi sử dụng dữ liệu trong cơ sở dữ liệu thống kê để suy ra thông tin liên quan tới một cá nhân. Ví dụ, nếu một cá nhân là thành viên duy nhất của một nhóm dân tộc riêng trong một cộng đồng và cơ sở dữ liệu chứa các tổng của các khoản tiền phúc lợi cho tất cả các nhóm dân tộc trong cộng đồng, thì khi đó ban điều tra tổng các khoản trả cho toàn bộ cộng đồng cùng với bản điều tra thứ hai về các khoản trả đối với tất cả các nhóm dân tộc ngoại trừ của cá nhân đang xét có thể tiết lộ những chi tiết về các khoản trả cho cá nhân đó. *Xem* multilevel database security, statistical database.

infinity ***vô cùng*** Trong toán học, một đại lượng lớn hơn bất kỳ số khả gán nào.

informatics ***tin học, informatic*** (1) Khoa học liên quan tới thu thập, truyền, lưu giữ, xử lý và hiển thị thông tin. (2) Phiên chuyển từ thuật ngữ Pháp informatique vốn thường được xem như

tương đương với xử lý dữ liệu.

information *thông tin* (1) Bất kỳ một sự truyền thông hoặc thu nhận tri thức nào như các sự kiện, dữ liệu hoặc các ý kiến, bao gồm các dạng số, đồ họa hoặc dạng tường thuật, cho dù bằng miệng hay lưu giữ trên phương tiện bất kỳ, kể cả các cơ sở dữ liệu máy tính hóa, giấy, vi dạng hoặc băng từ. (2) Thuật ngữ "dữ liệu", "thông tin", "tài liệu", "hồ sơ" và "vấn đề" được xem như đồng nghĩa và có thể dùng trao đổi cho nhau. Chúng chỉ mọi dữ liệu bất chấp dạng vật lý của nó (ví dụ, dữ liệu ở các bản in trên giấy, băng, đĩa hoặc chồng đĩa, trong các chip nhớ, bộ nhớ truy nhập ngẫu nhiên (RAM), trong bộ nhớ chỉ đọc (ROM), vi phim hoặc vi thẻ, trên các đường truyền thông và ở các thiết bị đầu cuối hiển thị. *Xem* RAM, ROM. (3) Tri thức vốn chưa biết đối với người nhận trước khi nhận được nó. Thông tin chỉ có thể được suy ra từ dữ liệu chính xác, hợp thời, thích hợp và bất ngờ. (4) Các ý nghĩa gán cho dữ liệu bởi các quy ước được thừa nhận dùng trong biểu diễn nó. Nếu nội dung của một thông báo đã được biết trước khi nhận nó thì không có thông tin mới nào được chuyển tải. Thông tin $I(x)$ đối với biến cố x có xác suất $p(x)$ được cho bởi $I(x) = -\log p(x)$ tức là thông tin là lớn nhất đối với biến cố có xác suất ít nhất). *Xem* information content, information theory.

information asset security *an toàn tài sản thông tin* *Đồng nghĩa với* data security.

information bearer channel *kênh mang thông tin* Trong truyền thông dữ liệu, kênh có khả năng mang thông tin cả điều khiển lẫn thông báo. Do đó nó có thể làm việc với tốc độ báo hiệu lớn hơn so với tốc độ chỉ truyền dữ liệu người dùng. *Xem* bearer.

information center *trung tâm thông tin* Trong tin học, chiến lược phục vụ cũng như tổ chức trong một cơ sở xử lý dữ liệu mà cung cấp giao diện trực tiếp cho tính toán đầu cuối của người dùng và cung cấp các dịch vụ cho tính toán đó. *Xem* end-user computing, fourth-generation language.

information content *lượng thông tin, nội dung thông tin* Trong lý thuyết thông tin, số đo thông tin chuyển tải bởi số lần xuất hiện của một ký hiệu do một nguồn phát ra, đo theo hartley hoặc shanon. Nó được định nghĩa bằng trừ loga của xác suất để ký hiệu cụ thể đó sẽ được phát đi. Nếu dùng các loga cơ số 2 thì đơn vị là shanon, còn nếu dùng cơ số 10 thì đơn vị là hartley. Trong thực tiễn, xác suất để một ký hiệu cụ thể nào đó được phát đi có thể là có điều kiện đối với các ký hiệu đứng trước nó. Mỗi kết quả kế tiếp của việc ném một đồng xu có thể có lượng thông tin là 1 shanon. *Xem* hartley, information theory, shanon.

information flow analysis *phân tích luồng thông tin* Trong an toàn dữ liệu, việc theo dõi luồng các loại thông tin chỉ ra trong một hệ thông tin để xác định xem các điều khiển áp dụng đối với thông tin có thích hợp hay không.

information flow control *điều khiển luồng thông tin, kiểm soát luồng*

thông tin 1. Trong an toàn dữ liệu, điều khiển đối với luồng thông tin bên trong hệ máy tính và khi nó rời hệ máy tính. 2. Trong an toàn dữ liệu, các kiểm soát liên quan tới quyền phổ biến thông tin, bất chấp đối tượng nào chứa thông tin. Trong khi các điều khiển truy nhập điều chỉnh sự truy nhập các đối tượng thì điều khiển luồng thông tin lập địa chỉ những chủ đề nào có thể liên hệ với thông tin chứa trong chúng. *Xem* access control, leakage, object, subject.

information hiding ***giấu (thông) tin*** Trong lập trình, nguyên tắc thiết kế các modun chương trình. Chỉ thông tin thiết yếu đối với người sử dụng modun (tức là giao diện) mới có thể sử dụng được; các chi tiết về cách thức cài đặt modun đều được dấu kín. Nguyên tắc này tạo điều kiện phát triển các chương trình lớn bởi những nhà lập trình độc lập. Người thiết kế một modun được tự do thay đổi các chi tiết cài đặt nó với điều kiện là giao diện không bị ảnh hưởng và người sử dụng có thể quyết định sử dụng một modun khác với cùng chức năng và giao diện.

information integrity ***tính toàn vẹn thông tin*** *Đồng nghĩa với* data integrity.

information loss ***mất mát thông tin, tổn thất thông tin*** Trong an toàn cơ sở dữ liệu, sự không cung cấp được lời đáp đúng cho một câu hỏi hợp pháp do sử dụng dang kiểm soát bằng suy luận. Mất mát thông tin có thể có dạng hạn chế không cần thiết đối với việc cung cấp các bảng thống kê hoặc lượng tạp nhiễu lẫn vào thống kê được phép. *Xem* inference control, perturbation.

information management ***quản lý thông tin*** Sự sử dụng công nghệ thông tin trong quá trình ra quyết định. Các nhà quản lý ngày càng phải ra các quyết định trong các khoảng thời gian giảm dần với các số lượng thông tin tăng lên. Áp lực này một phần do bản chất tỏa khắp của truyền thông và tin học ngày nay; phương thức khắc phục là sử dụng có hiệu quả hơn chính công nghệ thông tin. *Xem* Information Technology.

information networks ***(các) mạng thông tin*** Trong các cơ sở dữ liệu, sự nối thông một nhóm phân tán về mặt vật lý các cơ sở dữ liệu liên kết thông qua viễn thông, sao cho tổng tài nguyên thông tin có thể được dùng chung bởi số lượng người sử dụng lớn hơn.

information rate ***tốc độ thông tin*** Trong truyền thông dữ liệu, số ký hiệu phát đi từ một nguồn mỗi giây nhân với lượng thông tin trung bình trên mỗi ký hiệu. *Xem* information content.

information redundancy ***dư thừa thông tin*** Trong các phương tiện tin cậy, sự sử dụng các bit bổ sung trong tín hiệu số để cho phép kiểm tra tính hợp lệ của biểu diễn. *Xem* error-correcting code, error-detection code, redundancy.

information resources management ***quản lý tài nguyên thông tin*** Việc lập kế hoạch, dự thảo ngân sách, tổ chức, định hướng, đào tạo và điều khiển liên quan tới thông tin của tổ chức. Thuật ngữ này bao gồm cả bản thân thông tin lẫn các tài nguyên có liên quan, như nhân sự, thiết bị, vốn và công nghệ. *So*

sánh với information management.

information retrieval ***tìm kiếm thông tin, IR*** Trong tin học, các kỹ thuật để lưu giữ, rà soát những lượng lớn dữ liệu và khiến cho các dữ liệu đã lựa chọn trở nên khả dụng. Các kỹ thuật có thể bao gồm bộ nhớ trực tuyến, các danh mục từ khóa trong ngữ cảnh (KWIC) và các phương pháp cơ sở dữ liệu.

information security ***an toàn thông tin*** (1) Tổng cộng an toàn máy tính và an toàn mạng. *Xem* computer security, network security. (2) Kết quả của hệ thống các chính sách và thủ tục bất kỳ để nhận dạng, kiểm soát và bảo vệ chống tiết lộ trái phép đối với thông tin mà việc bảo vệ được phê duyệt qua nội quy hoặc quy chế thực hiện. (3) Việc bảo vệ chống lại sự tiết lộ, điều khiển, phá hủy hoặc thay đổi không được phép đối với thông tin. Tiết lộ ở đây nói tới sự tiết lộ thông tin được bảo vệ, như thông tin đã phân loại hoặc có sở hữu, hoặc thông tin lệ thuộc vào luật bảo vệ dữ liệu. Điều khiển ở đây liên quan tới việc thay đổi một thuộc tính nào đó của thông tin như quyền sở hữu tệp, mức phân loại an toàn, đích dữ liệu, v.v.. Dữ liệu có thể bị hủy nhanh và có hiệu quả mà không để lại dấu vết, trong các thiết bị nhớ điện tử hoặc từ tính; khử từ, loại bỏ nguồn khỏi bộ nhớ khả biến hoặc ghi đè, là những phương pháp hủy dữ liệu có hiệu quả. Sự thay đổi dữ liệu liên quan tới việc gây ra những thay đổi ở bản thân dữ liệu đã nhớ, ví dụ như các tổng lượng tài chính, các giá trị đã đo hoặc các tham số điều khiển hệ thống. *Đồng nghĩa với* data security.

information system ***hệ thông tin*** Hệ thu thập có tổ chức, xử lý, truyền và phổ biến thông tin phù hợp với các thủ tục xác định cho dù là tự động hóa hay thủ công.

information systems abuse ***lạm dụng hệ thông tin*** Trong an toàn dữ liệu hoạt động có chủ tâm hoặc cẩu thả làm ảnh hưởng tới tính sẵn sàng, tính bí mật hoặc tính toàn vẹn của các tài nguyên hệ thống thông tin. Hoạt động đó bao gồm lừa đảo, biển thủ, trộm cắp, gây hư hại có chủ ý, sử dụng không được phép, từ chối phục vụ và chiếm đoạt trái phép. *So sánh với* computer abuse. *Xem* information security.

information system director ***giám đốc các hệ thông tin*** Trong các ứng dụng, vai trò mở rộng của người quản lý xử lý dữ liệu phản ánh tầm quan trọng chiến lược của các hệ thông tin trong môi trường tập thể. *Xem* information center.

information system security ***an toàn hệ thống thông tin*** Trong an toàn dữ liệu, sự bảo vệ tạo cho các hệ thống thông tin nhằm bảo toàn tính khả dụng, tính toàn vẹn và tính bí mật của các hệ thống và thông tin chứa bên trong các hệ thống. Sự bảo vệ như thế là áp dụng tổ hợp tất cả các bộ môn an toàn mà ít nhất cũng bao gồm COMSEC, Tempest, an toàn máy tính, OPSEC, an toàn thông tin, an toàn nhân sự, an toàn công nghiệp, bảo vệ tài nguyên và an toàn vật lý. *Xem* computer security, COMSEC, OPSEC, physical security, personnel security, Tempest.

information technology ***công nghệ thông tin, IT*** Sự thu nhận, xử lý, lưu giữ và phổ biến thông tin tiếng nói, hình ảnh, văn bản và số nhờ sự kết hợp dựa trên vi điện tử của tin học, viễn thông và video. Công nghệ thông tin này sinh như một công nghệ tách riêng nhờ sự quy tụ của các kỹ thuật tin học, viễn thông và video, tin học cung cấp khả năng xử lý và lưu giữ thông tin, viễn thông cung cấp phương tiện để truyền thông nó và video cung cấp thiết bị hiển thị hình ảnh chất lượng cao. Sự quy tụ đó đã được xúc tác nhờ sẵn có các linh kiện và thiết bị vi điện tử phức tạp, tin cậy và chi phí có hiệu quả. Các phát triển tổng thể trong điện tử học cũng đã kích thích việc tìm kiếm những tiêu chuẩn quốc tế chung, nhất là trong tin học và viễn thông, mở đường cho các ứng dụng quy mô lớn của công nghệ thông tin.

information technology facility ***phương tiện công nghệ thông tin*** Tập hợp xác định rõ ràng về mặt tổ chức gồm nhân sự, phần cứng, phần mềm và các phương tiện vật lý mà chức năng đầu tiên của nó là hoạt động công nghệ thông tin. *Xem* information technology.

information technology security evaluation criteria ***(các) tiêu chuẩn đánh giá an toàn công nghệ thông tin*** Trong an toàn thông tin, tập hợp các tiêu chuẩn do Ủy ban châu Âu phát triển để đánh giá các hệ thống an toàn và các sản phẩm. Các tiêu chuẩn dựa trên công trình tiến hành trước đây của các chính phủ Anh, Đức, Pháp và Hà Lan.

Cơ sở hợp lý

Các tiêu chuẩn được phát triển bởi vì:

- nhiều kinh nghiệm đã tích lũy được ở những nước khác nhau và có thể có lợi nhiều nếu kết hợp xây dựng dựa trên những kinh nghiệm đó;
- ngành công nghiệp không muốn có những tiêu chuẩn khác nhau ở những nước khác nhau;
- các khái niệm và các cách tiếp cận cơ bản là giống nhau trong các nước và thậm chí trong những ứng dụng thương mại, quản lý và quốc phòng.

Một tài liệu phác thảo, Các tiêu chuẩn đánh giá an toàn thông tin (ITSEC), đã được công bố năm 1990 và Ủy ban của Cộng đồng Châu Âu đã tài trợ cho một hội nghị tư vấn vào tháng 9 năm 1990 ở Bruxen. Tài liệu đã sửa đổi được đưa ra vào năm 1991.

Sơ đồ ITSEC bao hàm phần lớn tài liệu ITSEC nhưng phạm vi các vấn đề an toàn được xem xét của nó rộng hơn. Hơn nữa, không giống Sách Da Cam, ITSEC tách riêng việc đánh giá hệ chức năng và mức độ đảm bảo. Như vậy có bảy mức đảm bảo từ *E*0 tới *E*6 và 10 mức chức năng.

Trong TCSEC các tiêu chuẩn tiến triển từ lớp *D* tới lớp *A*, bao hàm đồng thời một sự tăng về tính chức năng, tức là thông qua kiểm soát truy nhập tùy ý tới cả kiểm soát truy nhập bắt buộc và tùy ý, và bao hàm sự tăng mức đảm bảo gắn liền với hệ chức năng an toàn.

Mục tiêu đánh giá

ITSEC nghiên cứu đánh giá an toàn của cả các hệ thống lẫn các sản phẩm: thuật ngữ Mục tiêu đánh giá (TOE) được dùng để bao quát cả sản phẩm lẫn hệ thống

cần đánh giá. TOE sẽ bao gồm các thành phần mà một số trong đó sẽ liên quan tới an toàn, trong khi đó một số khác lại không. Việc đánh giá sẽ tập trung vào những thành phần được nêu rõ có liên quan tới an toàn, nhưng những thành phần khác cũng sẽ được xem xét và được chỉ ra là không liên quan tới an toàn.

Sự khác nhau căn bản giữa một sản phẩm và một hệ thống, theo sự đánh giá an toàn, là môi trường trong đó các hoạt động hệ thống được biết vào thời điểm đánh giá. Như vậy, những hiểm họa về an toàn trong môi trường đó và những mục tiêu an toàn của hệ thống có thể được mô tả vào thời điểm đánh giá hệ thống.

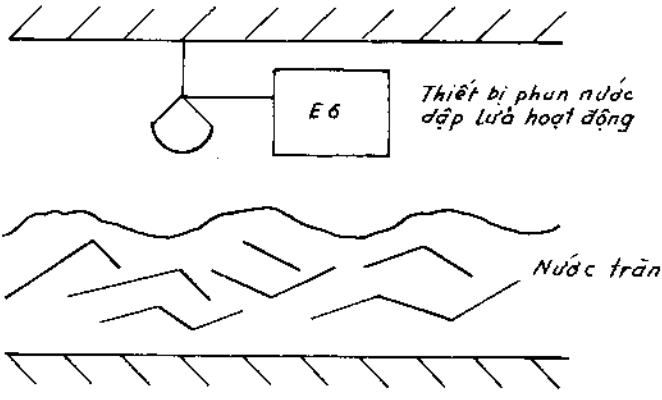
Trong trường hợp sản phẩm, người bán chỉ có thể cung cấp một cơ sở hợp lý về các tính năng an toàn, dựa trên một số giả thiết chung về môi trường và các mục tiêu an toàn. Do vậy người mua sau đó phải đảm bảo rằng, những giả thiết như vậy là tương hợp, với môi trường thực triển khai sản phẩm.

Sự đặt tả chính xác các tính năng an toàn của TOE được mô tả trong tập các tài liệu, gọi là đích an toàn. Các thuật ngữ mục tiêu an toàn, chức năng an toàn và cơ chế an toàn thường xuất hiện trong hồ sơ và chúng có thể được phân loại thành:

- các mục tiêu an toàn - tại sao lại cần hệ chức năng;
- các chức năng an toàn - cái gì được thực hiện trong thực tế;
- các cơ chế an toàn - nó được thực hiện như thế nào.

Đích an toàn có thể bao gồm chẳng hạn:

- các mục tiêu an toàn;
- các phát biểu về môi trường hệ thống hoặc các giả thiết về môi trường sản phẩm;
- các chức năng an toàn;
- cơ sở hợp lý cho các chức năng an toàn;



information technology security evaluation criteria: *các tiêu chuẩn đánh giá an toàn công nghệ thông tin*. Biện pháp đối phó đáp ứng các hiểm họa của môi trường thù địch.

- các cơ chế an toàn cần thiết;
- mức đánh giá cần thiết;
- hiệu lực tối thiểu cần thiết của cơ chế.

Các chức năng an toàn

Các đề xuất của ITSEC rộng hơn so với các đề xuất của TCSEC - Sách Da Cam, vì hãng tài trợ, cơ quan đệ trình TOE để đánh giá, có thể chỉ rõ một phạm vi rộng hệ chức năng an toàn. Không có sự hạn chế nào đối với hệ chức năng mà có thể được chỉ ra trong một đích an toàn theo ITSEC, nhưng người ta khuyến nghị rằng, hệ chức năng cần được mô tả trong tám tiêu đề chung:

- nhận dạng và xác thực - các chức năng thiết lập và kiểm chứng mã nhận dạng đã khai báo của một người sử dụng;
- kiểm soát truy nhập - các chức năng kiểm soát luồng thông tin giữa những người sử dụng, giữa các quá trình và các đối tượng và việc sử dụng các tài nguyên của những đối tượng đó kể cả quản trị và kiểm chứng các quyền truy nhập;
- phân định trách nhiệm - các chức năng ghi việc thi hành các quyền để thực hiện các hoạt động an toàn có liên quan;
- kiểm toán - các chức năng phát hiện và điều tra các biến cố mà có thể đe dọa đối với an toàn;
- tái sử dụng đối tượng - các chức năng kiểm soát việc tái sử dụng các đối tượng dữ liệu;
- độ chính xác - các chức năng đảm bảo tính đúng đắn và tính nhất quán của thông tin có liên quan tới an toàn;
- độ tin cậy của dịch vụ - các chức năng đảm bảo tính nhất quán và mức độ sẵn sàng của dịch vụ;
- trao đổi dữ liệu - các chức năng đảm bảo sự an toàn của dữ liệu trong quá trình truyền qua các kênh truyền thông.

Hệ chức năng cũng có thể được nêu theo các lớp chức năng xác định trước, hoặc như một tổ hợp nào đó của những lớp như thế. Mười lớp như vậy: FC1, FC2, FB1, FB2, FB3, FIN, FAV, FDI, FDC và FDX được định nghĩa trong ITSEC. Năm lớp đầu tiên được dẫn xuất từ các lớp C1, C2, B1, B2 và B3 của TCSEC.

Như vậy có thể xác định rõ các lớp:

- FC1 - kiểm soát truy nhập tùy ý, tương đương với lớp C1 của TCSEC;
- FC2 - kiểm soát truy nhập tùy ý, tương đương với lớp C2 của TCSEC;
- FB1 - kiểm soát truy nhập bắt buộc và tùy ý, tương đương với lớp B1 của TCSEC;
- FB2 - kiểm soát truy nhập bắt buộc và tùy ý, tương đương với lớp B2 của TCSEC;
- FB3 - kiểm soát truy nhập bắt buộc và tùy ý, tương đương với lớp B3 của TCSEC;
- FIN - dành cho các hệ thống có tính toàn vẹn cao đối với các dữ liệu và chương trình. Những yêu cầu như vậy rất quan trọng, chẳng hạn đối với các hệ cơ sở dữ liệu;
- FAV - quy định những yêu cầu cao đối với tính sẵn sàng của toàn hệ thống hoặc những chức năng riêng của một hệ thống. Những yêu cầu

như vậy là quan trọng, chẳng hạn đối với các hệ điều khiển quá trình;

- FDI - quy định những yêu cầu cao đối với việc bảo vệ tính toàn vẹn của dữ liệu trong trao đổi dữ liệu;
- FDC - dùng cho những hệ thống có những nhu cầu cao về độ tin cậy của dữ liệu trong quá trình trao đổi dữ liệu. Ví dụ về lớp này có thể là thiết bị mật mã;
- FDX - dùng cho các mạng có những nhu cầu cao về độ tin cậy và tính toàn vẹn của thông tin cần trao đổi. Ví dụ, đó có thể là trường hợp khi thông tin nhạy cảm cần trao đổi thông qua một mạng không an toàn.

Hệ chức năng có thể được biểu thị dưới các dạng phi hình thức, nửa hình thức hoặc hình thức, hoặc tổ hợp của những dạng đó. Các đặc tả phi hình thức sử dụng các ngôn ngữ tự nhiên là dễ hiểu nhất, nhưng chúng có thể chứa đựng sự không rõ ràng. Các đặc tả bán hình thức sử dụng cú pháp hạn chế, làm giảm xác suất của những sự không rõ ràng như thế. Một ngôn ngữ như vậy, ngôn ngữ Claims, do DTI của Anh đề xuất phác họa các tiêu chuẩn và đòi hỏi hãng tài trợ định rõ hệ chức năng an toàn có sử dụng một loạt các chương trình mẫu. Việc viết các đặc tả trong ngôn ngữ Claims hơi giống với tạo ra các chương trình máy tính theo cú pháp hạn chế của (chẳng hạn) ngôn ngữ Pascal.

Các đặc tả hình thức được viết theo ký pháp toán học dựa trên các khái niệm toán học đã xác lập. Những đặc tả như vậy rõ ràng và có thể được thử về tính nhất quán. Cũng có thể chứng minh rằng, một thiết kế chỉ ra tương tự sẽ phù hợp với bản đặc tả; tuy nhiên, những ngôn ngữ đặc tả như thế, ví dụ ngôn ngữ Z, lại đòi hỏi đào tạo đặc biệt thậm chí để đọc đặc tả.

Dạng cụ thể của đặc tả được dùng sẽ phụ thuộc vào mức đảm bảo mà đích an toàn yêu cầu. Các mức đảm bảo càng cao thì càng đòi hỏi các đặc tả hình thức hơn, nói chung có thể dùng một tổ hợp đặc tả hình thức và phi hình thức để cực đại hóa mức độ dễ hiểu và cực tiểu hóa xác suất không rõ ràng.

ITSEC, giống như TCSEC, quan tâm tới một đại lượng đo nào đó về mức an toàn đã tạo ra. Các đặc tả hệ chức năng được tạo ra để đáp ứng các mục tiêu an toàn của Mục tiêu đánh giá (TOE) và để ngăn chặn các mối đe dọa mà hệ thống phải đương đầu trong môi trường của nó, hoặc những mối đe dọa được giả định là một sản phẩm sẽ phải đương đầu. Tuy nhiên, hệ chức năng đó chỉ là một tuyên bố về cách đạt được an toàn. Nó không đảm bảo hệ chức năng đó được cài đặt đúng và có hiệu quả.

Các mức đánh giá

Bảy mức đánh giá được mô tả, trải từ *E*0 biểu thị độ đảm bảo không thích hợp, hơi giống Phần *D* của TCSEC, tới mức *E*6 cao nhất vốn đòi hỏi các mô tả hình thức của kiến trúc và tính nhất quán an toàn với mô hình hình thức của chính sách an toàn.

Việc đánh giá được thực hiện cả về tính đúng đắn lẫn về tính hiệu quả. Các tiêu chuẩn về tính đúng đắn được áp dụng đầu tiên, nhưng trong sự đánh giá hiệu quả sau đó, vẫn có thể cần mức độ lặp lại nào đó với các tiêu chuẩn về

tính đúng đắn. Trong đánh giá tính đúng đắn của các chức năng an toàn đối với TOE, các tiêu chuẩn ngày càng chặt chẽ được áp dụng cho các khía cạnh của quá trình phát triển, môi trường phát triển, hồ sơ hoạt động và các thủ tục hoạt động đối với các mức đánh giá *E*1 tới *E*6.

Quá trình phát triển được xem như gồm một số các giai đoạn tuần tự sau:

- Các yêu cầu - nhận dạng và mô tả đích an toàn đối với TOE;
- Thiết kế kiến trúc - định nghĩa mức đỉnh chung và thiết kế của TOE chỉ ra cấu trúc cơ bản, các giao diện ngoài của nó và sự tách nó thành các thành phần phần mềm và phần cứng chính;
- Thiết kế chi tiết - tinh chỉnh thiết kế kiến trúc tới mức chi tiết, có thể được dùng làm cơ sở cho lập trình và kết cấu phần cứng;
- Sự cài đặt - dịch thiết kế chi tiết thành phần cứng và phần mềm thực tế, và việc kiểm định cài đặt đó của TOE so với các đặc tả của nó.

Các yếu tố đóng góp vào sự phát triển tính bí mật được chỉ ra trong các tiêu chuẩn đối với mỗi giai đoạn ở trên. Trong nhiều trường hợp, hồ sơ cần thiết để đánh giá sẽ giống hệt với hồ sơ dùng trong quá trình phát triển bình thường được tạo ra theo đúng với thực tiễn kỹ thuật phần mềm tốt. Các tiêu chí về môi trường phát triển nhấn mạnh các chủ đề như các công cụ cấu hình, lựa chọn các ngôn ngữ lập trình và các công cụ lập trình, các biện pháp an toàn bên trong mà nhà phát triển chấp nhận v. v.. Như vậy, khía cạnh này của các tiêu chí là nhằm xác định thực tiễn làm việc của nhà phát triển. Hồ sơ hoạt động cho biết thông tin mà nhà phát triển cung cấp cho khách hàng, trong khi đó các thủ tục vận hành là những thủ tục thực sự được áp dụng khi sử dụng hệ thống. Trong trường hợp đánh giá hệ thống, có thể đánh giá các hệ quả an toàn của các thủ tục đã áp dụng, trong những trường hợp khác, người đánh giá chỉ có thể xem xét các thủ tục đã đề xuất như đã trình bày bởi nhà phát triển hoặc người sử dụng. Đối với mỗi mức trong sáu mức E1 tới E6, các tiêu chuẩn đánh giá chỉ rõ những yêu cầu đối với những giai đoạn phát triển và hoạt động xác định. Hồ sơ cần thiết, nội dung và cách trình bày nó hoặc các thủ tục và tiêu chuẩn mà nó phải xác định đều đã cho đối với mỗi mức. Thường có ba bên liên quan đến đánh giá:

- bên tài trợ - người hoặc tổ chức yêu cầu đánh giá;
- người phát triển hệ thống hoặc sản phẩm;
- người đánh giá.

Trừ ở mức *E*1, gánh nặng về cung cấp bằng chứng được đặt lên phía nhà tài trợ, người sau đó phải tìm được thông tin cần thiết từ nhà phát triển. Sau đó bằng chứng được kiểm tra hoặc soát xét bởi người đánh giá. Người đánh giá chỉ được yêu cầu đưa ra bằng chứng ở nơi nào việc tạo ra độc lập như thế được xem là cần thiết, nhằm cung cấp mức tin cậy cần thiết trong các kết luận của người đánh giá.

Việc đánh giá các tiêu chuẩn về tính hiệu quả được tiến hành sau đó để

đánh giá tính đúng đắn. Việc đánh giá tính đúng đắn chứng tỏ rằng, hộp đen quả thực thực hiện như đã được đảm bảo, vấn đề tiếp theo là "hộp đen đó có hiệu quả như thế nào trong một thế giới thù địch?". Việc đánh giá hiệu quả khác với việc đánh giá tính đúng đắn ở hai khía cạnh quan trọng, thứ nhất chúng không bị phân nhỏ bởi mức đánh giá, hoặc bởi các giai đoạn xây dựng và vận hành. Thứ hai, phần lớn công việc tiến hành trong giai đoạn đánh giá này đều do những người đánh giá thực hiện trực tiếp, mặc dù nhiều bằng chứng cần thiết sẽ nhận được trong đánh giá tính đúng đắn trước đó.

Các khía cạnh sau đây của TOE được xem xét khi đánh giá hiệu quả: Tính thích hợp của hệ chức năng, Sự liên kết của hệ chức năng, Đánh giá tính dễ tổn thương: Kết cấu; Sức mạnh của các cơ chế; Tính dễ sử dụng; Đánh giá chỗ dễ tổn thương: Vận hành.

Tính thích hợp của hệ chức năng - trong đánh giá tính thích hợp của hệ chức năng, đích an toàn được xem xét và người ta xác định xem các chức năng và cơ chế an toàn có chống lại những mối đe dọa mà TOE nhận diện được hay không. Trong trường hợp sản phẩm sử dụng một hoặc nhiều lớp chức năng xác định trước mà không mở rộng hoặc bỏ sót, thì TOE được giả định là thích hợp đối với các mục đích định sẵn.

Sự liên kết của hệ chức năng - mặc dù các chức năng an toàn có thể thích hợp với các mục đích riêng lẻ của chúng, song có thể là một số tổ hợp của các chức năng hoặc cơ chế có thể cản trở hoặc xung đột với nhau. Trong đánh giá sự liên kết của hệ chức năng, một nghiên cứu được tiến hành về các mối quan hệ qua lại của các chức năng an toàn và các cơ chế để đảm bảo rằng, chúng hỗ trợ lẫn nhau và tạo ra một chỉnh thể có hiệu quả và gắn kết.

Đánh giá điểm yếu: Kết cấu - trong việc đánh giá những chỗ dễ tổn thương trong kết cấu, các điểm yếu về an toàn mà có thể đã được nhận dạng trong quá trình đánh giá tính đúng đắn, được xem xét để quyết định xem chúng có thực sự làm tổn hại đến tính an toàn của TOE như đã xác định trong đích an toàn hay không. Có thể là những hiểm hoạ đã nhận dạng có thể không tồn tại trong thực tế, hoặc chúng có thể được những cơ chế an toàn khác trong TOE hoặc các phương tiện bên ngoài TOE chặn lại.

Sức mạnh của các cơ chế an toàn - trong bất kỳ hệ thống an toàn nào cũng đều có một số giả thiết về tính an toàn vốn có của các cơ chế về thuật toán nền tảng. Ví dụ, nếu thuật toán DES được sử dụng thì người ta thường giả thiết rằng, không kẻ tấn công nào có thể thử được tất cả các khóa DES có thể. Khi xét sức mạnh của các cơ chế nền tảng thì người ta sẽ xem xét mức tài nguyên mà một kẻ tấn công có thể cần đến để tổ chức một cuộc tấn công trực tiếp vào hệ thống. Cơ chế tới hạn được định nghĩa như cơ chế không được bảo vệ trước cuộc tấn công bởi một cơ chế mạnh hơn khác và sự hỏng hóc của nó có thể tạo nên một điểm yếu. Mục tiêu của đánh giá về sức mạnh của một cơ chế là xác nhận những mức sức mạnh danh định tối thiểu đã yêu cầu cho các

cơ chế tới hạn của TOE.

Các mức danh định tối thiểu đối với những cơ chế tới hạn của TOE được phân loại như sau:

- cơ bản - tất cả các cơ chế tới hạn tạo ra sự bảo vệ chống sự phá vỡ ngẫu nhiên không chủ ý, mặc dù có khả năng những kẻ tấn công thông thạo khắc phục được;
- trung bình - tất cả các cơ chế tới hạn tạo ra sự bảo vệ trước những kẻ tấn công có những cơ hội hoặc tài nguyên hạn chế;
- cao - tất cả những cơ chế tới hạn chỉ có thể bị những kẻ tấn công có một trình độ cao về chuyên môn có cơ hội và tài nguyên vượt qua được, một sự tấn công thành công sẽ được cho là nằm ngoài thực tiễn thông thường.

Tính dễ sử dụng - hoạt động an toàn của một hệ bất kỳ phụ thuộc vào con người và các thủ tục trong môi trường vận hành của nó. Nếu những thủ tục đó đòi hỏi quá mức hoặc không rõ ràng thì có nguy cơ chúng sẽ không được thực hiện đúng. Các biện pháp an toàn bên ngoài như các cơ chế kiểm soát thủ tục, vật lý và nhân sự cần thiết để hỗ trợ các chức năng và cơ chế an toàn của TOE phải được xem xét theo quan điểm này. Việc đánh giá mức độ dễ dàng trong sử dụng sẽ cho phép phân tích tất cả các kiểu sự cố khả dĩ (những nguyên nhân khả dĩ của các sự cố và hậu quả của chúng) do những loại sai sót vận hành của con người và những loại sai sót khác gây ra. Sự phân tích đó phải cho thấy rằng, mọi loại sai sót của con người hay những loại sai sót khác trong vận hành có những hậu quả tiềm ẩn về an toàn đều có thể dễ dàng phát hiện được.

Đánh giá điểm dễ bị tổn thương: Vận hành - giai đoạn đánh giá này tương tự với giai đoạn đánh giá mô tả ở trên đối với điểm yếu về kết cấu trừ một điều là, những điểm yếu gắn liền với môi trường vận hành, ví dụ như cấu hình, khởi động, phân bố của TOE được xem xét tới.

Quan hệ với TCSEC

Các tiêu chuẩn của ITSEC và TCSEC có mối quan hệ qua lại với nhau, chẳng hạn như sự tương ứng giữa các mức phân loại có thể sơ bộ đặt ngang nhau như:

ITSEC	TCSEC
E0	D
FC1, E1	C1
FC2, E2	C2
FB1, E3	B1
FB2, E4	B2
FB3, E5	B3
FB3, E6	A1

Sự phát triển của ITSEC có thể xem như một sự phát triển logic của TCSEC, khi mở rộng phạm vi phân loại nhằm tính đến những nghiên cứu dễ áp dụng hơn đối với khu vực thương mại và quản lý. Tuy nhiên, các vấn đề đánh giá mới là quan trọng; các tiêu chuẩn TCSEC chỉ liên quan tới sáu mức đánh giá chi tiết, đã có các vấn đề về phát triển các đội đánh giá có chuyên môn cao và kinh nghiệm trong lĩnh vực này. Có 1344 mức danh định tiềm năng trong ITSEC. Cho dù số những mức danh định đó không chắc nảy sinh thì vẫn tồn tại nguy cơ quá thừa các tổ hợp của các

mức danh định sẽ gây nhầm lẫn trên thị trường và gây ra các khó khăn cho việc triển khai những đội chuyên gia đánh giá tài năng thích hợp. *Xem* FCFIPS, information technology security evaluation facility, information technology security evaluation manual, object reuse, Orange Book, TCSEC.

information technology security evaluation facility ***cơ sở đánh giá an toàn công nghệ thông tin*** Trong an toàn thông tin, một tổ chức được công nhận và cấp giấy phép để thực hiện các đánhh giá an toàn ITSEC. *So sánh với* certification body. *Xem* information technology security evaluation criteria.

information technology security evaluation manual ***sách hướng dẫn đánh giá an toàn công nghệ thông tin*** Trong an toàn thông tin, sách hướng dẫn dựa trên ITSEC, mô tả cách đánh giá đích đánh giá theo các tiêu chuẩn. *Xem* information technology security evaluation criteria, target of evaluation.

information theory ***lý thuyết thông tin*** (1) Trong toán học, lý thuyết nghiên cứu về tốc độ thông tin, dung lượng kênh, tạp nhiễu và những yếu tố khác ảnh hưởng tới sự truyền thông tin. Ban đầu được phát triển cho liên lạc điện, hiện nay nó được áp dụng cho các hệ kinh doanh và những lĩnh vực khác liên quan tới các thiết bị thông tin và luồng thông tin trong các mạng. *Xem* information content, Shannon's law. (2) Trong mật mã học, các khái niệm lý thuyết hữu ích về mật mã đã được Shannon phát triển trong khuôn khổ lý thuyết thông tin. Có sự tương tự giữa sự phát hiện các thông báo đã bị sai lạc bởi tiếng ồn với sự giải mã các thông báo của nhà phân tích mật mã. Trong cả hai trường hợp, bên nhận thông báo cố khôi phục lại thông báo ban đầu nhờ sử dụng thông tin chứa trong thông báo đã nhận được, thông báo này đã bị sửa đổi bởi nhiễu hoặc sự mã hóa.

Mật mã có thể được xem như phép ánh xạ một tập hợp các thông báo gốc lên một tập hợp các thông báo mật mã nhờ một tập hợp các khóa mật mã. Hãy xét trường hợp trong đó, một thông báo gốc thuộc một tập hợp 26 thông báo như thế, có thể được mã hóa bằng một khóa thuộc một tập hợp 26 khóa khả dĩ, để tạo ra một trong 26 thông báo mã có thể. Ngoài ra, giả sử rằng, bất cứ một thông báo mã nào cũng có thể được tạo ra từ một trong 26 thông báo mã nếu dùng một khóa thích hợp.

Nhà mã thám khi nhận được thông báo mã không có thông tin nào về thông báo gốc ban đầu bởi vì bất kỳ một bản gốc nào có thể được truyền đi đều tạo ra một bản mã, tùy thuộc vào khóa đã chọn. Nói cách khác, xác suất có điều kiện để bản gốc (M) được gửi đi, khi bản mã (C) được nhận (tức là $P_c(M)$), là bằng xác suất không điều kiện ($P(M)$) để thông báo M được gửi đi. Đó là điều kiện cho độ mật hoàn thiện. Độ mật hoàn thiện nảy sinh do số khóa cũng có nhiều như số bản gốc và bản mã, và mỗi bản gốc đều có thể sinh ra một bản mã.

Tuy nhiên, trong nhiều hệ thống mật mã, số các khóa có thể nhỏ hơn nhiều

so với số các bản gốc có thể. Hơn nữa có thể loại ra một phần các bản gốc vì vô nghĩa; nhà mã thám do đó được trợ giúp bởi mức độ dư thừa trong ngôn ngữ tự nhiên.

Ta hãy xét ví dụ ở trên về 26 bản gốc/bản mã và các khóa, và giả sử mỗi bản mã tương ứng với một chữ cái của bảng chữ cái. Như vậy người viết mật mã sử dụng một phép thế đơn giản, thay thế mỗi chữ cái của bản gốc bằng một chữ cái của bản mã tương ứng; 26 bảng thay thế có sẵn sẽ tương ứng với 26 khóa. Nếu một câu tiếng Anh có nghĩa được truyền đi thì nhà mã thám thu được thông tin với các ký tự mới của bản mã. Ký tự đầu tiên có thể là một ký tự bất kỳ trong 26 ký tự, nhưng với ký tự thứ hai, có thể loại bỏ một số bộ đôi, ví dụ như QK, ZD v.v. và như vậy, số các khóa có thể sẽ giảm đi qua mỗi lần loại bỏ như thế. Nếu một câu có 20 ký tự được gửi đi thì tổng cộng sẽ có khoảng 26^{20} thông báo có thể; tuy nhiên, với một thông báo mã bất kỳ thì chỉ có 26 thông báo gốc có thể, tức là một thông báo cho mỗi khóa. Nếu nhà mã thám xem xét 26 thông báo gốc có thể tương ứng với 26 khóa, thì có rất ít khả năng có nhiều hơn một trong những thông báo gốc có thể đó sẽ tương ứng với một câu tiếng Anh có nghĩa.

Độ dư ngôn ngữ có thể được biểu thị toán học theo suất tin và suất tin tuyệt đối. Suất tin tuyệt đối của một ngôn ngữ được định nghĩa là số các bit cần để mã hóa mỗi ký tự với giả thiết rằng, tất cả các ký tự đều có cùng xác suất xuất hiện. Nếu mỗi ký tự của bảng chữ cái tiếng Anh đều có khả năng xuất hiện như nhau thì entropy của một ký tự của một thông báo có thể được cho bởi:

$$H = \sum_{26}[-(1/26)\log_2(1/26)]$$
$$= \log_2(26) = 4{,}7$$

tức là mỗi ký tự có thể cần 4,7 bit để mã hóa tối ưu và do đó, suất tin tuyệt đối của thông báo tiếng Anh là 4,7 bit trên một ký tự. Độ dư ngôn ngữ làm giảm mạnh lượng thông tin chuyển tải bởi mỗi ký tự và suất tin của một ngôn ngữ được định nghĩa như số trung bình các bit thông tin chứa trong mỗi ký tự của một thông báo, tức là $H(X)/N$ trong đó, N là số ký tự trong thông báo. Suất tin đối với các thông báo tiếng Anh nằm trong khoảng từ 1 tới 1,5 bit mỗi ký tự. Độ dư ngôn ngữ được định nghĩa là hiệu giữa suất tin tuyệt đối và suất tin của ngôn ngữ; như vậy, độ dư thừa của tiếng Anh nằm trong khoảng 3,2 và 3,7 bit trên mỗi ký tự.

Việc xác định một thông báo gốc, nếu cho bản mã tương ứng, là tương đương với xác định khóa đã dùng. Do đó, độ mật của mật mã có thể được đo theo độ bất định của khóa, xác định bởi:

$$H_C(K) = -\sum P(C) \sum P_C(K)\log_2(P_C(K))$$

trong đó

$P(C)$ = xác suất nhận được bản mã C

$P_C(K)$ = xác suất để khóa đã dùng là K với điều kiện là nhận được bản mã C.

Độ bất định khóa là số đo độ không chắc chắn của khóa với điều kiện nhận được một bản mã nào đó; độ bất định khóa bằng không có nghĩa là bản mã chứa đủ thông tin để xác định khóa một cách duy nhất. Nếu độ dài của khóa độc

lập với độ dài của thông báo thì độ bất định của khóa sẽ giảm theo độ dài bản gốc.

Khoảng duy nhất được định nghĩa là độ dài thông báo nhỏ nhất sao cho độ bất định của khóa tiến tới không. Nếu suất tin và suất tin tuyệt đối của một ngôn ngữ tương ứng là r và R thì tỷ số các thông báo có nghĩa và thông báo có thể độ dài N được cho bởi:

$$r = 2^{rN}/2^{RN} = 2^{DN}$$

trong đó

$D = R - r$ là độ dư.

Nếu $H(K)$ là entropy khóa, tức là số các bit cần để mã hóa khóa, thì với một bản mã đã cho, có tất cả $2^{H(K)}$ bản gốc có thể tương ứng, không kể các nghiệm sai. Tỷ lệ của những nghiệm sai tương ứng với các thông báo có nghĩa được cho bởi:

$$M = (2^{H(K)} - 1)r = (2^{H(K)} - 1)2^{DN}$$

Vì 2^{DN} tiến gần tới không với N lớn (miễn là $D > 0$), số các nghiệm sai xấp xỉ được cho bởi $2^{H(K)-DN}$. Như vậy khoảng duy nhất có thể được tính toán: $H(K) - DN = 0$, tức là $N = H(K)/D$.

Trong trường hợp DES, độ dài độc lập của khóa là 56 bit và như vậy, $H(K) = 56$; nếu lấy giá trị 3,2 bit trên mỗi ký tự làm độ dư thừa của tiếng Anh thì khoảng duy nhất bằng 56/3.2 = 17,5 ký tự, tức là xấp xỉ hai khối của một thông báo DES. Sự kiện bản gốc DES có thể được rút ra từ hai khối bản mã thoạt nhìn dường như đáng chú ý. Tuy nhiên, ta cần nhớ rằng, điều này chỉ có nghĩa là về mặt lý thuyết, nhà mã thám có đủ thông tin để xác định bản gốc; thực ra, trong thực tế việc xác định là không khả thi về mặt tính toán vì nó liên quan tới hơn 2^{57} phép giải mã DES.

Công trình của Shannon được tiến hành vào những năm 1940 khi độ phức tạp của các mã pháp bị hạn chế bởi khả năng tính toán của các máy mã điện cơ.

Độ mật hoàn thiện có thể được đảm bảo nếu độ dài của khóa mật bằng độ dài của thông báo gốc và mỗi khóa sẽ biến đổi cùng một thông báo gốc thành một thông báo mã khác. Tuy nhiên, trong thực tế hiện nay, các khóa ngắn hơn có thể được dùng với điều kiện là nhà mã thám chỉ có sự lựa chọn là rà soát triệt để vét cạn tất cả các khóa có thể, và kích thước của không gian khóa lớn tới mức không khả thi về mặt tính toán. *Xem* absolute rate, cryptanalysis, cryptographic key, entropy, equivocation, key equivocation, key space, noise, rate, redundancy, substitution cipher, reasonableness check.

INFOSEC *ATTT* Viết tắt của Information Security (an toàn thông tin). *So sánh với* COMPUSEC, COMSEC.

infra red motion detector ***máy dò chuyển động dùng hồng ngoại*** Trong an toàn vật lý, thiết bị phát hiện sự thâm nhập nhận biết được những thay đổi nhiệt độ xung quanh do chuyển động của một vật thể gây ra.

initialization vector ***vecto khởi đầu*** (1) Trong mật mã, một số dùng như điểm khởi đầu quá trình mã một dãy dữ liệu để tăng độ an toàn bằng cách đưa vào một biến trạng mật mã. Bổ sung và để đồng bộ hóa thiết bị mật mã. (2) Trong mật mã, nội dung của thanh ghi dịch trong các mã dòng, hoặc mã khối với sự móc nối ngay trước khi

mã hóa hoặc giải mã dòng vào. *Xem* block cipher chaining, cipher block chaining, cipher feedback, output feedback, stream cipher. *Đồng nghĩa với* initializing variable.

initializing variable ***biến khởi đầu*** *Đồng nghĩa với* initialization vector.

initial program load ***nạp chương trình ban đầu*** Trong tin học, thủ tục nạp hệ điều hành vào bộ nhớ máy tính để khởi động một giai đoạn xử lý bình thường hoặc tiếp sau một trục trặc hệ thống.

initial synchronization ***đồng bộ khởi đầu*** Trong an toàn truyền thông, kỹ thuật xáo trộn tiếng nói trong đó thông tin đồng bộ cần thiết để giải mã tín hiệu thu được chỉ được truyền đi vào lúc bắt đầu thông báo. *So sánh với* continuous synchronization. *Xem* voice scrambling.

initiator ***bộ khởi đầu*** *Đồng nghĩa với* originator.

input data validation ***kiểm tra tính hợp lệ của dữ liệu nhập, phê chuẩn dữ liệu nhập*** Trong lập trình, kỹ thuật điều khiển dùng để phát hiện dữ liệu nhập không chính xác hoặc không đầy đủ. Đó có thể bao gồm kiểm tra định dạng, kiểm tra tính đầy đủ, kiểm tra tính hợp lý và kiểm tra giới hạn.

input device ***thiết bị nhập*** *Đồng nghĩa với* input unit.

input/output channel ***kênh nhập/xuất*** *Xem* channel

input/output device ***thiết bị nhập/xuất, thiết bị vào/ra*** Trong tin học, thiết bị dùng để liên lạc với một máy tính. Vai trò của các khối nhập/xuất là chuyển đổi các tín hiệu của bộ xử lý tới, và từ, các luồng dữ liệu mà có thể diễn dịch được bởi con người, những thiết bị khác hoặc các mạng. *Xem* MODEM, speech recognizer, speech synthesizer, terminal.

input/output interface ***giao diện nhập/xuất, giao diện vào/ra*** Trong tin học, giao diện mà sẽ truyền tín hiệu ngắt từ một thiết bị ngoại vi tới CPU. *Xem* interface, interrupt, CPU.

input/output statement ***lệnh nhập/xuất*** Trong tin học, lệnh bất kỳ dẫn tới sự chuyển dữ liệu giữa bộ nhớ chính và thiết bị nhập/xuất.

input/output unit ***bộ nhập/xuất*** *Xem* input/output device.

input unit ***thiết bị nhập, thiết bị vào*** Trong tin học, thiết bị nhờ đó dữ liệu có thể được nhập vào một hệ máy tính. *Đồng nghĩa với* input device.

inquiry/response ***hỏi/đáp*** Trong các ứng dụng, phương pháp xử lý giao tác trong đó người sử dụng hỏi máy tính thông qua terminal và nhận được lời đáp hầu như tức thời.

insertion loss ***tổn hao đan xen*** Trong truyền thông, công suất bị hấp thụ do xen một phần tử thụ động vào một kênh hoặc thiết bị điện tử. Tổn hao này thường xuất hiện khi bổ sung bộ lọc hoặc bộ san bằng vào một kênh truyền thông. *Xem* channel, equalization, filter.

inside perimeter ***vành đai trong*** Trong an toàn vật lý, chỉ một đường bảo vệ, tiếp giáp vùng bảo vệ, đi qua

những điểm thâm nhập có thể, ví dụ như cửa ra vào, cửa sổ, đường hầm, cửa sổ trên trần.

installation time *thời gian cài đặt* Trong tin học, thời gian cần cho việc cài đặt, thử nghiệm và nghiệm thu phần cứng và phần mềm.

install-deinstall *cài đặt/bỏ cài đặt* Trong bảo vệ phần mềm, phương pháp bảo vệ thực hiện trên đĩa mềm mà có thể được chuyển sang đĩa cứng. Khi được cài đặt lên đĩa cứng, phần mềm bảo vệ đánh dấu đĩa cứng theo cách nào đó và đồng thời đĩa mềm được khử kích hoạt sao cho nó không thể sao được sang đĩa cứng khác. Nếu người sử dụng muốn thay đổi các máy, chương trình phải được bỏ cài đặt, nhờ đó kích hoạt lại bản sao đĩa mềm và khử kích hoạt bản sao đĩa cứng. *Xem* execute protection, floppy disk, hard disk.

instructing bank *ngân hàng thanh toán* Trong hoạt động ngân hàng, ngân hàng ra lệnh cho người gửi thực hiện giao dịch.

instructing party *bên thanh toán* Trong hoạt động ngân hàng, bên ra lệnh cho người gửi thực hiện giao dịch.

instruction *lệnh, chỉ lệnh, chỉ thị* (1) Trong tin học, chỉ dẫn cơ bản người lập trình tạo ra dưới dạng máy tính có thể chấp nhận và thực hiện. (2) Trong tin học, câu lệnh chỉ rõ thao tác nào cần phải thực hiện và giá trị hoặc vị trí của các toán hạng. (3) Trong hoạt động ngân hàng, thông tin hoặc một phần của thông tin chứa đựng một ủy quyền và những chi tiết cần thiết để chuyển tiền.

instruction format *khuôn lệnh, dạng thức lệnh* Trong tin học, khuôn thức cấp phát các bit của một lệnh mã máy cho mã thao tác, các toán hạng v.v.. *Xem* instruction set, machine code instruction, operand, operation code.

instruction repertoire *danh mục lệnh* *Đồng nghĩa với* instruction set.

instruction set *tập hợp lệnh* Trong lập trình, danh sách đầy đủ các kiểu lệnh mã máy mà có thể được giải mã và thực hiện bởi một kiểu bộ xử lý trung tâm nào đó. Các lệnh bao gồm mã phép toán và một hoặc nhiều toán hạng mà sử dụng một trong các chế độ lập địa chỉ khả dụng cho tập hợp. *Xem* addressing, central processing unit, machine code instruction, operand, operation code. *Đồng nghĩa với* instruction repertoire.

INTAMIC *Xem* International Association for Microcircuit Cards.

integer *số nguyên* Trong tin học, số nguyên có dấu. Trong ký pháp nhị phân cần có những quy ước đặc biệt để biểu diễn các số nguyên âm và dạng thông thường nhất là bù hai. Ở ký pháp này, bit đầu tiên là bit dấu (1 chỉ âm, 0 chỉ dương). Bù hai của số âm thu được bằng cách đảo ngược các chữ số 0 và 1 và sau đó thêm 1 vào vị trí thấp nhất. Do đó một byte có thể biểu diễn các số trong khoảng -128 tới +127 và 16 bit có thể biểu diễn -32 768 tới 32 768. *So sánh với* ordinal.

integral controller *bộ điều khiển tích hợp* Trong truyền thông dữ liệu, một thiết bị truyền thông cài ở máy tính mini hoặc máy tính chính. *So sánh*

với front end processor, cluster control unit.

integrated circuit ***mạch tích hợp, IC*** Trong điện tử học, tổ hợp các phần tử mạch liên thông liên kết không thể tách rời trên hoặc trong đế liên tục. Mạch tích hợp có thể chứa hàng nghìn tranzito, điện trở, điot và tụ.

integrated computing ***tính toán tích hợp*** Trong lập trình, sự sử dụng tương tranh dữ liệu bởi hai hoặc nhiều bộ chương trình phần mềm (ví dụ, bộ chương trình đồ họa hiển thị dữ liệu bảng tính điện tử).

integrated database ***cơ sở dữ liệu tích hợp*** Cơ sở dữ liệu mà đã được hợp nhất để loại bỏ các dữ liệu dư thừa. *Xem* database.

integrated digital network ***mạng kỹ thuật số tích hợp, mạng số kết hợp*** Trong truyền thông dữ liệu, mạng sử dụng truyền số và chuyển mạch số. *Xem* digital switching, digital transmission system, integrated services digital network.

integrated home system ***hệ gia dụng tích hợp*** Trong các ứng dụng, một số các hệ gia dụng có liên quan tích hợp thành hệ lớn hơn (ví dụ, tổ hợp các thiết bị cho các hệ truyền hình và phát thanh, audio-video đơn thể).

integrated injection logic ***mạch logic phun tích hợp, IIL*** Trong vi điện tử, mạch logic tiêu thụ công suất rất thấp trong đó tốc độ chuyển mạch tỷ lệ với lượng dòng phun vào. *Xem* logic circuit.

integrated modem ***modem tích hợp*** Trong truyền thông dữ liệu, modem là một bộ phận không tách rời của thiết bị mà nó cùng làm việc. *Xem* modem.

integrated optical circuit ***mạch quang tích hợp*** Trong truyền thông, tương đương quang của mạch vi điện tử. Nó tác động lên ánh sáng trong hệ sóng ánh sáng để thực hiện các chức năng truyền thông: tạo ra, tách sóng, chuyển mạch và truyền ánh sáng.

integrated services digital network ***mạng số dịch vụ tích hợp, mạng số phục vụ kết hợp, ISDN*** Trong truyền thông dữ liệu, mạng số tích hợp trong đó, cùng các chuyển mạch số và các đường số được sử dụng để thiết lập các dịch vụ khác nhau (ví dụ, điện thoại và dữ liệu).

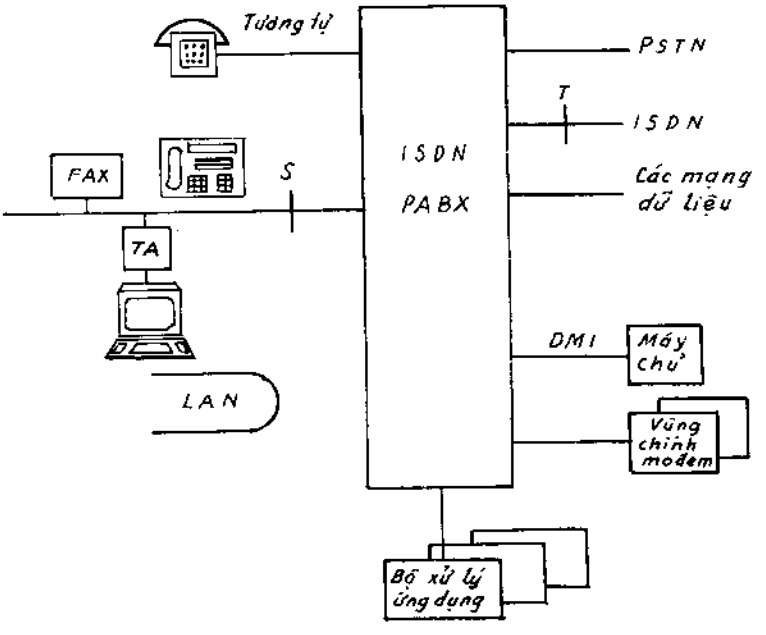
Khái niệm ISDN biểu thị một sự phát triển logic trong việc cung cấp các dịch vụ truyền thông công cộng, thừa nhận có thể có được những lợi ích kinh tế nhờ sự xuất hiện các công nghệ số, những nhu cầu đang tăng lên với rất nhiều dịch vụ truyền thông và nhu cầu cung cấp cho khách hàng, chỉ một giao diện có thể nối rất nhiều thiết bị truyền thông của người dùng (tức là, tiếng nói, fax, dữ liệu, videotex, các bộ cảm biến báo động v.v.).

Mạng điện thoại công cộng trên toàn thế giới đã mở rộng nhanh chóng về khối lượng và các phương tiện người dùng trong ba bốn chục năm lại đây. Tuy vậy công nghệ tương tự của mạng tiếng nói đã không thích hợp với các nhu cầu truyền thông dữ liệu máy tính nảy sinh đầu tiên vào những năm 1960 và đã bùng nổ trong hai ba thập niên sau đó. Sự biến đổi tất yếu dữ liệu số thành dạng tương thích với tín hiệu

tiếng nói đã đòi hỏi các modem đắt tiền ở mỗi đầu của đường truyền thông và tốc độ dữ liệu rất hạn chế: các thiết bị rẻ tiền hoạt động ở tốc độ vài trăm bit mỗi giây, còn đầu đắt tiền của dải modem chỉ có thể cho tốc độ dữ liệu vài nghìn bit mỗi giây.

Các yêu cầu truyền thông dữ liệu cho các tổ chức liên quan tới những sự chuyển dữ liệu quy mô lớn, do đó được đáp ứng bằng những kênh truyền thông dữ liệu tốc độ cao chuyên dụng. Tuy nhiên, rất nhiều người sử dụng chờ đợi hệ thống điện thoại cung cấp nhiều loại dịch vụ (ví dụ, thư điện tử, fax, videotex, đo từ xa, các mạng thông báo điện tử v.v.) và tăng cường việc cung cấp truyền thông tiếng nói về chất lượng và các dịch vụ. Nếu những dịch vụ đó thực hiện bên trong dịch vụ tiếng nói thì sẽ hợp lý khi biến đổi các tín hiệu tiếng nói cho phù hợp với các tín hiệu dữ liệu chứ không phải ngược lại. Việc sử dụng điều biến mã xung để biến đổi tín hiệu tiếng nói thành các chuỗi xung nhị phân cho phép tuyến truyền thông chỉ quan hệ với một kiểu tín hiệu cho mọi dạng truyền: tiếng nói, dữ liệu, fax. Các thể báo hiệu của điện thoại (tức là các tín hiệu điều khiển thiết lập và đóng các cuộc gọi) đã được biến đổi từ dạng tương tự sang dạng số ở các nước tiên tiến do những tiến bộ trong vi điện tử và công nghệ số.

Như vậy, khái niệm hệ truyền thông chỉ quan hệ tới truyền dữ liệu số và dùng các tín hiệu số cho các mục đích báo

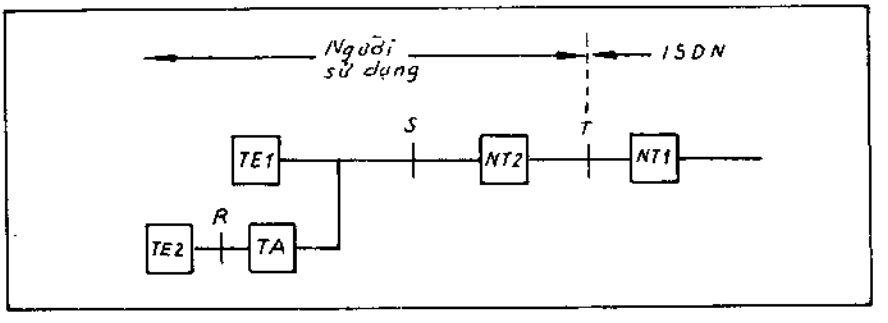


integrated services digital network: *mạng số dịch vụ tích hợp.* Hình 1. Các giao diện ISDN PABX.

hiệu, được đề xuất lần đầu tiên vào những năm 1960, đã thúc đẩy mạnh thế giới truyền thông trong hai ba thập niên gần đây. Tuy nhiên, thành công của ý đồ táo bạo đó gắn chặt với những thực tại kinh tế của lưu lượng truyền thông, sự phát triển của các tiêu chuẩn quốc tế, chính sách quốc gia và quốc tế về truyền thông, các chính sách tiếp thị của các nhà sản xuất và tính sẵn sàng của người tiêu dùng thích nghi với những ý tưởng mới và trả tiền cho chúng.

Một tổ chức cài đặt tổng đài nhánh lẻ tự động (PABX) ISDN sẽ cung cấp cho người dùng các mạch ghép nối tương thích minh hoạ trên hình 1. Ở phía những người sử dụng của PABX, các giao diện sẽ hỗ trợ các điện thoại tương tự, điện thoại số, fax, terminal máy tính, máy tính cá nhân, trạm làm việc đa chức năng và các cổng nối tới các mạng cục bộ. Rõ ràng những thiết bị ghép tương thích như vậy cũng sẽ hỗ trợ các hệ cảnh báo, vidotex, thư điện tử và thậm chí các hệ vidéo quét chậm cho các mục đích giám kiểm hoặc báo động. Các thiết bị ghép tương thích thực sự là điện thoại tương tự, thiết bị đầu cuối được thiết kế để làm việc với ISDN công cộng và các bộ thích ứng thiết bị đầu cuối được dùng để nối thiết bị không tuân theo các giao diện chuẩn ISDN (hình 2).

ISDN định nghĩa ba điểm tham chiếu *R,S* và *T*. Giao diện *R* dành cho các thiết bị hiện hành (thiết bị *TE*2) không được thiết kế để ghép nối với các mạng ISDN và do đó đòi hỏi bộ thích ứng thiết bị đầu cuối (terminal). Giao diện *S* cho phép rất nhiều thiết bị (thiết bị *TE*1) (vốn được thiết kế với các giao



integrated services digital network: *mạng số dịch vụ tích hợp.* Hình 2. cấu hình tham chiếu ISDN của CCITT (phần người sử dụng). Các định nghĩa: NT1: Khớp cuối 1 của mạng, chứa cả các chức năng truyền; NT2: Khớp cuối 2 của mạng, gồm cả các chức năng chuyển mạch và dồn kênh; R: Điểm tham chiếu R của ISDN; S: Điểm tham chiếu S của ISDN; T: Điểm tham chiếu T của ISDN; TA: Bộ thích ứng đầu cuối; TE1: Thiết bị đầu cuối kiểu 1, kiểu thiết bị đầu cuối phù hợp với giao diện chuẩn ở điểm tham chiếu S; TE2: Thiết bị đầu cuối kiểu 2, kiểu thiết bị đầu cuối không phù hợp với giao diện chuẩn ở điểm tham chiếu S.

diện ISDN) được nối trực tiếp với hệ ISDN, do đó cung cấp cho người sử dụng phương tiện nối thông dụng được đảm bảo cho rất nhiều thiết bị văn phòng hoặc gia dụng. Điểm tham chiếu *T* là giao diện giữa khớp cuối 2 của mạng (*NT*2) có các chức năng chuyển mạch và dồn kênh và khớp cuối 1 của mạng (*NT*1) vốn cung cấp các chức năng ngắt kênh ISDN ở phía người dùng.

Các phương tiện có thể nối trực tiếp với PABX bao gồm: điện thoại số, fax, trạm làm việc đa chức năng và mạng cục bộ. Điện thoại số có thể có một loạt các tính năng được liệt kê dưới đây.

(*a*) Hiển thị chữ số để chỉ báo các số được gọi, các số gọi nội bộ và các tên, số gọi bên ngoài, thời giờ và ngày tháng, thông báo nhắc nhở, thông tin xử lý cuộc gọi, các thông báo hộp thư, chỉ báo sự cố cuộc gọi, thông tin cảnh báo cuộc gọi và các lời nhắc người dùng.

(*b*) Các phím người dùng lập trình và các phím chức năng đơn cho chuyển cuộc gọi, gọi ngược tự động, chuyển tiếp cuộc gọi và quay lại số cuối cùng.

(*c*) Vận hành không dùng tay.

(*d*) Tính năng an toàn (ví dụ, bộ đọc thẻ để kiểm soát truy nhập).

Các thiết bị fax mà có thể nối với hệ bao gồm fax tương tự hiện tại và fax nhóm 4 nối trực tiếp với giao diện S. Một tính năng đặc biệt của môi trường ISDN có lẽ là trạm làm việc đa chức năng, có khả năng tích hợp tiếng nói, văn bản, hình ảnh và dữ liệu với rất nhiều tính năng bao gồm:

(*a*) Truy nhập tới các hộp thư.

(*b*) Các đặc điểm tiếng nói được nâng cao tương tự như các đặc điểm của điện thoại số.

(*c*) Mô phỏng thiết bị đầu cuối cho các cuộc hội thoại với máy tính chủ từ xa.

(*d*) Các chức năng viễn truyền văn bản.

(*e*) Truy nhập các cơ sở dữ liệu tư nhân và công cộng (ví dụ, viđeotex).

(*f*) Trao đổi và hiển thị các tài liệu giữa hai hoặc nhiều terminal.

(*g*) Các chức năng tính toán cá nhân, xử lý văn bản, các bảng tính điện tử v.v.

(*h*) Các danh mục điện thoại.

(*i*) Các phương tiện thiết bị trỏ (ví dụ, bút quang, chuột).

Các mạng cục bộ (LAN) có thể có các nối tới mạng ISDN, cho phép các LAN được nối liên thông và do đó cung cấp cho người dùng các ưu điểm kết hợp của các LAN (tức là truyền thông các khối dữ liệu tốc độ cao giữa những người sử dụng cục bộ) và các hệ PABX vốn chủ yếu định hướng chuyển mạch và liên quan tới lưu lượng truyền thông tiếng nói. Các LAN hoạt động ở những vị trí khác nhau của tổ chức, liên kết thông qua ISDN, vì thế tạo ra dáng vẻ của mạng tích hợp lớn.

PABX trong hệ ISDN sẽ không hạn chế chỉ ở các chức năng chuyển mạch và vận tải thông tin. Các phương tiện để lưu giữ và xử lý thông tin, khi được thực hiện trong các bộ xử lý ứng dụng (hình 1) sẽ cung cấp các chức năng như thư fax, thư văn bản và thư tiếng nói. Các phương tiện fax hiện thời đã chứng tỏ lợi ích của nó đối với truyền thông trong tổ chức, nhưng chúng có cùng

những nhược điểm như hệ điện thoại truyền thống: truyền thông phải được thiết lập với bên thu, truyền thông phải diễn ra trong thời gian người sử dụng thiết lập nối và với nhiều địa chỉ, đường nối mới phải được thiết lập cho mỗi bên thu. Thư fax có thể cung cấp những tính năng như:

(*a*) phân phối định thời các tài liệu;

(*b*) phương tiện phát rộng;

(*c*) chỉ dẫn chờ thông báo;

(*d*) thư mật;

(*e*) biến đổi văn bản-fax; và

(*f*) chuyển đổi viễn thông văn bản-fax.

Các phương tiện thư văn bản tương tự như thư điện tử do các mạng máy tính cung cấp, nhưng có các ưu điểm bổ sung là thư có thể được phân phối thông qua điện thoại số hoặc trạm làm việc đa chức năng. Các phát triển tương lai có thể bao gồm các dịch vụ chuyển đổi, cung cấp dịch vụ phân phát "văn bản thành tiếng nói" và "văn bản thành fax". Thư tiếng nói sử dụng các phương pháp lưu giữ và chuyển tiếp cho truyền thông tiếng nói, cho phép phân phát thông báo theo nhu cầu cho người nhận. Những người sử dụng riêng lẻ có thể được gán hộp thư và sự truy nhập tới nó thường được kiểm soát bằng mật khẩu. Các thông báo có thể được truyền đề phân phối định thời, phát rộng cho các nhóm chọn lọc và các phương tiện đổi "văn bản thành thư" sẽ cho phép người nhận thu được các thông báo gốc văn bản từ những máy nhánh điện thoại.

Giao diện giữa ISDN PABX và mạng sẽ là giao diện *T* (hình 1 và hình 2); *NT*2 của người dùng nối với các mạng *NT*1 ở một đầu của đường truyền thông, còn khớp cuối đường dây (*LT*) ghép nối với tổng đài ISDN ở đầu kia của tuyến đường dây. Các giao diện với mạng ISDN có thể được cung cấp với tốc độ cơ bản và tốc độ truy nhập sơ cấp. Có hai lớp kênh trong ISDN. Kênh *B* được dùng cho các thông báo ở tốc độ 64 kilobit trên giây, và kênh *D* (16 kilobit trên giây hoặc 64 kilobit mỗi giây) cung cấp các dịch vụ cả báo hiệu kênh chung ngoài dải lẫn thông báo phụ trợ (ví dụ, giám sát các hệ báo động). Truy nhập tốc độ cơ bản ($2B + D$) bao gồm hai kênh B và một kênh *D* (16 kilobit mỗi giây) cho tổng dung lượng 144 kilobit mỗi giây. Nếu nối tới mạng ISDN thông qua một PABX thì các terminal sẽ được nối tới PABX nhờ sử dụng truy nhập tốc độ cơ bản hoặc riêng lẻ hoặc như các chùm terminal dùng chung kênh. Truy nhập tốc độ sơ cấp bao gồm các kênh 32 x 64 kilobit mỗi giây ở Châu Âu và Australia; ở Bắc Mỹ và Nhật nó gồm các kênh 24 x 64 kilobit mỗi giây. Truy nhập tốc độ sơ cấp ở Châu Âu gồm 30 kênh *B* cho thông tin người dùng, một kênh *D* 64 kilobit mỗi giây cho báo hiệu và một lênh dành cho tín hiệu đồng bộ hệ thống và các tín hiệu báo động. Sự báo hiệu giữa thiết bị khách hàng ISDN và tổng đài ISDN được tiến hành qua các kênh *D*. Báo hiệu giữa các tổng đài ISDN sử dụng báo hiệu CCITT No 7 và các giao thức X.25 và hoặc X.75 được dùng cho nối giữa các tổng đài ISDN và các mạng chuyển mạch dữ liệu công cộng.

Các tiêu chuẩn quốc tế có tầm quan trọng tối cao trong các hệ truyền thông

tích hợp và quốc tế. CCITT đã thiết lập nhóm nghiên cứu đặc biệt ngay đầu năm 1968 để xem xét tất cả các vấn đề liên quan tới điều biến mã xung; vào năm 1984 seri khuyến nghị I đã được thông qua. Trong seri khuyến nghị này, I.100 có tư cách là mở đầu chung cho các khái niệm ISDN, I.200 liên quan tới các dịch vụ, I.300 với các khía cạnh mạng và I.400 với các giao diện mạng.

(*a*) Tính linh hoạt trong phân phối dải thông cho các ứng dụng và các tuyến đặc biệt.

(*b*) Điều khiển phân phối các tài nguyên mạng.

(*c*) Tái cấu hình các tuyến ở mạng tư nhân thực sự và các cấp phát dải thông.

(*d*) Tính đa dạng theo các định tuyến mạng luân phiên.

(*e*) Kiểm soát chi phí từ thông tin quản lý mạng, tạo điều kiện cho các kiểm soát quá trình tái cấu hình và phát triển mạng.

(*f*) Các giao diện mang tích hợp cho một dải các kiểu dịch vụ viễn thông, do đó giảm được sự phát triển mạnh các modem v.v.

(*g*) Khả năng báo hiệu người dùng, tạo điều kiện phát triển các ứng dụng tại nhà để cung cấp các dịch vụ tích hợp (ví dụ, mã hóa, đo xa, theo dõi v.v.).

(*h*) Các cơ hội cho các dịch vụ bổ sung giá trị, nhắc nhở bằng tiếng nói, truy nhập cơ sở dữ liệu, thư điện tử v.v.. *Xem* baud, bulletin board, CCITT, digital telephone, electronic mail, facsimile, facsimile mail, local area network, MODEM PABX, PCM, open systems interconnection, primary rate access, store and forward, telemetering, videotex, voice mail, X.25, X.75.

integrity ***(tính) toàn vẹn, (tính) nguyên vẹn*** (1) Trong an toàn dữ liệu, đặc tính an toàn của máy tính đảm bảo rằng, các tài nguyên của máy tính vận hành đúng và dữ liệu trong các cơ sở dữ liệu là đúng. Đặc trưng này bảo vệ chống lại sự thao tác không được phép có chủ ý hoặc vô ý của hệ thống cùng với đảm bảo và duy trì sự an toàn của các thực thể của một hệ máy tính trong mọi điều kiện. (2) Trong an toàn dữ liệu, chất lượng hoặc trạng thái còn nguyên vẹn; trạng thái tốt. (*a*) Trong an toàn dữ liệu, khả năng của một hệ thống tự động hóa thực hiện chức năng đã định của nó theo một cách không bị suy suyền, không có sự thao tác bất hợp pháp cố ý hoặc vô ý đối với hệ thống. (*b*) Trong an toàn dữ liệu, chất lượng vốn có của sự bảo vệ vốn đảm bảo và duy trì sự an toàn của các thực thể của một hệ máy tính trong mọi điều kiện. (3) Trong an toàn máy tính, sự đảm bảo trong mọi điều kiện để hệ thống phản ánh tính đúng đắn logic và độ tin cậy của hệ điều hành; tính hoàn chỉnh logic của phần cứng và phần mềm thực hiện các cơ chế bảo vệ; và tính nhất quán của các cấu trúc dữ liệu và độ chính xác của dữ liệu đã nhớ. Trong một mô hình an toàn hình thức, tính toàn vẹn được giải thích hẹp hơn với nghĩa sự bảo vệ chống lại việc sửa đổi bất hợp pháp hoặc phá hủy đối với thông tin. *Xem* data integrity, system integrity. (4) Trong an toàn dữ liệu, quá trình ngăn ngừa sự thay đổi dữ liệu không phát hiện được. Thuật ngữ này phù hợp với xác thực bởi vì xác thực

thường được dùng trong truyền thông dữ liệu để chỉ sự kiểm chứng thực thể ngang hàng. *Xem* authentication, data integrity, system integrity. (5) Trong tin học, sự bảo toàn các tệp cho mục đích đã định của chúng. *Xem* data integrity.

integrity check value ***giá trị kiểm tra tính nguyên vẹn*** Trong an toàn truyền thông, mã xác thực thông báo hoặc tổng kiểm tra mật mã gắn với một gói tin trong một mạng cục bộ dựa trên IEEE 802 để kiểm tra tính toàn vẹn. *Xem* message authentication code, IEEE 802.

integrity level ***mức toàn vẹn*** Trong kiểm soát truy nhập, mức đáng tin cậy gắn với một chủ thể hoặc đối tượng. *Xem* Biba model, trustworthiness.

integrity locking ***khóa nguyên vẹn*** *Đồng nghĩa với* spray paint.

integrity policy ***chính sách toàn vẹn*** Trong an toàn dữ liệu, chính sách an toàn để ngăn ngừa những người sử dụng không được phép sửa đổi, tức là ghi thông tin nhạy cảm. *So sánh với* secrecy policy. *Xem* Biba model, security policy.

integrity validation procedure ***thủ tục phê chuẩn tính toàn vẹn*** Ở các mô hình hình thức, thuật ngữ dùng trong mô hình Clark-Wilson đối với một thủ tục được yêu cầu để kiểm tra xem tập hợp các mục dữ liệu ràng buộc có tương ứng với một trạng thái an toàn không. *Xem* Clark-Wilson model, constrained data item.

intelligence ***tin tức tình báo; tin tức; tính thông minh; trí tuệ*** (1) Tin tức tình báo là sản phẩm rút ra từ việc thu thập, đánh giá, phân tích, tích hợp và giải thích toàn bộ thông tin có liên quan tới một hoặc nhiều khía cạnh về các nước hoặc vùng bên ngoài mà có ý nghĩa trực tiếp hoặc tiềm ẩn đối với sự phát triển và thực hiện các kế hoạch, chính sách và hoạt động. (2) Trong truyền thông, tin tức là dữ liệu, thông tin hoặc các thông báo cần được truyền đi. (3) Trong tin học, tính thông minh là tính chất của một thiết bị có khả năng xử lý cục bộ. *Xem* intelligent device. (4) Định nghĩa trí tuệ tự nhiên có tầm quan trọng ngày càng tăng trong xem xét tính năng của các hệ trí tuệ nhân tạo. Các định nghĩa đã được đề xuất bao gồm: (*a*) khái niệm liên quan tới sự sáng tạo, sự định hướng và phán xét nhanh chóng; (*b*) năng lực tập hợp hoặc tổng thể của các cá nhân hành động hoàn toàn có mục đích, suy nghĩ hợp lý và giải quyết có hiệu quả các môi trường của họ; và (*c*) khả năng chung của các cá nhân điều chỉnh có ý thức tư duy của mình tới những yêu cầu mới và tính thích ứng chung đối với những vấn đề và điều kiện mới. *Xem* artificial intelligence.

intelligent card reader ***bộ đọc thẻ thông minh*** Trong kiểm soát truy nhập, bộ đọc thẻ so sánh các dữ liệu đọc từ một thẻ kiểm soát truy nhập với các tham số đã lập trình trước. *So sánh với* on line card reader. *Xem* card reader. *Đồng nghĩa với* off line card reader.

intelligent device ***thiết bị thông minh*** Trong tính toán, thiết bị hoặc thiết bị ngoại vi bất kỳ mà có thể lập trình được. *So sánh với* dumb device. *Xem* intelligent terminal.

intelligent disk server ***trình phục vụ***

đĩa thông minh Trong tính toán, trình phục vụ đĩa cung cấp cơ chế đơn giản để cho các máy vi tính trong mạng yêu cầu và truy nhập tới các thiết bị ngoại vi và các volum đĩa tập trung. Hệ có thể quản lý việc dùng chung hiệu quả các máy in, các ổ băng, các máy vẽ v.v. và cũng có thể cung cấp một mức độ an toàn bằng cách điều khiển truy nhập của người dùng riêng lẻ vào các phương tiện. *Xem* disk server, file server.

intelligent knowledge based system ***hệ dựa trên tri thức thông minh*** *Xem* expert systems.

intelligent terminal ***terminal thông minh, thiết bị đầu cuối thông minh*** Trong sử dụng các máy tính, thiết bị có bộ hiển thị, bàn phím, bộ nhớ của bộ xử lý và phần mềm cục bộ nối với máy tính chủ. Terminal có khả năng xử lý đủ để cung cấp các câu nhắc nhở người dùng, các khả năng soạn thảo v.v. và có thể tiếp tục vận hành ở chế độ hạn chế, trong thời gian nhất định mà không cần liên lạc với máy tính chủ. Các terminal thông minh thường được dùng ở các cửa hàng bán lẻ, nhà băng, thu thập dữ liệu công nghiệp v.v. *So sánh với* dumb terminal. *Xem* host computer, intelligence, terminal.

intelligent token ***thẻ bài thông minh*** *Đồng nghĩa với* supersmart card.

intelligible crosstalk ***xuyên âm rõ*** Trong truyền thông, chỉ xuyên âm có độ rõ hợp lý. *Xem* crosstalk.

interactive ***tương tác*** Trong tin học, hệ kiểu hội thoại trong đó có thể diễn ra sự đối thoại liên tục giữa người sử dụng và máy tính. *Xem* inquiry/response.

interactive computing ***tính toán tương tác*** Trong tin học, việc sử dụng máy tính sao cho người sử dụng trong lúc điều khiển có thể nhập dữ liệu hoặc đưa ra những yêu cầu khác đối với hệ thống và được đáp lại bằng việc xử lý lập tức các yêu cầu của người dùng và đưa ra những lời đáp thích hợp cho những yêu cầu đó.

interactive videotex ***videotex tương tác*** *Xem* videotex. *Đồng nghĩa với* viewdata.

intercept ***chặn (thu)*** Trong an toàn truyền thông, chỉ việc tạo đích cho một nguồn truyền thông và sau đó thu được thông tin đã truyền.

interceptability ***tính dễ bị chặn*** Trong an toàn truyền thông, tính dễ bị chặn thu của một hệ truyền thông. *Xem* intercept.

interchange ***trao đổi*** (1) Trong hoạt động ngân hàng, sự chấp nhận và sự trao đổi lẫn nhau các thông báo dữ liệu giữa các cơ sở tài chính. (2) Trong hoạt động ngân hàng, hệ trong đó nơi phát hành thẻ và nơi nhận thẻ không phải cùng các cơ quan. *So sánh với* local network. *Xem* acquirer, issuer.

interchange group ***nhóm trao đổi*** *Xem* ANSI - X.12, EDIFACT.

interchange key ***khóa trao đổi*** (1) Trong quản lý khóa, khóa dùng bởi hai bên trong một sơ đồ mã hóa điểm tới điểm như khóa mã hóa khóa. *Xem* electronic mail security, end-to-end encryption, key-encrypting key. (2) Trong

quản lý khóa, khóa thứ cấp dùng làm cơ sở của một khóa mã hóa khóa trong sơ đồ công chứng khóa. Khóa trao đổi gắn liền với một nút, hoặc một cặp nút. Nó được kết hợp với các ký hiệu nhận dạng của người dùng để tạo thành một khóa được công chứng mà đến lượt mình nó lại được dùng để mã hóa các khóa mã hóa dữ liệu. *Xem* data-encrypting key, key-encrypting key, key notarization, secondary key.

interchange transaction ***giao dịch trao đổi*** Trong hoạt động ngân hàng, giao dịch trong những tình huống trong đó ATM, hoặc đầu cuối EFTPOS, không bị kiểm soát bởi cơ sở tài chính phát hành thẻ. *So sánh với* local transaction. *Xem* EFTPOS, PIN management and security.

interdiction ***(sự) cấm sử dụng*** Trong an toàn máy tính, hành động ngăn cản hoặc từ chối cho người dùng sử dụng các tài nguyên hệ thống. *Xem* delay/denial of service, denial of service, resource.

interface ***giao diện,mạch ghép nối, khớp nối*** (1) Biên chung giữa các hệ hoặc modun độc lập mà ở đó diễn ra truyền thông. (2) Trong truyền thông dữ liệu, biên dùng chung giữa hai thiết bị hoặc thành phần có liên quan được xác định nhằm quy định kiểu và dạng các tín hiệu đi qua chúng (ví dụ, cổng nối EIA RS-232C biểu diễn bộ chuẩn của các đặc trưng tín hiệu - thời điểm, thời khoảng, điện áp và dòng điện - được mô tả bởi Hiệp hội công nghiệp điện tử (EIA) để sử dụng ở các terminal truyền thông). Nó cũng bao gồm cách bố trí bộ nối phích/đầu cắm chuẩn. *Xem* RS-232C. (3) Trong lập trình, đặc tả của truyền thông giữa các modun của một chương trình. *Xem* information hiding. (4) Ở các máy vi tính có ba kiểu giao diện chính, không nhất thiết loại trừ nhau. Đó là: Giao diện dãy lệnh đáp ứng các lệnh do người dùng gõ vào; giao diện dựa trên thực đơn; giao diện đồ họa.

interface data unit ***đơn vị dữ liệu giao diện*** Trong truyền thông dữ liệu, thông báo chuyển từ tầng này sang tầng khác trong Mô hình chuẩn hợp mạng hệ mở. Đơn vị dữ liệu giao diện bao gồm đơn vị dữ liệu dịch vụ cộng với thông tin điều khiển. *So sánh với* protocol data unit, service data unit. *Xem* open systems interconnection.

interface message processor ***bộ xử lý thông báo giao diện*** Trong truyền thông dữ liệu, thuật ngữ bắt nguồn từ mạng ARPA để mô tả một máy tính chuyển mạch gói. *Xem* ARPA, DATA communications, interface processor, packet switch node.

interface processor ***bộ xử lý giao diện*** Trong truyền thông dữ liệu, bộ xử lý tác động như giao diện giữa terminal hoặc máy tính và mạng hoặc máy tính được dùng để điều khiển luồng dữ liệu vào mạng. *Xem* interface.

interference ***nhiễu*** Trong truyền thông, nhiễu là những tín hiệu không mong muốn bất kỳ xuất hiện trên một kênh với mức đủ để làm giảm hiệu suất của kênh ở mức độ lớn. Nhiễu có thể là kết quả của các tiếng ồn hoặc tín hiệu do tự nhiên hoặc con người gây ra. *Xem* EMI/RF radiation.

interim approval ***phê duyệt tạm thời***

Trong an toàn máy tính, sự cho phép tạm thời một hệ thông tin xử lý thông tin nhạy cảm hoặc quan trọng trong môi trường vận hành của nó dựa trên các kết quả sơ bộ của đánh giá an toàn toàn diện đối với một hệ thông tin.

interlock ***khóa liên động*** Ngăn ngừa máy hoặc thiết bị bắt đầu những thao tác tiếp cho tới khi thao tác hiện thời hoàn thành.

intermediary bank ***ngân hàng trung gian, ngân hàng môi giới*** Trong hoạt động ngân hàng, một ngân hàng hoặc các ngân hàng giữa ngân hàng nhận và ngân hàng của người được hưởng phải có sự chuyển tiền qua đó nếu được ngân hàng gửi chỉ ra. Trong những trường hợp như thế đó là bên có của ngân hàng nhận. *Xem* credit party.

intermediate text block ***ký tự khối văn bản trung gian, ITB*** Trong truyền thông dữ liệu, ký tự điều khiển dùng để kết thúc một khối ký tự trung gian. *Xem* end of text.

intermittent error ***lỗi thất thường*** Lỗi xuất hiện rời rạc ngẫu nhiên. Cực kỳ khó tái tạo nó và do vậy cực kỳ khó sửa.

intermodulation distortion ***méo điều biến tương hỗ*** Trong điện tử học, méo do sự tương tác của hai hoặc nhiều tần số khi có quan hệ phi tuyến giữa các tín hiệu đầu vào và đầu ra.

internal audit ***kiểm toán nội bộ, kiểm tra nội bộ*** Trong hoạt động kiểm toán, sự kiểm toán một hệ thống được tiến hành bởi một nhân viên được chỉ định chứ không phải bởi một kiểm toán viên bên ngoài. *So sánh với* external audit. *Xem* internal security audit.

internal auditor ***kiểm tra viên nội bộ, kiểm toán viên nội bộ*** Trong hoạt động kiểm toán, một nhân viên của một tổ chức có trách nhiệm đảm bảo để các nhân viên tuân theo các chính sách, các tiêu chuẩn và các thủ tục của tổ chức.

Các trách nhiệm của kiểm toán viên nội bộ đã được mô tả bởi Quy chế kiểm toán viên nội bộ, là "một hoạt động đánh giá độc lập..." và như "một sự kiểm soát hoạt động theo cách xem xét và đánh giá tính thích hợp và hiệu quả của những sự kiểm soát khác".

Kiểm toán nội bộ liên quan tới việc đánh giá và giám sát các hệ và các cơ chế của kiểm soát nội bộ. Những hệ thống và những cơ chế như thế thường có thể bao gồm những hệ mà:

- đảm bảo tôn trọng các quy định từ bên ngoài và các chính sách quản lý;
- bảo vệ tài sản và đảm bảo sự đúng đắn của những trách nhiệm pháp lý;
- đảm bảo độ chính xác và độ tin cậy của các bản ghi, các báo cáo tài chính và thông tin quản lý;
- xác nhận rằng, các kết quả của các hoạt động hợp tác là phù hợp với các mục tiêu của chúng.

Xem external auditor. *Xem* internal audit.

internal control documentation ***hồ sơ kiểm soát nội bộ*** Các chính sach được ghi lại, các biểu đồ tổ chức, các bản tường trình thủ tục, các bản hướng dẫn, các bản ghi nhớ, các lưu đồ, các bảng quyết định, các bản câu hỏi hoàn

chính, phần mềm và những tài liệu đã ghi có liên quan dùng để mô tả các phương pháp và biện pháp kiểm soát nội bộ, để thông báo những trách nhiệm và quyền hạn vận hành những phương pháp và biện pháp như thế và để dùng làm tài liệu tham khảo cho những người xét duyệt các kiểm soát nội bộ và hoạt động của chúng. *Xem* internal controls.

internal control review ***xét duyệt kiểm soát nội bộ*** Việc xem xét chi tiết kiểm soát nội bộ để xác định xem liệu các biện pháp kiểm soát thích đáng có tồn tại và được thực hiện để ngăn ngừa hoặc phát hiện sự xuất hiện của những rủi ro tiềm tàng trong phương thức chi phí hiệu quả hay không. *Xem* internal controls.

internal controls ***(các) kiểm soát nội bộ*** Kế hoạch của tổ chức và tất cả các phương pháp và biện pháp được chấp nhận trong một cơ quan, nhằm bảo vệ các tài nguyên, đảm bảo độ chính xác và độ tin cậy của thông tin của nó, đảm bảo tuân thủ các luật, các quy định và các chính sách áp dụng được và thúc đẩy sự tiết kiệm và hiệu quả trong hoạt động.

internal reciprocal ***hỗ trợ nội bộ*** Trong quản lý rủi ro, chiến lược khôi phục sau sự cố được chấp nhận trong phạm vi một tổ chức bằng cách bố trí dự phòng lẫn nhau giữa các hệ thống thiết bị trong tổ chức. *So sánh với* reciprocal.

internal security audit ***kiểm toán an toàn nội bộ*** Trong an toàn máy tính, sự kiểm toán an toàn được tiến hành bởi nhân sự chịu trách nhiệm quản lý tổ chức được kiểm toán. *So sánh với* external security audit. *Xem* audit, security audit.

internal security controls ***(các) kiểm soát an toàn nội bộ*** Trong an toàn máy tính, các tính năng phần cứng, phần sụn và phần mềm bên trong một hệ tự động hóa làm hạn chế truy nhập vào các tài nguyên (phần cứng, phần mềm và dữ liệu) chỉ đối với các đối tượng được phép (người, chương trình hoặc thiết bị). Các kiểm soát đó cũng có thể cung cấp các kiểm tra giới hạn, các kiểm tra tính hợp lý v.v. *Xem* firmware, reasonableness check, subject.

internal subject ***chủ thể nội bộ*** Trong an toàn máy tính, chủ thể không hoạt động như một đại diện trực tiếp cho một người sử dụng. Một quá trình không gắn liền với bất kỳ người sử dụng nào nhưng thực hiện những chức năng rộng rãi của hệ thống như chuyển mạch gói, lưu giữ dữ liệu tạm thời cho máy in dòng v.v.. *Xem* subject. *Đồng nghĩa với* daemon, service machine.

internal use ***sử dụng nội bộ*** Trong an toàn dữ liệu, mức phân loại an toàn không đòi hỏi sự bảo vệ chống lại sự tiết lộ trong một tổ chức. *Xem* classification.

international alphabet number 5 ***bảng chữ cái quốc tế số 5*** Trong mã hóa, tập hợp con của ISO-7 trong đó các ký tự cho sử dụng ở một quốc gia hoặc được đặc tả hoặc không được dùng. *Xem* ISO-7.

International Association for Microcircuit Cards ***Hiệp hội quốc***

tế về thẻ vi mạch, INTAMIC Tổ chức của các sở tài chính được thành lập để nghiên cứu thẻ vi mạch và khảo sát việc ứng dụng nó trong các lĩnh vực tài chính. Nó được thành lập năm 1981 với số hội viên là các ngân hàng trong bảy quốc gia: Bỉ, Pháp, Đức, Ailen, Luxămbua, Hà Lan và LH Anh. Vào năm 1985 tư cách hội viên được mở rộng, kết nạp thêm Thụy Điển, ngân hàng Chase Manhattan (Mỹ), Nauy, Niu Di Lân, ngân hàng Mỹ và Đan Mạch. Các mục tiêu của INTAMIC là: (*a*) xây dựng những tiêu chuẩn tối thiểu cho việc sử dụng các thẻ vi mạch như một công cụ tài chính và cho thanh toán quốc tế. (*b*) Nghiên cứu phối hợp về các khả năng về chi phí, an toàn và vận hành có thể của các thẻ vi mạch. *Xem* microcircuit card.

International Information Integrity Institute ***Viện toàn vẹn thông tin quốc tế*** Viện do SRI quốc tế thành lập và chuyên về đảm bảo tính toàn vẹn và an toàn của thông tin như một tài sản kinh doanh của khu vực tư nhân trên khắp thế giới.

International Information Systems Security Certification Consortium ***Consocxiom chứng nhận an toàn hệ thống thông tin quốc tế*** Trong an toàn thông tin, consocxiom được thành lập năm 1990 bởi sáu hiệp hội công nghiệp máy tính để đạt được sự chứng nhận của các chuyên gia an toàn.

International Network Working Group ***nhóm làm việc mạng quốc tế, INWG*** Diễn đàn thảo luận các tiêu chuẩn và các giao thức mạng. Nó là nhóm làm việc trong phạm vi Liên đoàn quốc tế về xử lý thông tin dưới tên gọi "International Packet Switching for Computer Sharing" (Chuyển mạch gói cho dùng chung máy tính quốc tế). *Xem* IFIP.

International Packet Switched Service ***dịch vụ chuyển mạch gói quốc tế, IPSS*** Trong truyền thông dữ liệu, hệ chuyển mạch gói hoạt động giữa Châu Âu và Hoa Kỳ.

International Standards Organization ***Tổ chức tiêu chuẩn hóa quốc tế, tổ chức ISO*** Cơ quan của Liên hợp quốc nghiên cứu tiêu chuẩn hóa quốc tế đối với một lĩnh vực rộng các sản phẩm công nghiệp. *Xem* protocol standards.

International Telecommunications Union ***Liên đoàn viễn thông quốc tế, ITU*** Cơ quan khuyến khích sự hợp tác quốc tế trong viễn thông với quan điểm cải tiến hiệu suất các dịch vụ trên thế giới. Nó là tổ chức chuyên môn hóa của Liên hợp quốc và có ba ủy ban thường trực: IFRB (Cơ quan đăng ký tần số quốc tế), CCIR và CCITT. Các quy tắc của nó có địa vị các hiệp ước chính thức giữa các nước tham gia và là bắt buộc đối với các bên ký kết vốn đã tán thành chúng. *Xem* CCIR, CCITT, protocol standards.

Internet ***(mạng) Internet*** (1) Trong truyền thông dữ liệu, đường truyền dẫn mạng bao gồm ba mạng: Arpanet, Milnet và NSFnet (mạng Quỹ khoa học quốc gia). Nó được sử dụng cho nghiên cứu tiến hành cho Bộ quốc phòng Mỹ bởi những cơ quan chính phủ khác nhau, các trung tâm nghiên cứu và các đại học. *Xem* Arpanet Morris Worm.

(2) Internet còn là mạng máy tính toàn cầu - một mạng liên kết các mạng máy tính trên toàn thế giới qua vệ tinh và điện thoại, nối những người sử dụng với các dịch vụ mạng, ví dụ như thư điện tử và Web.

Internet protocol ***giao thức Internet*** Trong truyền thông dữ liệu, giao thức mạng không nối kết nhằm điều khiển sự kết nối các mạng LAN và WAN trong Internet ARPA. *Xem* ARPANET, network layer, TCP/IP.

Internetworking ***liên kết mạng*** Trong truyền thông dữ liệu, quá trình nối các mạng máy tính không đồng nhất vốn có thể có các giao thức khác nhau với nhau. Các chỗ nối giữa các mạng được gọi là cổng nối và chúng chịu trách nhiệm đảm bảo để các thông báo khi chuyển sang mạng khác sẽ tuân thủ những giao thức cần thiết của mạng đó. *Xem* gateway, protocol.

interoperability ***khả năng liên vận hành, khả năng cùng hoạt động*** (1) Trong an toàn truyền thông, khả năng và mức độ mà một hệ có thể trao đổi thông tin với hệ khác. (2) Trong quản lý khóa, khả năng trao đổi các khóa mật mã, cho dù thủ công hay trong một môi trường tự động hóa, với một bên bất kỳ khác. *Xem* cryptographic key. (3) Trong quản lý khóa, khả năng trao đổi các khóa, cả thủ công lẫn trong môi trường tự động hóa, với một bên bất kỳ khác thực hiện tiêu chuẩn đó, với điều kiện là cả hai sự thực hiện đều sử dụng các lựa chọn tương thích của tiêu chuẩn đó và các phương tiện truyền thông tương thích. *Xem* ANSI X9.17 - 1985, cryptographic key.

interprocess communication ***truyền thông liên quá trình, liên lạc giữa các quá trình*** Trong an toàn máy tính, sự liên lạc giữa hai quá trình khác nhau sử dụng các kết cấu do hệ thống cung cấp; ví dụ như các tệp dùng chung.

interrupt ***ngắt*** (1) Trong tin học, phương tiện cho phép bộ xử lý trung tâm xử lý tương tranh một số thiết bị nhập/xuất trên cơ sở thứ tự ưu tiên. Ngắt được gửi từ thiết bị nhập/xuất tới bộ xử lý trung tâm (CPU) yêu cầu tác động (ví dụ, nhận dữ liệu). CPU tạm dừng thực hiện nhiệm vụ hiện thời, chuyển điều khiển tới một vị trí xác định trong bộ nhớ mà sau đó gọi thường trình để giải quyết ngắt. Khi hoàn thành, điều khiển được trả lại cho nhiệm vụ đã bị ngắt. *So sánh với* DMA. *Xem* CPU, input/output unit, virus. (2) Trong truyền thông dữ liệu, ngắt là tiến hành tác động ở trạm thu khiến cho trạm truyền kết thúc buổi truyền.

interrupt controlled I/O ***I/O điều khiển bằng ngắt*** Trong tin học, kỹ thuật để điều khiển sự chuyển dữ liệu giữa bộ xử lý và các thiết bị nhập/xuất. Mỗi thiết bị I/O, hoặc bộ điều khiển của nó, đều được nối với một đường ngắt và mỗi khi thiết bị cần một sự chú ý thì nó tạo ra một tín hiệu để ngắt bộ xử lý. *So sánh với* DMA, polling. *Xem* interrupt.

intersymbol dependence ***(sự) phụ thuộc liên ký hiệu*** Trong mật mã, tính chất của một mã pháp trong đó mỗi bit của khối bản mật mã là một hàm đủ phức tạp của mỗi bit trước đó trong bản gốc đầu vào. Liên kết khối

mật mã thể hiện sự phụ thuộc giữa các ký hiệu. *So sánh với* strong intersymbol dependence. *Xem* cipher block chaining.

intervention signal ***tín hiệu xen vào*** Trong truyền thông dữ liệu, tín hiệu điều khiển cho thiết bị ở mỗi đầu của kênh chứ không phải cho bản thân kênh.

intractable ***không giải được*** Trong toán học, chỉ một bài toán không thể giải được trong thời gian đa thức. *So sánh với* tractable. *Xem* time and space requirements.

intruder ***kẻ đột nhật, kẻ xâm nhập*** Trong an toàn dữ liệu, người cố tìm cách sử dụng bất hợp pháp hệ truyền thông dữ liệu. Kẻ xâm nhập có thể nghe lén và cố giải mã thông báo mã hóa hoặc tìm cách chủ động can thiệp vào các thông báo. *Xem* attacker, ciphertext, Trojan horse, wiretapp.

intruder detector system ***hệ phát hiện đột nhập*** Trong an toàn vật lý, bộ chương trình phần mềm cảnh báo cho sĩ quan an toàn khi một kẻ tấn công đinh xâm nhập vào hệ thống. *Xem* intruder.

intrusion ***xâm nhập, xâm phạm*** Trong lập pháp, sự xâm phạm bằng bất kỳ phương tiện nào vào tài sản tư nhân hoặc tài sản công cộng có kiểm soát.

intrusion detection ***phát hiện xâm nhập*** Trong kiểm soát truy nhập, chỉ các kỹ thuật nhằm phát hiện sự xâm nhập vào một máy tính hoặc mạng bằng các quan sát các sổ trực an toàn hoặc dữ liệu kiểm toán.

Có một sự quan tâm lớn đối với việc phát triển các hệ thống đủ thông minh để phát hiện sự truy nhập đáng ngờ bất hợp pháp và các hệ hoặc các mạng máy tính bằng cách phân tích trực tiếp các bản ghi kiểm toán hoặc các nhật ký an toàn. Hệ gọi là IDES (hệ chuyên gia phát hiện thâm nhập) được báo cáo bởi Denning là một mô hình được trích dẫn rộng rãi về phương pháp phát hiện thâm nhập, dựa trên các sự sai lạc quan sát được của các bản ghi kiểm toán so với một mẫu chuẩn nào đó.

Denning gợi ý rằng, các ví dụ về động thái bất thường gắn liền với các cuộc tấn công vào hệ thống bao gồm:

- đột nhập thử: tỷ lệ hỏng mật khẩu cao, hoặc đối với một người sử dụng duy nhất hoặc đối với toàn hệ thống;
- đột nhập giả mạo/thành công: sự thay đổi so với thời gian đăng nhập, vị trí đăng nhập, việc sử dụng các tài nguyên, kiểu lệnh thực hiện thông thường;
- sự thâm nhập của người sử dụng hợp pháp: sự thay đổi so với mẫu sử dụng bình thường, con số vi phạm bảo vệ được báo cáo cao;
- rò rỉ bởi người sử dụng hợp pháp: những lần đăng nhập bất bình thường, đầu ra được hướng tới máy in bất bình thường;
- suy luận bởi người sử dụng hợp pháp: số các bản ghi truy lục được cao bất thường;
- con ngựa thành Toroa: sự thay đổi trong sử dụng CPU hoặc tài nguyên I/O.
- virut: số lượng bất thường các chương trình khả thi được ghi lại, sự tăng nhu cầu nhớ của những chương trình khả thi;

- sự từ chối phục vụ: mức hoạt động tài nguyên cao bởi một người sử dụng và mức hoạt động thấp bất thường bởi tất cả những người sử dụng khác.

Mô hình IDES có sáu thành phần chính:

- Các chủ thể - những người khởi phát hoạt động trong hệ thống đang được giám sát;
- Các đối tượng - các tài nguyên được quản lý bởi hệ thống;
- Các bản ghi kiểm toán - do hệ thống tạo ra khi các chủ thể thực hiện, hoặc cố gắng thực hiện, các hành động trên các đối tượng, khởi nhập, các truy nhập tệp v.v.;
- Các lược tả (profile) - các cấu trúc dữ liệu đặc trưng cho cách thức mà các chủ thể cư xử đối với các đối tượng, ví dụ như số lần đăng nhập trung bình mỗi ngày của một người sử dụng nào đó tại một thiết bị đầu cuối xác định;
- Các bản ghi bất thường - được tạo ra khi các dữ liệu kiểm toán được coi là bất thường theo một lược tả;
- Các quy tắc hoạt động - hành động được tiến hành khi một điều kiện được thỏa mãn.

Các bản ghi kiểm toán cung cấp thông tin về tương tác giữa một chủ thể và một đối tượng riêng lẻ; nếu có nhiều hơn một đối tượng có liên quan trong tương tác thì các bản ghi kiểm toán riêng lẻ được phát triển đối với mỗi tương tác. Ví dụ, một người sử dụng sao chép ngày tháng từ Tệp A tới Tệp B sẽ tạo ra ba bản ghi kiểm toán tương ứng với hành động thực hiện của chương trình Copy, hành động đọc trên Tệp A và hành động ghi trên Tệp B.

Bản ghi kiểm toán chứa sáu trường: chủ thể, hành động, đối tượng, điều kiện ngoại lệ, sử dụng tài nguyên và tem thời gian/ngày tháng. Do đó một bản ghi kiểm toán điển hình có thể ghi rõ rằng "Jones đọc 1500 bản ghi của Tệp B vào lúc 11.00.01.07 ngày 24 tháng 11 năm 1990 và không đưa ra điều kiện ngoại lệ."

Các lược tả được xác định để nhận diện cách ứng xử bất bình thường mà có thể chỉ báo về một sự xâm nhập vào hệ thống. Các bản lược tả có thể có mức chi tiết dẫn lên về một người sử dụng đơn lẻ và một đối tượng đơn lẻ, cung cấp một số đo nào đó về "biến diễn bình thường", sao cho sự sai lệch so với chuẩn đó có thể là một chỉ báo tốt về một cuộc tấn công, ví dụ như số lượng trung bình các bản ghi mà Smith truy nhập từ một cơ sở dữ liệu Census trong một ngày. Sự tăng đột biến và nhiều trong những truy nhập như thế có thể chỉ ra rằng, Smith đang tiến hành một cuộc tấn công bằng suy luận lên cơ sở dữ liệu, bằng cách tích góp một lượng dữ liệu khổng lồ.

Các lược tả cũng có thể được xác định đối với những lớp chủ thể và những nhóm đối tượng; ví dụ, các cuộc tấn công của virut không gắn với một người sử dụng riêng, hoặc tệp riêng, mà chúng có thể tự biểu hiện khi truy nhập ghi cao bất bình thường lên một nhóm các tệp .EXE. Hơn nữa, bằng cách giám sát cách ứng xử của lớp, có thể so sánh cách ứng xử của một người sử dụng với cách ứng xử trung bình của các thành viên cùng lớp.

Các lược tả có thể tạo dựng một mẫu "hoạt động bình thường" bằng cách lưu một số đo thống kê nào đó về động thái, ví dụ như những lần đăng nhập không thành công, ở một chủ thể hoặc lớp chủ thể. Một số đo như vậy chẳng hạn có thể chỉ ra các kỹ năng gõ bàn phím kém cỏi của một người sử dụng cụ thể nào đó.

Các biến cố xuất hiện trong hệ thống, hoặc do việc tạo ra một bản ghi kiểm toán, hoặc một tín hiệu đồng hồ cho biết rằng, một khoảng thời gian xác định đã hoàn thành. Một bản ghi kiểm toán có thể cập nhật các dữ liệu thống kê trong một lược tả, hoặc dữ liệu của lược tả như vậy có thể được cập nhật bởi dữ liệu thu gom được trong một khoảng thời gian xác định.

Các biến cố bản ghi kiểm toán hoặc tín hiệu đồng hồ cũng có thể khiến cho một cuộc kiểm tra được tiến hành về một trạng thái bất thường bất kỳ khi được chỉ ra bởi sự chênh lệch giữa một giá trị đã báo cáo và các dữ liệu trong lược tả tương ứng. Ví dụ, nếu một lớp các thiết bị đầu cuối có số lần khởi nhập không thành công cao bất thường trong một ngày làm việc thì điều đó có thể cho biết rằng, một kẻ tấn công đang cố thử một mật khẩu "phỏng đoán" đối với một số lớn người sử dụng. Một sự tấn công như thế chỉ có thể gây ra một sự cố nhập mạng được ghi lại đối với mỗi người sử dụng, và do vậy, không thể được các bản ghi kiểm toán nhận biết như một biến cố bất thường đối với mỗi người sử dụng riêng lẻ.

Hành vi bất thường được ghi lại nhờ một bản ghi kiểm toán, hoặc dữ liệu thu thập được trong một khoảng thời gian xác định, sẽ tạo ra một bản ghi bất thường. Bản ghi bất thường do một bản ghi kiểm toán riêng lẻ tạo ra sẽ thông báo cho sĩ quan an toàn biết về một kiểu xâm nhập đáng ngờ, bản ghi được tạo ra vào cuối thời gian sẽ tạo ra một báo cáo tổng kết.

Cách tiếp cận IDES dự phòng việc phát triển thông tin thống kê đối với động thái bình thường, sao cho có thể nhận dạng và ghi lại được động thái sai lệch. Bởi thế nó không dựa trên sự giả định các kịch bản tấn công, và việc thu thập dữ liệu thích hợp cho những kịch bản như thế. Tuy nhiên, nó đòi hỏi một sự nhận thức trước nào đó về các kiểu hành vi gắn liền với một sự tấn công, sao cho có thể phát triển các lược tả thích hợp. Nếu có quá nhiều kiểu lược tả hình thành thì sĩ quan an toàn sẽ phải nghe những cảnh báo về hành vi sai lệch chẳng có gì liên quan tới an toàn, còn nếu có quá ít thì các cuộc tấn công có thể tiếp diễn mà không bị thông báo.

Một cách tiếp cận khác đối với vấn đề phát hiện xâm nhập đã được đề xuất và nhấn mạnh nhiều tới sự dự phòng các công cụ phần mềm và các phương tiện cho sĩ quan an toàn. ISOA (trợ giúp sĩ quan an toàn thông tin) cung cấp một môi trường linh hoạt đối với phân tích kiểm toán tự động hóa và giám sát an toàn mạng. Hệ thống này nhấn mạnh việc sử dụng các công cụ cho sĩ quan an toàn kể cả hiển thị các bản ghi kiểm toán, hiển thị đồ họa trạng thái an toàn mạng, các báo động khởi phát bằng biến cố, nén bản ghi kiểm toán, lưu giữ

dữ liệu kiểm toán, thao tác lược tả v.v. *Xem* audit data, expert systems, inference, security log, Trojan Horse, virus.

intrusion detector ***thiết bị phát hiện thâm nhập*** *Xem* area mat, beam break, bistatic microwave sensor, break alarm, buried-line intrusion pad, cord trap, duress alarm, electric field sensor, electrostatic field sensor, foil, Guardwire, infrared motion detector, laser intrusion detector, line sensor, microwave sensor, modulated photoelectric sensor, point protection, radar sensor, ultrasonic motion detector, volumetric sensor, video motion detector.

Invader ***virut Invader*** Trong an toàn máy tính, virut tự mã hóa, kết thúc và lưu trú, lây nhiễm các tệp COM, EXE và OVL, lây nhiễm cung khởi động của đĩa mềm và đĩa cứng, làm sai lạc cung khởi động, các tệp chương trình, OVL và dữ liệu và liên kết tệp, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

invariant ***bất biến*** Trong toán học, tính chất mà vẫn giữ nguyên đúng sau một phép biến đổi nào đó.

inversion ***phép đảo; (sự) đảo*** (1) Trong toán học, quá trình bù trong số học nhị phân, ở đó tất cả các 1 ở một số nhị phân được thay đổi thành các 0 và ngược lại. *Xem* complement. (2) Trong truyền thông, quá trình xáo trộn tiếng nói để giữ bí mật bằng cách phách tín hiệu tiếng nói bằng tần số âm thanh cố định, cao hơn và chỉ dùng các hiệu tần.

inverted file ***tệp đảo*** Trong các cơ sở dữ liệu, cấu trúc tệp tạo điều kiện cho các tìm kiếm thuộc tính bằng cách chuẩn bị các danh sách hoặc danh mục đặc biệt (ví dụ, tệp nhân sự sử dụng số hiệu nhân viên làm khóa chính, nhưng tệp đảo có thể cung cấp danh sách theo thứ tự phòng ban với các số hiệu nhân viên có kèm theo). Như vậy có thể truy nhập tất cả các nhân viên trong một phòng nào đó mà không cần rà soát toàn bộ tệp nhân sự.

investigation ***khảo sát, điều tra nghiên cứu*** Trong an toàn máy tính, xem xét và phân tích các tính năng an toàn hệ thống (ví dụ như khảo sát các chương trình điều khiển hệ thống có sử dụng các lưu đồ, các danh sách lắp ráp và hồ sơ có liên quan) để xác định tính an toàn do hệ điều hành cung cấp. *Xem* operating system.

invitation ***mời gọi*** Trong truyền thông dữ liệu, quá trình trong đó bộ xử lý tiếp xúc với trạm cho phép trạm truyền thông báo có sẵn. *Xem* polling.

INWG *Xem* International Network Working Group.

I/O *Xem* input/output.

ionization smoke sensor ***bộ cảm biến khói ion hóa*** Trong an toàn vật lý, bộ cảm biến khói bao gồm một hoặc nhiều khoang, mỗi khoang chứa những lượng nhỏ chất phóng xạ và hai điện cực mang điện. Vật liệu phóng xạ ion hóa không khí trong khoang và không khí bị ion hóa tạo ra một dòng điện nhỏ qua các điện cực, các hạt khói đi vào khoang tự gắn với các ion, làm giảm độ linh động của chúng và do đó làm giảm dòng điện. Những hệ như thế là tự an toàn (hệ an toàn khi có sự cố),

So sánh với photoelectric beam smoke detector. *Xem* combination smoke detector, fail safe.

IP *Xem* Internet protocol.

IPC *Xem* interprocess communication.

IPL *Xem* initial program load.

IPSE ***IPSE*** Viết tắt của Integrated Project Support Environment (môi trường hỗ trợ dự án kết hợp).

IPSS *Xem* International Packet Switched Service.

IR *Xem* information retrieval.

Iraqi Warrior ***virut Iraqi Warrior*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

IRE ***Viện IRE*** Viết tắt của Institute of Radio Engineers (Viện kỹ thuật vô tuyến Mỹ).

irreversible encryption ***mã hóa không đảo được*** (1) Trong mật mã, phép biến đổi DEA của bản rõ theo cách sao cho không thể giải mã được bản mã ngược trở về bản rõ ban đầu bởi những thủ tục khác với thủ tục vét cạn. *So sánh với* reversible encryption. *Xem* cleartext, exhaustive attack, DEA, PIN management and security. (2) Trong mật mã, phép biến đổi mật mã bản gốc sao cho không có phép giải mã tương ứng. Ví dụ, kỹ thuật này có thể được sử dụng để nhớ các mật khẩu theo một cách an toàn. Mật khẩu mà người sử dụng nhập vào sau này cũng được mã hóa như vậy và kết quả được so sánh với mật khẩu được lưu dưới dạng mã hóa.

isarithmic control ***điều khiển đẳng trị*** Trong truyền thông dữ liệu, điều khiển luồng trong mạng chuyển mạch gói để duy trì tổng số các gói được chuyển dưới một giới hạn nhất định. *Xem* flow control, packet switching.

ISC² *Xem* International Information Systems Security Certification Consortium.

ISDN *Xem* integrated services digital network.

ISN ***ISN*** Trong hoạt động ngân hàng, viết tắt của Input Sequence Number (số hiệu trình tự nhập), số hiệu trình tự kế tiếp cho phép kiểm soát thông báo nhập giữa ngân hàng gửi và dịch vụ. *So sánh với* OSN.

ISO *Xem* International Standards Organization.

ISO-7 ***ISO-7*** Trong mã hóa, mã bảy bit với 128 ký tự, đồng nhất với ASCII, vốn là bảng mã của Mỹ, với ngoại lệ là một số mẫu bit có thể được dùng tùy chọn cho các ký tự quốc gia. *Xem* ASCII, International Alphabet Number 5.

ISO 7498 ***chuẩn ISO 7498*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về liên thông mạng các hệ thống mở (OSI). *Xem* open systems interconnection.

ISO 7810 ***chuẩn ISO 7810*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về các đặc trưng vật lý của các thẻ nhận dạng.

ISO 7811 ***chuẩn ISO 7811*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức

tiêu chuẩn hóa quốc tế về các kỹ thuật ghi các thẻ nhận dạng. *Xem* magnetic stripe card.

ISO 7816 ***chuẩn ISO 7816*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về các thẻ thông minh. *Xem* smart card.

ISO 7982-1 ***chuẩn ISO 7982-1*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, viễn thông ngân hàng - Các thông báo chuyển tiền - Phần 1: Từ vựng và các phần tử dữ liệu.

ISO 8372 ***chuẩn ISO 8372*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, xử lý thông tin - các chế độ hoạt động đối với một thuật toán mật mã khối 64 bit. *Xem* data encryption standard.

ISO 8583 ***chuẩn ISO 8583*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, Các thông báo khởi phát bằng thẻ giao dịch tài chính - Các đặc tả thông báo trao đổi. *Xem* smart card.

ISO 8730 ***chuẩn ISO 8730*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, hoạt động ngân hàng - các yêu cầu xác thực thông báo (bán buôn). *Xem* message authentication.

ISO 8731 ***chuẩn ISO 8731*** Trong tiêu chuẩn hóa, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, hoạt động ngân hàng - các thuật toán đã phê duyệt để xác thực thông báo. *Xem* message authentication algorithm.

ISO 8732 ***chuẩn ISO 8732*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, hoạt động ngân hàng - quản lý khóa (bán buôn). *Xem* ANSI X.17-1985, key management.

ISO 9564 ***chuẩn ISO 9564*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, quản lý và an toàn PIN.

ISO 9735 ***chuẩn ISO 9735*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về EDIFACT. *Xem* EDIFACT.

ISO 9992 ***chuẩn ISO 9992*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về các thẻ giao dịch tài chính - các thông báo giữa thẻ mạch tích hợp và thiết bị nhận thẻ. *Xem* smart card.

ISO 9807 ***chuẩn ISO 9807*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, hoạt động ngân hàng - các yêu cầu về xác thực thông báo (bán lẻ). *Xem* message authentication.

ISO 10126 ***chuẩn ISO 10126*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế, hoạt động ngân hàng - mã hóa các thông báo tài chính bán buôn.

ISO 10202 ***chuẩn ISO 10202*** Trong các tiêu chuẩn, một chuẩn của Tổ chức tiêu chuẩn hóa quốc tế về các thẻ giao dịch tài chính - kiến trúc an toàn của các hệ giao dịch tài chính sử dụng các thẻ mạch tích hợp. *Xem* smart card.

ISOA ***ISOA*** Trong kiểm soát truy nhập, viết tắt của Information Security Officer's Assistant (hệ hỗ trợ sĩ quan an toàn thông tin), tập hợp các công cụ và

phương tiện để trợ giúp sĩ quan an toàn phát hiện những xâm nhập bị nghi ngờ vào hệ hoặc mạng máy tính. *Xem* intrusion detection.

isochronous transmission ***truyền đẳng thời*** Trong truyền thông dữ liệu, quá trình truyền dữ liệu trong đó bất kỳ hai biến cố có ý nghĩa nào cũng luôn luôn tách nhau bởi một số nguyên các khoảng đơn vị. *So sánh với* anisochronous transmission. *Xem* synchronous transmission.

isolated adaptive routing ***định tuyến thích ứng tách ly*** Trong truyền thông dữ liệu, phương pháp chuyển mạch tín hiệu trong đó các quyết định định tuyến chỉ được thực hiện độc lập trên cơ sở thông tin có sẵn ở mỗi nút. *Xem* adaptive routing.

isolation ***cách ly*** (1) Trong an toàn máy tính, kiềm chế những người sử dụng và tài nguyên trong một hệ xử lý dữ liệu tự động theo cách để những người sử dụng và các xử lý được cách ly với những người sử dụng và quá trình khác, cũng như với các điều khiển bảo vệ của hệ điều hành. *Xem* ADP, compartmentalization, isolation enforcement, operating system. (2) Trong truyền thông, các phương pháp được dùng để ngăn ngừa để không đưa các điện áp cao vào các mạng truyền thông công cộng. *Xem* common carrier.

isolation enforcement ***thi hành cách ly, (sự) tuân thủ cách ly*** Trong an toàn dữ liệu, kỹ thuật để đảm bảo cho thông tin an toàn được phân hoạch thành các tập hợp rời nhau sao cho nó không thể được truyền từ ứng dụng an toàn này tới ứng dụng an toàn khác mà không có đặc quyền truy nhập cần thiết. Cách ly có thể đạt được bằng ngăn cách vật lý, thời gian, logic hoặc mật mã. Sự cách ly vật lý ngụ ý là thông tin không thể chạy giữa các hệ tách biệt về mặt vật lý; sự truyền bức xạ không mong muốn được ngăn ngừa bởi những biện pháp thích hợp. Nếu các đường truyền thông nối thông các thiết bị vật lý cách ly thì các luồng thông tin bị hạn chế ở vài kênh xác định có thể giám sát được. Sự tách tạm thời ngụ ý rằng, thông tin được xử lý trong một hệ nào đó ở một thời điểm cụ thể và sau đó được thanh lọc trước khi hệ thống được gán cho một vùng an toàn khác. Sự cách ly logic đạt được bằng những thuật toán tin cậy được cài đặt bằng một tổ hợp phần cứng và phần mềm. Sự cách ly mật mã sử dụng những khóa mật mã khác nhau để mã hóa dữ liệu gán cho những vùng an toàn khác nhau. *Xem* cryptography, periods processing, Tempest proofing, temporal separation.

ISO OSI *Xem* open systems interconnection.

ISRD ***tài liệu ISRD*** Viết tắt của Information System Requirements Document (tài liệu các yêu cầu hệ thông tin).

ISSA ***ISSA*** Viết tắt của Information Systems Security Agency (cơ quan an toàn hệ thông tin).

ISSO ***ISSO*** Viết tắt của Information Systems Security Officer (sĩ quan an toàn hệ thông tin). *Xem* information systems security.

issuer ***hội sở phát hành*** Trong hoạt động ngân hàng, hội sở trong một mạng

trao đổi giao dịch vốn phát hành và kiểm chứng thông tin nhận dạng và xác thực về một khách hàng. *Xem* authentication, customer, interchange.

IT *Xem* information technology.

ITAR ***ITAR*** Viết tắt của U.S. International Traffic in Arms Regulations (các quy định buôn bán vũ khí quốc tế của Hoa Kỳ). Các quy định đó bao gồm thiết bị mật mã trong mục thiết bị quân sự phụ trợ và do đó việc kiểm soát xuất khẩu thiết bị như thế khỏi Hoa Kỳ.

ItaVir ***virut ItaVir*** Trong an toàn máy tính, virut lây nhiễm các tệp EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL, liên kết tệp và cung khởi động. *Xem* virus names.

item ***mục, khoản*** Trong tin học, nhóm các ký tự có liên quan được xử lý như một đơn vị (ví dụ, bản ghi có thể gồm một số mục mà những mục đó lại có thể gồm một số mục khác). *Xem* record.

Items of Intrinsic Military Utility ***(các) hạng mục tiện ích quân sự bên trong*** Các hạng mục đầu cuối khác với các hạng mục nhận dạng trong Danh mục công nghệ quân sự tới hạn của Bộ quốc phòng Hoa Kỳ mà việc chuyển giao cho các đối thủ tiềm tàng sẽ bị kiểm soát vì những lý do sau đây: (*a*) Sản phẩm đầu cuối đang xét có thể làm tăng cường đáng kể khả năng quân sự hoặc tiến hành chiến tranh hoặc do hàm lượng công nghệ của nó hoặc số lượng cần bán; hoặc (*b*) Sản phẩm có thể được phân tích để phát hiện các đặc trưng hệ thống của Hoa Kỳ và do đó góp phần phát triển các biện pháp chống trả đối với thiết bị tương đương của Hoa Kỳ. *Xem* military critical technology.

iteration ***lặp*** Trong lập trình, quá trình lặp lại cùng một loạt các bước xử lý cho tới khi đạt được trạng thái hoặc điều kiện rẽ nhánh xác định trước. *So sánh với* recursive routine. *Xem* loop.

ITSEC *Xem* information technology security evaluation criteria.

ITSEF *Xem* information technology security evaluation facility.

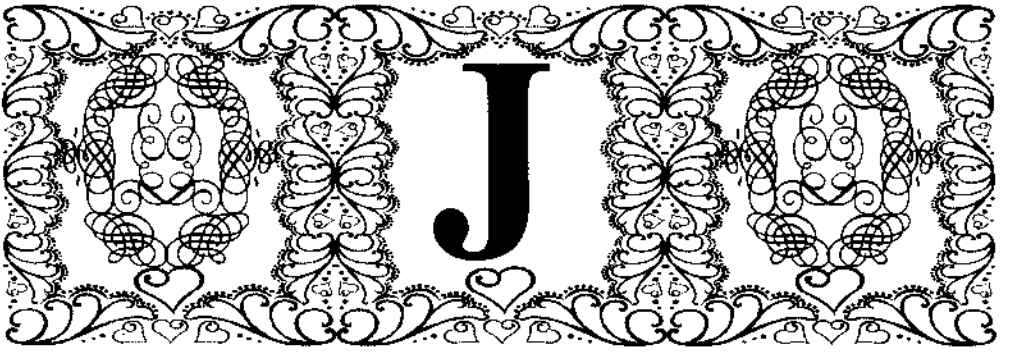
ITSEM *Xem* information technology security evaluation manual.

ITU *Xem* International Telecommunications Union.

IV *Xem* initialization vector.

IVP *Xem* integrity validation procedure.

IV&V *Xem* Independent Verification and Validation.



jamming ***gây nhiễu, phá rối*** Trong an toàn truyền thông, dạng nhiễu bức xạ có suy tính nhằm vào các buổi truyền vô tuyến, vi ba hoặc vệ tinh. Việc sử dụng các máy phát năng lượng cao buộc máy gây nhiễu phải sử dụng các hệ truyền phát mạnh hơn và do đó đắt hơn. Sự truyền dải thông phổ rộng được phân phối trên một dải tần số, do đó cũng làm tăng vấn đề của máy làm nhiễu, trong khi đó kỹ thuật linh động tần làm thay đổi tần số phát ngẫu nhiên trên phổ trong khi truyền phát. *Xem* EMI/RF radiation, frequency agility.

Jeff ***virut Jeff*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu, tạo khuôn và ghi đè tất cả hoặc một phần đĩa. *Xem* virus names.

Jerusalem ***virut Jerusalem*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

job transfer and manipulation ***chuyển và xử lý công việc*** Trong truyền thông dữ liệu, giao thức được dùng để chuyển các công việc (job) xử lý theo lô cho các máy tính chính trên một mạng. *Xem* protocol.

join ***toán tử nối, toán tử hợp*** Trong các cơ sở dữ liệu, toán tử hợp trong đại số quan hệ. Phép hợp ở hai quan hệ chia sẻ một kiểu mục dữ liệu chung, tạo ra quan hệ tổ hợp với các thuộc tính xác định trong phép hợp. *Xem* relational algebra, relational database.

JoJo ***virut JoJo*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Joker ***virut Joker*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây

nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

Joshi ***virut Joshi*** Trong an toàn máy tính, virut lấy lén kết húc và lưu trú, lây nhiễm cung khởi động của đĩa mềm và đĩa cứng và bảng phân đĩa, làm sai lạc các tệp cung khởi động và dữ liệu, ảnh hưởng tới hoạt động thời gian chạy. *Xem* virus names.

journal ***nhật ký*** (1) Trong các hoạt động, bản ghi theo trật tự thời gian các thay đổi đối với một tập hợp dữ liệu, thường dùng để khôi phục lại phương án trước đó của tập hợp dữ liệu trong trường hợp có sai lạc. *Xem* corruption. (2) Trong an toàn cơ sở dữ liệu, vết kiểm toán của các hoạt động cơ sở dữ liệu. *Xem* audit trail.

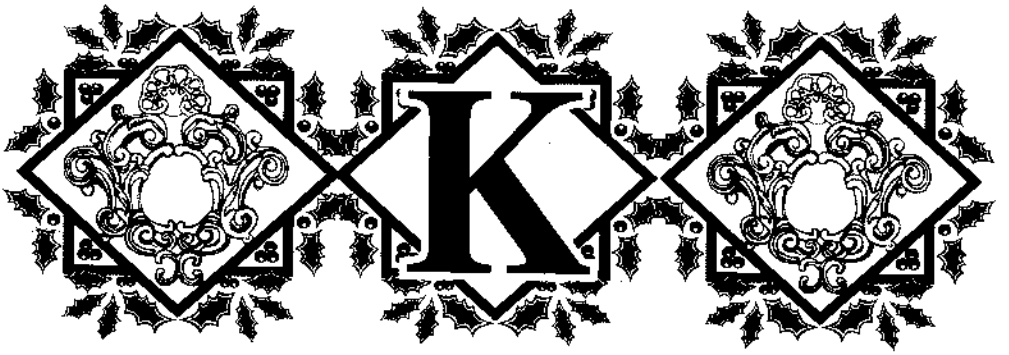
JTM *Xem* job transfer and manipulation.

July 13th ***virut 13 tháng 7*** Trong an toàn máy tính, virut tự mã hóa, lây nhiễm các tệp EXE, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình, OVL và dữ liệu và liên kết tệp. *Xem* virus names.

jump out ***bỏ qua*** Trong an toàn vật lý, bỏ qua toàn bộ hay một phần hệ thống báo động.

June 16th ***virut 16 tháng Sáu*** Trong an toàn máy tính, virut lây nhiễm các tệp COMMAND.COM và COM, tạo khuôn hoặc ghi đè toàn bộ hoặc một phần đĩa, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

Justice ***virut Justice*** Trong an toàn máy tính, virut kết thúc và lưu trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.



KDC *Xem* key distribution center.

KEEPROM ***EPROM an toàn*** Trong an toàn máy tính, loại bộ nhớ EPROM chỉ đọc được nội dung khi đưa trước vào nó một giá trị dữ liệu đặc biệt. *Xem* EEPROM.

Kennedy ***virut Kennedy*** Trong an toàn máy máy tính, loại virut chấm dứt và thường trú, lây nhiễm tới các tệp đuôi COM, ảnh hưởng tới các thao tác trong thời gian thực hiện, làm ngắt các chương trình và các tệp OVL. *Xem* virus names.

Keberos ***dịch vụ Keberos*** Trong xác thực, dịch vụ xác thực được thiết kế cho các hệ thống mạng mở. Ban đầu nó được phát triển cho dự án Athena của MIT.

Dịch vụ này cho phép người dùng truy nhập an toàn tới các máy chủ trong mạng khách/chủ. Khách - có thể là người sử dụng hoặc quá trình bằng trình giấy ủy nhiệm tới máy chủ để chứng minh danh tính của mình. Hệ thống dùng phép mã khóa riêng và giấy ủy nhiệm chứa các nhãn (thẻ) hoặc dấu xác thực. Nhãn chứa tên của khách, tên của máy chủ, địa chỉ mạng của khách, tem thời gian, thời hạn hợp lệ của nhãn và khóa phiên. Nhãn được mã bằng khóa mật mà chỉ máy chủ và dịch vụ Keberos biết. Khóa phiên do khách tạo ra trong nhãn (dùng cho phiên liên lạc giữa máy chủ và khách) được khách chuyển tới máy chủ.

Một dấu xác thực đi kèm theo một nhãn và cho bằng chứng về yêu cầu do khách tạo ra. Dấu xác thực chứa tên khách, địa chỉ mạng và tem thời gian, nó được mã bằng khóa phiên ghi trên nhãn.

Đầu tiên, người sử dụng đăng nhập vào trạm làm việc và một yêu cầu được gửi tới chương trình xác thực Keberos để dùng cùng với dịch vụ cấp nhãn. Chương trình dịch vụ xác thực sẽ kiểm

tra những điều người sử dụng đã biết, tạo ra một khóa phiên ngẫu nhiên và triển khai nhãn với nội dung chứa khóa phiên, tên khách, tên của dịch vụ cấp nhãn, thời gian hiện thời, thời hạn tồn tại của nó và địa chỉ mạng của khách. Sau đó nhãn này được mã bằng khóa riêng mà chỉ có chương trình dịch vụ xác thực và chương trình cấp nhãn biết. Thông báo bao gồm nhãn và khóa phiên đã mã bằng khóa riêng của khách mà chỉ khách và chương trình xác thực biết. Như vậy, thông báo do chương trình dịch vụ xác thực gửi tới khách có dạng:

$$eK_c(K_{c,tgs},\ eK_{tgs}(T_{c,tgs}))$$

K_c: khóa riêng của khách.

K_{tgs}: khóa riêng của chương trình cấp nhãn.

$K_{c,tgs}$: khóa phiên dùng trong phiên liên lạc giữa khách và dịch vụ cấp nhãn.

$T_{c,tgs}$: nhãn được trình lên dịch vụ cấp nhãn, nó chứa tên khách, tên dịch vụ cấp nhãn, địa chỉ mạng khách, tem thời gian, thời hạn tồn tại hợp lệ của nhãn và khóa phiên $K_{c,tgs}$.

Khi trạm làm việc nhận được nhãn đã mã từ chương trình (dịch vụ) xác thực, nó yêu cầu mật khẩu của người sử dụng; khóa riêng của khách K_c được tính từ mật khẩu và được dùng để giải mã câu trả lời $eK_c(K_{c,tgs},\ eK_{tgs}(T_{c,tgs}))$ từ chương trình xác thực. Mật khẩu của người sử dụng và khóa riêng sau đó bị xóa khỏi bộ nhớ của trạm làm việc. Khóa phiên và nhãn nhận từ trạm làm việc sau đó dùng để xác thực người sử dụng.

Khi người sử dụng yêu cầu truy nhập vào máy chủ, máy khách sẽ gửi một thông báo chứa ba thành phần cho dịch vụ cấp nhãn:

$s,\ eK_{tgs}(T_{c,tgs}),\ eK_{c,tgs}(A_c)$

Dấu xác thực A_c chứa tên khách, địa chỉ và tem thời gian. Vì nó được mã bằng khóa phiên của nhãn nên dịch vụ cấp nhãn bị thuyết phục rằng nó xuất phát từ máy khách vào thời điểm chỉ ra trên tem thời gian.

Dịch vụ cấp nhãn lúc này tạo ra một nhãn cho máy khách dùng để nó nhận được các dịch vụ từ máy chủ. Quá trình đồng nhất với quá trình mô tả ở trên trong trường hợp dấu xác thực thừa nhận một nhãn cho dịch vụ cấp nhãn. Nhãn chứa một khóa phiên, dùng liên lạc giữa máy chủ và khách (khóa này được mã bằng khóa mật chỉ máy chủ và dịch vụ cấp nhãn biết) và một thông báo chứa nhãn đã mã và khóa phiên khách/chủ (khóa này được mã bằng khóa phiên dùng chung của khách và dịch vụ cấp nhãn).

Khách có thể yêu cầu xác thực lẫn nhau với máy chủ. Trong trường hợp này, máy chủ trích tem thời gian từ thông báo của máy khách, tăng nó lên 1, mã nó bằng khóa phiên và trả kết quả cho khách hàng. *Xem* authenticator, server, session key, ticket.

kernel ***nhân*** (1) Trong an toàn máy tính, *xem* security kernel. (2) Trong các hệ điều hành, mức thấp nhất của một hệ điều hành chứa những đoạn chương trình được thử nghiệm chặt chẽ để cấp phát các tài nguyên cứng cho hệ điều hành xử lý và các chương trình chạy dưới hệ điều hành. *Xem* nucleus.

kernelized ***(được) nhân hóa*** Trong

an toàn máy tính, chỉ một hệ điều hành được thiết kế để phân hoạch các lớp người sử dụng để họ chỉ có thể truy nhập tới những phương tiện mà họ được quyền. Những hệ thống như vậy cho ấn tượng rằng, có sẵn các máy tính khác nhau cho những người dùng thuộc các nhân khác nhau. *Xem* security kernel.

key ***khóa*** (1) Trong mật mã, một dãy các ký hiệu điều khiển các thao tác mã và giải mã. *Đồng nghĩa với* cryptographic key. (2) Trong mật mã, một ký hiệu hay dãy các ký hiệu (điện tử hay cơ học) dùng điều khiển các phép mã và giải mã. *Xem* encrypt, decrypt. (3) Trong các cơ sở dữ liệu, một hay nhiều ký tự được dùng để nhận diện một tập dữ liệu. *Xem* primary key, secondary key.

key agreement ***thỏa thuận khóa*** Trong quản lý khóa, một phương pháp cho phép hai nhóm không cần thỏa thuận trước với nhau vẫn có thể trao đổi các thông báo dựa trên một khóa mật chỉ có họ biết. *Xem* Diffie-Hellman technique.

key certification center ***trung tâm cấp chứng chỉ khóa, trung tâm chứng nhận khóa*** Trong quản lý khoá, một phương tiện do người được ủy quyền xác nhận điều khiển nhằm tạo và hoàn trả các thông báo chứng nhận. *Xem* certificate, certification authority, digital signature.

key check value ***giá trị kiểm tra khóa*** *Đồng nghĩa với* key verification code.

key ciphertext avalanche ***thác khóa bản mã*** Trong mật mã, một thuộc tính của một mã pháp trong đó, với một bộ bản rõ - mã cho trước, mỗi sự thay đổi một bit trong khóa sẽ tạo nên sự thay đổi toàn bộ bản mã. *So sánh với* ciphertext, plaintext, plaintext ciphertext avalanche, cryptographic key.

key collision ***chạm khóa*** Trong mật mã, một hiện tượng xảy ra trong thuật toán DES. Đó là những trường hợp mà với hai khóa khác nhau, phép mã hóa một khối dữ liệu chỉ ra sẽ cho ra cùng bản mã. *Xem* ciphertext, cryptographic key, data encryption standard.

key component ***thành phần khóa*** Trong mật mã, một trong ít nhất là hai tham số có định dạng của khóa mã được cộng theo phép hoặc - loại trừ với một hoặc nhiều hơn các tham số để tạo nên một khóa mã. *So sánh với* threshold. *Xem* cryptographic key, EXCLUSIVE OR.

key crunching ***tốc hoạt khóa*** Trong quản lý khóa, một kỹ thuật để chuyển một dòng ký tự dễ nhớ thành một khóa DES. Một khóa DES chứa 64 bit, trong đó 8 bit là bit chẵn lẻ và như vậy, người dùng chỉ có sự lựa chọn tự do trong 56 bit, tức 7 byte. Việc dùng 7 byte các dòng ký tự gồm các ký tự chữ - số dễ nhớ sẽ hạn chế chặt chẽ số khóa có thể. Nếu sử dụng tốc hoạt khóa, người dùng nhập một dòng ký tự dễ nhớ về cơ bản dài hơn 7 ký tự. Dòng ký tự này được mã ở chế độ xích khối mã và trả về 56 bit nằm bên phải của khối cuối cùng như khóa yêu cầu. *Xem* cipher block chaining, cryptographic key, DES, long key, native key, parity bit.

key distribution and control ***kiểm soát và phân phối khóa*** Trong quản lý khóa, các quá trình trong kiểm soát và phân phối khóa bao gồm:

- chỉ định người mã hóa;
- các trách nhiệm của người mã hóa;
- gửi và nhận tài liệu về khóa;
- cất giữ tài liệu khóa và thiết bị mã/xác thực, các khóa vật lý;
- sử dụng tài liệu khóa;
- hủy tài liệu về khóa;
- lưu trữ khóa.

Cá nhân chịu trách nhiệm đối với quản lý khóa do người quản lý cấp cao hơn quy định. Không cá nhân nào được kiểm soát hoàn toàn tài liệu mã và khóa mã và ít nhất hai người trông coi khóa luôn sẵn sàng hoạt động mọi lúc để thực hiện những thay đổi khóa theo hoặc không theo kế hoạch. Những người giữ khóa có thể được nhân viên phụ tá hỗ trợ cho những nhiệm vụ đặc biệt, chẳng hạn nhập khóa.

Các trách nhiệm của những người giữ khóa gồm tiếp nhận, kiểm tra, cất giữ, ghi chép lại, nhập vào, thay đổi và hủy tài liệu khóa, và những thao tác nhạy cảm như vậy sẽ được thực hiện dưới sự kiểm soát kép. Việc gửi và nhận tài liệu khóa cũng có thể thực hiện dưới sự kiểm soát kép nhờ dùng thư có bảo đảm (có đăng ký) hoặc tốt hơn là qua một người đưa thư. Sự phát triển các thủ tục nhằm giải quyết việc kiểm tra các gói, sự trao đổi các tài liệu, kiểm tra tủ sắt, ký nhận tài liệu khóa không bị giả mạo hay hư hại ... là phần cơ bản, còn việc bao gói sẽ tạo thuận lợi cho các kiểm tra sơ bộ trước khi mở gói.

Tài liệu khóa sẽ được cất giữ trong thùng chứa an toàn đặt ở môi trường an toàn và giám sát được. Việc tiếp cận tới tài liệu như vậy sẽ cần phải có hai người trông coi, chẳng hạn các khóa kép trên các hòm an toàn và mỗi người giữ một khóa. Tất cả những truy nhập như vậy sẽ được ghi vào sổ theo dõi. Các khóa dự phòng cho thùng an toàn cũng được đặt ở nơi bí mật và việc truy nhập tới những khóa đó cần có mặt cả hai người trông coi. Nếu các khóa mã vật lý được lưu cất bằng phương tiện điện tử thì nơi lưu trữ phải được bảo vệ chống các tác động của việc ngừng chạy do tắt nguồn trong thời gian ngắn.

Không hủy tài liệu khóa trước khi có những chỉ dẫn rõ ràng. Luân phiên nhau, những người trông coi sẽ làm chứng về việc hủy những tài liệu như vậy mà không cần xem nội dung. Tất cả các tài liệu về khóa phải được hủy sao cho không thể khôi phục lại được. Tất cả việc hủy tài liệu khóa cần phải được ghi chép lại một cách chi tiết để chỉ ra được tài liệu, ngày tháng/thời gian, người trông coi... của quá trình hủy tài liệu. Những bản ghi này phải được giữ trong môi trường an toàn.

Những yêu cầu về cất trữ các khóa lưu trữ phụ thuộc vào thời hạn an toàn của tài liệu về khóa. Nếu về cơ bản, nó có mức an toàn như khóa hiện tại thì cần dùng những thủ tục trên để lưu khóa, hoặc các khóa đã lưu trữ phải được mã hóa. Trong trường hợp sau, khóa mã khóa phải là đối tượng cho các thủ tục an toàn nêu trên. Nếu tính bí mật của các khóa đã lưu không phải là nhân tố

chủ yếu thì những khóa đó sẽ được cung cấp cùng mức bảo vệ lưu cất như các bản ghi quan trọng của tổ chức. *Xem* cryptographic key, dual control, key-encrypting key, keying material, security life.

key distribution center ***trung tâm phân phối khóa*** Trong quản lý khóa, một trung tâm được thiết lập nhằm cung cấp các khóa mã cho hai nhóm khi họ:

- muốn liên lạc an toàn với nhau nhưng không dùng chung các khóa hiện tại;
- từng bên dùng chung một khóa mã khóa hay một cặp khóa với trung tâm;
- không có khả năng tạo khóa.

Nhóm muốn khởi đầu một thông báo mã yêu cầu trung tâm cung cấp các khóa dữ liệu và đưa danh tính người nhận. Trung tâm sẽ tìm hoặc tạo hai tập khóa dữ liệu, mã hóa và chuyển chúng cho nhóm khởi đầu. Một trong hai tập khóa được mã bằng khóa mã khóa hiện thời để chuyển khóa giữa người khởi đầu và trung tâm, còn tập khóa dữ liệu thứ hai cùng với thông tin định danh (để chống lạm dụng khóa) sẽ được mã tương tự như vậy bằng khóa mã khóa dành cho liên lạc giữa trung tâm với người nhận sau cùng. Người khởi đầu sau đó sẽ gửi tập các khóa thứ hai cùng thông tin định danh tới người họ muốn liên lạc. *So sánh với* key translation center, point to point. *Xem* ANSI X9.17-1985, cryptographic key, data key, key-encrypting key, key-encrypting key pair.

key-encrypting key ***khóa mã khóa*** (1) Trong quản lý khóa, một khóa mã được dùng để mã hóa (và giải mã) các khóa mã dữ liệu hoặc các khóa mã khóa khác. (2) Trong quản lý khóa, một khóa được dành riêng để mã hoặc giải mã các khóa. *So sánh với* data key. *Xem* key-encrypting key pair. *Đồng nghĩa với* secondary key.

key-encrypting key pair ***cặp khóa mã khóa*** Trong quản lý khoá, hai khóa mã dùng cùng nhau để mã các khóa khác. *Xem* ANSI X9.17-1985, key-encrypting key, multiple DES encipherment.

key equivocation ***độ bất định khóa*** Trong lý thuyết thông tin, độ bất định của khóa đối với việc nhận một bản mã cho trước được cho bởi:

$$H_C(K) = -\sum P(C) \sum P_C(K) \log_2(P_C(K))$$

trong đó $P(C)$ = xác suất nhận được bản mã C,

$P_C(K)$ = xác suất để khóa K được dùng với điều kiện nhận được bản mã C.

Nếu độ bất định khóa bằng 0 thì không có sự không chắc chắn nào về khóa nào được dùng. Độ bất định khóa thường giảm khi độ dài thông báo tăng lên. *Xem* cryptographic key, equivocation.

key exhaustion ***vét cạn khóa*** Trong mã thám, một kỹ thuật tấn công toàn diện trong đó kẻ tấn công có một đoạn bản rõ, đoạn bản mã tương ứng và có kiến thức về thuật toán mã. Anh ta chọn một khóa để thử, đoạn bản rõ được mã bằng khóa thử này và kết quả được so sánh với đoạn bản mã đã biết. Một cách khác, nếu chỉ có bản mã được biết thì nó sẽ được giải mã bằng khóa thử, bản rõ nhận được sẽ được xem xem liệu nó có ứng với một thông báo

có nghĩa nào không. *So sánh với* message form, exhaustion. *Xem* cryptographic key, exhaustive attack, known plaintext.

key generation ***(sự) tạo khóa*** Trong mật mã, sự tạo thành một khóa hoặc một tập các khóa khác nhau. *Xem* key generator, key management.

key generator ***bộ tạo khóa, thiết bị tạo khóa, chương trình tạo khóa*** Trong mật mã, một thiết bị gồm cả các bộ phận báo động và tự kiểm tra để tạo ra các khóa mã (và nơi nào cần thì cả các vectơ khởi tạo IV). *Xem* cryptographic key, IV, key generation, key management, key stream generator.

key gun ***súng gài khóa, thiết bị ghi khóa, nòng phun khóa*** Trong quản lý khoá, một thiết bị chuyển tải các khóa mã được lưu ở dạng điện tử. Một súng gài khóa điển hình có kích thước một máy tính bỏ túi và nó có các đầu nối để nhận các khóa từ nguồn và để phân phối chúng tới thiết bị đích, chẳng hạn thiết bị đầu cuối. Có thể dùng ghép nối quang hay điện để nối kết thiết bị.

Súng gài khóa phải có các cơ chế để ngăn chặn:

- kẻ tấn công nạp khóa;
- kẻ tấn công đọc được khóa đã nạp;
- nạp được các khóa vào thiết bị đầu cuối của kẻ tấn công.

Các mật khẩu của súng gài khóa có thể bảo đảm chỉ những thiết bị đích và bộ tạo khóa hợp pháp mới giao tiếp được với súng; việc hủy các khóa đã ghi dựa vào dữ liệu đọc ra và các modun chống can thiệp vào súng có thể ngăn chặn hiệu quả kẻ tấn công lấy được khóa. *Đồng nghĩa với* key loader, key transport module.

key hashing ***băm khóa*** *Xem* key crunching.

keying identifier ***ký hiệu nhận dạng khóa, chương trình nhận dạng khóa*** *Đồng nghĩa với* IDA.

keying material ***dữ liệu tạo khóa, tài liệu tạo khóa*** Trong quản lý khoá, dữ liệu (chẳng hạn khóa và các vectơ khởi tạo) cần thiết để thiết lập và duy trì các mối quan hệ tạo khóa mã. *Xem* cryptographic key, IV, key distribution and control, keying relationship.

keying relationship ***quan hệ lập khóa*** Trong quản lý khóa, trạng thái tồn tại giữa cặp đối tượng liên lạc trong thời gian họ chia sẻ ít nhất một khóa dữ liệu hoặc khóa mã khóa. *Xem* communicating pair, cryptographic key, data key, key-encrypting key.

keyless cryptography ***mật mã không khóa*** Trong quản lý khóa, một phương pháp liên lạc các khóa mã có sự trao đổi các thông báo giữa các nhóm liên lạc để thiết lập nên các khóa mã. Các thông báo này không mật song người khởi đầu lại được giữ bí mật. Những người khởi đầu sẽ chọn tên cho khóa (gọi là K) và sau đó tạo độc lập một số nhị phân $2n$ bit. Như vậy, Alice A sẽ tạo ra số $A(1), A(2), A(3),... A(2n)$, còn Bob tạo ra một số $B(1), B(2), B(3),... B(2n)$.

Tiếp theo Alice đưa ra $2n$ thông báo có dạng:

Thông báo K: bit thứ i của tôi là $A(i)$

Tương tự như vậy đối với Bob.

Các thông báo được trao đổi sao cho kẻ

nghe trộm thụ động không thể xác định được người khởi đầu mặc dù có thể đọc được các thông báo. Ví dụ, mỗi nhóm có thể dùng một kênh an toàn để liên lạc với trung tâm, sau đó hiển thị những thông báo trong khi không để lộ thông tin gì về những người khởi đầu của mỗi bên.

Trong khi đọc cặp thông báo:

Thông báo *K*: bit 5 của tôi là 1

Thông báo *K*: bit 5 của tôi = 0, Bob biết rằng bit 5 do anh ta tạo ra là 1 và như vậy, Alice đã truyền một bit 0 vào bit thứ 5. Tuy nhiên, những người nhận thông báo bất hợp pháp sẽ không biết gì về bit thứ 5 do Alice chuyển cho Bob. Song nếu các bit có giá trị bằng nhau thì kẻ tấn công sẽ biết chính xác giá trị bit. Khi Alice và Bob đọc các thông báo và tìm thấy các bit trùng nhau thì cả hai sẽ khử các bit đó khỏi khoá, tạo ra một khóa mới ngắn hơn. Ví dụ:

Alice gửi lúc đầu: 01110110001

Bob gửi lúc đầu: 10111000010

Khóa mới của Alice: 0101101

Khóa mới của Bob: 1010010

Nếu cần, quá trình được lặp lại để tạo ra một khóa dài hơn. Theo quy ước, khóa được truyền đi là khóa do Alice tạo ra cuối cùng, nghĩa là phần bù của khóa mà Bob tạo ra cuối cùng. *Xem* cryptographic key.

key library ***thư viện khóa*** Trong mật mã, một tập hợp các khóa mã được lưu cất để một nhóm hay một cá nhân sử dụng. Việc truy nhập tới thư viện được kiểm soát bởi một khóa mật, riêng biệt. *Xem* cryptographic key.

key list ***danh sách khóa*** Trong mật mã, một tài liệu chứa các khóa mật mã dùng cho các hệ thống mã trong thời gian mã chỉ ra. *Xem* cryptographic key, cryptoperiod, cryptosystem.

key loader ***thiết bị nạp khóa, chương trình nạp khóa*** Trong quản lý khóa, một đơn vị điện tử độc lập, có khả năng lưu trữ ít nhất một khóa và chuyển khóa đó tới thiết bị mã theo yêu cầu. *Xem* cryptographic key, cryptographic equipment. *Đồng nghĩa với* key gun, key transport module.

key management ***(sự) quản lý khóa*** (1) Trong mật mã, các hoạt động bao gồm tạo, lưu cất, phân phối, xóa bỏ, lưu giữ và sử dụng các khóa theo một chính sách an toàn. *Xem* key. (2) Trong mật mã, những quá trình liên quan tới việc tạo, phân phối, cất trữ và hủy các khóa mã và các thông tin liên quan, chẳng hạn các vectơ ban đầu.

Phép mã hóa quy một cách hiệu quả bài toán bảo đảm tính bí mật của một lượng lớn dữ liệu thành bài toán bảo vệ tính bí mật của khóa mã. Những vấn đề kèm theo những khía cạnh khác nhau của quản lý khóa phụ thuộc vào phạm vi của các kỹ thuật mật mã, của môi trường và những ứng dụng dùng khóa mã.

Tạo khóa mã

Sự tạo khóa mã phải được thực hiện sao cho nó bảo đảm rằng:

- kết quả của quá trình tạo không thể dự đoán được;
- dải các khóa có thể tạo ra bằng với dải đầy đủ các khóa hợp lệ;
- không làm lệch về cơ bản phân bố

xác suất của các khóa được tạo ra;

- kẻ tấn công không thể tác động tới quá trình tạo khóa;
- kẻ tấn công không thể thay đổi đầu ra của bộ tạo khóa;
- kẻ tấn công không thể theo dõi được tín hiệu ra của bộ tạo khóa.

Nếu dự đoán được tín hiệu ra từ bộ tạo khóa ở mức độ nào đấy thì kẻ tấn công có thể tạo ra một cách độc lập cùng khóa đó, hay tập các khóa chứa khóa đã sinh ra. Nếu phạm vi dãy khóa ra là tập con thuộc phạm vi hợp lệ của khóa, hoặc nếu xác suất để tập con nhất định các khóa sẽ tạo ra tăng lên, thì độ bền của quá trình tạo khóa sẽ nhỏ hơn độ bền của hệ thống mã.

Phân phối khóa - tổng quan

Phân phối khóa là một trong những vấn đề phức tạp nhất trong các hệ thống mật mã hiện đại. Nếu cần phân phối một số lượng khóa hạn chế một cách thủ công thì phải đòi hỏi những thủ tục quản lý hết sức chặt chẽ để duy trì tính an toàn của tư liệu khóa. Tuy nhiên, trong nhiều trường hợp, số khóa dùng trong hệ thống, tần suất thay đổi khóa, tập hợp người dùng đông đảo và đa dạng đã đòi hỏi sử dụng một loạt các kỹ thuật phân phối khóa tự động. Mật mã đối xứng, chẳng hạn như DES đòi hỏi cả hai bên giải mã dùng cùng một khóa và như vậy, khóa mã phải được trao đổi bí mật nhóm liên lạc.

Các hệ thống mã khóa công khai đặt các điều kiện về bảo đảm bí mật trong quản lý khóa nhẹ nhàng hơn nhiều vì khóa mã được tự do công khai hóa, song mặt khác nó đòi hỏi bảo đảm tính xác thực của các khóa công khai.

Quản lý khóa trong các hệ cơ sở dữ liệu cần được giải quyết bằng việc phân phối các khóa dùng cho việc mã các bản ghi cho những người sử dụng. Ví dụ, những người dùng như vậy có thể được cấp một thẻ chất dẻo có khóa được lưu ở dạng từ tính; việc dùng thẻ đòi hỏi đưa mật khẩu vào thiết bị đầu cuối để tối thiểu hóa ảnh hưởng của việc mất thẻ. Tuy nhiên, phương pháp này chắc chắn làm tăng mối nguy hiểm làm mất tính tin cậy của cơ sở dữ liệu nảy sinh do khả năng làm tổn thương các người sử dụng. Một biện pháp tốt hơn là lưu các khóa vào một hệ cơ sở dữ liệu và dựa vào các kiểm soát truy nhập để đảm bảo chỉ những người sử dụng có đặc quyền mới được truy nhập tới các khóa và từ đó tới các bản ghi đã giải mã.

Một kỹ thuật nữa là lưu cất khóa của tệp cơ sở dữ liệu, khóa này đã mã bằng khóa riêng của cá nhân người dùng, cùng với dữ liệu đã mã. Khi người dùng yêu cầu truy nhập tới hệ thống, chương trình quản lý khóa sẽ phân phối khóa riêng của người sử dụng và truy nhập tới bản ghi chứa khóa tệp đã mã bằng khóa của người dùng; khóa tệp được tạo ra bằng cách giải mã bằng khóa của người dùng, còn các bản ghi của cơ sở dữ liệu sau đó được giải mã để cho văn bản rõ.

Tuy nhiên, việc truy nhập tới cơ sở dữ liệu mà không cần biết khóa người dùng có thể cho phép kẻ tấn công thay đổi bản mã. Điều này có thể chỉ đơn thuần là thay thế ác ý dữ liệu bằng bản mã ngẫu nhiên (được giải mã thành văn bản không hiểu được), hoặc trong

trường hợp biết cặp bản mã/bản rõ, kẻ tấn công có thể thay thế một bản ghi chứa bản mã tương ứng với bản rõ đã biết bằng một bản ghi khác. Những kiểu này có thể chấm dứt được bằng việc dùng một bản ghi phê chuẩn hợp lệ chứa khóa tệp, hoạt động trên cơ sở hàm một chiều và được lưu trong cơ sở dữ tương ứng. Khóa tệp - được tạo ra bởi phép giải mã bằng khóa của người dùng - chịu tác dụng của cùng hàm một chiều như vậy và được so sánh với bản ghi phê chuẩn hợp lệ trước khi cho phép sự cập nhật bất kỳ vào cơ sở dữ liệu. Đối với phép mã tệp, nếu dùng hệ thống hai khóa thì những người dùng có thể được bảo đảm các quyền ghi, hoặc đọc và ghi.

Thông thường, quản lý khóa đối với liên lạc giữa máy chủ - thiết bị đầu cuối sẽ dùng các khóa phiên để mã các thông báo trong chuyển tiếp. Với những thông báo được chuyển đi trong một phiên người dùng riêng lẻ, những khóa phiên này có thời gian tồn tại bị hạn chế. Những khóa phiên như vậy do máy chủ tạo ra theo yêu cầu từ phía người dùng, vừa được cất trong máy chủ vừa được truyền đi, được mã hóa bằng khóa mã khóa (gọi là khóa thiết bị đầu cuối), tới thiết bị đầu cuối. Một nguyên tắc đối với những hệ thống như vậy là khóa phiên không bao giờ được lộ ở dạng rõ bên ngoài các modun chống thay đổi của hệ thống. Như vậy, khóa mã khóa được gọi là khóa lưu cất tại máy chủ, trong khi đó, mỗi thiết bị đầu cuối đều có khóa terminal riêng của mình. Thông thường, có hai khóa chính là $km0$ và $km1$ đều được cất trong các modun chống thay đổi tại máy chủ, còn khóa terminal, kt, cũng được giữ một cách an toàn tại thiết bị đầu cuối.

Một khóa phiên ks được tạo ra và sau đó được lưu cất ở dạng $ekm0(ks)$, tức là nó được mã bằng khóa $km0$ tại máy chủ. Khóa phiên đã mã này được giải mã bằng $km0$ và lại được mã hóa lại bằng kt để truyền tới thiết bị đầu cuối, tại đây, nó được giải mã và được lưu trong các modun chống thay đổi như ks. Các thông báo đều được mã hóa và giải mã tại máy chủ trong modun chống thay đổi chứa khóa chính $km0$. Để mã hóa, thông báo rõ được gửi tới modun (đã chuyển sang chế độ mã) cùng với khóa phiên đã mã $ekm0(ks)$. Trong phạm vi modun, khóa phiên lộ ra nhờ phép giải mã $ekm0(ks)$ bằng $km0$, ks sau đó được dùng để mã dữ liệu; giải mã dữ liệu được thực hiện tương tự trong modun nếu được chuyển sang chế độ giải mã.

Kỹ thuật này cho phép một số lượng lớn khóa phiên được mã bằng $km0$ được cất giữ trong máy chủ bên ngoài modun chống giả mạo và bảo đảm rằng, dạng rõ của khóa phiên không bao giờ có sẵn bên ngoài những modun an toàn này. Tương tự, các phép mã và giải mã được bố trí sẵn sàng trong modun chống thay đổi tại thiết bị đầu cuối có chứa khóa terminal kt.

Có thể quản lý khóa tệp an toàn trên cơ sở tương tự như đối với các hệ thống cơ sở dữ liệu mô tả ở trên, hoặc giống như phần mở rộng của các hệ thống liên lạc giữa thiết bị đầu cuối - máy chủ. Trong trường hợp sau, khóa tệp kf có thể được dùng để mã/giải mã

một tệp và khóa này lại được mã bằng khóa tệp thứ cấp *kg*. Kết quả *ekg(kf)* thường được lưu cất cùng phần tiêu đề của tệp.

Sau đó, có thể truyền đi một nhóm các tệp và chỉ cần cung cấp khóa tệp thứ cấp *kg* cho người nhận. Các tệp có thể được mã hóa và giải mã bằng cùng modun mã/giải mã đã dùng trong liên lạc thiết bị đầu cuối - máy chủ; tuy nhiên, cần có đầu vào khóa cho những modun mã/giải mã này, tức *ekm0(kf)*.

Phân phối khóa - các mạng tài chính

Các mạng tài chính, chẳng hạn EFTPOS đặt ra những vấn đề cụ thể về quản lý khóa. Các thiết bị đầu cuối sẽ được đặt tại nhà của người bán lẻ và sẽ có một số lớn thiết bị đầu cuối như vậy. Các thiết bị đầu cuối phải không quá đắt, chúng không được giám sát ngoài giờ làm việc, chúng được những người không có kỹ năng thao tác tốt, thời gian hoàn tất giao dịch phải tối thiểu và các thiết bị đầu cuối phải chấp nhận nhiều kiểu thẻ khác nhau.

Mạng có khả năng chứa nhiều máy tính chủ khác nhau, do các cơ sở tài chính khác nhau điều khiển. Các cơ sở tài chính đảm trách nhiều chức năng khác nhau trên mạng, chẳng hạn tiếp nhận, phát hành thẻ và sẽ yêu cầu liên lạc hiệu quả với mỗi thiết bị đầu cuối, có thể đi qua một hay nhiều nút máy tính trung gian. Các cơ sở tài chính tất nhiên sẽ yêu cầu rằng, họ không bị đòi hỏi để lộ thông tin mật, ví dụ PIN, cho những người dùng khác của mạng và rằng, việc làm mất tính an toàn của một cơ sở sẽ không làm ảnh hưởng tới tính an toàn của các cơ sở tài chính khác.

Dưới đây là những yếu tố làm tình huống phức tạp hơn nữa:

- số lần giao dịch trên mạng trên một đơn vị thời gian sẽ rất lớn;
- tổng thời gian giao dịch bao gồm các trễ do kênh liên lạc, xử lý của máy tính chủ phải được giữ ở mức chấp nhận được đối với hàng dãy khách hàng đang đợi;
- những hỏng hóc của hệ thống không làm cho những máy bán lẻ phải ngừng công việc;
- công nghệ mang không thể vì nâng cấp mà gây tổn phí cao cho những thiết bị đầu cuối của những máy bán lẻ v.v. nếu không, những kẻ tấn công luôn lợi dụng những phát triển công nghệ gần nhất;
- Những đền đáp về mặt tài chính cho cuộc tấn công thành công sẽ lôi cuốn sự chú ý cao của bọn tội phạm có tổ chức.

Có một số chuẩn quốc gia và quốc tế chỉ đạo việc quản lý khóa Chuyển giao các qũy điện tử. Cuốn Các chuẩn của Australia - AS2805 gồm:

Phần 6.1 Các nguyên tắc quản lý khóa;

Phần 6.2 Quản lý khóa - các khóa giao dịch;

Phần 6.3 Quản lý khóa - các khóa phiên nút tới nút;

Phần 6.4 Quản lý khóa - các khóa phiên - thiết bị đầu cuối tới bên nhận.

Các chuẩn này đã đề xuất hai biện pháp quản lý khóa hiệu quả:

- các khóa phiên;
- các khóa giao dịch.

Trong mỗi loại, phải cung cấp các modun chống thay đổi để cất giữ các

khóa và để xử lý mật mã.

Hệ thống khóa phiên tương tự với hệ thống đã mô tả ở trên cho bảo đảm tính an toàn giữa thiết bị đầu cuối - máy chủ. Các khóa được phân cấp thành: khóa chính, khóa mã khóa và khóa phiên.

Các khóa chính được dùng để mã các khóa bậc thấp hơn dành cho lưu trữ, các khóa mã khóa bảo đảm các khóa mã không bị tổn hại khi truyền trên mạng, còn các khóa phiên được dùng cho dữ liệu giao dịch. Trong các hệ thống DES, các khóa bậc cao hơn thường là các khóa có độ dài gấp đôi và dùng thao tác mã hóa - giải mã - mã hóa để bảo vệ các khóa bậc thấp hơn.

Thường thì có ba loại khóa phiên: khóa dữ liệu, khóa MAC và khóa mã PIN. Điều cơ bản là có sự tách bạch về mật mã các khóa để bảo đảm chống lại được kẻ tấn công thay thế một khóa bằng khóa khác. Ví dụ, khóa dữ liệu dùng để bảo vệ thông tin nhạy cảm như tổng lượng giao dịch và tổng lượng này có thể để lộ hợp pháp tại máy chủ nhận. Tuy nhiên, có thể kiểm tra PIN trong modun chống thay đổi và không bao giờ bị lộ ra tại máy chủ. Kẻ tấn công không thể có khả năng thực hiện giải mã PIN khi dùng các phương tiện giải mã dữ liệu.

Thường thì người ta dùng các phương án cho khóa mã hóa khóa và các khóa chính để tách bạch mật mã sao cho các khóa phiên được mã hóa bằng phép mã khóa khác hoặc các khóa chính khác.

Người ta còn phát triển những phương pháp phức tạp hơn để ngăn chặn những khóa nhầm cho mục đích này lại dùng cho mục đích khác. Các hệ thống khóa đích dùng các bit chẵn lẻ của khóa DES để nhận diện các chức năng của chúng. Các vectơ kiểm soát có thể đi kèm với các khóa, ghép với các khóa mã khóa tương ứng để chỉ rõ quá trình xử lý có thể cho phép của các khóa.

Các hệ thống khóa phiên cần chứa quá trình nạp thủ công các khóa mã khóa như nhau tại mỗi phía liên kết. Sau đó, các khóa này được cập nhật một cách riêng rẽ tại mỗi bên theo giao thức thỏa thuận nào đó.

Trong trường hợp các hệ thống khóa giao dịch, một tập các khóa phiên chỉ được dùng cho một giao dịch. Các thông báo giao dịch được kết nối để có thể phát hiện tự động sự thay đổi, mất mát bất kỳ hoặc bổ sung thêm các giao dịch. Về cơ bản, vấn đề phân phối khóa sẽ được cải thiện bằng kỹ thuật cho phép tạo độc lập các khóa phiên tại thiết bị đầu cuối và máy chủ.

Mỗi thiết bị đầu cuối và máy chủ đầu tiên sẽ lưu giá trị khóa terminal ban đầu giống nhau. Các khóa phiên được tính từ khóa terminal này và một hàm một chiều (OWF). Các mã xác thực thông báo MAC được tạo ra cho các thông báo yêu cầu và trả lời, còn các thặng dư MAC tương ứng sẽ được lưu trữ. Vào lúc hoàn tất giao dịch, bản thân khóa thiết bị đầu cuối (khóa terminal) sẽ được cập nhật cùng với OWF nhờ dùng khóa thiết bị đầu cuối hiện tại, các thặng dư MAC của các thông báo nhận và trả lời. Một đặc tính cơ bản của hệ thống khoá giao dịch là đặc tính "Dữ liệu thẻ khác", tức là dữ liệu được lưu trên những tấm thẻ sọc

từ của khách hàng, được đọc tại một thiết cuối song không được truyền đi. Dữ liệu này sẽ đưa ra một khóa tách riêng nhằm ngăn kẻ nghe trộm khỏi chen các thông báo hoặc xác định ra các PIN (số hiệu nhận diện cá nhân) ngay cả khi khóa thiết bị đầu cuối bị tổn thương.

Phân phối khóa - công chứng khóa

Các hệ thống phân phối khóa không chỉ bảo vệ chống làm lộ khóa mà còn chống lại sự thay đổi, gài thêm hoặc dùng lại của kẻ tấn công.

Công chứng khóa cung cấp cho những người tiếp nhận với sự bảo lãnh rằng, khóa dữ liệu do nhóm khởi đầu cuộc liên lạc gửi đi được dành cho người nhận, tức là kẻ tấn công không được truyền khóa dành cho cuộc liên lạc giữa các cặp liên lạc khác. Ví dụ, khi Alice tại nút i khởi đầu cuộc liên lạc với Bob nằm tại nút j, thì khóa mã khóa trao đổi giữa các nút IK_{ij} sẽ được chọn. Alice và Bob có các ký hiệu nhận dạng (với các khóa DES thì chúng là những số 28 bit). Hai ký hiệu nhận dạng này được kết hợp được cộng modulo 2 với nhau tạo thành khóa IK_{ij} 56 bit; sau đó thêm vào các bit chẵn lẻ để chuyển nó thành khóa DES 64 bit hợp lệ. Khóa này sau đó được dùng làm khóa mã khóa để truyền khóa dữ liệu từ Alice tới Bob.

Phân phối khóa - mật mã khóa công khai

Các hệ thống mật mã khóa công khai có ưu điểm so với các mã pháp đối xứng, chẳng hạn như DES, vì ta không cần phải truyền khóa mã khóa trên kênh an toàn.

Tuy nhiên, phân phối công khai các khóa lại dẫn đến khả năng những kẻ tấn công lạm dụng các hệ thống mã khóa công khai. Ví dụ, nếu Alice, trong khi mã hóa một thông báo để truyền cho Bob, có thể bị thuyết phục rằng, dùng khóa mã E_k tốt hơn là E_b (ở đây E_k và E_b tương ứng là khóa mã của kẻ tấn công và Bob) thì kẻ tấn công (thay vì Bob) có thể giải mã các thông báo dành cho Bob. Các chứng chỉ hay thông báo chứng nhận do người có thẩm quyền tin cậy ký có thể khắc phục được vấn đề này.

Tính an toàn của khóa giải mã trong các hệ thống mã khóa công khai chỉ là trách nhiệm của một cá nhân, tức người nhận các thông báo đã mã. Tình huống này có ưu điểm là không bao giờ phải truyền khóa giải mã đi sau khi người dùng đã nhận được nó từ bộ tạo khóa.

Phân phối khóa - trao đổi khóa

Người ta đã nghĩ ra một số sơ đồ tinh vi, chẳng hạn kỹ thuật của Diffie-Hellman và mật mã không khóa cho phép một cặp liên lạc trao đổi các khóa mã mà không cần kênh liên lạc an toàn để truyền thông tin. *Xem* acquirer, ANSI X9.17 - 1985, AS 2805, card issuer, control vector, cryptographic key, database security, decoupling key, DES, Diffie-Hellman technique, digital signature, EFTPOS, host computer, initialization vector, key distribution and control, key-encrypting key, key management device, keying material, keyless cryptography, MAC, MAC residue mental poker, one-way function, PIN, public key cryptography, session key, strength, symmetric cryptosystem, tagged keys, tamper resistant module, transaction key, two key cryptosystem.

key management device ***thiết bị quản lý khóa*** Trong quản lý khóa, một thiết phân phối điện tử an toàn các khóa mã dữ liệu cho những người dùng hợp pháp. Trong trường hợp DES, những khóa này bằng 56 bit trong các khối 64 bit, bởi vậy, có thể phân phối điện tử các khối 64 bit nhờ trung tâm quản lý khoá. *Xem* data encryption standard, key management facility.

key management facility ***phương tiện quản lý khóa*** Trong quản lý khóa, một khu vực (phòng hay thiết bị) được bảo vệ về mặt vật lý được đặt các thành phần (tức phần cứng, phần mềm, phần sụn (vi chương trình) về mật mã, các khóa, hay vectơ ban đầu). *Xem* cryptographic key, firmware, key management device, IV.

key notarization ***công chứng khóa*** (1) Trong quản lý khoá, một phương pháp cho thêm tính an toàn vào khóa nhờ dùng danh tính của người khởi đầu và người nhận cuối cùng. (2) Trong quản lý khoá, công chứng khóa được dùng kết hợp các phương tiện mật mã, gọi là các phương tiện công chứng khóa, tại mỗi nút mạng để tạo sự bảo đảm dựa trên tính xác thực cho các khóa trao đổi.

Các khóa trao đổi được kết hợp với các nút và cặp nút trên mạng. Khóa trao đổi IK_{ij} lập cơ sở cho khóa mã hóa khóa dùng để mã các khóa mã dữ liệu cục bộ, trong khi đó khóa IK_{ij} được thiết kế dùng để mã các khóa dữ liệu dùng trong các cuộc liên lạc giữa nút i và j. Các khóa mã khóa thực sự dùng để mã dữ liệu cục bộ và truyền thông là một hàm của khóa trao đổi thích hợp và các ký hiệu nhận dạng của người dùng.

Nếu dùng phép mã DES thì khóa trao đổi 64 bit IK_{ij} được cấp cho cuộc liên lạc từ nút i tới nút j. Alice và Bob tại nút i và j tương ứng được cấp các ký hiệu nhận dạng 28 bit a và b. Khóa mã khóa 64 bit để mã hóa khóa dữ liệu dùng trong liên lạc giữa Alice và Bob được tạo ra bằng cách biến đổi toán học IK_{ij} và các ký hiệu nhận dạng a và b:

- 7 bit đầu tiên trong ký tự nhận dạng 28 bit a được cộng theo phép loại trừ - hoặc với 7 bit đầu tiên của khóa trao đổi IK_{ij};
- bit thứ 8 của khóa trao đổi IK_{ij} được dùng làm bit chẵn lẻ của 7 bit đã tạo ra theo cách đó;
- 7 bit tiếp theo của ký tự nhận dạng a được cộng loại trừ - hoặc với các bit từ 9 đến 15 của IK_{ij};
- bit thứ 16 của IK_{ij} được mở rộng thành bit chẵn lẻ của 7 bit đã được tạo ra theo cách đó;
- quá trình lặp lại với 14 bit còn lại của ký tự nhận dạng a và 28 bit của ký tự nhận dạng b. Kết quả của các quá trình này là khóa IK_{ijab} DES 64 bit đã được công chứng và được kiểm tra chẵn lẻ.

Bob tại nút j nhận được bản mã của Alice tại nút i, bản mã được mã bằng khóa mã dữ liệu k_d. Bob cũng nhận được khóa mã dữ liệu k_d được mã bằng khóa đã công chứng IK_{ijab}. Để khôi phục lại thông báo rõ, Bob tự xưng danh với bộ phận công chứng khóa bằng mật khẩu PW_b và nhập danh tính của Alice, văn bản mã, khóa mã dữ liệu

ở dạng mã và một lệnh giải mã. Khóa trao đổi IK_{ij} được lưu trong bộ phận công chứng khóa và sau đó lập khóa công chứng IK_{ijab} từ các ký tự nhận dạng a và b bằng thuật toán toán học mô tả ở trên. Khóa dữ liệu k_d được khôi phục từ $eIK_{ijab}(k_d)$ bằng phép giải mã với khóa IK_{ijab} trong phạm vi bộ phận công chứng khóa chống giả mạo; khóa này sau đó dùng để giải mã bản mã.

Công chứng khóa hạn chế được việc dùng khóa của những người dùng cụ thể tại nút mạng cụ thể cho những mục tiêu cụ thể. Như vậy, Bob có thể dùng khóa dữ liệu k_d (nhận được từ phép mã bằng khóa IK_{ijab}) để giải mã các thông báo của Alice gửi từ nút i, khóa không thể dùng cho các mục đích khác.

Có thể lợi dụng sự hạn chế sử dụng các khóa DES này trong các sơ đồ chữ ký số. Alice tại nút i tự xưng danh bằng bằng số hiệu nhận dạng ID_a của mình và mật khẩu PW_a. Mật khẩu được giữ trong kho lưu trữ thứ cấp được mã bằng khóa đã công chứng IK_{aa}. Như vậy, mật khẩu do người dùng đưa vào được mã hóa và được so sánh với giá trị đã lưu. Dựa trên việc xác thực người dùng, phương tiện được đặt ở trạng thái hoạt động đối với người dùng và sau đó có thể thực hiện các chức năng mã, giải mã, xác thực, giải mã/mã hóa lại ... Các khóa dữ liệu và các vectơ khởi đầu đều được tạo ra trong phạm vi phương tiện theo các yêu cầu của người dùng.

Phương tiện cũng chứa các khóa trao đổi cho các nút liên lạc, tuy nhiên, những khóa này được đòi hỏi tại cả hai nút gửi và nhận và bởi vậy phải được một cá nhân có thẩm quyền (hoặc ủy nhiệm) nạp vào phương tiện trong những điều kiện an toàn. *Xem* cryptographic facility, cryptographic key, DES, digital signature, EXCLUSIVE OR, initialization vector, interchange key, key management, parity bit.

key offset ***phần bù khóa*** Trong quản lý khóa, quá trình cộng phép loại trừ - hoặc tín hiệu ra từ một bộ đếm với một khóa. *Xem* ANSI X9.17 - 1985, cryptographic key, EXCLUSIVE OR. *Đồng nghĩa với* offset.

key pair ***cặp khóa*** Trong quản lý khoá, một cặp khóa dùng để mã dữ liệu hoặc nhiều khóa dữ liệu. Trong quá trình mã hóa, một khóa được dùng để mã văn bản rõ, khóa thứ hai hoạt động dựa trên khối đã mã bằng thuật toán giải mã và dùng khóa thứ nhất mã hóa lại kết quả. Kỹ thuật này bảo vệ chống lại kiểu tấn công "gặp ở điểm giữa" và cũng bảo đảm rằng, hệ thống cặp khóa tương hợp với hệ thống khóa đơn. *Xem* ANSI X9.17 - 1985, data key, key-encrypting key, multiple DES encipherment.

key partitioning ***phân hoạch khóa*** Trong quản lý khóa, việc dùng các khóa chính và các biến thể của nó để mã hóa các khóa sơ cấp và khóa thứ cấp. Kỹ thuật này bảo đảm rằng, các khóa được xác định cho một thao tác mã không thể bị lạm dụng hoặc bị điều khiển bởi thao tác mã khác. Như vậy có thể đạt được tính tách biệt và độc lập giữa các ứng dụng khác nhau, ví dụ như giữa liên lạc và an toàn tệp. *Xem* key

management, key variant, primary key, secondary key.

Keypress ***virut Keypress*** Trong an toàn máy tính, một virut gây chấm dứt và nằm thường trú, làm lây nhiễm các tệp COMMAND.COM, COM và các tệp EXE, gây tác động đến thao tác thời gian chạy, làm ngắt chương trình, các tệp dữ liệu và OVL. *Xem* virus names.

key register ***thanh ghi khóa*** Trong hoạt động ngân hàng, vị trí bộ nhớ trong thiết bị đầu cuối và thiết bị tiếp nhận chứa một giá trị chỉ có thiết bị đầu cuối và thiết bị tiếp nhận biết. Giá trị này dùng để tính khóa giao dịch giữa thiết bị đầu cuối và thiết bị tiếp nhận. *Xem* acquirer, key management, transaction key.

key service message ***thông báo dịch vụ khóa*** Trong quản lý khóa, một thông báo truyền một khóa từ người khởi đầu tới người nhận. *Xem* ANSI X9.17-1985.

key space ***không gian khóa*** Trong mật mã, dải chứa tất cả các giá trị có thể mà một khóa mã có thể lấy. Trong một hệ thống mã, không gian khóa phải đủ lớn để ngăn được các tấn công phân tích vét cạn khoá. *So sánh với* cryptogram space, message space. *Xem* key exhaustion.

keystone equipment ***thiết bị chủ chốt*** bao gồm thiết bị sản xuất, kiểm tra, thử nghiệm và là thiết bị cần thiết cho sự áp dụng hiệu quả thông tin kỹ thuật và bí quyết sản xuất. Các tài liệu chủ chốt có cùng sự áp dụng quan trọng. *Xem* know-how.

key stream ***dòng khóa, chuỗi khóa*** *Đồng nghĩa với* cryptographic bit stream.

key stream generator ***bộ tạo khóa dòng*** Trong mật mã, bộ tạo tạo ra dòng bit mật mã dùng cho mã dòng. *Xem* key generator, cryptographic bit stream, stream cipher.

keystroke dynamics analysis ***phân tích động sự gõ phím*** Trong kiểm soát truy nhập, một kỹ thuật sinh trắc học dựa trên các ký tự gõ riêng biệt của những người dùng, thí dụ, các điều chỉnh trên tài liệu giữa các nhóm ký tự nào đó, biểu thị một đặc trưng sinh trắc học đối với người dùng khi đăng nhập vào các thiết bị đầu cuối máy tính.

Những hệ thống như vậy có thể đo trên 100 đặc trưng đặc thù về việc đánh máy của người dùng. Thời gian ghi nhận có thể cần tới 10.000 lần gõ phím song dữ liệu ghi nhận này có thể lọc được từ hành động bàn phím thông thường của người dùng. Với các thiết bị trực tuyến, nơi mỗi lần nhấn phím được đọc trực tiếp vào máy tính thì kỹ thuật này có thể không đòi hỏi thiết bị bổ sung vì các cơ chế bấm giờ cần thiết có thể được chính máy tính tiến hành.

Tuy nhiên, nếu việc đăng nhập được tiến hành trên mạng thì sẽ cần phải có cơ chế bấm giờ cục bộ vì sự truyền trên mạng sẽ tạo ra sự trễ giữa những lần nhấn phím. Quyết định cho truy nhập có thể được đưa ra dựa trên khoảng một tá lần nhấn phím. *Xem* biometrics.

key tape ***băng khóa*** Trong mật mã, băng từ lưu các giá trị khóa mật mã.

key translation center ***trung tâm dịch khóa*** Trong quản lý khóa, một

trung tâm hoạt động trong một hệ thống tương tự như hoạt động của trung tâm phân phối khóa trừ việc nhóm khởi đầu có khả năng tạo khóa dữ liệu. Một dữ liệu hay khóa mã khóa được dùng để liên lạc với người nhận cuối cùng sẽ do người khởi đầu tạo ra, được mã bằng khóa mã khóa hiện tại, được chia sẻ giữa người khởi đầu và trung tâm và được chuyển tiếp tới trung tâm. Trung tâm dịch khóa sẽ giải mã khóa nhận được, mã hóa lại nó khi dùng công chứng cùng với khóa dùng chung giữa trung tâm và người cuối cùng rồi trả lại nó cho người khởi đầu. Sau đó người khởi đầu lại chuyển tiếp khóa đã mã hóa lại cho người nhận cuối cùng. *So sánh với* key distribution center, point to point. *Xem* cryptographic key, data key, key-encrypting key, key notarization.

key transport module ***modun chuyển khóa*** *Đồng nghĩa với* key gun.

key variant ***biến thể khóa*** Trong quản lý khóa, một khóa chính nhận được từ một khóa chính khác qua một phép toán đơn giản, ví dụ đảo các bit đã chọn, cộng với một hằng số theo modulo 2. Kỹ thuật này cho phép dùng phân cấp các khóa chính trong khi chỉ yêu cầu lưu trữ một khóa trong chúng. *Xem* cryptographic key, key partitioning, master key.

key verification code ***mã xác minh khóa, mã kiểm chứng khóa*** Trong mật mã, một số liên quan tới giá trị của một khóa mã DES lưu trữ. Khóa mã lưu trữ được dùng để mã hóa một khối gồm 64 bit 0 và một mã xác minh khóa bằng 24 bit có trọng số lớn nhất của bản mã. Có thể kiểm tra giá trị lưu trữ của khóa bằng cách tính mã xác minh khóa của nó và so sánh nó với giá trị nhận được mà không để lộ giá trị của khóa mã. *Xem* ciphertext, cryptographic key, data encryption standard. *Đồng nghĩa với* key check value.

keyword ***từ khóa, mật khẩu*** Trong an toàn máy tính, *đồng nghĩa với* password.

kiss off tone ***âm không chạm*** Trong truyền thông, một âm do trạm trung tâm tạo ra sau khi nó nhận ra một mã truyền thông và nhận tất cả các tín hiệu vào từ một máy thông tin số. Máy liên lạc số sẽ khôi phục kênh điện thoại cho liên lạc tiếng nói và liên lạc thông thường dựa trên việc nhận được âm này. *Xem* central station, digital communicator.

kiting ***mánh lâu cá*** Trong hoạt động ngân hàng, một quá trình rút séc trên tài khoản sau một thời gian và trả tiền cho một tài khoản khác. Tài khoản thứ hai sẽ vào sổ bên có, còn tài khoản thứ nhất sẽ không vào sổ bên nợ. Bởi vậy lượng tiền sẽ tăng quá lên.

knapsack cipher ***mã ba lô, mã knapsack*** Trong mật mã khóa công khai, dạng đầu tiên của mã khóa công khai do Merkle và Hellman đề xuất vào năm 1978. Dạng khác của mã pháp ba lô do Graham và Shamir đề xuất. *So sánh với* RSA. *Xem* Graham-Shamir knapsack cipher, Merkle-Hellman knapsack cipher.

KNF ***phương tiện công chứng khóa, phương tiện KNF*** Viết tắt của từ Key

Notarization Facility. *Xem* key notarization.

know how ***bí quyết*** Gồm cả bí quyết thiết kế lẫn sản xuất và bí quyết và thông tin kỹ thuật liên quan cần thiết để đạt được sự phát triển quan trọng, tạo và sử dụng. Thuật ngữ bí quyết bao gồm các dịch vụ, các quá trình, các thủ tục, các đặc tả, tiêu chuẩn và dữ liệu thiết kế và các kỹ thuật thử nghiệm.

knowledge base ***cơ sở kiến thức, cơ sở tri thức*** Trong lập trình, cơ sở dữ liệu chứa kiến thức đã hệ thống hóa của một nhà chuyên môn hay các chuyên gia. *Xem* expert systems.

knowledge engineering ***công nghệ tri thức*** Trong lập trình, quá trình xây dựng các hệ thống chuyên gia. *Xem* expert systems.

known plaintext ***bản rõ đã biết, bản rõ biết trước*** Trong mật mã, nói tới một kỹ thuật được sử dụng trong mã thám khi nhà mã thám có sẵn bản mã và bản rõ đối chứng. *So sánh với* chosen plaintext, ciphertext only. *Xem* ciphertext, cryptanalysis, plaintext.

KNS ***hệ thống công chứng khóa, hệ KNS*** Viết tắt của key notarization system. *Xem* key notarization.

Korea ***virut Korea*** Trong an toàn máy tính, một virut lây nhiễm cung khởi động của đĩa cứng và đĩa mềm, tác động trong thời gian chạy. *Xem* virus names.

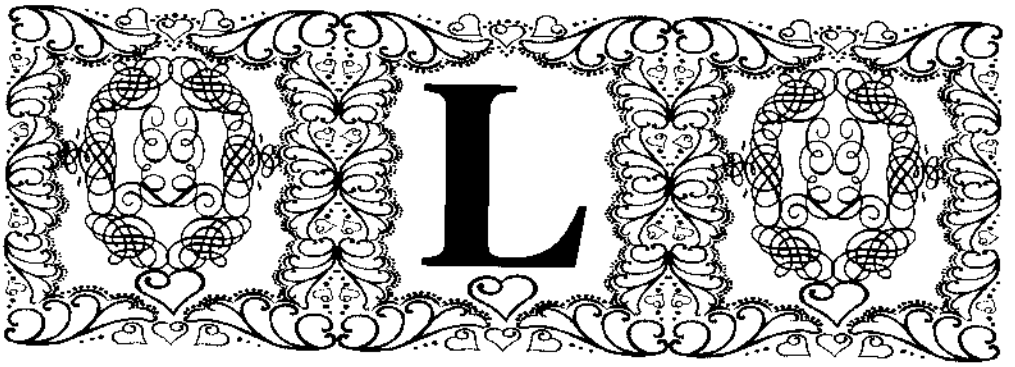
KSM *Xem* key service message.

KSOS ***hệ điều hành an toàn nhân hóa, hệ KSOS*** Viết tắt của Kernelized Secure Operating System. Dự án tăng cường hệ điều hành Unix với một nhân an toàn để nó phù hợp với các hoạt động nhiều mức. *Xem* kernelized, operating system, security kernel, UNIX.

Kukaturbo ***virut Kakuturbo*** Trong an toàn máy tính, một virut chấm dứt và nằm thường trú, lây nhiễm tới các tệp COMMAND.COM và COM. *Xem* virus names.

KVC *Xem* key verification code.

KVM/370 ***phiên bản KVM/370*** Trong an toàn máy tính, VM/370 nhân hóa, một phiên bản VM/370 của hãng IBM dành cho kiến trúc xeri S/370 đã được Hãng phát triển hệ thống kiểm tra và xây dựng. *Xem* kernelized, operating system, security kernel.



label ***nhãn*** (1) Trong an toàn máy tính, một đoạn thông tin biểu diễn mức an toàn của một đối tượng, và mô tả tính nhạy cảm của thông tin trong đối tượng. *Xem* object. (2) Trong an toàn dữ liệu, sự đánh dấu một mục thông tin để phản ánh phân loại và tập các loại hình của nó biểu diễn tính nhạy cảm của thông tin.

a) Nhãn nội bộ. Dấu hiệu một mục thông tin để phản ánh phân loại và tính nhạy cảm của thông tin trong phạm vi hạn chế các vật tải thông tin.

b) Nhãn đối ngoại. Dấu hiệu nhìn thấy được bên ngoài phương tiện hay vỏ của vật mang tin phản ánh phân loại và tính nhạy cảm của thông tin nằm bên trong phương tiện. (3) Trong tính toán, một hay nhiều ký tự hoặc một ký hiệu để nhận diện một câu lệnh chương trình, hoặc một điểm vào một chương trình con. *Xem* statement, subroutine. (4) Trong tính toán, một biểu ghi nhận dạng cho từ hay một tệp tin đĩa.

Label ***virut Label*** Trong an toàn máy tính, một virut làm ngắt các chương trình và nằm thường trú trong bộ nhớ, gây nhiễm tới các tệp COMMAND.COM và COM. *Xem* virus names.

Lamport Diffie signature ***chữ ký Lamport Diffie*** Trong xác thực, một phương pháp tạo chữ ký số.

Nếu một thông báo có N bit cần được gửi đi thì người gửi sẽ tạo ra $2N$ số nhị phân $(x_1, X_1, x_2, X_2, \ldots x_N, X_N)$, mỗi số có k bit. Hàm một chiều (f) được dùng để tạo ra $2N$ số nhị phân nữa là $(y_1, Y_1, y_2, Y_2, \ldots y_N, Y_N)$, trong đó $y_m = f(x_m)$ và $Y_m = f(X_m)$ với $m = 1 \div N$.

$2N$ số $(y_1, Y_1, y_2, Y_2, \ldots y_N, Y_N)$ và hàm một chiều (f) tạo nên một khóa công khai. Thông báo gửi đi $(m_1, m_2, \ldots m_N)$ có N bit; người gửi truyền x_p nếu $m_p = 0$ và truyền X_p nếu $m_p = 1$.

Người nhận sẽ kiểm tra giá trị của bit thứ p bằng cách xem xét số nhận được

với hàm một chiều (f) và so sánh kết quả với y_p ($m = 0$) và Y_p ($m = 1$). Chỉ người gửi biết giá trị của x_p tạo nên y_p là đầu vào của hàm một chiều và bởi vậy thông báo được ký.

Tuy nhiên kỹ thuật này chứa một khóa công khai rất dài, khóa này sẽ thay đổi trong mỗi thông báo gửi đi, và thông báo sẽ giãn rộng đáng kể. Kích thước k của mỗi số trong khóa công khai phải đủ lớn để ngăn kẻ tấn công thử các số đưa vào hàm một chiều bằng phương pháp vét cạn, hòng tạo ra các số khóa công khai tương ứng (y và Y). *So sánh với* DSS, ElGamal digital signature, Rabin signature. *Xem* digital signature, one-way function.

LAN ***mạng cục bộ, mạng vùng, mạng nội hạt, mạng LAN*** *Xem* local area network.

Landwehr's security model for military message systems ***mô hình an toàn của Landwehr cho các hệ thống quân sự*** Trong các mô hình hình thức, một mô hình được phát triển cho các hệ thống thông báo quân sự.

Các hệ thống thông báo thường bao gồm những người xử lý các thông báo và các tệp như phân loại của một phần của một tệp hoặc phân loại của thông báo, khác với phân loại của những tệp khác. Một người dùng đã được phân tới mức truy nhập tối mật có thể muốn trích một đoạn tin đã gắn nhãn mật từ tệp tin tuyệt mật và chuyển đoạn đó tới một tệp có phân loại mật. Mô hình Landwehr về các hệ thống thông báo quân sự cung cấp xử lý tự động cho cả các thông báo hình thức trao đổi giữa các tổ chức, lẫn các thông báo không hình thức trao đổi giữa các cá nhân. Những hệ thống như vậy cho phép tạo, hiệu đính và truyền các thông báo chuẩn bị gửi đi, hiển thị và in các thông báo mới tới và lưu và phục hồi, cho phép tổ chức và tìm kiếm các thông báo trên cơ sở các tệp thông báo.

Theo quan điểm an toàn, việc quản lý các thông báo không giống với các ứng dụng xử lý dữ liệu thông thường, tại đó một người sử dụng xử lý dữ liệu ở một mức an toàn đơn lẻ, với một thời hạn kéo dài. Một người sử dụng MMS có thể liên quan tới số các thông báo riêng lẻ, mỗi thông báo có một phân loại an toàn khác nhau trong một phiên liên lạc, ví dụ, việc quét các thông báo đến mới hơn và in tất cả những tin tuyệt mật đã phân loại đó. Ngoài ra, các thông báo riêng lẻ có thể gồm các thành phần phân loại an toàn khác nhau, như vậy, cấu trúc thông tin nhiều mức là một kiểu vật chứa.

Đối với các hệ thống an toàn quân sự, thích hợp với các chính sách an toàn mà chúng phải tuân thủ, mô hình Landwehr nhằm cung cấp một mô hình an toàn tích hợp đơn lẻ. Mô hình độc lập với những kỹ thuật hay cơ chế dữ liệu thực hiện chính sách an toàn.

Trong hệ thống thông báo quân sự, những người sử dụng đăng nhập bằng phiếu nhận dạng người dùng của mình và sau đó tự xác thực bằng mật khẩu, thẻ bài... Hệ thống sẽ lưu các chi tiết về những thao tác mà những người sử dụng có thể thực hiện trên những đối tượng cho trước. Sau khi đăng nhập, trong phạm vi những quyền có sẵn, người sử dụng giữ một vai trò cụ thể

và đảm trách những thao tác trên những thông báo theo vai trò đó. Ví dụ, người sử dụng có thể quyết định quét những thông báo vừa tới và in tất cả những cái không được phân loại. Như vậy, người sử dụng có một vai trò cụ thể với những thao tác ban đầu nhất định trên các thông báo, hệ thống sẽ hoặc cho phép, hoặc ngăn cản người dùng khỏi thực hiện những thao tác như vậy theo những quyền đã lưu và theo chính sách an toàn.

Tính an toàn của hệ thống như vậy phụ thuộc vào người dùng và chính sách an toàn. Điều quan trọng đối với tính an toàn hệ thống là những người dùng hiểu được đầy đủ những hậu quả về an toàn trong những thao tác của họ. Ví dụ, hệ thống sẽ không được xác nhận cho những hành động liên quan tới an toàn từ phía người dùng trong khi họ có thể không đánh giá đủ tầm quan trọng của những sự ủy quyền như vậy.

Hệ thống không thể ngăn được người dùng làm tổn hại tới thông tin nếu họ có quyền truy nhập hợp pháp tới thông tin đó. Bởi vậy, người ta đã xây dựng một số giả thuyết cho mô hình:

- nhân viên an toàn hệ thống sẽ gán chính xác các phân loại an toàn cho thiết bị, các mức truy nhập và các tập vai trò;
- người dùng nhập các phân loại đúng khi soạn, hiệu đính và phân loại lại thông tin;
- trong phạm vi một phân loại, người dùng xác định những thông báo cho những chủ thể có yêu cầu cần biết;
- người dùng tự do chuyển thông tin từ những vật chứa được đánh dấu CCR (xem ở dưới) vào những vật chứa không bị đánh dấu như vậy.

Một số thuật ngữ, chẳng hạn như phân loại, mức truy nhập số hiệu nhận dạng người dùng, người dùng, đối tượng... có những định nghĩa gần với những thuật ngữ an toàn thông thường; những định nghĩa chỉ tới mô hình này là:

- Vai trò - một công việc mà một người sử dụng đang đảm nhận, như người giáng cấp, người giải phóng hoặc người phân phối. Người dùng luôn gắn kết ít nhất với một vai trò tại thời điểm bất kỳ và có thể thay đổi vai trò trong một phiên làm việc. Để hoạt động ở vai trò cho trước, người dùng phải được uỷ quyền (cấp phép). Một số vai trò có thể chỉ được cấp cho duy nhất một người dùng tại một thời điểm (ví dụ người phân phối). Với mỗi người, vai trò trở thành khả năng thực hiện những thao tác nhất định.
- Vật chứa - một cấu trúc thông tin nhiều mức. Một vật chứa có một phân loại và có thể chứa những đối tượng (mỗi đối tượng có phân loại riêng) và/hoặc những vật chứa khác. Trong hầu hết các thiết bị của hệ thống thông báo quân sự, ví dụ các máy in, các tệp thông báo đều là những vật chứa.
- Thực thể - đối tượng hoặc vật chứa.
- CCR (Container Clearance Required) - mức truy nhập cho vật chứa được đòi hỏi - một thuộc tính của một số vật chứa mà ở đó điều quan trọng là có mức truy nhập tối thiểu để ít nhất nếu một người dùng không có mức

truy nhập này, người sử dụng đó không thể nhìn thấy bất kỳ thực thể nào trong vật chứa. Những vật chứa như vậy được đánh dấu bằng thuộc tính CCR.

- Ký hiệu định danh - một ID đặt tên cho một thực thể mà không cần tham chiếu tới những thực thể khác. Ví dụ, tên của một tệp thông báo là một ID của tệp đó. Một số chứ không phải tất cả các thực thể có thể được đặt tên theo các ký hiệu định danh. Có thể đặt tên theo các cách khác cho các thực thể, ví dụ, đoạn thứ ba của trường văn bản của thông báo - một tham chiếu gián tiếp, xem ở dưới.
- Tham chiếu trực tiếp - một tham chiếu tới một thực thể là trực tiếp nếu nó là ID của thực thể.
- Tham chiếu gián tiếp - một tham chiếu tới một thực thể là gián tiếp nếu nó là một dãy gồm hai hay nhiều hơn các tên của thực thể (trong đó tên đầu tiên có thể là ID), xem ID ở trên.
- Tập truy nhập - một tập các bộ ba (ID của người dùng hoặc vai trò, thao tác, chỉ số toán hạng) đi kèm theo một thực thể. Một số thao tác đòi hỏi hơn một toán hạng, trong trường hợp đó, chỉ số toán hạng sẽ chỉ ra chức năng cụ thể của thực thể đó trong thao tác. Như vậy, nếu một thao tác đòi hỏi hai toán hạng, và chỉ số toán hạng là 2 thì với bộ ba này, thực thể sẽ tương ứng với toán hạng thứ hai.
- Thông báo - một loại cụ thể do hệ thống thông báo quân sự thực hiện, trong hầu hết các thành viên họ MMS, một thông báo sẽ là một vật chứa. Một thông báo sẽ gồm các trường Đến, Đi, Nhóm ngày-tháng, Chủ thể, Người phát và trường Text, cộng thêm các trường phụ, ví dụ thông báo dự thảo đạo luật sẽ chứa thêm trường Người phác thảo.

Khái niệm quan trọng trong mô hình này là khái niệm vật chứa. Thông báo có kiểu vật chứa vì nó chứa nhiều trường khác nhau có thể có các phân loại mật khác nhau. Bản thân văn bản thông báo có thể cũng là một vật chứa với một số đoạn được phân loại mật, một số khác lại không mật... Những thiết bị như đĩa, máy in... cũng là những vật chứa. Phân loại của bản thân vật chứa ít nhất cũng bằng mức phân loại cao nhất của các thực thể trong nó. Vật chứa không giống với đối tượng theo nghĩa nó dựa trên loại hơn là nội dung hiện chứa, như vậy, một thông báo sẽ là vật chứa ngay cả khi chỉ là một đối tượng riêng lẻ.

Trong một số trường hợp, người dùng chưa được phân loại được phép nhìn thấy những đoạn không mật của một thông báo chứa cả những đoạn phân loại mật. Trong những trường hợp khác, những người dùng không được phân loại được tham chiếu gián tiếp tới một thông báo, ví dụ yêu cầu truy nhập tới đoạn thứ ba của văn bản thông báo 39AZ sẽ không được phép nhìn dù chỉ phần không mật của một thông báo mật.

Mô hình điều khiển yêu cầu sau cùng này nhờ dùng các phân loại mức truy nhập vật chứa (CCR). Thông thường, người dùng có thể truy nhập tới một thực thể trong một vật chứa nếu mức

truy nhập của anh ta ít nhất là bằng phân loại của thực thể. Tuy nhiên, nếu một vật chứa được đánh dấu CCR thì người dùng chỉ có thể nhìn thấy thực thể trong nó nếu anh ta có mức truy nhập ít nhất cũng bằng phân loại mật của chính vật chứa.

MMS (Hệ thống thông báo quân sự) an toàn nhiều mức sẽ là chủ thể của những khẳng định (assertion) liệt kê dưới đây.

1. Sự ủy quyền - người dùng chỉ có thể gọi tới một thao tác trên một thực thể nếu số hiệu nhận dạng hay vai trò hiện tại của anh ta xuất hiện trong bộ truy nhập tới thực thể đi theo thao tác đó và với một giá trị chỉ số mà tương ứng với vị trí toán hạng để thực thể tham chiếu tới theo thao tác cần thiết.

2. Phân cấp phân loại - sự phân loại của vật chứa bất kỳ ít nhất cũng luôn cao bằng phân loại cực đại của các thực thể mà nó chứa.

3. Những thay đổi đối với các đối tượng - thông tin bị khử bỏ khỏi một đối tượng sẽ thừa kế phân loại của đối tượng đó. Thông tin được gài vào một đối tượng phải không có phân loại cao hơn phân loại của đối tượng đó.

4. Nhìn - một người dùng chỉ có thể nhìn thấy một thực thể có phân loại thấp hơn hoặc bằng mức truy nhập của người dùng và phân loại của phương tiện ra (xác nhận này áp dụng cho những thực thể được tham chiếu trực tiếp hay gián tiếp).

5. Truy nhập tới các thực thể CCR - một người dùng có thể truy nhập được tới một thực thể được tham chiếu gián tiếp trong phạm vi một vật chứa được đánh dấu CCR chỉ khi mức truy nhập của người dùng lớn hơn hoặc bằng phân loại của vật chứa.

6. Dịch tham chiếu gián tiếp - một người dùng có thể nhận được số hiệu nhận dạng cho một thực thể gián tiếp chỉ khi anh ta có quyền hợp pháp nhìn thấy thực thể đó qua tham chiếu đó.

7. Lập nhãn cho yêu cầu - thực thể bất kỳ mà người dùng nhìn thấy phải được gắn nhãn bằng phân loại của nó.

8. Thiết lập các mức truy nhập - chỉ người dùng nào có vai trò là nhân viên an toàn hệ thống mới có thể thiết lập được mức truy nhập và tập vai trò cho số hiệu nhận dạng người dùng hoặc phân loại cho thiết bị. Vai trò hiện tại của người dùng chỉ có thể thay đổi bởi người dùng đó hoặc bởi người dùng có vai trò nhân viên an toàn hệ thống.

9. Giảm cấp - không có sự đánh dấu phân loại nào có thể được giảm cấp trừ phi người dùng có vai trò là người giảm cấp thực hiện thao tác giảm cấp.

10. Phát hành - không có thông báo dự thảo nào có thể được phát đi trừ phi người dùng có vai trò của người phát hành. Số hiệu nhận diện của người phát hành phải được ghi vào trường phát hành của thông báo dự thảo.

Mô hình giải quyết vấn đề kết hợp. Một mặt, hoàn toàn có thể cho phép một người dùng không mật nhìn thấy các đối tượng không xếp vào loại mật trong một vật chứa được phân loại mật. Mặt khác, hoạt động này có thể cho phép kết hợp dữ liệu ở mức độ nào đó. Người dùng có thể thu thập cùng lúc một số lớn các tài liệu không mật. Những tài liệu này nếu bị lộ toàn bộ

thì sẽ gây nguy hiểm tới tính an toàn. Mô hình kiểm soát tình huống này nhờ dùng phép đánh dấu CCR và tham chiếu trực tiếp/gián tiếp (khẳng định 4 và 5). Giả sử vật chứa được đánh dấu bằng CCR và có phân loại mật trong khi nó chứa một số đối tượng không mật. Người dùng không được xếp vào loại mật có các quyền gọi tới thao tác nhìn đối tượng và người biết ID của một trong những đối tượng không mật này có thể nhìn thấy nó qua tham chiếu trực tiếp (khẳng định 4). Tuy nhiên, nếu người dùng cố gắng lượm lặt thông tin bằng cách quét hết các nội dung của vật chứa thì việc đánh dấu CCR sẽ ngăn chặn truy nhập tới mục giống nhau bằng tham chiếu gián tiếp tới vật chứa (khẳng định 5). *So sánh với* Bell-La Padula model. *Xem* aggregation, container, multilevel device, object.

language ***ngôn ngữ*** Trong tính toán, một tập hợp các ký tự, quy ước, quy tắc dùng để truyền đạt thông tin. Một ngôn ngữ có thể được xem xét một cách hình thức các đoạn, cú pháp và ngữ nghĩa. *Xem* formal language, grammar, program language, semantics, syntax.

LAN security ***an toàn mạng nội hạt, an toàn mạng cục bộ, an toàn LAN*** Trong an toàn liên lạc, các mạng cục bộ ban đầu được hiểu như những hệ thống tạo thuận tiện cho việc liên lạc giữa rất nhiều người và trạm làm việc trong một vùng hạn chế về địa lý, có các cổng nối tới các mạng diện rộng. Bởi vậy, chúng có những yếu điểm tiềm ẩn của các hệ thống máy tính và các mạng diện rộng. Có thể chứng tỏ rằng, bản chất của LAN có ít vấn đề hơn so với các mạng WAN:

- thiết bị được cài đặt dưới các giả thuyết an toàn;
- các tuyến đường truyền ngắn và lưu thông được định vị hóa tới vùng chỉ ra;
- bảo vệ truy nhập được bảo đảm bởi mật khẩu;
- có thể dùng cáp quang để trách mắc rẽ đường dây nghe trộm.

Thực tế, tính an toàn của LAN có thể biểu thị hoàn toàn qua những vấn đề sau:

- mạng được thiết kế để tạo thuận lợi cho việc nối thêm các trạm làm việc và giao tiếp được với nhiều thiết bị do các nhà máy khác nhau sản xuất.
- thông thường mạng có thể hoạt động trong chế độ quảng bá để mỗi thông báo được truyền tới mỗi trạm làm việc và như vậy, bảo đảm để người nghe tại vị trí bất kỳ truy nhập được tới mỗi thông báo;
- có thể truyền qua mạng nhiều kiểu tín hiệu khác nhau và như vậy, khó có thể phát hiện ra những người dùng và những thông báo bất hợp pháp;
- một tỷ lệ cao những vụ lạm dụng máy tính là do nhân viên làm công;
- tính linh hoạt và dễ truy nhập tới các phương tiện mạng làm tăng phạm vi những mục tùy chọn có sẵn đối với những nhân viên có thiên hướng gian lận và có khả năng kỹ thuật;
- những bức xạ ở dải tần số vô tuyến phát ra từ mạng lẫn những điểm nối sẽ bị ghi lại nếu không có những biện pháp ngăn chặn đặc biệt.

Sự lạm dụng có tính toán các mạng LAN có thể nảy sinh từ cả những mạch rẽ bất hợp pháp lẫn sự suy thoái đạo đức của những người sử dụng hay sự hỏng hóc của các trạm làm việc. Những khớp nối thưa nhằm mở rộng mạng trong tương lai có thể tạo điều kiện thuận lợi cho những mạch rẽ trái phép. Việc dùng những mạnh rẽ trái phép như vậy cũng được đơn giản hoá bởi những giao thức thân thiện với người dùng được quảng cáo rộng rãi của LAN. Việc nghe thụ động trên các mạng LAN qua các máy tính cá nhân là chủ yếu. Một trạm làm việc trái phép nối tới một LAN có thể dùng để nghe trộm những thông tin nhạy cảm, hoặc để chen vào các thông báo bất hợp pháp. Người ta dùng những thông báo như vậy để phá vỡ mạng hoặc để khởi sự việc phát hành thông tin liên quan tới an toàn, ví dụ trạm làm việc có thể đóng giả một máy chủ để người dùng các trạm làm việc khác tin cậy và làm lộ mật khẩu.

Có thể ngăn hay phát hiện ra một trạm làm việc bất hợp pháp bằng các kiểm soát truy nhập vật lý hợp lý, song kẻ tấn công cũng có thể là người dùng hợp pháp của một trạm làm việc. Trong trường hợp này, có thể những kẻ tấn công dùng một thiết bị đầu cuối trong vùng cố truy nhập tới dữ liệu nhạy cảm từ một cơ quan khác. Kẻ tấn công cũng có thể phá hoại chính trạm làm việc bằng cách thay đổi phần cứng hay mềm. Điều này cho thấy khả năng trạm làm việc liên tục giám sát và lưu dữ liệu của mạng cho kẻ tấn công dùng sau này - kẻ khá chắc chắn là sẽ không bị phát hiện.

Các mạng LAN dễ bị tổn thương không chỉ trước cuộc tấn công có tính toán mà còn dễ tổn thương trước những sự cố mạng, những sự cố này có thể gây nên những tác động nghiêm trọng tới hiệu quả hoạt động chức năng của tổ chức. Những vấn đề có thể nảy sinh do:

- bảo vệ không đầy đủ chống lại sự đột biến hay ngắt điện;
- những hỏng hóc mạng hay thực hiện không đầy đủ do nhân viên nối cáp không có kinh nghiệm hoặc do không chú ý thỏa đáng tới những điểm đặc biệt của mạng, các mối nối cáp xấu (chẳng hạn những điểm rẽ) là những nguồn chính gây ngắt mạng;
- các mạng vòng, không giống với mạng hình sao, rất dễ bị ảnh hưởng bởi sự cố mạng, những nút không phục vụ có thể cho qua song những hỏng hóc như vậy có thể gây ngắt tạm thời dữ liệu mạng; nói chung, những kinh nghiệm về mạng thì hạn chế song những công cụ chẩn đoán không đầy đủ thì lại sẵn.

Dưới đây liệt kê các đặc điểm an toàn quan trọng của một mạng LAN:

- tính toàn vẹn của cuộc truyền, tức tất cả những thông báo hợp lệ đều nhận được đầy đủ và chính xác, còn những thông báo không hợp lệ từ những người dùng bất hợp pháp hay những biến thể của những thông báo xác thực và dùng lại thì sẽ được ngăn chặn;
- tính bí mật của các thông báo, nếu cần thì dùng mật mã;
- kiểm soát truy nhập đối với dữ liệu và các tài nguyên, tức là không dùng trái phép các trạm làm việc; điều này

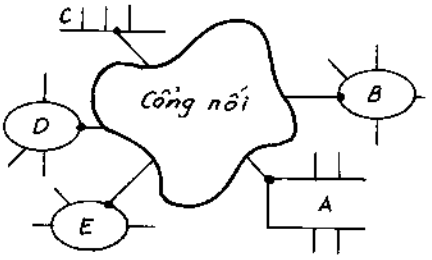
đặc biệt quan trọng nếu LAN có cổng tới mạng WAN;

- chống lại việc sử dụng lén các mạng, chẳng hạn thông qua các tín hiệu mã hóa;
- tính sẵn sàng phục vụ khi cuộc tấn công nhắm trực tiếp tới việc làm mất khả năng làm việc của mạng hoặc làm giảm hiệu suất của nó bằng cách gửi ào ạt các thông báo.

Có thể xử lý việc bảo vệ LAN ở một mức như bài toán quản lý. Mức an toàn được áp dụng phải phù hợp với những mất mát từ một cuộc tấn công hay hỏng hóc hệ thống.

Đầu tiên, các mạng LAN được thiết kế nhằm trao đổi thông tin dễ dàng giữa những chuyên gia và những người làm công tác văn phòng. Đối với những người dùng, tác động của những biện pháp phòng xa về an toàn là phải cho họ nhận ra mục đích cũng như tầm quan trọng của những biện pháp như vậy. Quá nhiều các thủ tục hạn chế người dùng có thể làm nản lòng việc sử dụng mạng hoặc phá vỡ những biện pháp an toàn; có những báo cáo chung về các mật khẩu phức tạp được viết trên mặt ngoài của thiết bị đầu cuối để giúp người dùng đỡ phải nhớ. Các kiểm soát truy nhập hợp lý tới các trạm làm việc, sự bảo vệ dây cáp chống mắc rẽ trái phép, sự giám sát lưu lượng trên mạng... trong nhiều trường hợp có thể tạo mức an toàn thích đáng.

Bản thân cấu hình liên kết mạng cũng có thể được thiết kế để tăng tính an toàn. Ví dụ, nếu mạng được chia thành các mạng con thì lưu lượng đến và đi khỏi những khu vực nhạy cảm có thể giám sát qua các cổng có kiểm soát. Trong những ứng dụng mà tính an toàn



LAN security: *an toàn LAN.*
Các cổng LAN.

là tham số chủ yếu thì việc thiết kế bản thân mạng hay ít nhất các giao tiếp với nó phải được xem xét theo quan điểm an toàn. Một mạng LAN có thể được thiết kế như một hệ thống an toàn phân tán nếu như việc tối thiểu hóa dòng thông tin từ một ngăn an toàn tới ngăn an toàn khác là quan trọng. Những thủ tục an toàn đã được đề xuất khác cho các mạng LAN đều được dựa trên khái niệm về các mạng LAN được bảo vệ và không được bảo vệ.

Tính an toàn của mạng LAN không được bảo vệ dựa trên giả thuyết rằng, mạng không được tin cậy và không được bảo vệ, còn bản thân trạm làm việc có thể là đối tượng bị phá hoại, bởi vậy, an toàn là trách nhiệm có tính chức năng của máy chủ. Một đơn vị tin cậy được gọi là Khối Giao tiếp Thiết bị đầu cuối Đặc biệt (STIU) được đặt giữa giao diện mang và trạm làm việc. Máy chủ sẽ có Khối Giao tiếp Máy chủ Đặc biệt (SHIU) tương ứng được nối giữa máy tính và mạch giao tiếp LAN. Các thông báo nhạy cảm sẽ được mã hóa

trên cơ sở điểm nối điểm, song dữ liệu kiểm soát mạng phải được gửi ở dạng rõ.

Máy chủ được giả thiết là một thiết bị tin cậy; STIU và SHIU thiết lập các danh tính cho nhau nhờ dùng các khóa mã. Sau đó máy chủ sẽ thiết lập danh tính của những người dùng bằng cách yêu cầu người dùng trực tiếp đưa số tài khoản và mật khẩu vào STIU nhằm phòng ngừa một tấn công có tính phá hoại lên trạm làm việc. Thông tin về tài khoản sẽ được gửi ở dạng rõ song tính hợp lệ của các mật khẩu lại có thể gồm thông báo đã mã bằng khoá phiên, và bản thân các khóa này là các hàm của mật khẩu và bởi vậy, chỉ có máy chủ và người dùng biết.

Mặt khác, LAN được bảo vệ là một mạng LAN cung cấp dịch vụ bảo đảm tính xác thực, giữ bí mật và phân phối các thông báo cho các máy chủ của nó. LAN được bảo vệ không tin cậy tất cả các máy chủ, các trạm làm việc và người dùng. Các khối Giao tiếp Mạng Tin cậy (TNIU) chống lại sự phá rối và không thể giả mạo được xây dựng vào mạng.

Có thể dùng mật mã để liên lạc mạng, song không cơ bản nếu như việc cài đặt vật lý làm nó không có tác dụng trước các nối mạch rẽ trái phép. Việc kiểm soát liên lạc trên LAN là trách nhiệm của Dịch vụ Xác thực An toàn (SAS). Trong trạng thái không hoạt động, TNIU chỉ có thể liên lạc với SAS. Người dùng nhập tài khoản, mật khẩu và các yêu cầu về các tài nguyên, liên lạc với các trạm làm việc khác.. TNIU truyền thông tin này tới SAS để kiểm tra danh tính, mật khẩu, các quyền và các yêu cầu hợp pháp. Nếu chúng hợp lệ, SAS sẽ thiết lập các kết nối cần thiết và đặt TNIU ở trạng thái cho phép liên lạc trên các kết nối này. Khi người dùng ra khỏi mạng, TNIU trở về trạng thái không hoạt động. *Xem* electromagnetic emanations, fiber optics, flooding, local area network, masquerading, tamper resistant module, trusted, vulnerability, WAN, wide area network.

LAP ***giao thức LAP, giao thức truy nhập liên kết*** Trong truyền thông, viết tắt của Link Access Protocol, giao thức truy nhập liên kết, một giao thức tầng liên kết dữ liệu là tập con của HDLC và được dùng trên các mạng theo chuẩn X.25. *Xem* data link layer, HDLC, protocol, X.25.

laser intrusion detector ***thiết bị phát hiện xâm nhập bằng laze*** Trong an toàn vật lý, một thiết bị mà tín hiệu báo động được kích hoạt khi một chùm tia laze công suất thấp bị ngắt; hoạt động của nó tương tự với hoạt động của bộ cảm biến quang điện. *Xem* photoelectric sensor.

last in first out ***vào sau ra trước*** Trong tính toán, một hệ thống trong đó mục dữ liệu vào sau được chọn là mục gần nhất được thêm vào danh sách. *So sánh với* first in first out. *Xem* stack.

lattice ***lưới, giàn*** Trong toán học, một tập phần tử được sắp thứ tự đặc biệt sao cho mỗi cặp phần tử có một giới hạn dưới lớn nhất và một giới hạn trên nhỏ nhất. *Xem* lattice model.

lattice model ***mô hình giàn*** Trong an toàn cơ sở dữ liệu, một mô hình dữ

liệu trong một cơ sở dữ liệu thống kê dùng để nghiên cứu các kiểm soát suy luận. Các biểu ghi chứa các thuộc tính chung khác với thông tin định danh trực tiếp về cá nhân. Với *m* thuộc tính sẽ lập nên một bảng *m* chiều. Ví dụ, với 2 thuộc tính, sẽ tạo ra một bảng hai chiều, sau đó các hàng và các cột được chia thành các dải giá trị cho các thuộc tính. Như vậy, thuộc tính tuổi có thể được chia thành 10 cột biểu diễn các độ tuổi từ 0 - 9, 10 - 19.. Khi đó các mục nhập vào trong các ô riêng lẻ của bảng sẽ biểu diễn một thống kê, chẳng hạn số lượng tất cả các biểu ghi cùng với các thuộc tính trong phạm vi mà ô biểu diễn. Như vậy, trong trường hợp hai chiều, mục vào ô có thể biểu diễn số các cá nhân ở độ tuổi từ 30 đến 39 với 1 tới 3 điểm phụ thuộc. Bảng *m* chiều biểu diễn tập các thống kê chi tiết nhất; các bảng *m* - 1 chiều sẽ lập nên các bộ thống kê tương ứng thô hơn. Như vậy trong trường hợp hai chiều kể trên, một trong các bảng một chiều tương ứng sẽ đưa ra tổng số các cá nhân ở những độ tuổi khác nhau, còn bảng kia là số đếm tất cả các cá nhân có với số biến phụ thuộc khác nhau. Ở mức trên cùng của giàn, một bảng một ô chứa tổng số những biểu ghi về cá nhân. *Xem* database security, inference control, stastistical database.

LAVA ***phương pháp luận LAVA*** Trong quản lý rủi ro, một phương pháp luận phân tích rủi ro. *Xem* risk analysis methodologies.

Law Enforcement Incident Reporting System ***Hệ thống báo cáo những vụ việc liên quan tới thi hành luật*** Trong luật pháp, một cơ sở dữ liệu chung của Hoa Kỳ về tin tức tội phạm lấy được từ Cục công viên Quốc gia, Cục cải tạo, Cục quản lý đất đai, Cục nội vụ người da đỏ và Sở bảo vệ Thiên nhiên. *Xem* data protection, data protection - U.S.A.

Lazy ***virut Lazy*** Trong an toàn máy tính, một loại virut chấm dứt và thường trú, lây nhiễm các tệp COMMAND.COM và các tệp đuôi COM, làm ảnh hưởng tới hoạt động trong thời gian chạy, làm ngắt chương trình và các tệp OVL. *Xem* virus names.

LCD *Xem* liquid crystal display.

LCG ***bộ tạo đồng dư tuyến tính*** Viết tắt của Linear Congruential Generator. *Xem* randon number.

LCM ***BSCNN*** *Xem* least common multiple.

LDDS ***bộ dữ liệu khoảng cách hạn chế, bộ LDDS*** Viết tắt của Limited Distance Data Set. *Xem* limited distance modem.

leaf ***nút lá*** Trong tính toán, nút tại điểm cuối của một nhánh trong cấu trúc dạng cây. *Xem* tree structure.

leakage ***(sự) rò rỉ*** Trong an toàn dữ liệu, đề cập tới dòng thông tin trái phép chảy từ người dùng có các đặc quyền truy nhập tới những người không có những đặc quyền đó. *Xem* Bell-La Padula model, information flow control.

Leapfrog virus ***virut Leapfrog*** Trong an toàn máy tính, loại virut chấm dứt và thường trú, lây nhiễm tới tệp COMMAND.COM và các tệp đuôi COM, ảnh hưởng tới hoạt động thời gian chạy

và làm ngắt chương trình, các tệp OVL và tệp dữ liệu. *Xem* virus names.

leased circuit ***mạch thuê bao*** Trong truyền thông dữ liệu, một mạch cho thuê dài hạn để dùng riêng. Nó có thể là mạch nối điểm tới điểm hoặc nhiều điểm. *Xem* multidrop circuit, point to point. *Đồng nghĩa với* nonswitched line.

leased line ***đường thuê bao*** *Xem* leased circuit.

least common mechanism ***cơ chế chung ít nhất*** Trong an toàn máy tính, nguyên tắc về cơ chế chung ít nhất - một trong những nguyên tắc của các hệ thống an toàn phát biểu rằng, để đạt được tính an toàn chung, cần sử dụng các cơ chế chia sẻ tối thiểu hóa giữa những người sử dụng. *Xem* principles of secure systems.

least common multiple ***bội số chung nhỏ nhất*** Trong toán học, số nguyên bé nhất chia hết cho cả hai số nguyên chỉ ra, chẳng hạn, bội số chung nhỏ nhất của 6 và 8 là 24. *So sánh với* greatest common divisor.

least cost network design ***thiết kế mạng rẻ nhất*** Trong truyền thông dữ liệu, một mạng thiết kế tối ưu đáp ứng chỉ tiêu kỹ thuật thiết kế với giá ít tới mức có thể.

least privilege ***đặc quyền tối thiểu*** Trong an toàn máy tính, nguyên tắc đặc quyền tối thiểu, một trong những nguyên tắc của các hệ thống an toàn phát biểu rằng, mỗi quá trình cần hoạt động với mức đặc quyền tối thiểu cần thiết để thực hiện tác vụ yêu cầu. *Xem* principles of secure systems.

least significant bit ***bit nhỏ nhất, bit cực phải*** Trong tính toán, một bit xuất hiện ở vị trí cực phải trong một số nhị phân. *Xem* bit.

least significant digit ***chữ số có trọng số nhỏ nhất*** Trong tính toán. một chữ số xuất hiện ở vị trí cực phải trong một số và bởi vậy có trọng số nhỏ nhất.

Lehigh ***virut Lehigh*** Trong an toàn máy tính, một virut chấm dứt và thường trú, lây nhiễm tệp COMMAMD.COM, phá hoại chương trình và các tệp đuôi OVL, định dạng hoặc ghi đè lên tất cả hay một phần đĩa. *Xem* virus names.

LEIRS *Xem* Law Enforcement Incident Reporting System.

Leprosy ***virut Leprosy*** Trong an toàn máy tính, một loại virut chấm dứt và thường trú, lây nhiễm tới tệp COMMAND.COM, các tệp có đuôi COM, EXE và OVL. *Xem* virus names.

Leprosy-B ***virut Leprosy-B*** Trong an toàn máy tính, một loại virut gây nhiễm các tệp COMMAND.COM, COM và EXE. *Xem* virus names.

letter bomb ***bom thư*** Trong an toàn máy tính, một dạng bom logic chứa trong thư điện tử, nó sẽ khởi sự khi thư được đọc. *Xem* logic bomb, malicious code.

level ***mức*** (1) Trong an toàn máy tính, *xem* security level, integrity level. (2) Trong truyền thông, một thuật ngữ chung để chỉ độ lớn của tín hiệu thường dùng chỉ điện áp, dòng và nguồn điện. (3) Trong liên lạc dữ liệu,

số các bit trong mỗi ký tự của một hệ thống mã thông tin. (4) Trong truyền thông dữ liệu, chỉ số các phần tử tín hiệu rời rạc có thể được truyền đi ở chế độ điều chế định trước. *Xem* modulation.

LSFR ***thanh ghi LSFR, thanh ghi dịch phản hồi tuyến tính*** *Xem* linear feedback shift register.

Liberty ***virut Liberty*** Trong an toàn máy tính, một virut chấm dứt và thường trú, lây nhiễm các tệp COMMAMD.COM, COM, EXE, tác động trong thời gian hoạt động, phá hoại các tệp chương trình và tệp OVL. *Xem* virus names.

LIFO ***vào sau ra trước*** *Xem* last in first out.

light conduit ***ống dẫn ánh sáng*** Trong truyền thông, một tập hợp các sợi trong cáp sợi quang được dùng để truyền các nguồn ánh sáng hay đúng hơn là truyền các tín hiệu quang học đã mã. *Xem* fiber optics.

light guide ***ống dẫn sáng*** *Xem* fiber optics.

LIMDIS ***phân phối hạn chế*** Trong an toàn dữ liệu viết tắt của LIMited DIStribution, một phân phối thông tin kết hợp bị hạn chế chỉ ra bằng dấu đặc biệt hoặc bằng quy định trước về mục quản. *Xem* handling caveats, special markings.

limited access ***truy nhập hạn chế*** Trong kiểm soát truy nhập, sự hạn chế truy nhập tới các tài nguyên của một hệ thống đối với cá nhân được ủy quyền, những người sử dụng, các chương trình, các quá trình hoặc các hệ thống khác, chẳng hạn các mạng máy tính. *Xem* limited ADP access security mode.

limited ADP access security mode ***chế độ truy nhập an toàn tới các hệ xử lý tự động hạn chế*** Trong kiểm soát truy nhập, một hệ thống ADP hay mạng đang hoạt động ở chế độ an toàn hạn chế truy nhập khi kiểu dữ liệu đang được xử lý được xếp vào loại không mật, chế độ này đòi hỏi thực hiện các kiểm soát truy nhập đặc biệt để hạn chế truy nhập tới dữ liệu mà chỉ những người do chức năng của mình có nhu cầu mới được truy nhập tới. *Xem* limited access.

limited distance modem ***modem khoảng cách hạn chế*** Trong truyền thông dữ liệu, một modem không dùng sơ đồ điều chế phức tạp dữ liệu trước khi truyền đi song lại áp dụng đầu vào dạng số lên kênh truyền. Nó chỉ được dùng để truyền ở cự ly ngắn. *Xem* MODEM. *Đồng nghĩa với* baseband modem.

limited protection ***bảo vệ hạn chế*** Trong an toàn thông tin, một dạng giữ an toàn thông tin trong thời gian ngắn được áp dụng đối với việc truyền thông tin không mật ở dạng âm thanh và điện tử, cho phép bảo vệ chống lại sự phân tích đơn giản và lợi dụng dễ dàng song không cần phải ở mức bảo vệ như đối với thông tin được xếp vào loại mật.

Lindop Committee ***Ủy ban Lindop*** Một ủy ban của Anh thành lập để xem xét các vấn đề về bảo vệ và giữ bí mật dữ liệu và đã báo cáo vào năm 1976.

Xem data protection, data protection - U.K., privacy, Younger Committee.

line ***đường dây, đường truyền; dòng*** (1) Trong truyền thông, đường dây là dây dẫn kim loại dùng để truyền tín hiệu. (2) Trong truyền thông dữ liệu, dòng là một chuỗi các ký tự được máy tính trung tâm chấp nhận như một khối tín hiệu vào đơn lẻ, chẳng hạn tất cả các ký tự được nhập vào trước khi có lệnh xuống dòng.

line adaptor unit ***khối thích ứng đường truyền*** *Xem* MODEM.

linear complexity ***độ phức tạp tuyến tính*** Trong toán học, độ dài của thanh ghi dịch phản hồi tuyến tính ngắn nhất có thể được dùng để tạo nên một dãy các chữ số nhị phân cho trước; bởi vậy nó là tính chất của dãy đó. *Xem* binary digit, linear feedback shift register. *Đồng nghĩa với* linear equivalence, recursion length.

linear congruential generator ***bộ tạo đồng dư tuyến tính*** *Xem* random number.

linear equivalence ***tương đương tuyến tính*** *Đồng nghĩa với* linear complexity.

linear feedback shift register ***thanh ghi dịch phản hồi tuyến tính*** Trong mật mã, một thanh ghi dịch trong đó, chữ số đưa vào tầng đầu tiên là một hàm tuyến tính của những giá trị hiện tại ở các tầng khác của thanh ghi dịch. Những thanh ghi dịch như vậy có thể dùng để tạo ra các số giả ngẫu nhiên hoặc các dòng bit mật mã cho các mã dòng. *Xem* cryptographic bit stream, linear recurrence relation, random number, recursion analysis, shift register, stream cipher.

linear function ***hàm tuyến tính*** Trong toán học, hàm chứa tổng các số hạng, mỗi số hạng là một hằng số nhân với một trong các biến bậc nhất, chẳng hạn $P = 5X + 10Y$.

linear query ***lệnh truy vấn tuyến tính, lệnh hỏi tuyến tính*** Trong an toàn cơ sở dữ liệu, câu lệnh truy vấn trong một cơ sở dữ liệu thống kê là một hàm tuyến tính của một trường cụ thể không phải trường khóa của một tập các bản ghi. Ví dụ, nếu lương của nhân viên trong bản ghi 1, 2, 3... n là S_1, S_2,- S_n thì lệnh truy vấn tuyến tính trên những trường này là $c_1S_1 + c_2S_2 + ... + c_nS_n$ trong đó c_i là số thực tùy ý do người hỏi chọn. Kẻ tấn công có thể dùng các lệnh truy vấn tuyến tính để nhận thông tin liên quan tới các cá nhân từ các cơ sở dữ liệu thống kê, trừ phi chúng được áp dụng các biện pháp kiểm soát suy luận thích hợp. *Xem* database security, inference control, statistical database.

linear recurrence relation ***hệ thức truy toán tuyến tính*** Trong mật mã, một hệ thức có dạng:

$$S_{r+n} = d_0S_r + d_1S_{r+1} + ... + d_{n-1}S_{r+n-1}$$

trong đó S là dãy S_0, S_1, S_2...

Các mối quan hệ truy toán tuyến tính được dùng để xác định các đầu ra của các thanh ghi dịch tuyến tính. Nếu các thanh ghi dịch tuyến tính được dùng để tạo ra dãy bit mật mã trong mã dòng, thì điều quan trọng là người mã thám sẽ không thể suy ra hệ thức truy toán tuyến tính từ một đoạn dòng bit

mật mã có sẵn. *Xem* cryptographic bit stream, linear feedback shift register, recursion analysis, stream cipher.

line communications ***liên lạc hữu tuyến, truyền thông hữu tuyến*** Trong truyền thông, sự truyền và nhận các tín hiệu điện qua dây cáp.

line control ***kiểm soát đường truyền*** Trong truyền thông dữ liệu, một dãy các tín hiệu dùng để kiểm soát kênh. *Xem* channel.

line driver ***bộ điều khiển đường truyền*** Trong truyền thông dữ liệu, một thành phần cứng ghép nối với một thiết bị tới đường truyền, cung cấp các chức năng như: thêm các ký tự điều khiển vào tín hiệu ra, thông dịch các ký tự điều khiển trên dữ liệu vào, chuyển đổi truyền song song thành truyền nối tiếp v.v... *Xem* parallel transmission, serial transmission.

line impedance ***trở kháng đường dây, trở kháng đường truyền*** Trong truyền thông, trở kháng của đường truyền viễn thông.

line level ***mức đường truyền; cấp đường truyền*** (1) Trong truyền thông dữ liệu, mức đường truyền là cường độ tín hiệu trên kênh truyền. (2) Trong truyền thông dữ liệu, cấp đường truyền là một tập các giao thức liên quan tới sự truyền trong suốt và kiểm soát dòng bit dọc theo kênh truyền. *Xem* decibel, protocol, transparent.

line load ***tải đường truyền*** Trong truyền thông, lượng lưu lượng trên kênh được biểu thị theo tỷ lệ sử dụng kênh trên khả năng tổng cộng của nó (tính theo %). *Xem* traffic.

line protocol ***giao thức kênh, giao thức đường truyền*** *Đồng nghĩa với* link protocol.

line sensor ***bộ cảm biến đường truyền*** Trong an toàn vật lý, một bộ cảm biến kèm mẫu phát hiện trong phạm vi một kênh dải hẹp nằm giữa hai điểm hoặc nhiều hơn, chẳng hạn chùm tia lade. *Xem* laser intrusion detector, point protection.

line speed ***tốc độ kênh truyền*** Trong an toàn liên lạc, tốc độ truyền tín hiệu đo bằng baud trên một kênh cho trước. Tốc độ thay đổi theo các khả năng của thiết bị được dùng và lượng nhiễu trên kênh. *Xem* baud, Shannon's law.

line termination equipment ***thiết bị cuối đường truyền*** Trong truyền thông dữ liệu, thiết bị cuối mạch dữ liệu thường dùng cho mạch không phải điện thoại. *Xem* data circuit terminating equipment.

line transient ***xung chuyển tiếp đường dây*** Trong truyền thông, một xung điện không mong muốn xuất hiện trong thời gian rất ngắn, thường có thể tạo ra lỗi trong các mạch số đã không thiết kế để tối thiểu hóa các tác động của nhiễu như vậy.

link ***tuyến liên kết; thường trình kết nối*** (1) Trong truyền thông, tuyến liên kết là một nhánh truyền giữa hai điểm có các đặc trưng chỉ ra, ví dụ đường dây điện thoại hoặc chùm tia sóng cực ngắn. Cũng như khía cạnh truyền vật lý, tuyến liên kết gồm các giao thức đi theo các thiết bị và phần mềm, tức là nó cũng có thể là liên kết logic. *Xem* protocol, logical channel. (2) Trong tính

toán, thường trình kết nối là một chương trình kết nối hai chương trình riêng và nhờ đó thông tin điều khiển đi qua được.

linkage ***(sự) nối liền, (sự) móc nối*** Trong an toàn máy tính, sự kết hợp có mục đích dữ liệu hoặc thông tin từ một hệ thống thông tin mà chúng lại lấy từ một hệ thống khác với hy vọng nhận được thông tin bổ sung; trong thực tế, là sự kết hợp trên máy tính các tệp từ hai hay nhiều nguồn. *Xem* computer matching.

link encryption ***mã kết nối, mã liên kết*** (1) Trong mật mã, mã điểm nối điểm trong phạm vi mỗi kết nối trong mạng liên lạc. (2) Trong an toàn liên lạc, sự áp dụng các hoạt động mật mã trực tuyến cho một kết nối của một hệ thống liên lạc để tất cả các thông tin chuyển qua nó trên tuyến kết nối đều được mã hóa trọn vẹn. *Xem* online crypto-operation. *So sánh với* end-to-end encryption, node encryption. *Xem* network encryption, OSI security. *Đồng nghĩa với* data link encryption, link to link encryption.

link to link encryption ***mã qua các điểm kết nối*** *Đồng nghĩa với* data link encryption, link encryption.

liquid crystal display ***màn hình tinh thể lỏng*** Trong tính toán, một thiết bị hiện hình làm bằng hai tấm kính ở giữa có loại chất lỏng đặc biệt. Chất lỏng sẫm màu lại khi tác dụng điện áp.

Lisbon ***virut Lisbon*** Trong an toàn máy tính, một loại virut máy tính lây nhiễm các tệp COM, phá hoại chương trình và các tệp OVL. *Xem* virus names.

list ***danh sách, danh mục//lập danh sách, liệt kê*** (1) Trong tính toán, danh sách là một tập sắp xếp các mục dữ liệu. *So sánh với* stack. (2) Trong tính toán, lập danh sách là tác động in hay hiển thị các đề mục dữ liệu đáp ứng các tiêu chuẩn chỉ ra. *So sánh với* write.

Little Pieces ***virut Little Pieces*** Trong an toàn máy tính, một loại virut máy tính làm chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COM và EXE, tác động trong thời gian chạy, phá hoại chương trình và các tệp OVL. *Xem* virus names.

load ***nạp, tải*** Trong tính toán, việc nhập dữ liệu hay chương trình vào bộ nhớ máy tính từ thiết bị lưu trữ bổ trợ.

loading ***(sự) đặt phụ tải, (sự) gia cảm*** Trong truyền thông, phương pháp cải thiện đặc trưng truyền dẫn của một đường dây điện thoại bằng cách gài một loạt các cuộn cảm dọc đường dây ở những khoảng cách bằng nhau.

load life ***tuổi thọ thiết bị*** Trong truyền thông, số giờ một thiết bị có thể tiêu tán năng lượng dưới những điều kiện thao tác chỉ ra khi duy trì hiệu suất hoạt động quy định.

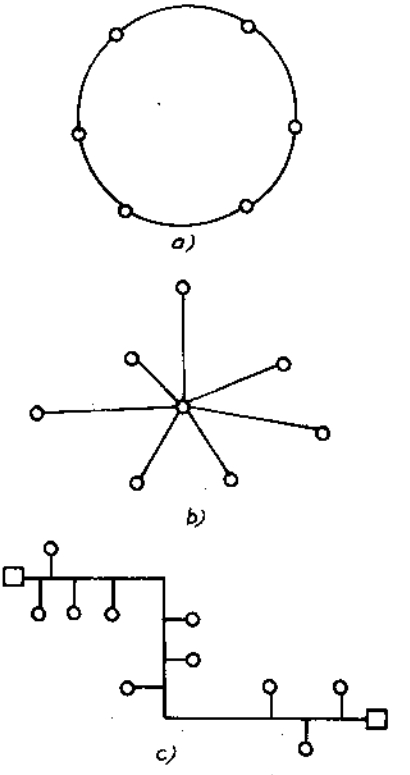
load sharing ***(sự) chia tải*** Trong các mạng máy tính, một kỹ thuật trong đó các máy tính trên mạng chia sẻ các tải làm việc để có sự phân phối đều và hợp lý. Điều này đạt được bằng cách giảm bớt tải do công việc từ máy tính có tải lớn cho những máy tính tải ít hơn. *Xem* job.

loan utilization ***tận dụng khoản vay*** *Đồng nghĩa với* current utilization.

local alarm system ***hệ thống báo động tại chỗ*** Trong an toàn vật lý, một hệ thống báo động độc lập được thiết kế để bảo vệ các tài sản của người sử dụng, thường thì nó là thiết bị âm thanh; có thể nối hoặc không nối với trạm trung tâm ở xa. *Xem* central station.

local area network ***mạng cục bộ, mạng địa phương, mạng LAN*** Trong truyền thông dữ liệu, một mạng liên lạc hai chiều ở dải thông cao hoạt động trên vùng địa lý hạn chế, điển hình là một toà nhà văn phòng hay một trường đại học. Động cơ phát triển các mạng LAN này sinh từ sự phát triển các máy tính nhỏ và máy vi tính trong các tổ chức lớn và xu hướng cung cấp cho các nhân viên văn phòng các thiết bị thông tin: fax, bộ xử lý từ, video và các hệ thống tiếng nói... Người ta muốn đưa vào sử dụng một biện pháp liên lạc thống nhất giữa các thiết bị khác nhau. LAN cung cấp cho người dùng máy tính cơ hội liên lạc với những người khác, cơ hội cung ứng và truy nhập tới dữ liệu chung và chia sẻ các thiết bị ngoại vi đắt tiền, các thiết bị lưu trữ trên đĩa cứng, các máy in phức tạp...

LAN gồm một mạng lưới dây cáp kết nối tới các nút thành phần. Mỗi nút tương ứng với một trạm làm việc của người sử dụng được trang bị một thiết bị giao tiếp mạng vật lý. Topo mạng có thể là vòng, hình sao hay dạng tuyến... Mạng hình sao là mạng logic kế thừa theo máy tính cỡ lớn truyền thống - cấu hình nhiều thiết bị đầu cuối, mặc dù có giao thức truy nhập đơn giản song nó có ba nhược điểm: khi bộ điều khiển trung tâm bị ngắt điện sẽ gây hỏng mạng, tốc độ thấp tại các nút cổ chai và hệ thống đường dây lớn. Xu hướng hiện nay ưa thích các cấu hình dạng vòng và dạng tuyến hơn.



local area network: *mạng cục bộ*.
a) vòng; b) hình sao; c) dạng tuyến.

Chế độ truyền có thể ở dải gốc, hoặc ở dải rộng; môi trường truyền dẫn có thể là cặp dây đồng xoắn, cáp đồng trục hoặc cáp quang. Các giao thức truy nhập có sẵn đối với các mạng vòng và tuyến là CSMA-CD, giao thức này kiểm soát thẻ bài hoặc khe thông báo. Thành công của mạng LAN phụ thuộc vào sự tin tưởng của những người dùng trong

việc thiết lập các chuẩn để bảo đảm kết nối và thao tác không bị trở ngại trong rất nhiều thiết bị khác nhau của người sử dụng.

Hai chuẩn chung là Ethernet và Cambrride Ring. Những hệ khác dùng các giao thức CSMA-CD thường được coi là thuộc kiểu Ethernet. IBM cũng đã phát triển một chuẩn LAN dùng cấu hình dạng vòng ở dải gốc và giao thức chuyển thẻ bài. ECMA đã phê chuẩn chuẩn LAN tương thích với Ethernet vào năm 1982.

Một nghiên cứu quan trọng đối với người sử dụng mạng LAN là cạc ghép nối nối trạm làm việc với mạng. Các cấu trúc bus tốc độ cao nội bộ trong máy tính thuận tiện cho việc nối tới LAN và cạc ghép nối được cắm rất đơn giản vào tấm sau của máy. Cạc ghép nối cũng chứa các phần mềm để điều khiển sự chuyển dữ liệu. Cấu trúc 7 tầng ISO-OSI rất quan trọng trong thiết kế theo chuẩn LAN, đặc biệt ở nơi các mạng LAN đòi hỏi các cổng nối tới các mạng LAN khác và mạng diện rộng. *So sánh với* metropolitan area network, wide area network. *Xem* blackplane, bandwidth, baseband, Cambridge Ring, coaxial cable, control token, CSMA-CD, ECMA, Ethernet, facsimile, fiber optics, gateway, ISO/OSI, LAN security, message slot, node, protocol, topology, twisted pair, videotext.

local echo ***vọng cục bộ, vọng tại chỗ*** Trong truyền thông dữ liệu, một kỹ thuật dùng phần mềm liên lạc trong máy tính mà bên phát sẽ hiển thị dữ liệu được truyền lên kênh liên lạc trên thiết bị đầu cuối cục bộ. *So sánh với* echoplex. *Xem* terminal. *Đồng nghĩa với* local software echo.

local fire alarm system ***hệ thống báo cháy tại chỗ*** Trong an toàn vật lý, một hệ thống điện tử sẽ tạo ra tín hiệu báo động tại một hay nhiều nơi trong khu vực bảo vệ. *Xem* local alarm system.

local mode ***chế độ tại chỗ, chế độ cục bộ*** Trong truyền thông dữ liệu, một trạng thái hoạt động nội tại của thiết bị đầu cuối dữ liệu. Trong trạng thái đó, thiết bị đầu cuối không thể nhận tín hiệu gọi đến được.

local network ***hệ thống cục bộ, mạng cục bộ*** Trong hoạt động ngân hàng, một hệ thống trong đó trình phân phát và kiểm tra thông tin về khách hàng (issuer) trên thẻ và trình nhận và kiểm tra thông tin về khách (acquirer) trên thẻ đều trên một thiết bị và giống nhau. *So sánh với* interchange, local area network. *Xem* acquirer, issuer.

local noninterfering coded station ***trạm báo cháy dùng tín hiệu mã không nhiễu cục bộ*** Trong an toàn vật lý, một trạm báo động hỏa hoạn để khi hoạt động sẽ phát không ít hơn bốn vòng các tín hiệu báo động đã mã, không bị ngắt. *Xem* coded system, alarm station, positive noninterfering and succession coded station.

local software echo ***vọng mềm cục bộ*** *Đồng nghĩa với* local echo.

local transaction ***giao tác cục bộ, giao dịch địa phương*** Trong hoạt động ngân hàng, một giao tác giữa máy trả tiền từ xa ATM hoặc EFTPOS và cơ quan tài chính là những nơi cùng phát

hành thẻ và kiểm soát thiết bị đầu cuối. *So sánh với* interchange transaction. *Xem* ATM, PIN management and security EFTPOS.

lock ***khóa*** (1) Trong tính toán, cơ chế kiểm soát các đa truy nhập tới một thiết bị chung như bus hay bộ nhớ. *Xem* bus. (2) Trong tính toán, *xem* file lock, record lock.

lock-and-key protection system ***hệ thống bảo vệ bằng khóa và chìa*** Trong an toàn máy tính, một hệ thống bảo vệ gồm cả chức năng so khớp khóa hay mật khẩu với một yêu cầu truy nhập chỉ ra. *Xem* access, key, password.

locking ***(sự) bám sát*** Trong truyền thông, một thuật ngữ được sử dụng cho quá trình đồng bộ một nguồn tín hiệu lặp đi lặp lại thông qua các tín hiệu định thời.

lockout ***ngăn chặn, đóng lại, khóa chặn*** (1) Trong các thiết bị ngoại vi, một hoạt động bàn phím chỉ ghi nhận sự ấn phím đầu tiên khi một số phím được ấn đồng thời. (2) Trong cơ sở dữ liệu, một kỹ thuật được thiết kế để tránh sự cập nhật không thống nhất. Chỉ một người sử dụng được phép truy nhập tới mục dữ liệu để cập nhật hoặc thay đổi vào bất kỳ lúc nào. Nhược điểm của kỹ thuật này là nó có thể dẫn tới sự tắc nghẽn hẳn. Nếu những người sử dụng Alice và Bob cùng muốn cập nhật một cặp bản ghi đồng thời X và Y thì việc khóa chặn có thể dẫn tới các tình huống không mong muốn sau:

- Alice yêu cầu X;
- Bob cần Y;
- Alice cần Y nhưng nó bị Bob khóa lại;
- Bob yêu cầu X nhưng nó bị Alice khóa.

Xem record, update inconsistency. (3) Trong truyền thông, sự không có khả năng gọi được của người thuê bao trên mạch (được điều khiển qua bộ triệt âm dội để có sự thông suốt tới người gọi) do tạp âm quá nhiều hoặc do tiếng nói liên tục từ một thuê bao. *Xem* echo suppressor. (4) Trong tính toán, một kỹ thuật dùng để ngăn chặn sự truy nhập tới dữ liệu quan trọng bởi hai chương trình riêng biệt trong môi trường đa chương trình. *So sánh với* lock up. *Xem* file lock, record lock.

lock up ***trạng thái treo, treo*** Trong tính toán, một trạng thái không mong muốn của hệ thống làm chương trình không thoát ra được, chẳng hạn trạng thái tắc nghẽn trong khi yêu cầu về các tài nguyên chung. *So sánh với* lockout.

lockword ***từ khóa*** Trong an toàn dữ liệu, mật khẩu đi theo tệp hay bộ dữ liệu. Một người tạo tệp có thể chỉ ra một từ khóa và sau đó những người sử dụng phải nhập từ khóa vào mới truy nhập được tới tệp hay bộ dữ liệu. Nếu từ khóa bị lộ cho những người sử dụng khác thì người dùng đó thông thường sẽ chỉ được phép truy nhập đọc tới tệp, chỉ có người tạo mới có sự kết hợp duy nhất về kiến thức từ khóa và danh tính người sử dụng cần thiết cho truy nhập ghi. *Xem* database security, data set, file access, password.

loco ***độ từ kháng*** *Xem* coercivity card. *Đồng nghĩa với* low coercivity.

log ***sổ nhật ký, tệp theo dõi*** Tệp hồ sơ hay tệp nhật ký ghi lại dãy các sự

kiện về các công việc thực hiện trên máy tính.

logarithm ***loga*** Trong toán học, lũy thừa mà một cơ số phải nâng lên để bằng số đã cho. Như vậy, theo số học thập phân, loga của 100 (với cơ số 10) là 2 vì $10^2 = 100$. *Xem* base.

logging ***bản ghi chép theo dõi*** Trong tính toán, một bản ghi được lập ra thủ công hoặc bằng hệ thống máy tính để theo dõi các sự kiện xảy ra đối với hệ thống. *Xem* security log.

logic ***(mạch) logic*** Trong tính toán, các mạch vật lý thực hiện các phép tính và các chức năng logic. *Xem* logical operator.

logical ***(thuộc) logic // lượng logic*** (1) Logic là dựa trên quan niệm hay thực thể ảo khi so sánh về mặt vật lý hay về mặt thực tế. (2) Trong tính toán, lượng logic là đại lượng hai trạng thái mà có thể được lưu giữ như một bit đơn lẻ. Thường được dùng như các cờ trạng thái. *Xem* bit, flag.

logical access control ***kiểm soát truy nhập logic*** Trong kiểm soát truy nhập, việc sử dụng các thủ tục liên hệ với thông tin và tri thức, chẳng hạn như các mật khẩu, thay vì các thủ tục an toàn vật lý. *So sánh với* physical security.

logical channel ***kênh logic*** Trong truyền thông dữ liệu, một mạch được dùng cho thao tác chuyển mạch gói giữa các thiết bị đầu cuối và các nút mạng. Mạch có thể là một kết nối ảo thường trực hoặc một thiết lập trong khoảng thời gian gọi. *Xem* packet switching, permanent virtual circuit, virtual circuit.

logical completeness measure ***độ đầy đủ logic*** Trong an toàn máy tính, phương tiện đánh giá tính hiệu quả và mức độ mà một tập cơ chế kiểm soát truy nhập đáp ứng các yêu cầu của một tập các đặc tả an toàn. *Xem* access control mechanisms.

logical database ***cơ sở dữ liệu logic*** Trong cơ sở dữ liệu, một cơ sở dữ liệu theo cách nhìn của người sử dụng. Cấu trúc dữ liệu này không cần giống với cơ sở dữ liệu vật lý. *So sánh với* physical database.

logical data independence ***tính độc lập dữ liệu logic*** Trong cơ sở dữ liệu, tính chất của cấu trúc của dữ liệu cho phép một sơ đồ được thay đổi mà không làm ảnh hưởng tới cách nhìn về dữ liệu của người lập trình ứng dụng. *So sánh với* physical data independence. *Xem* data independence, scheme.

logical expression ***biểu thức logic*** Trong toán học, một mệnh đề chứa các toán tử logic và các toán hạng và có thể quy về giá trị chỉ có thể hoặc đúng hoặc sai. Ví dụ, công thức hàm Boole EXCLUSIVE OR: $Z = (A$ AND NOT $B)$ OR (NOT A AND B) là một biểu thức logic. *Xem* Boolean algebra, EXCLUSIVE OR, logical operator.

logical operator ***toán tử logic*** Trong tính toán, một toán tử có thể được dùng trong biểu thức logic để biểu thị phép tính cần được thực hiện trên các số hạng trong biểu thức. Các toán tử logic là AND, OR và NOT. Tất cả các biểu thức logic có thể được biểu diễn theo ba toán tử logic cơ bản này.

logical party ***nhóm logic*** Trong quản lý khóa, một thành viên đại diện cho một hay nhiều nhóm vật lý trong cặp liên lạc. *Xem* communicating pair.

logical record ***bản ghi logic*** Trong tính toán, một bản ghi được xác định theo các chức năng hơn là theo nghĩa vật lý mà nó được lưu trữ. *So sánh với* physical record. *Xem* record.

logical security ***an toàn logic*** Trong an toàn dữ liệu, tính an toàn do hệ điều hành và phần mềm cơ sở cung cấp. *So sánh với* physical security. *Xem* operating system.

logical threat ***hiểm họa logic, mối đe dọa logic*** Trong an toàn máy tính, một hiểm hoạ về khả năng phá hoại hay thay đổi phần mềm hoặc dữ liệu. Nó được hiện thực hóa bởi sự thao tác thủ công về mặt logic hơn là bởi sự tấn công về mặt vật lý. Ví dụ, một hiểm hoạ có thể nảy sinh từ kẻ sử dụng bất hợp pháp có động cơ không trung thực, hoặc từ người sử dụng bất hợp pháp - kẻ xoay xở để truy nhập tới hệ thống trên mạng tại chỗ hoặc từ một vị trí ở xa. *So sánh với* accidental threat, active threat, deliberate threat, passive threat, physical threat. *Xem* threat.

logical unit ***khối logic, đơn vị logic, bộ logic*** Trong truyền thông dữ liệu, một cổng từ đó người sử dụng có thể truy nhập tới các dịch vụ của mạng. *Xem* port.

logic bomb ***bom logic*** Trong an toàn máy tính, một dạng con ngựa thành Torroa có hành vi ác ý sẽ khởi sự khi có sự kiện đặc biệt xảy ra, chẳng hạn số lần chạy chương trình. *So sánh với* time bomb. *Xem* malicious code, Trojan Horse.

logic circuit ***mạch logic*** Trong tính toán, một mạch chứa một hoặc nhiều cửa để thực hiện một chức năng logic cụ thể.

logic path analysis program ***chương trình phân tích rẽ nhánh logic*** Trong tính toán, một tiện ích phần mềm chuyển một chương trình nguồn thành một biểu đồ cấu trúc hay một lưu đồ. Người kiểm toán viên có thể dùng nó để hiểu về tính logic của chương trình. *Xem* computer audit packages.

log in ***đăng nhập*** *Đồng nghĩa với* log on.

log off ***ra khỏi mạng, rời hệ thống*** Trong tính toán, một lệnh mà người sử dụng đưa ra để hệ thống máy tính chấm dứt phiên làm việc. *So sánh với* log on. *Đồng nghĩa với* log out.

log on ***đăng nhập, vào mạng*** (1) Trong kiểm soát truy nhập, thủ tục được dùng để định danh người sử dụng và mức ủy quyền và truy nhập được phép. *Đồng nghĩa với* log in, sign in, sign on. (2) Trong tính toán, một yêu cầu của người sử dụng được truy nhập vào một máy tính, thường là hệ thống chia sẻ thời gian. Lúc khởi đầu một nối, người sử dụng có thể phải cung cấp danh tính như số tài khoản và mật khẩu. *So sánh với* log off. *Xem* time sharing, password. *Đồng nghĩa với* log in.

log out ***rời hệ thống*** *Đồng nghĩa với* log off.

long haul network ***mạng tầm xa***

Trong truyền thông dữ liệu, những mạng nối với máy tính chủ ở các thành phố khác dùng mạng điện thoại công cộng, liên lạc vệ tinh... *Xem* host.

longitudinal party check ***kiểm tra chẵn lẻ dọc*** (1) Trong tính toán, một kiểm tra tính chẵn lẻ trên một nhóm các chữ số nhị phân dọc theo mỗi rãnh ghi trên băng từ. (2) Trong truyền thông dữ liệu, một hệ thống kiểm tra lỗi ở mỗi trạm thu sau khi một ký tự kiểm tra khối được tích lũy. *Xem* block character check, parity checking.

longitudinal redundancy check ***kiểm tra dư thừa dọc*** Trong các mã, kỹ thuật mã dư dùng một byte kiểm tra 8 bit cho mỗi khối dữ liệu truyền đi. Bit trọng số lớn nhất của byte kiểm tra cung cấp một bit kiểm tra tính chẵn lẻ cho các bit trọng số lớn nhất của các ký tự trong khối và tiếp tục cho tất cả các vị trí bit khác. *Xem* bit, byte, parity checking, redundant code, X-modem.

long key ***khóa dài*** Trong mật mã, một chuỗi ký tự được dùng ở dạng dễ nhớ của khóa trong tương ứng. *Xem* key crunching, native key.

loop ***vòng lặp, vòng*** (1) Trong tính toán, một dãy các lệnh lặp lại cho tới khi thoả mãn điều kiện đặt ra nào đó. (2) Trong truyền thông, một kết nối hay một kênh.

loopback test ***thử mạch ngược vòng*** Trong truyền thông, một phương pháp cách ly lỗi trên mạch vòng cục bộ tại đó tín hiệu được gửi đi từ trạm thử trên modem và quay trở lại modem. *Xem* MODEM.

loop checking ***kiểm tra vòng lặp*** Trong truyền thông dữ liệu, một phương pháp phát hiện các lỗi truyền trong đó dữ liệu thu được được quay trở lại trạm phát để so sánh với dữ liệu ban đầu.

loophole ***hở vòng*** Trong an toàn máy tính, một lỗi bỏ sót hoặc quên trong phần mềm hoặc cứng tạo điều kiện phá vỡ quá trình kiểm soát truy nhập. *Xem* access control. *Đồng nghĩa với* fault, flaw.

loop network ***mạng vòng lặp*** Trong truyền thông, một cấu hình mạng có một tuyến đơn qua tất cả các nút và tuyến là một mạch kín. *So sánh với* star. *Xem* node, ring.

loop plant ***thiết bị vòng*** Trong truyền thông, tất cả các cáp, ống dẫn, các hộp nối, các buồng và thiết bị hỗ trợ được dùng để nối các thuê bao tới các tổng đài hay đài địa phương.

loro account ***tài khoản của bên thứ ba, tài khoản loro*** Trong hoạt động ngân hàng, một tài khoản được một ngân hàng phục vụ nhân danh ngân hàng chủ sở hữu tài khoản.

loss ***thất thoát, tổn hao*** (1) Trong quản lý rủi ro, đại lượng đo định lượng sự mất mát tài nguyên hệ thống. *Xem* annual loss expectancy, threat, vulnerability. (2) Trong truyền thông, một thuật ngữ chung chỉ thất thoát năng lượng tín hiệu trong quá trình truyền trên dây, được biểu thị như tỷ số công suất tín hiệu tại điểm bắt đầu mạch nối trên công suất tín hiệu tại máy thu và được đo theo dexiben. *Xem* attenuation, decibel, signal.

low coercivity ***độ từ kháng thấp***

Trong kiểm soát truy nhập, một thuật ngữ được dùng cho các thẻ sọc từ trong đó chất liệu từ có độ từ kháng khoảng 300 ơstet. *So sánh với* high coercivity. *Xem* coercivity, high coercivity card, oersted.

low level language ***ngôn ngữ bậc thấp*** Trong tính toán, một ngôn ngữ liên quan chặt chẽ tới ngôn ngữ mã máy của máy tính, tức ngôn ngữ được dịch bởi hợp ngữ. *So sánh với* high level language.

low speed ***tốc độ thấp*** Trong truyền thông dữ liệu, những hệ thống hoạt động ở tốc độ nhỏ hơn 2400 bit/giây.

low water mark ***mốc an toàn thấp*** Trong an toàn dữ liệu, nói tới hai hay nhiều mức an toàn, thấp nhất trong các bậc phân loại và giao tập hợp của loại hình không phân cấp. *Xem* Bell-La Padula model.

LRC ***kiểm tra dư thừa dọc*** *Xem* longitudial redundancy check.

LTE ***thiết bị LTE, thiết bị đầu cuối đường dây*** *Xem* line terminal equipment.

Lucipher ***mã pháp Lucipher*** Trong mật mã, một mã tích do IBM phát triển, lập nên cơ sở cho sự phát triển của các chuẩn mã dữ liệu. Nó dùng các khối dữ liệu 128 bit và khóa 128 bit. *Xem* data encryption standard, product cipher.

L



MAA *Xem* message authentication algorithm.

MBA *Xem* message authentication block.

MAC *Xem* mandatory access control, medium access control, message authentication code. *Đồng nghĩa với* AC, DAC.

machine code instruction ***lệnh mã máy*** Trong tính toán, một lệnh được biểu thị theo ngôn ngữ máy cho bộ xử lý riêng. Các lệnh ngôn ngữ bậc thấp và cao cuối cùng đều được dịch thành các lệnh máy tương ứng trước khi chúng được bộ xử lý thực hiện. *Xem* high level language, low level language, machine language.

machine independence ***độc lập với máy*** Trong tính toán, nói tới triết lý thiết kế phần mềm cho phép các chương trình viết cho loại máy tính này chạy được trên loại máy tính khác mà không cần thay đổi lại chương trình. *Xem* portability.

machine language ***ngôn ngữ máy*** Trong tính toán, một ngôn ngữ cho các chương trình biểu thị trực tiếp ở dạng nhị phân mà các thiết bị xử lý trung tâm có thể chấp nhận được. Tất cả các ngôn ngữ lập trình khác, bậc thấp hay cao đều được dịch ra thành mã máy nhị phân trước khi được thi hành trong khối xử lý trung tâm. *So sánh với* high level language, low level language. *Xem* machine code instruction, translator.

MAC residue ***thặng dư MAC, phần dư MAC*** Trong xác thực, 32 bit trong tổng kiểm tra 64 bit đầu ra được tạo ra để lập nên MAC, nghĩa là không được chuyển đi như một phần của khối xác thực. *Xem* checksum, MAC, transaction key system.

macrobend loss ***mất mát do uốn cong nhiều*** Trong truyền thông, sự rò rỉ ánh sáng khi cáp quang bị uốn cong. *So sánh với* microbend loss. *Xem* fiber optics.

magnetically encoded card *thẻ mã bằng từ tính* Trong kiểm soát truy nhập và ngân hàng, thẻ có thể được dùng để kiểm soát truy nhập hoặc để ủy quyền khởi đầu cuộc giao dịch. Thẻ chất dẻo chứa thông tin được mã bằng từ tính trên bề mặt hoặc được nhúng trong nó. Thẻ có thể chứa đốm từ tính, vạch từ hoặc kiểu hiệu ứng Wiegand. *So sánh với* smart card. *Xem* magnetic spot card, magnetic stripe card, Wiegand effect.

magnetic disk *đĩa từ* Trong tính toán, một đĩa phẳng có lớp bề mặt từ hóa, trên đó có thể lưu dữ liệu bằng cách ghi từ tính. Có hai loại đĩa chính: cứng và mềm, loại đĩa cứng dùng đế kim loại hay kính, loại đĩa mềm có đế bằng chất dẻo uốn được. Đĩa cứng quay ở tốc độ cao (2400 vòng trên phút) sao cho có thể truy nhập tới dữ liệu không quá chậm. Đĩa được định dạng logic thành các rãnh, mỗi rãnh có một số cung. *Xem* floppy disk, hard disk.

magnetic field intensity *cường độ từ trường* Trong điện tử, lực từ cần thiết để tạo ra thông lượng từ mong muốn, được ký hiệu là *H*. *Xem* oersted.

magnetic flux *từ thông, thông lượng từ* Trong điện tử học, các đường lực biểu diễn từ trường. *Xem* magnetic field intensity.

magnetic remanence *độ cảm ứng từ dư* *Xem* remanence.

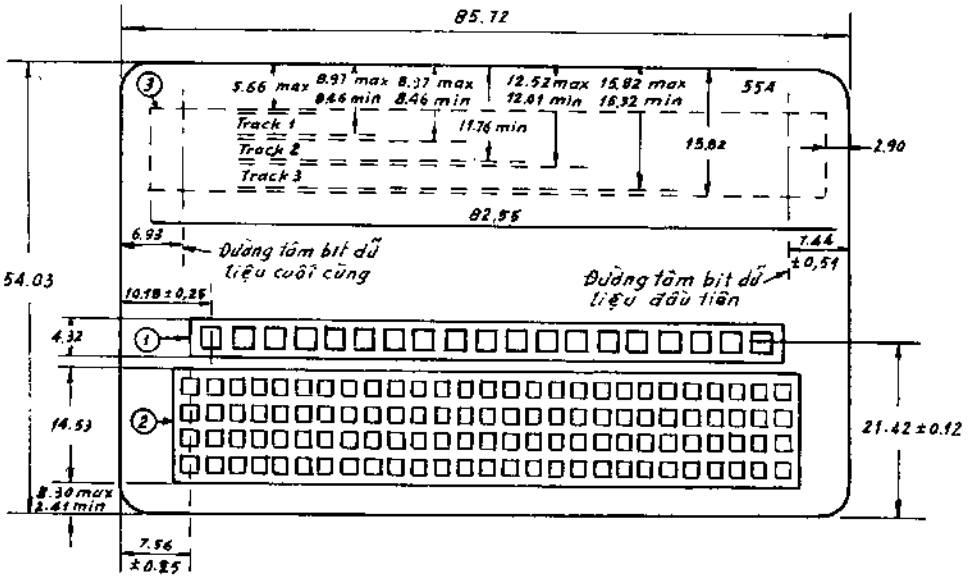
magnetic saturation *(sự) bão hòa từ* Trong điện tử, trạng thái trong đó sự tăng lực từ hóa sẽ tạo nên hay dẫn đến tăng chút ít hoặc không tăng thông lượng từ. *Xem* magnetic flux.

magnetic sensor *bộ cảm biến từ* Trong an toàn vật lý, bộ cảm biến hoạt động thông qua việc phát hiện một sự thay đổi trong từ trường. *So sánh với* electric field sensor.

magnetic spot card *cạc chấm từ, thẻ vệt từ* Trong kiểm soát truy nhập, một cạc có các vệt từ được gắn sâu trong chất liệu dát mỏng để tạo mã cho bộ phận nhận dạng duy nhất. *So sánh với* magnetic stripe card, Wiegand effect. *Xem* magnetically encoded card.

magnetic stripe card *cạc vạch từ, thẻ sọc từ* Trong kiểm soát truy nhập và ngân hàng, một tấm cạc bằng chất dẻo có một vạch từ hẹp có thể dùng để kiểm soát truy nhập hoặc làm căn cứ để khởi đầu cuộc giao dịch. Dữ liệu thông thường được mã theo ba rãnh dọc theo vạch từ. Các từ trường có thể có cường độ thấp hoặc cao, trường cường độ thấp dùng cho các thẻ tín dụng, trong khi các hệ thống kiểm soát truy nhập an toàn cao lại dùng trường cường độ cao vì nó cho độ ổn định cao hơn. Các tấm cạc có vạch từ có thể được mã hay mã lại bằng thiết bị tương đối rẻ tiền, bởi vậy, đôi khi người ta dùng các vạch từ đặc biệt để ngăn chặn việc làm các tấm cạc giả. *So sánh với* magnetic spot card, Wiegand effect. *Xem* sandwich tape. Watermark tape. *Đồng nghĩa với* mag stripe card.

magnetic tape *băng từ* Trong tính toán, một phương tiện lưu trữ phổ dụng dữ liệu và phần mềm máy tính. Trong các ứng dụng máy tính cá nhân, băng từ có độ rộng 1/2 hoặc 1/4 insơ và chứa lớp từ tính có các hạt oxit sắt nhỏ mịn lơ lửng trong chất liên kết trơ



magnetic stripe card: *thẻ sọc từ*. Kích thước theo milimet.
① Đường số tài khoản; ② Tên và vùng địa chỉ; ③ Vùng sọc từ (đảo lại).

trên nền polyeste. Băng từ được cất trong cuộn caset hoặc hộp băng. *So sánh với* magnetic disk.

mag stripe card ***thẻ sọc từ*** *Đồng nghĩa với* magnetic stripe card.

mail box ***hộp thư điện tử*** *Xem* electronic mail.

mainframe ***máy chính, máy tính cỡ lớn, máy tính trung tâm*** Trong tính toán, một thuật ngữ thường gắn liền với việc cài đặt một máy tính đa dụng lớn, phục vụ những phần chính của một tổ chức hay một viện nghiên cứu. *So sánh với* microcomputer.

main memory ***bộ nhớ chính*** Trong tính toán, một phần của máy tính để lưu giữ các dữ liệu và chương trình để các khối xử lý trung tâm truy nhập ngẫu nhiên tới ở dạng các chữ số nhị phân. Bộ lưu trữ và bộ nhớ là một. Bộ nhớ chính thường truy nhập nhanh song đo giá cả còn tương đối đắt nên kích thước của nó thường bị hạn chế.

maintainability ***khả năng bảo trì*** Trong tính toán, khả năng cần thiết để định vị và giữ cố định lỗi sai trong một chương trình hoạt động.

maintenance ***bảo trì, bảo dưỡng; bảo trì phần mềm*** (1) Trong kỹ thuật tin cậy, bảo trì là hoạt động bất kỳ nhằm giữ cho máy ở trong điều kiện hoạt động chỉ ra, nó bao gồm cả bảo trì phòng ngừa và bảo trì sửa chữa. *Xem* preventive maintenance, corective maintenance. (2) Trong tính toán, bảo trì phần mềm, *xem* software maintenance.

make v. buy ***làm hay mua*** Trong tính

toán và truyền thông dữ liệu, sự lựa chọn mà người quản lý chính phải tiến hành trong việc hoặc phát triển phần mềm trong tổ chức, hoặc mua các sản phẩm/dịch vụ của những nhà cung cấp khác.

malfunction ***trục trặc, sai chức năng, sự cố*** Trong an toàn thông tin, một hỏng hóc trong hoạt động của phần cứng trong hệ thống.

malicious code ***mã ác ý, lệnh ác ý*** Trong an toàn thông tin, một đoạn phần mềm cố tình đưa vào trong hệ thống nhằm mục đích gây mất mát hoặc tổn hại (ví dụ con ngựa thành Toroa). *Xem* blob, check kiting, cookie monster, flying dutchman, french round-off, logic bomb, malicious logic, Morris worm, salami technique, time bomb, trapdoor, Trojan Horse, virus, worm.

malicious logic ***logic ác ý, logic độc hại*** Trong an toàn máy tính, phần cứng, phần mềm hoặc phần sụn cố ý đặt trong hệ thống để gây mất mát hay tổn hại thông tin (chẳng hạn con ngựa thành Toroa). *Xem* malicious code, Trojan Horse.

malware ***phần mềm ác ý*** Trong an toàn máy tính, phần mềm chứa những đoạn mã ác ý. *Xem* malicious code. *Đồng nghĩa với* vandalware.

MAN *Xem* metropolitan area network, municipal area network.

managed data network ***mạng dữ liệu có quản lý*** Trong truyền thông, việc dùng một tổ chức dịch vụ độc lập để quản lý hoặc điều khiển các cuộc liên lạc dữ liệu của các tập đoàn. *So sánh với* value added network service.

Manchester encoding ***mã hóa Manchester*** Trong truyền thông dữ liệu, một phương pháp mã biến đổi dữ liệu nhị phân để truyền đảm bảo mỗi bit 1 hoặc 0 sẽ tạo nên một chuyển tiếp tín hiệu trong mỗi chu kỳ bit. Bit 1 được mã biến đổi thành tín hiệu cao trong nửa chu kỳ đầu và một tín hiệu thấp trong nửa sau. Bit 0 được mã biến đổi thành tín hiệu thấp sau đó là tín hiệu cao.

mandatory access control ***kiểm soát truy nhập bắt buộc*** Trong kiểm soát truy nhập, một biện pháp hạn chế truy nhập tới các đối tượng dựa trên tính nhạy cảm (như được biểu diễn bằng một nhãn) của thông tin chứa trong các đối tượng và sự cấp phép hình thức (chẳng hạn mức truy nhập - clearance) cho các chủ thể truy nhập tới thông tin có tính nhạy cảm như vậy. *So sánh với* discretionary access control. *Xem* object, sensitivity label, subject.

mandatory security ***an toàn bắt buộc*** (1) Trong an toàn máy tính, sự áp đặt các biện pháp an toàn trên các thực thể. (2) Trong an toàn máy tính, khía cạnh của chính sách an toàn được các nhà quản trị hệ thống nhấn mạnh, nó đòi hỏi cung các dịch vụ an toàn cho một hay nhiều trường hợp cá biệt trong truyền thông. *So sánh với* discretionary security.

mandatory security policy ***chính sách an toàn bắt buộc*** Trong kiểm soát truy nhập, một chính sách kiểm soát truy nhập trong đó quyền của người sử dụng truy nhập tới một tập dữ liệu được xác định trên cơ sở mức truy nhập (clearance) an toàn của người

dùng và phân loại an toàn của dữ liệu, ví dụ một người dùng được phân mức truy nhập tới mức mật sẽ không được phép đọc một tệp có phân loại tối mật. *So sánh với* discretionary access control. *Xem* mandatory security.

manipulation detection ***phát hiện thao tác*** Trong an toàn dữ liệu, một cơ chế dùng để phát hiện liệu một đơn vị dữ liệu có bị thay đổi (hoặc cố ý hoặc không) hay không.

man-made noise ***tạp âm nhân tạo*** Trong truyền thông, nhiễu do các thiết bị điện tử, hệ thống mồi lửa của ôtô v.v. gây ra. *Xem* interference.

man month ***khối lượng công việc/tháng, người tháng*** Lượng công việc hữu ích mà một cá nhân sẽ đóng góp khi giải quyết một nhiệm vụ đặt ra trong một tháng; nó thường được dùng để định giá việc viết một chương trình hay thiết kế một hệ thống.

manual alarm initiating device ***thiết bị khởi báo bằng tay*** Trong an toàn vật lý, một thiết bị tiếp âm tín hiệu báo động khi nó được vận hành bằng tay. *So sánh với* automatic alarm initiating device.

manufacturing automation protocol ***giao thức tự động hóa sản xuất*** Trong truyền thông dữ liệu, một giao thức được phát triển để liên lạc trong môi trường tự động hóa của nhà máy. *So sánh với* technical and office protocol.

MAP *Xem* manufacturing automation protocol.

mapping ***ánh xạ*** (1) Trong toán học, một mối quan hệ giữa hai hay nhiều đại lượng. (2) Trong cơ sở dữ liệu, mối quan hệ giữa một cấu trúc logic cho trước và biểu diễn vật lý của nó trên máy tính. *Xem* logical database, physical database.

Mardi Bros ***virut Mardi Bros*** Trong an toàn máy tính, một loại virut chấm dứt và thường trú trong bộ nhớ, lây nhiễm tới các thiết bị đầu cuối và secto khởi động của đĩa cứng, làm hỏng secto khởi động, ảnh hưởng tới hoạt động lúc chạy. *Xem* virus names.

Marion ***phương pháp phân tích rủi ro Marion*** Trong quản lý rủi ro, một phương pháp luận phân tích rủi ro. *Xem* risk analysis methodologies.

mark ***xung đánh dấu, dấu, dấu hiệu*** Trong truyền thông, một xung trên mạch dữ liệu tương ứng với điều kiện hoạt động của máy thu. *So sánh với* space. *Xem* bit.

marking ***(sự) đánh dấu*** Trong an toàn dữ liệu, quá trình đặt một ký tự ghi rõ tính nhạy cảm (ví dụ "mật") cùng với dữ liệu sao cho truyền đạt được tính nhạy cảm của nó. Có thể đánh dấu như vậy được bằng một con dấu trên tài liệu, một tiêu đề trên thông báo mạng, một trường đặc biệt trong bản ghi cơ sở dữ liệu... *Xem* header, label, spray paint.

masking ***(sự) ngụy trang*** Trong an toàn thông tin, một kỹ thuật che dấu thông tin truyền đi bằng cách thêm vào tín hiệu tạp âm, nhạc, các âm...

masquerade ***(sự) giả mạo*** Trong xác thực, một thực thể giả mạo để thành thực thể khác. *Xem* masquerading.

masquerading ***giả danh*** Trong an toàn dữ liệu, một nỗ lực truy nhập được tới một hệ thống bằng cách đóng giả làm người sử dụng hợp pháp. *So sánh với* spoofing. *Đồng nghĩa với* impersonation, mimicking.

mass storage device ***thiết bị lưu trữ dung lượng lớn*** Trong tính toán, một thiết bị có khả năng lưu trữ lớn, ví dụ đĩa từ, trống từ. *Xem* magnetic disk, mass storage.

master code card ***cạc mã chính*** (1) Trong kiểm soát truy nhập, một tấm cạc kiểm soát truy nhập được dùng trong bộ đọc cạc để thiết lập các mã được đòi hỏi, những tấm cạc sau đó dùng để truy nhập. (2) Trong kiểm soát truy nhập, một cạc kiểm soát truy nhập đa dụng cho phép vào/ra khi được đưa vào bộ đọc thẻ bất kỳ trong hệ thống. *Xem* card reader.

master code system ***hệ thống mã chính*** Trong an toàn vật lý, một cấu hình trong đó tín hiệu báo động được mã chung sẽ được tiếp âm ít nhất bốn vòng; sau đó có thể ngắt âm bằng tay hay tự động. *Xem* coded system.

master file ***tệp chủ*** Trong tính toán, một tệp chứa thông tin tương đối ổn định được sử dụng như một nguồn tham chiếu và được cập nhật định kỳ. *Xem* file.

master key ***khóa chính*** (1) Trong quản lý khóa, một khóa mã hóa khóa. Trong hệ thống phân cấp các khóa mã khóa, khóa chính sẽ là khóa mã hóa khóa mức cao nhất. *Xem* key-encrypting key, key management, three-layer architecture, two-layer acrchitecture. (2) Trong mật mã, một khóa có tuổi thọ lớn đối với chức năng mật mã, được dùng để mã hóa dữ liệu dài hoặc các khóa mật mã khác.

master station ***trạm chính*** Trong truyền thông dữ liệu, một trạm có nhiệm vụ chuyển dữ liệu tới một hay nhiều trạm phụ khác. Tại thời điểm bất kỳ, trên mạng chỉ có một trạm chính. *Xem* station, slave.

matching ***so khớp, đối chiếu*** Trong tính toán, sự so khớp các mục dữ liệu từ luồng xử lý của một ứng dụng với những luồng xử lý được phát triển độc lập khác để nhận diện các mục dữ liệu không được xử lý qua cả hai hệ thống song song.

matching network ***mạng đối chiếu, mạng so khớp*** Trong an toàn vật lý, sự bố trí thiết bị và mạch cần thiết để nối một tín hiệu âm thanh tới đường báo động. *Xem* alarm line.

material ***tư liệu, tài liệu*** Trong an toàn dữ liệu, dữ liệu được xử lý, được lưu trữ hoặc được dùng trong và cùng với thông tin được tạo ra bởi hệ thống ADP bất kể tới dạng thức hoặc phương tiện tải tin trung gian nào, chẳng hạn, các chương trình, báo cáo, các bộ dữ liệu hoặc các tệp, các bản ghi và các phần tử dữ liệu.

materiality ***tính nghiêm trọng*** Trong kiểm toán, nói tới lượng tiền tối thiểu sẽ được phát hiện ra trong những cuộc kiểm tra bằng các thủ tục kiểm toán

mathematical model ***mô hình toán học*** Một mệnh đề hình thức về mối quan hệ toán học giữa các phần tử đáng quan tâm đặc biệt của một hệ

thống. Các mô hình toán học thường biểu diễn ở dạng đơn giản hóa thực tế và thường được dùng để dự báo.

matrix ***ma trận*** (1) Trong toán học, một mảng nhiều chiều các đại lượng được biến đổi theo các quy tắc đại số ma trận. (2) Trong tính toán, một mạng logic mà cấu hình của nó là một mảng với những điểm giao nhau là các đầu vào hoặc ra của nó, một số những điểm giao nhau này nối tới các mạch logic. Mạng thường hoạt động như một bộ mã hóa hoặc giải mã.

matrix methodology ***phương pháp luận ma trận*** Trong phân tích rủi ro, một kỹ thuật tương đối đơn giản để phân tích tính an toàn hệ thống và đánh giá mức rủi ro.

Phương pháp luận ma trận là phương pháp đặc biệt thích hợp với các hệ thống trả tiền điện tử. Bản kê khai sau đây được dựa trên một báo cáo khoa học do các ngân hàng trung tâm của Nhóm 10 nước dưới sự bảo hộ của Ngân hàng Thanh toán quốc tế phát ra.

Giới thiệu

Các yếu tố của phương pháp luận gồm một mô tả các yêu cầu về an toàn và một tập các biện pháp bảo vệ được khuyến nghị. Trên cơ sở cách tiếp cận này, phương pháp luận xác định lần lượt:

- xử lý tới hạn/các chức năng liên lạc;
- những hiểm họa gắn với mỗi chức năng;
- tính dễ tổn thương hay điểm yếu gắn với mỗi hiểm họa;
- những biện pháp bảo vệ tương ứng với mỗi điểm yếu.

Bằng cách này, một chuỗi các ma trận được phát triển một cách logic: ma trận các chức năng - hiểm họa, ma trận các hiểm họa xuất phát từ các điểm yếu (hiểm họa - điểm yếu), ma trận các biện pháp bảo vệ các điểm yếu - các biện pháp bảo vệ. Sản phẩm logic của ba ma trận này là ma trận các chức năng - các biện pháp bảo vệ cuối cùng (sẽ được giải thích sau) là ma trận đáng quan tâm của quản lý hệ thống và những người sử dụng.

Các chức năng của hệ thống là các chức năng vĩ mô (macro) tự động hóa, đặc trưng hóa cho khía cạnh hoạt động của hệ thống và thậm chí, trong một số trường hợp có thể đồng nhất với chính hệ thống. Những ví dụ về các chức năng là: chuyển tiền, ngân hàng tự động hóa, hệ thống quản trị thông báo...

Những hiểm họa gắn với mỗi chức năng đều được xác định như những sự kiện có thể phá vỡ hệ thống hoặc làm giảm tính bí mật trong hệ thống. Có thể xác định những hiểm họa có đặc điểm chung khác nhau và có thể nhóm lại với nhau, chẳng hạn thành ba loại sau:

- làm lộ trái phép thông tin (bởi những kẻ trong nội bộ hay bên ngoài);
- biến đổi trái phép dữ liệu (vô tình hay cố ý, do nội bộ hay bên ngoài) và không phân phối các giao dịch;
- từ chối phục vụ (trong thời gian ngắn hoặc dài).

Ba hiểm họa này có bản chất chung và có thể được xem là hiểm họa điển hình của một hệ thống chi trả tiền điện tử. Những điểm yếu đều được xác định như những phương tiện để những hiểm họa xuất hiện, chẳng hạn nghe trộm,

dùng trái phép các thiết bị đầu cuối, làm hỏng phần mềm ứng dụng...

Sử dụng phương pháp này có thể hy vọng phát hiện ra 30 tới 40 điểm yếu. Trong một ứng dụng của phương pháp luận này, người ta đã xác định được những điểm yếu liên quan tới quá trình liên lạc, phần mềm, con người, các phương tiện vật lý, các kiểu dữ liệu và các cách thức nhận được dữ liệu.

Cuối cùng, những biện pháp bảo vệ là những biện pháp phòng ngừa tương ứng với điểm yếu. Hiển nhiên là có rất nhiều biện pháp bảo vệ; trong một nghiên cứu, người ta đã xác định tới trên 100 biện pháp, được tổ chức thành các loại khác nhau liên quan tới các biện pháp bảo vệ bằng kỹ thuật, bằng vật lý và tới các các thủ tục và các chính sách.

Các ma trận

Chìa khóa hoạt động đối với phương pháp luận nằm trong sự phát triển và sử dụng các ma trận dựa trên các yếu tố, tức các chức năng, các hiểm họa, các điểm yếu và các biện pháp phòng vệ. Những ma trận đang nói tới đều tăng dần mức độ phức tạp:

- chức năng - các hiểm họa;
- các hiểm họa - các điểm yếu;
- các điểm yếu - các biện pháp bảo vệ;

những ma trận khác đều nhận được từ việc nhân chúng, ma trận quan trọng nhất nhận được là ma trận các chức năng - các biện pháp bảo vệ.

Hai lưu ý có tầm quan trọng đối với việc ứng dụng có hiệu quả phương pháp luận. Thứ nhất, phải đánh giá cẩn thận khi xác định giá trị các ô của ma trận và điều này ngày càng khó khi số phần tử tăng lên, gây nên vấn đề về tính nhất quán.

Thứ hai, với lý do này và vì tính phức tạp của chính các ma trận, cần phải tự động hóa phương pháp luận, chẳng hạn, bằng cách dùng máy tính cá nhân. Độ phức tạp của các ma trận thường dẫn đến hàng nghìn quyết định liên quan tới các ô của ma trận. Do đó điều quan trọng cả trong tác động của phép nhân ma trận, cả trong việc xác định các mâu thuẫn là cần thiết thực hiện một quá trình lặp, cho phép xác định những giá trị chính xác nhất cho các ô của ma trận - duyệt lại chúng dưới góc độ các mâu thuẫn trong khi kiên trì xét đoán một cách cẩn thận.

Những nghiên cứu chung

Giá trị của phương pháp luận ma trận nằm trong yếu tố dùng một kỹ thuật tự động dựa trên một tập các phần tử cơ sở độc lập và vào việc sử dụng các ma trận có sự tương quan giữa các phần tử, nhưng lại dựa chủ yếu vào sự xét đoán: biện pháp không thay thế cho các cơ chế xét đoán. Quả thực, người tiến hành nghiên cứu lập một đánh giá theo một vài mức:

- trong quá trình gán ban đầu các giá trị vào các ô của các ma trận;
- trong quá trình xem xét các mâu thuẫn nảy sinh cùng với các ma trận nhận được;
- trong quá trình đánh giá một loạt các biện pháp bảo vệ nhằm tạo nên một tập tối thiểu kiến trúc an toàn.

Thực tế, đối với ma trận các điểm yếu - các biện pháp phòng vệ, kết quả tính toán sẽ cho ra số lần mà mỗi biện pháp phòng vệ được yêu cầu.

M

Rõ ràng là, theo sự kiểm tra thì hầu hết các biện pháp phòng vệ thường được chọn rất cần thiết; do vậy, mặc dù cần phải thêm một số biện pháp phòng vệ vào để bao quát điểm yếu (mà với chúng, những biện pháp phòng vệ được chọn lại không cho sự bảo vệ nào) nhưng vẫn có thể phải bỏ đi những biện pháp phòng vệ không cần thiết.

Việc dùng cơ chế đánh giá dẫn tới hai tập con các biện pháp phòng vệ, một tập con chính các biện pháp phòng vệ "trên tuyến" và một tập con phụ các biện pháp phòng vệ "dưới tuyến".

Đặc trưng nữa của phương pháp luận là có một vài ma trận, một số là cơ sở, một số là nhận được từ ma trận khác, mỗi cái đều có giá trị riêng đối với một đánh giá cụ thể. Đặc biệt, có hai ma trận đáng được xem xét, một ma trận rất đáng chú ý đối với các nhà kỹ thuật: ma trận các điểm yếu - các biện pháp phòng vệ; còn ma trận kia lại đáng quan tâm về nguyên tắc đối với người sử dụng và quản lý: ma trận các chức năng - các biện pháp phòng vệ. Sự phân biệt này hiếm khi xuất hiện trong các phương pháp luận khác và nó có tầm quan trọng đáng kể trong trường hợp bắt đầu với các phần tử giống nhau, hai tình huống khác nhau đều được nêu bật lên và mỗi cái được lập địa chỉ tới một khu vực khác.

Điều này nhấn mạnh quan điểm rằng, khi kiến trúc của một mạng đang được thiết kế thì các hiệu chỉnh đối với các ma trận với sự lặp đi lặp lại có thể xuất phát từ các nguồn khác nhau: nhà quản lý, kỹ thuật viên và người sử dụng. Ngoài ra, theo quan điểm quản lý, có thể tiến hành các kiểm tra ngay tại chỗ bị tác động trong quá trình hệ

Bảng 1. **Ma trận các chức năng - các hiểm họa**

CÁC CHỨC NĂNG	CÁC HIỂM HỌA					
	Làm lộ trái phép bởi người ngoài	Làm lộ trái phép bởi nội bộ	Thay đổi trái phép bởi người ngoài	Sự thay đổi vô ý	Không phân phối các thông báo	Từ chối dịch vụ trong thời gian dài
Các thông báo chuyển khoản	L	H	H	M	M	M
Các thông báo thanh toán	L	H	M	M	M	M
Các thông báo quản trị nhạy cảm	H	M	M	M	M	M

H = tầm quan trọng lớn; L = tầm quan trọng thấp; M = tầm quan trọng trung bình

Bảng 2. **ma trận các hiểm họa - các điểm yếu.** Các hiểm họa: 1) bị lộ trái phép bởi người ngoài; 2) thay đổi trái phép bởi người trong nội bộ; 3) thay đổi trái phép bởi người bên ngoài; 4) thay đổi vô tình; 5) không phân phối các thông báo; 6) từ chối phục vụ trong thời gian dài; 7) số các hiểm hoạ/ điểm yếu.

1	2	3	4	5	6	7	CÁC ĐIỂM YẾU
-	Y	Y	-	-	-	2	C1 Gài thông báo thông qua dây nối trộm
-	Y	Y	-	-	-	2	C2 Biến đổi thông báo qua dây nối trộm
Y	-	-	-	-	-	1	C3 Nghe trộm
Y	Y	Y	-	-	-	3	C4 Nghe trộm bằng quan sát
Y	Y	Y	-	-	-	3	C5 các thiết bị đầu cuối hợp pháp
-	-	-	Y	-	-	1	C6 các sai sót trên đường truyền
-	-	-	Y	-	-	1	C7 Các khả năng giao tiếp người-máy của người vận hành
Y	Y	Y	Y	Y	-	5	S1 Thiết kế/phát triển phần mềm ứng dụng
-	Y	-	-	-	-	1	S2 bảo dưỡng phần mềm ứng dụng
-	-	-	Y	Y	-	2	S3 Các chuyển đổi phần mềm
-	-	-	Y	Y	-	2	S4 Hỏng môi trường phần mềm
-	-	-	Y	Y	-	2	S5 Hỏng phần mềm ứng dụng
-	-	-	Y	Y	-	2	S6 Dữ liệu sản xuất
-	-	-	-	-	-	1	S7 Các chương trình nguồn
-	-	-	Y	-	-	2	S8 Các thư viện hệ thống
-	-	-	-	Y	-	1	S9 Các thiết bị đầu cuối thông minh dùng nhập thông báo
Y	-	-	-	-	-	2	S10 Dữ liệu an toàn
-	Y	-	-	-	-	1	S11 Các phương tiện bảo dưỡng/chẩn đoán
-	Y	-	Y	-	-	2	S12 Các phương tiện quản lý dữ liệu
Y	Y	Y	Y	Y	Y	6	P1 Các thủ tục đưa giao dịch vào
-	-	Y	-	-	-	1	P2 Các đầu cuối chặn bắt/giám sát
-	Y	-	-	-	-	1	P3 Các điều kiện vận hành không bình thường
-	-	-	Y	Y	-	2	F1 Hỏng phần cứng
-	-	-	-	Y	Y	2	F2 Hỏng tiện ích
-	-	-	Y	Y	Y	3	F3 Hỏng kênh liên lạc
-	-	-	Y	Y	Y	3	F4 Tai họa do con người - thiên nhiên gây ra
6	12	8	13	11	4	-	tổng số hiểm họa

Y = hiểm họa có thực đối với một điểm yếu cho trước.

Bảng 3. **Ma trận các điểm yếu - các biện pháp phòng vệ viễn thông.** Các điểm yếu: 1) C1 Chèn - nối trộm; 2) C2 Biến đổi - nghe qua đường nối trộm; 3) C3 Nghe trộm; 4) C4 Nghe trộm qua hình ảnh; 5) C5 Các thiết bị đầu cuối hợp pháp; 6) C6 các sai sót khi truyền; 7) C7 Bàn giao tiếp người - máy của người vận hành.

1	2	3	4	5	6	7	CÁC BIỆN PHÁP PHÒNG VỆ
Y	-	-	-	-	-	-	1.1 Các thông báo số hiệu dãy
-	-	-	-	-	Y	-	1.2 Báo nhận điểm tới điểm
Y	Y	-	-	Y	Y	Y	1.3 Phương pháp điều hòa
Y	Y	-	-	-	Y	Y	2.1 mã xác thực thông báo
Y	Y	Y	-	-	Y	-	2.2 Mã hóa
-	-	-	-	-	-	-	3 Phần mềm hệ thống
-	-	-	-	Y	Y	Y	4.1 Định danh nói chung/xác thực/kiểm soát truy nhập
-	-	-	-	-	-	Y	4.2 Mật khẩu truy nhập tới các đối tượng nhạy cảm
-	-	-	-	-	-	Y	4.3 Mã hóa các đối tượng nhạy cảm
-	-	-	-	-	-	Y	4.4 Thiết lập các nhóm người dùng kín
-	-	-	-	-	-	Y	4.5 Kiểm soát bàn giao tiếp người - máy của người vận hành
-	-	-	-	-	-	-	5.1 Các thủ tục ghi chép dự phòng/khôi phục lại
-	-	-	-	-	-	Y	5.2 Kiểm nghiệm các thủ tục khôi phục/tái khởi động trong các chương trình ứng dụng
-	-	-	-	-	-	Y	5.3 các phương tiện khôi phục/khởi động lại trong môi trường mềm
-	-	-	-	-	-	Y	5.4 Sao chép dự phòng các dữ liệu/phần mềm, các thủ tục
-	-	-	-	-	-	Y	6.1 Kiểm soát sổ ghi bàn giao tiếp người - máy
-	-	-	-	-	-	-	6.2 Ghi lại những thay đổi vào bảng an toàn
-	-	-	-	Y	-	-	6.3 Báo cáo những hoạt động trái phép
-	-	-	-	Y	-	-	6.4 Chấm dứt những vụ đăng nhập hỏng và lập báo cáo
-	-	-	-	-	-	-	6.5 Ghi lại các kết xuất hệ thống
-	-	-	-	-	-	-	6.6 Năng lực theo dõi
-	-	-	-	-	-	-	6.7 Các vệt kiểm toán
-	-	-	-	Y	-	-	7.1 Khóa các phương tiện liên lạc
Y	Y	Y	-	-	-	-	7.2 Kiểm soát thiết bị thử nghiệm mạch
-	-	-	Y	-	-	-	7.3 Hạn chế truy nhập trực quan
Y	Y	Y	Y	Y	-	Y	7.4 Kiểm soát các truy nhập trái phép/truy nhập của nhà cung cấp
-	-	-	-	-	-	-	7.5 Các phương tiện dự phòng
-	-	-	-	-	-	-	7.6 Nguồn điện dự phòng

Bảng 3. **Ma trận các điểm yếu - các biện pháp phòng vệ viễn thông (tiếp theo)**

1	2	3	4	5	6	7	CÁC BIỆN PHÁP PHÒNG VỆ
-	-	-	-	-	Y	-	8.1 Các lược đồ bảo dưỡng phòng ngừa
-	-	-	-	-	-	Y	8.2 Xem xét lại các sổ ghi bàn giao tiếp người-máy
-	-	-	-	-	-	-	8.3 Các tính năng an toàn phần mềm
-	-	-	-	Y	-	-	8.4 Bỏ qua/ghi lại/báo động các vi phạm
-	-	-	-	-	-	-	8.5 Kiểm soát các thiết bị giám sát phần cứng
-	-	-	-	-	-	-	8.6 Các phương tiện và các chương trình chẩn đoán
-	-	-	-	-	Y	-	8.7 Thu thập các thống kê về lưu lượng/hiệu suất
-	-	-	-	-	-	Y	8.8 Làm đơn giản hộp hội thoại với người thao tác
-	-	-	-	-	-	-	9.1 Cập nhật sổ tay hướng dẫn người dùng; các sổ hướng dẫn vận hành
-	-	-	-	-	Y	-	9.2 Các thủ tục báo cáo/theo dõi
-	-	-	-	-	-	Y	9.3 Các thủ tục báo cáo những vi phạm về an toàn
-	-	-	-	-	-	-	10 Chính sách an toàn
4	3	1	-	4	5	11	Các kiểm soát về kỹ thuật
2	2	2	2	2	-	1	Các kiểm soát về vật lý
-	-	-	-	2	3	3	Các kiểm soát về thủ tục
6	5	3	2	8	8	15	Tổng các điểm yếu

Y = biện pháp phòng vệ thực tế

thống vận hành thông qua ba khu vực độc lập và có thể đối lập nhau: công cụ quản lý kế tiếp hiệu quả hơn những công cụ thông thường dùng kiểm tra an toàn.

Các dạng thức khác của phương pháp luận nói trên có thể ở sự lựa chọn các biện pháp phòng vệ cho các loại máy tính cá nhân. Quả thực, trên thực tế, nhiều công việc (các thao tác giao tiếp người - máy, các nhà lập trình, phân tích hệ thống...) theo góc độ an toàn đều có tính nhạy cảm đáng kể, người ta có thể xác định một ma trận chứa các biện pháp phòng vệ phân loại công việc đặc biệt, và rõ ràng những biện pháp phòng vệ này khác với những biện pháp phòng vệ được xác định sẵn cho các ma trận khác. Một giá trị cao, thấp hay trung bình được gán cho mỗi ô của ma trận.

Ví dụ

Hãy xem xét một hệ thống ngân hàng xử lý từ xa nối trung tâm EDP của ngân hàng tới khoảng 200 chi nhánh và các hệ thống máy cho khách hàng; hệ thống xử lý chủ yếu các thông báo

Bảng 4. **Ma trận các chức năng - các biện pháp phòng vệ**

CÁC PHÒNG VỆ	CÁC CHỨC NĂNG		
	Các thông báo chuyển kênh	Các thông báo kiểm toán	Các thông báo quản trị nhạy cảm
1.1 Các thông báo số hiệu dãy	H	-	M
1.2 Báo nhận điểm tới điểm	H	M	M
1.3 Phương pháp điều hoà	H	H	H
2.1 Mã xác thực thông báo	H	M	H
2.2 Mã hóa	H	M	H
3.1 Thiết kế cấu trúc	H	H	H
3..2 Chương trình thư viện	H	H	H
3.3 Tài liệu ứng dụng	H	H	H
3.4 Các thủ tục phát hành ứng dụng	H	H	H
3.5 Kiểm định ứng dụng	H	M	M
3.6 Thủ tục thay đổi phần mềm khẩn cấp	H	H	H
3.7 Thủ tục kiểm soát các thay đổi	H	H	H
3.8 Tài liệu hệ thống	H	H	H
3.9 Kiểm định hệ thống	M	M	M
3.10 Từ điển dữ liệu	H	H	H
3.11 Quản trị dữ liệu	H	M	M
4.1 Định danh nói chung/xác thực/kiểm soát truy nhập	H	H	H
4.2 Mật khẩu truy nhập tới các đối tượng nhạy cảm	H	H	H
4.3 Mã hóa các đối tượng nhạy cảm	H	M	H
4.4 Thiết lập các nhóm người dùng kín	M	-	M
4.5 Kiểm soát bàn giao tiếp người - máy của người vận hành	H	H	M
5.1 Các thủ tục ghi chép dự phòng/khôi phục lại	H	H	H
5.2 Kiểm định các thủ tục khôi phục/tái khởi động trong các chương trình ứng dụng	H	H	H
5.3 Các phương tiện khôi phục/khởi động lại trong môi trường mềm	M	M	M
5.4 Sao chép dự phòng các dữ liệu/phần mềm	H	H	H

Bảng 4. **Ma trận các chức năng - các biện pháp phòng vệ (tiếp theo)**

6.1 Kiểm soát sổ ghi bàn giao tiếp người - máy	H	H	M
6.2 Ghi lại những thay đổi vào bảng an toàn	H	H	H
6.3 Báo cáo những hoạt động trái phép	H	H	H
6.4 Chấm dứt những vụ đăng nhập hỏng và báo cáo lại	H	H	H
6.5 Ghi lại các kết xuất hệ thống	M	-	M
6.6 Năng lực theo dõi	M	M	M
6.7 Các vệt kiểm toán	H	H	H
7.1 Các phương tiện khóa liên lạc	H	-	M
7.2 Thiết bị kiểm tra để kiểm soát mạch	M	-	M
7.3 Hạn chế truy nhập trực quan	H	-	M
7.4 Kiểm soát các truy nhập trái phép/truy nhập của nhà cung cấp	H	M	H
7.5 Các phương tiện dự phòng	H	M	M
7.6 Nguồn điện dự phòng	H	M	M
8.1 Ngăn chặn các lược đồ bảo dưỡng	H	H	H
8.2 Xem xét lại các sổ ghi ban giao tiếp người - máy	M	M	M
8.3 Các tính năng an toàn phần mềm	H	H	H
8.4 Bỏ qua/ghi lại/báo động các vi phạm	H	H	H
8.5 Kiểm soát các thiết bị giám sát phần cứng	M	M	M
8.6 Các phương tiện và các chương trình chẩn đoán	M	M	M
8.7 Thu thập các thống kê về lưu lượng/hiệu suất	M	M	M
8.8 Làm đơn giản hộp hội thoại với người thao tác	M	M	M
9.1 Cập nhật sổ tay hướng dẫn người dùng; sổ hướng dẫn vận hành...	H	H	H
9.2 Các thủ tục báo cáo/theo dõi	M	M	
9.3 Các thủ tục báo cáo những vi phạm về an toàn	H	H	
10.1 Chính sách an toàn và bảo mật	H	M	
10.2 Quản trị an toàn	H		
10.3 Các kế hoạch bất thường	H		
10.4 Các vùng kiểm toán nhạy cảm	H		

H = tầm quan trọng cao; M = Tầm quan trọng

thanh toán và chuyển khoản qua đường dây.

Bởi vậy, các chức năng cần kiểm tra gồm 3 cái như sau:

- Các thông báo chuyển kênh;
- các thông báo thanh toán;
- các thông báo quản trị nhạy cảm.

Bảng 1 biểu diễn ma trận các chức năng - các hiểm họa. Sáu hiểm họa đã được xác định:

- sự tiết lộ trái phép thông tin do người ngoài;
- sự thay đổi hợp pháp dữ liệu do người bên trong nội bộ;
- sự biến đổi trái phép dữ liệu do người ngoài;
- sự biến đổi thiếu thận trọng dữ liệu;
- không phân phối các thông báo;
- từ chối phục vụ trong thời gian dài.

Bảng 2 biểu diễn ma trận các hiểm họa từ các điểm yếu. Chỉ ra 26 điểm yếu (7 điểm về liên lạc, 12 điểm về phần mềm, 3 điểm do con người/thủ tục và 4 điểm do các phương tiện vật lý).

Bảng 3 đưa ra ma trận các điểm yếu - các biện pháp phòng vệ trong truyền thông; có thể phát triển các ma trận tương tự đối với các phần mềm và phương tiện thủ tục/vật lý

Cuối cùng bảng 4 đưa ra ma trận các ức năng-các biện pháp phòng vệ được ra từ tất cả các ma trận các điểm các biện pháp phòng vệ. *Xem* risk s.

n miscellaneous common carier.

ype system ***hệ thống kiểu*** Trong an toàn vật lý, một a thiết bị và dây dẫn có cho phép hệ thống báo động hoạt động bất chấp có sự hở và/hoặc tiếp đất cùng lúc.

MC system ***hệ thống MC*** *Xem* master coded system.

MDC ***mã MDC, mã phát hiện thao tác, mã phát hiện thay đổi*** Trong xác thực, viết tắt của Manipulation Detection Code hay Modification Detection Code, là mã xác thực thông báo hay mã phát hiện thay đổi. Đó là một khối dữ liệu được gắn với một thông báo trước khi mã hóa, tạo nên độ dư nào đó để lộ những thay đổi trong bản mã. MDC được tạo ra như một hàm của thông báo đầy đủ. *So sánh với* MAC. *Xem* message authentication.

MDN *Xem* managed data network.

mean life ***thời gian sống trung bình, tuổi thọ trung bình*** Trong kỹ thuật độ tin cậy, tuổi thọ trung bình của một thiết bị cho trước, thông thường là một hàm của các tham số thiết kế và thói quen sử dụng. *So sánh với* mean time between failure.

mean time between failure ***thời gian trung bình giữa các sự cố*** Trong lĩnh vực độ tin cậy, với một khoảng thời gian cho trước trong tuổi đời của một bộ phận thiết bị, là khoảng thời gian trung bình giữa những lần hỏng hóc liên tiếp dưới những điều kiện định sẵn. *So sánh với* mean life.

mean time to recover ***thời gian khôi phục trung bình*** Trong lĩnh vực độ tin cậy, khoảng thời gian trung bình cần thiết để đưa hệ thống vào hoạt động sau khi sửa chữa, chẳng hạn, nó có thể bao gồm tái xử lý từ điểm kiểm

tra cuối cùng. *Xem* checkpoint.

mean time to repair ***thời gian sửa chữa trung bình*** Trong lĩnh vực độ tin cậy, thời gian cần thiết trung bình để sửa chữa hay bảo dưỡng một bộ phận thiết bị.

medium access control ***kiểm soát truy nhập trung gian*** Trong truyền thông dữ liệu, một tầng con trong Mô hình Tham chiếu OSI liên quan tới quá trình cấp phát một kênh quảng bá cho những người sử dụng cạnh tranh (contending user). *Xem* broadcast, carrier sense multiple access with collision detection, open systems interconnection.

medium speed ***tốc độ trung bình*** Trong truyền thông dữ liệu, các tốc độ truyền trong khoảng từ 2400 đến 9600 baud (bốt) là tốc độ giới hạn của mạch ở cấp tiếng nói. *Xem* baud, voice grade channel.

meet in the middle ***tấn công gặp điểm giữa*** Xem multiple DES encipherment.

memo advice ***thông báo ghi nhận*** Trong hoạt động ngân hàng, một thông báo do ngân hàng phục vụ tiền gửi gửi cho nhóm thứ ba về việc ghi tiền nợ hay tiền gửi cho người chủ tài khoản. Thông báo chỉ được gửi khi có sự ủy quyền của người chủ tài khoản. *Xem* account servicing bank.

memory bounds ***(các) giới hạn bộ nhớ*** Trong an toàn máy tính, những hạn chế về phạm vi các địa chỉ nhớ đối với vùng được bảo vệ trong bộ nhớ.

memory bounds checking ***kiểm tra các giới hạn bộ nhớ*** *Đồng nghĩa với* bounds checking.

memoryless control ***kiểm soát không nhớ*** Trong an toàn cơ sở dữ liệu, một dạng kiểm soát suy luận trong đó tiêu chuẩn cho phép một câu truy vấn sẽ không phụ thuộc vào bản ghi của những câu truy vấn trước đó hay vào một danh sách các thống kê được phép. *So sánh với* a priori control, audit based control. *Xem* cell restriction, inference control, table restriction.

memory protection ***bảo vệ bộ nhớ*** Trong tính toán, một phương pháp phần cứng hay phần mềm đảm bảo rằng, một chương trình ứng dụng sẽ không truy nhập tới dữ liệu, hoặc ghi vào một vị trí nhớ được cấp cho người dùng khác hay một tiện ích hệ thống. Khi một tác vụ truy nhập tới khối bộ nhớ cho trước, một kiểm tra sẽ được tiến hành để xác định liệu nó có quyền truy nhập không và nếu không có quyền thì một ngắt sẽ được tạo ra. *So sánh với* file protection. *Xem* application program, bounds checking.

mental poker ***bài poke trí tuệ*** Trong mật mã, một dạng liên lạc trong đó thông tin có thể được giấu kín trước những nhóm trao đổi dữ liệu riêng song vẫn đảm bảo rằng tất cả các nhóm có thể kiểm tra được thông tin được giấu này.

Ở dạng đơn giản nhất, nó là cuộc chơi bài poke từ xa qua điện thoại giữa Alice và Bob. Không ai tin ai đã chơi đẹp và phải dùng hệ thống mật mã để đáp ứng những chỉ tiêu liệt kê sau:

- Alice và Bob phải giữ các chân chơi bài poke riêng biệt, giấu những tay

chơi bài khác và có khả năng như những tay chơi bài khác.

- Những quân bài bổ sung bất kỳ mới được trong khi chơi phải tuân theo các yêu cầu ở trên và người chơi phải có khả năng để lộ một quân bài mà không làm lộ những quân bài khác trên tay.
- Cuối bài, những người tham gia chơi bài phải khẳng định được rằng ván bài đã được chơi rất trung thực và không có ai gian lận.

Có thể dùng mật mã lũy thừa để giải quyết vấn đề này. Các khóa mã/giải mã cho Alice và Bob tương ứng là E_1, D_1, E_2, D_2. Phép biến đổi mật mã phải giao hoán để:

$$eE_1(eE_2(M)) = eE_2(eE_1(M))$$

Quá trình chơi bài như sau:

Mỗi một trong 52 quân bài được biểu diễn bằng 52 thông báo M_1, M_2, ... M_{52}, chẳng hạn M_1 = quân át nhép.

- Alice mã 52 thông báo trên bằng khóa mật mã E_1 và tạo ra 52 thông báo mã $eE_1(M_1)$, $eE_1(M_2)$, ... $eE_1(M_{52})$. Những thông báo đã mã này được chuyển tới cho Bob theo thứ tự ngẫu nhiên.
- Bob chọn 5 thông báo và trả lại chúng cho Alice, Alice nhận chúng như quân bài đang chơi của cô. Alice giải mã những thông báo này bằng khóa D_1.
- Bob sau đó chọn 5 thông báo làm xấp bài riêng của mình, mã chúng bằng khóa E_2, tạo thành 5 thông báo có dạng $eE_2(eE_1(M_i))$. 5 thông báo đã mã kép này sau đó cũng được gửi trả lại cho Alice.
- Alice giải mã 5 thông báo được mã kép bằng khóa giải mã D_1, tức là $dD_1(eE_2(eE_1(M_i))) = dD_1(eE_1(eE_2(M_i))) = eE_2(M_i)$ vì thuật toán mã hóa là giao hoán.
- 5 thông báo đã được Alice giải mã sau đó lại được chuyển tới cho Bob - người sau đó để lộ chúng qua việc giải mã bằng khóa D_2 và nhận chúng như xấp bài đang chơi.
- Ván bài được chơi bằng những quân bài bị lộ của cả hai người; có thể phân phối những quân bài mới cũng bằng những kỹ thuật nêu trên.
- Cuối ván, cả hai người để lộ các khóa của họ để có thể kiểm tra được quá trình chơi.

Mã pháp lũy thừa cung cấp các đặc tính mã giao hoán cần thiết, tức là:

$$eE(M) \equiv M^E \bmod n$$

$$M \equiv dD(eE(M)) \equiv (eE(M))^D \bmod n$$

trong đó M nguyên tố cùng nhau với n và $E.D = 1 \bmod (\phi(n))$; $\phi(n)$ là hàm Euler.

Kỹ thuật có thể bị tấn công, có nghĩa là người chơi có thể gian lận nếu thông báo bất kỳ M là một thặng dư bậc hai modulo n. Nếu thông báo M là thặng dư bậc 2 modulo n thì nó vẫn giữ được tính chất này dưới phép mã hóa bằng lấy lũy thừa. Thông tin này có thể đặt Bob vào vị trí có lợi.

Khi bắt đầu, Bob biết rằng có thể chia các quân bài làm hai bộ, tức những thông báo là thặng dư bậc hai và những thông báo không phải thặng dư bậc hai. Dựa trên những thông báo đã mã nhận được, có thể tách chúng thành hai lớp và khi đó Bob có thêm những

thông tin phụ cho việc lựa chọn và tiếp tục chơi. Ví dụ, nếu Bob luôn chọn những thông báo là thặng dư bậc hai cho Alice thì anh ta biết rằng, Alice không thể giữ những quân bài nhất định nào đó. *Xem* disjoint, Euler's Genelization, Euler totient function, exponentiation cipher, modulo arithmetic, quadratic residue, RSA.

meridional ray ***tia kinh tuyến*** Trong lĩnh vực viễn thông, một tia sáng đi qua trục cáp sợi quang là kết quả của sự phản xạ bên trong và được giữ theo theo mặt phẳng đơn. *Xem* fiber optics.

Merkle-Hellman knapsack cipher ***mã pháp ba lô Merkle-Hellman, mã pháp knapsack Merkle-Hellman*** Trong mật mã, một hệ thống mã khóa công khai do Merkle và Hellman đề xuất dựa trên bài toán ba lô.

Bài toán này lấy tên từ một ba lô hình trụ và một bộ những khúc gỗ có cùng đường kính như ba lô. Những khúc gỗ có các độ dài khác nhau và cần xác định những tập con những khúc gỗ sao cho nó vừa khít ba lô. Theo thuật ngữ toán học, bài toán này có thể biểu diễn như một mảng một chiều gồm các số nguyên $(a_1, a_2, .. a_n)$ và một số nguyên C cho trước. Bài toán xác định một tập con những số nguyên này sao cho tổng của chúng đúng bằng C.

Quá trình tìm kiếm vét cạn gồm 2^n phép tính và nỗ lực tính toán như vậy sẽ tăng theo hàm mũ với số các số nguyên n. Bài toán ba lô là một bài toán NP vì rất dễ kiểm tra lời giải song lại rất khó tìm ra một lời giải đúng.

Tuy nhiên, với một dãy siêu tăng các số nguyên, lời giải không khó lắm. Trong trường hợp này, các số nguyên $(a_1, a_2.. a_n)$ được sắp theo thứ tự và thành viên bất kỳ của tập đều lớn hơn tổng của tất cả các số hạng đứng trước. Hãy xét các dãy siêu tăng (1, 5, 10, 20, 40), nếu độ dài của ba lô C bằng 26 thì tập con các số nguyên có tổng bằng C có thể được xác định nhanh chóng bằng một tìm kiếm như mô tả dưới đây:

- Bắt đầu với quyết định dựa trên sự có mặt hay không của số nguyên lớn nhất $a_5 = 40$. Vì $C = 26$ nên a_5 không thể thuộc tập cần lấy.
- Tiếp theo $a_4 = 20$ và $C = 26$. Trong trường hợp này, a_4 nhỏ hơn C và nó phải thuộc tập vì tổng của tất cả các số hạng (1 + 5 + 10) không thể vượt quá 20 thông qua việc xác định một dãy siêu tăng.
- Bây giờ có thể xác định lại bài toán theo độ dài mới của ba lô 26 − 20 = 6 và tập tập các số nguyên nhỏ hơn (1, 5, 10).
- Tiếp tục như trên ta sẽ thấy rằng 10 không thuộc tập song 5 và 1 lại thuộc.
- Do vậy, tập con các số nguyên là 20 + 5 + 1 = 26.

Như vậy, bài toán ba lô biểu diễn một hàm cửa sập một chiều. Nó là hàm một chiều vì khi cho trước một tập các số nguyên, dễ dàng xác định được tổng C của chúng; tuy nhiên trong trường hợp tổng quát, phép tính đảo nhằm xác định tập con khi biết trước C lại không dễ tính được với n lớn, khi đó phải tiến hành tìm kiếm theo kiểu vét cạn tất cả 2^n khả năng.

Cửa sập này sinh vì có thể chuyển bài toán từ dạng tổng quát sang bài toán

ba lô dễ tính với dãy siêu tăng khi biết trước thông tin mật nào đó.

Quá trình mã hóa và giải mã dùng mã pháp ba lô được mô tả dưới đây:

- Chọn một chuỗi siêu tăng $(a_1, a_2, .. a_n)$ với giá trị n đủ lớn để việc tìm kiếm theo kiểu vét cạn không thực hiện được về mặt tính toán.
- Hai số nguyên tố cùng nhau w và m được chọn với $w < m$. Số nghịch đảo w^{-1} được tính, ở đây $w.w^{-1} \equiv 1 \pmod m$. Phép tính này có thể thực hiện được bằng phương pháp dựa trên thuật toán Euclid.
- Một tập mới các số nguyên được tính trên cơ sở: $b_i = a_i.w \pmod m$ với $i = 1.. n$.
- Tập $(b_1, b_2,.. b_n)$ sau đó được công bố như một khóa mã công khai. Các giá trị của b có thể được sắp lại để che dấu dãy siêu tăng ban đầu; các giá trị w và m được giữ bí mật.
- Dữ liệu cần mã hóa được biểu thị dưới dạng các khối chữ số nhị phân với n bit mỗi khối, chẳng hạn $(d_1, d_2, .. d_n)$ trong đó $d_i = 0$ hoặc $= 1$.
- Các khối n bit sau đó được mã hóa bằng cách tính tích vô hướng $(d_1, d_2,.. d_n).(b_1, b_2, .. b_n)$
  $C = \sum_{i=1..n} b_i d_i$
  Như vậy, b_i chỉ nằm trong tổng C khi $d_i = 1$.
- Thông báo đã mã gồm một dãy các số nguyên C_j (ứng với tích vô hướng cho khối j) được truyền đi.
- Bên thu đang sở hữu thông tin mật w^{-1} và m sẽ chuyển mỗi giá trị C thành P với $P \equiv C.w^{-1} \pmod m$.
- Dữ liệu ban đầu $(d_1, d_2,.. d_n)$ được xác định dễ dàng từ P và dãy siêu tăng $(a_1, a_2,.. a_n)$ như mô tả ở trên.

Thông tin mật w^{-1} và m cung cấp thông tin về cửa sập vì nó chuyển (biến đổi) bài toán ba lô khó với chuỗi $(b_1, b_2,.. b_n)$ thành bài toán ba lô dễ $(a_1, a_2,.. a_n)$. Việc chuyển thành bài toán ba lô dễ được minh họa dưới đây.

- $P \equiv C.w^{-1} \pmod m$.
- $w^{-1} \sum^n (d_i b_i) \pmod m$
- $\sum^n (a_i d_i) \pmod m$
- Dãy siêu tăng $(a_1, a_2,.. a_n)$ cho phép xác định $(d_1, d_2,.. d_n)$ nhanh chóng từ số nguyên P.

Mã pháp ba lô có ưu điểm là công tính toán trong các quá trình mã/giải mã tương đối thấp so với RSA vì nó chỉ có một số hữu hạn phép nhân và cộng. Tuy nhiên chúng có hai nhược điểm. Trước hết, khóa dài tới vài kilobit so với khóa vài trăm bit của RSA và 64 bit của DES. Thứ hai, sự giãn thông báo và bản mã trung bình gấp hai lần bản rõ ban đầu.

Các mã pháp ba lô đã bị tấn công và đã có những thuật toán nhanh cho các tấn công mã thám. Shamir đã đưa ra một bài báo năm 1982 về một cuộc tấn công thành công mã pháp ba lô. *So sánh với* DES, Euclid's algorithm, Graham Shamir knapsack cipher, modulo arithmetic, NP Class, scalar product, superincreasing series, trapdoor one-way function.

Mersenne prime ***số nguyên tố Mersenne*** Trong toán học, một số nguyên tố có dạng $2^n - 1$. Nếu với một số n cho trước, $2^n - 1$ là một số nguyên tố thì n phải là một số nguyên tố, tuy

Các số nguyên tố Mersenne

p với $2^p - 1$ là nguyên tố	Người phát hiện	Năm
19	Cataldi	1588
31	Euler	1722
61	Pervushin	1883
89	Powers	1911
107	Powers	1914
127	Lucas	1876
512, 607 1, 279 2, 203 2, 281	Lehmer-Robinson	1952
3, 217	Riesel	1957
4, 253 4, 423	Hurwitz-Selfridge	1961
9, 689 9, 941 11, 213	Gillies	1963
19, 937	Tuckerman	1971
21, 701	Nickel-Noll	1978
23, 209	Noll	1978
44, 497	Slowinsky-Nelson	1979
86, 243	Slowinsky	1982

nhiên ngược lại lại không đúng, tức là nếu n là số nguyên tố thì $2^n - 1$ không nhất thiết là số nguyên tố. *So sánh với* Fermat prime. *Xem* prime number.

mesh ***mạng mắt lưới*** Trong các mạng máy tính, một cấu hình có hai hoặc nhiều hơn tuyến giữa hai nút mạng. *So sánh với* ring, star. *Xem* node.

message ***thông báo, bức điện*** (1) Một cuộc liên lạc có một hay nhiều giao dịch hoặc một hay nhiều đề mục thông tin liên quan. (2) Trong truyền thông dữ liệu, một lượng thông tin tùy ý mà thời điểm bắt đầu hay kết thúc nó đều được xác định hoặc được báo hàm sẵn. *Xem* message format.

message authentication ***xác thực thông báo*** (1) Trong hoạt động ngân hàng, kỹ thuật được dùng giữa người gửi và người nhận để xác nhận tính hợp lệ của nguồn và một phần hay tất cả văn bản của thông báo. (2) Trong xác thực, các quá trình thực hiện nhằm đảm bảo rằng:

- thông báo được bắt đầu với người gửi có chủ đích;
- nội dung thông báo không được thay đổi hoặc sắp xếp lại một cách vô tình hay có chủ ý;
- thông báo đã được nhận theo trình tự mà người khởi đầu cuộc liên lạc đã gửi nó;
- Người nhận nhầm trước sẽ nhận được thông báo.

Xác thực thông báo bởi vậy liên quan tới danh tính của người gửi và người nhận, tới những biến đổi nội dung thông báo và tới vấn đề quay lại (phát

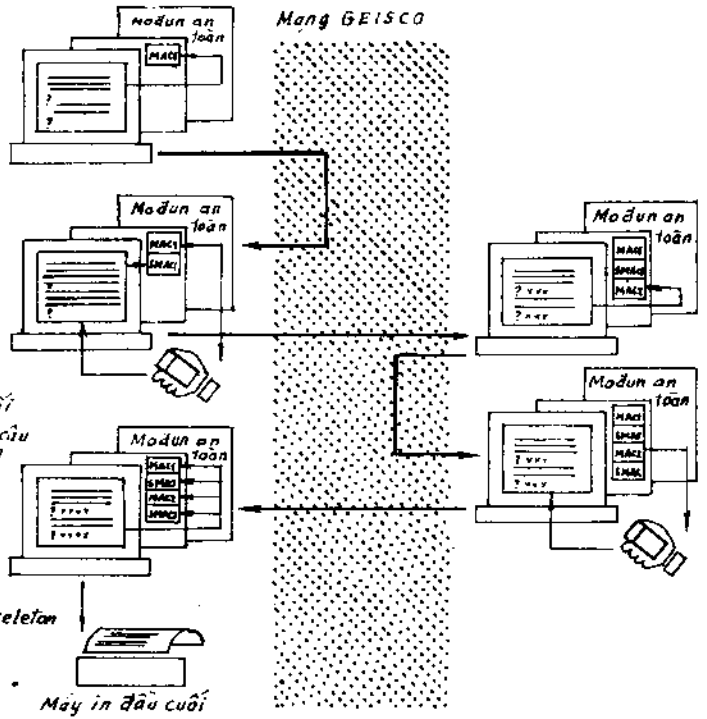
lại). Những thay đổi không mong muốn được giả thiết có thể là do vô tình, chẳng hạn tạp âm trên kênh truyền hoặc do sự ác ý của nhóm thứ ba. Vấn đề tranh cãi khi người gửi tố cáo người nhận thay đổi thông báo hoặc những cố gắng hủy bỏ thông báo đều thuộc lĩnh vực chữ ký số.

Xác thực người gửi thông báo đòi hỏi phương pháp nào đó cho phép người nhận Bob có thể khẳng định được rằng thông báo chỉ có thể do người gửi - Alice - có chủ đích tạo ra. Điều này hàm ý rằng Alice giữ thông tin mật nào đó mà nhóm thứ ba không có. Rõ ràng, thông tin mật như vậy không thể đơn giản nằm trong thông báo, chẳng hạn như mật khẩu, vì kẻ tấn công có thể truy nhập tới thông tin đó. Mã hóa thông tin đó vẫn chưa đủ. Giả sử rằng Alice có một mật khẩu bí mật P và mã hóa nó bằng khóa mật k để gộp vào thông báo gửi cho Bob. Kẻ tấn công không thể nhận được P từ $ek(P)$; Bob đang sở hữu k và P sẽ có khả năng khẳng định rằng, phép giải mã $ek(P)$ sẽ tạo ra mật khẩu P của Alice. Tuy nhiên, nếu dùng khóa mã giống nhau cho một số thông báo thì kẻ tấn công sẽ đưa ra một thông báo chứa bản mã $ek(P)$ mà bản thân nó không mật và anh ta có thông báo được Bob chấp nhận như thông báo đích thực. Rõ ràng là thông tin mật phải được tiết chế một cách an toàn đối với toàn thông báo.

Nếu thông báo có độ dư nào đó, phép mã hóa toàn thông báo bằng một khóa mật sẽ cho Bob khả năng kiểm tra xem có phải thông báo có ý nghĩa cho trước chỉ có thể do Alice hiểu biết về khóa đó tạo ra. Khẳng định này có được dưới điều kiện là các quá trình mã không cho phép các khối bản mã được sắp xếp lại hoặc được thay thế bởi các khối lấy từ thông báo khác. Nếu Alice gửi đi hai thông báo dùng DES ở chế độ từ điển điện tử thì cả hai đã được mã bởi cùng một khóa nên kẻ tấn công có thể sắp xếp lại các khối của thông báo mã, hoặc thay thế các khối của thông báo này vào các khối của thông báo khác và không có gì bảo đảm rằng, Bob sẽ nhận ra những thay đổi trong bản rõ nhận được sau đó.

Một phương pháp có hiệu quả để đảm bảo một thông báo đã được Alice tạo ra trọn vẹn, không bị làm hỏng hoặc biến đổi một cách có chủ ý là dùng một hàm ánh xạ thông báo thành khối dấu hiệu xác thực. Một thuật toán băm (hash) sẽ nhận một thông báo có độ dài bất kỳ làm đầu vào và tạo một đầu ra có độ dài cố định. Việc thay đổi một bit hay ký tự trong thông báo vào chắc chắn sẽ gây nên sự thay đổi ở đầu ra của hàm băm; cũng như vậy, sự trao đổi lẫn nhau giữa các bit hay ký tự trong thông báo vào chắc sẽ tác động tới đầu ra.

Vì hàm băm ánh xạ thông báo có độ dài bất kỳ thành khối dấu xác thực có độ dài cố định nên số các khối dấu xác thực tiềm ẩn sẽ ít hơn số thông báo vào có thể. Ta hãy xem một khối dấu xác thực chỉ có 3 bit. Thực tế sẽ có 8 khối dấu xác thực và tất cả thông bao tiềm ẩn có thể được chia nhỏ thành 8 loại; tất cả các thông báo thuộc một loại cho trước băm thành khối dấu xác thực như nhau.



message authentication: *xác thực thông báo.* Xác thực và cấp phép trên hệ thống chuyển tiền GEISCO. Giải pháp an toàn do Racal-Guardata phát triển là một hệ thống dựa trên mật mã hai tầng nhờ dùng thuật toán DEA, tầng đầu dùng ANSI X 9.9 và tầng thứ hai dùng cách tích hợp xác thực cá nhân và xác thực thông báo. Hai kỹ thuật này cùng nhau cung cấp một cơ chế đảm bảo xác thực và cấp phép thông báo điểm tới điểm, cơ chế này sẽ cho định danh thiết bị khởi đầu và nhân viên cấp phép. Các viết tắt: skeleton - chỉ dẫn trả tiền đã định khuôn sẵn; MAC1 - mã xác thực thông báo cho skeleton; SMAC1 - chữ ký cấp phép cho skeleton; MAC2 - mã xác thực thông báo cho dữ liệu trả tiền kết hợp; SMAC2 - chữ ký cấp phép cho dữ liệu trả tiền kết hợp.

Rõ ràng điều cần chú ý là các thông báo đầu vào khi ánh xạ lên cùng một dấu xác thực sẽ khác nhau khá nhiều; nếu không thì một sự thay đổi nhỏ trong thông báo sẽ không bảo đảm có sự thay đổi trong khối dấu xác thực. Bởi vậy, khối dấu xác thực phải đủ lớn để đảm bảo một số lượng lớn các loại thông báo, còn thuật toán băm sẽ đảm bảo các thành viên cùng loại khác xa nhau. Trong lĩnh vực tài chính, khối dấu xác thực (MAC) dài 32 bit.

Alice có thể gắn khối dấu xác thực được tạo ra từ hàm băm vào một thông báo, tạo cho Bob có một mức bảo đảm rằng thông báo không bị sai lạc. Khi nhận được thông báo, Bob thao tác nó với cùng thuật toán băm và kiểm tra kết quả bằng khối dấu xác thực gắn kèm theo nó: nếu ăn khớp thì Bob có thể chắc chắn rằng thông báo đã không bị sửa đổi một cách ngẫu nhiên. Với hàm băm được thiết kế tốt, không thể xảy ra sự sửa đổi ngẫu nhiên làm thay đổi thông báo đầu vào thành thông báo thứ hai được ánh xạ vào cùng khối dấu xác thực. Tuy nhiên, Bob không thể thuyết phục được rằng, kiểm tra như vậy là đảm bảo chống lại được hoạt động ác ý của kẻ tấn công. Nếu dấu xác thực được truyền đi trên kênh an toàn và hàm băm không thể thực hiện được về mặt tính toán để tạo ra thông báo thứ hai tương ứng với khối dấu xác thực cho trước thì Bob, quả thực có thể có bí mật nào đó chống lại được sự thay đổi ác ý. Ví dụ, kỹ thuật này có thể được lợi dụng để đảm bảo phần mềm đã phân phối không bị thay đổi ác ý. Bob nhận phần mềm và cũng có thể nhận được khối dấu xác thực đã bảo đảm, chẳng hạn từ sổ tay hướng dẫn phần mềm lấy từ nguồn tin cậy. Sau đó Bob có thể kiểm tra tính toàn vẹn của phần mềm bằng cách so sánh kết quả của phép băm phần mềm với khối dấu xác thực đã công bố. Nếu thông báo hay phần mềm chứa tên của Alice thì có thể xác thực nguồn thông báo hay phần mềm.

Nếu Alice và Bob trao đổi các thông báo EDI trên kênh công cộng thì thông thường họ sẽ không truy nhập tới kênh an toàn để truyền khối dấu xác thực. Nếu khối dấu xác thực được gắn đơn giản vào thông báo thì Bob sẽ đối mặt với khả năng kẻ tấn công đã tạo ra một thông báo, đã tính dấu xác thực tương ứng và đã gắn nó vào thông báo. Trong trường hợp này, Alice phải dùng thông tin mật nào đó chỉ cô ta biết và có thể cả Bob, cùng với khối dấu xác thực.

Alice có thể dùng mật mã đối xứng, chẳng hạn DES và một khóa k_a chỉ Alice và Bob biết để mã hóa khối dấu xác thực. Tương tự, Bob dùng khóa mật thứ hai k_b cho các thông báo gửi cho Alice. Alice có thể ký khối dấu xác thực bằng khóa mật của mã không đối xứng phù hợp, chẳng hạn RSA. Như vậy, Alice chuẩn bị một thông báo M và

- tính dấu xác thực A bằng cách đưa M vào thuật toán băm h, tức là $A = h(M)$;
- mã A bằng khóa mật k_a của cô, tạo ra bản mã $ek_a(A)$;
- truyền M và $ek_a(A)$ tới Bob.

Bob nhận được M' và $ek_a(A')$ và kiểm tra tính toàn vẹn của thông báo bằng cách:

- tính dấu xác thực $A'' = h(M')$;
- trong trường hợp mã đối xứng, anh ta giải mã $ek_a(A')$ bằng khóa k_a, nhận được A', trong trường hợp mã khóa công khai, Bob dùng khóa công khai của Alice để nhận được A';
- Bob so sánh A'' với A', nếu chúng giống nhau, anh ta được thuyết phục rằng thông báo xuất phát từ Alice và đã không bị sửa đổi hay làm sai lạc trong khi truyền.

Sự chắc chắn mà Bob tìm thấy phụ thuộc vào sự bất lực của kẻ tấn công khi mã dấu xác thực bằng khóa mật của Alice. Tuy nhiên, kẻ tấn công vẫn có thể có một số mánh khóe. Giả sử thuật toán băm tương đối đơn giản để kẻ tấn công trên thực tế có thể tạo ra một thông báo thứ hai tương ứng với dấu xác thực A đã cho. Trong trường hợp này, một khả năng tấn công có thể xảy ra:

- Alice tạo ra thông báo M, tính $A = h(M)$ và chuyển M, $ek_a(A)$ tới Bob;
- kẻ tấn công chặn lấy bản sao M và $ek_a(A)$;
- kẻ tấn công lập một thông báo giả và nhào nặn nó cho tới khi nhận được thông báo M_1 sao cho $A_1 = h(M_1) = A = h(M)$, việc nhào nặn như vậy có thể xảy ra với thông báo dạng tài chính có một trường chú thích rộng tùy ý, có thể cho phép sự thông báo như vậy;
- kẻ tấn công truyền M_1 và $ek_a(A)$ tới Bob;
- Bob tính $h(M_1) = A$, giải mã $ek_a(A)$ và chấp nhận thông báo là thông báo thực.

Để ngăn chặn kiểu tấn công này, Alice hoặc dùng một hàm băm mạnh mà kẻ tấn công không có khả năng xác định M_1, hoặc kết hợp luân phiên phép băm và phép mã để tạo ra một mã xác thực thông báo như mô tả trong ANSI X9.9. Trong trường hợp sau, thông báo bị lệ thuộc vào liên kết khối mã dùng khóa k_a và giữ lại khối cuối cùng, các khối trung gian bị loại bỏ. Khối cuối cùng được gọi là khối xác thực thông báo. 32 bit bên trái nhất của khối xác thực thông báo được gọi là mã xác thực thông báo (MAC) và được truyền đi thay vì $ek_a(A)$.

Một dạng tấn công khác là tấn công quay lại (phát lại, replay) tức là kẻ tấn công chỉ đơn giản lặp lại thông báo trước đó có đầy đủ dấu xác thực; Bob chấp nhận thông báo được quay lại vì khối xác thực thỏa mãn tất cả các kiểm tra ở trên. Để chống kiểu tấn công quay lại, Alice phải đưa thêm trường nào đó vào thông báo để phân biệt nó với tất cả các thông báo trước đó, chẳng hạn thêm tem ngày tháng, số hiệu dãy thông báo. Một số hệ thống xác thực đưa cả các trường tùy chọn trong quá trình xác thực; rõ ràng trường làm thông báo trở nên duy nhất phải tính đến trong các trường xác thực.

Nếu dùng mã đối xứng thì Alice và Bob phải dùng các khóa khác nhau để truyền thông báo của mình, nếu không kẻ tấn công có thể đơn giản chỉ quay lại một trong những thông báo của Alice và chuyển ngược trở lại cho Alice, cô ta sẽ nhận nó như một thông báo của Bob. Tấn công này có thể thành công ngay cả khi dùng tem ngày tháng hay số hiệu dãy thông báo vì những biện pháp chống quay lại thông báo của

Alice chỉ áp dụng để quay lại những thông báo của Bob.

Các số hiệu dãy thông báo đã xác thực cũng cho phép Bob kiểm tra thấy các thông báo của Alice được xử lý theo thứ tự. Alice cũng có thể yêu cầu một thông tin biên nhận từ Bob, những biên nhận như vậy sẽ được xác thực và chứa đủ thông tin để định danh duy nhất Bob và thông báo mà biên nhận đề cập tới. *Xem* ANSI X.9 - 1986, asymmetric cipher, authentication, authenticator, block cipher, CBC, cipher block chainning, ciphertext, digital signature, DES, electronic codebook, hash function, key, message authentication code, message sequence number, public key cryptography, RSA, replay, symmetric cipher, time date stamp.

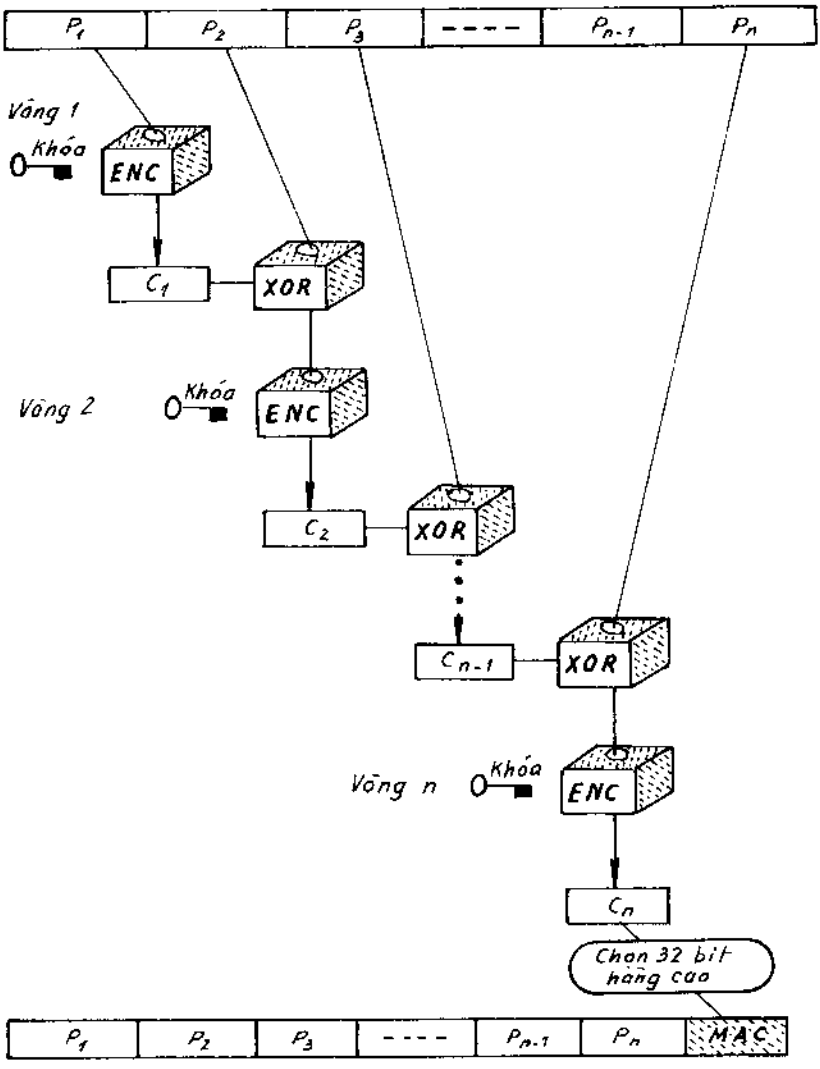
message authentication algorithm ***thuật toán xác thực thông báo*** Trong hoạt động ngân hàng, một thuật toán khai triển một số được gửi cùng với thông báo để người nhận có thể kiểm tra nó có bị thay đổi từ lúc được gửi đi không. ISO 8732 đã mô tả một thuật toán được thiết kế đặc biệt cho nơi có dung lượng dữ liệu cao và quá trình thực hiện hiệu quả bằng phần mềm là đặc trưng mong muốn. Thuật toán dùng hai số 32 bit làm khóa và kết quả của thuật toán là một dấu xác thực 32 bit. *So sánh với* message authentication code.

message authentication block ***khối xác thực thông báo, MAB*** Trong hoạt động ngân hàng, một khối là một hàm mật mã của tất cả các dữ liệu trong một thông báo hay một thông báo mở rộng được tạo ra dưới sự kiểm soát của khóa giao dịch. MAB được chặt nhỏ ra tạo nên mã xác thực thông báo (MAC) và thặng dư MAC. *Xem* MAC, MAC residue, message authentication.

message authentication code ***mã xác thực thông báo*** (1) Trong xác thực, một số là kết quả chuyển một thông báo qua thuật toán xác thực nhờ dùng một khóa đặc biệt. (2) Trong hoạt động ngân hàng, một mã (code) nằm trong một thông báo giữa người gửi và người nhận, dùng để xác nhận tính hợp lệ của nguồn và một phần hay tất cả văn bản của thông báo. Mã (code) là kết quả của một tính toán có thỏa thuận. (3) Trong hoạt động ngân hàng, một nhóm các ký tự nằm trong thông báo để xác minh (kiểm tra) xem thông báo có bị thay đổi gian lận hay không. Mã là một hàm mật mã của tất cả dữ liệu trong thông báo được tạo ra dưới sự kiểm soát của một khóa giao dịch và bởi vậy, mang tính duy nhất thống kê đối với thông báo đó. MAC là một phần của khối xác thực thông báo. *So sánh với* message authentication algorithm. *Xem* message authentication, message authentication block, transaction key.

message certification ***chứng thực thông báo*** Trong xác thực, một thủ tục trong đó, bên nhận cung cấp bằng chứng cho bên gửi rằng đã nhận được một thông báo. Giấy báo nhận từ bên nhận cần được ký để đảm bảo rằng nó không xuất phát từ kẻ tấn công. *Xem* digital signature.

message digest ***bản tóm lược thông báo*** Trong xác thực, một hàm toán học ánh xạ các giá trị từ một vùng lớn, có thể rất lớn vào một vùng nhỏ hơn. Một bản tóm lược thông báo tốt phải



message authentication code: *mã xác thực thông báo.*

sao cho các kết quả áp dụng hàm vào một tập lớn các giá trị trong vùng sẽ được phân phối ngẫu nhiên và đều trên phạm vi. *Xem* domain, range.

message exhaustion ***vét cạn thông báo*** Trong mã thám, một dạng tấn công trong đó tất cả những tổ hợp bản rõ có thể đều được mã hóa và các bản mã tương ứng sẽ được lưu trữ để đối chiếu sau này. Trong mật mã khóa công khai, người mã thám biết khóa mã và như vậy có thể kiểm tra bản mã thu

được dựa vào cặp bản rõ - bản mã đã lưu. Nếu người mã thám không biết khóa mã thì quá trình được tiến hành với mọi khóa có thể, sau đó nếu có sẵn một đoạn bản rõ và bản mã tương ứng thì có thể tìm kiếm các cặp rõ/mã đã lưu và xác định các khóa tương ứng. *So sánh với* key exhaustion. *Xem* block cipher, blocksize, cryptography key, public key cryptography.

message format ***khuôn (thức) thông báo*** Trong truyền thông dữ liệu, các quy tắc sắp xếp các phần của một thông báo như tiêu đề, địa chỉ, chủ đề, và kết thúc của thông báo. *Xem* address, message heading, message text.

message heading ***tiêu đề thông báo*** Trong liên lạc dữ liệu, phần đầu của một thông báo chứa thông tin như mã nguồn hoặc mã đích của thông báo, quyền ưu tiên của thông báo và kiểu thông báo. *So sánh với* message text.

message identifier ***ký hiệu nhận dạng thông báo, danh tính thông báo*** Trong xác thực, một trường có tới 8 ký tự dùng để nhận diện duy nhất một thông báo hay giao dịch tài chính. Điển hình, trường này là số hiệu dãy. *Xem* ANSI X.9 - 1986.

message integrity code ***mã toàn vẹn thông báo*** Trong xác thực, một giá trị được khai triển (nhờ một phép biến đổi toán học) của một thông báo và đặc trưng cho thông báo đó. Do vậy, một thay đổi nhỏ bất kỳ trong thông báo bởi phép thay thế hay sao chép một ký tự sẽ dẫn tới thay đổi trong mã toàn vẹn thông báo. Mã này có thể hoặc không thể tính toán được bằng khóa mật mã bí mật. *So sánh với* message authentication code. *Xem* electronic mail security.

message numbering ***số hiệu thông báo*** Trong truyền thông dữ liệu, một số duy nhất cho sẵn trên mỗi thông báo trong một hệ thống nhằm mục đích định danh.

message oriented text exchange ***trao đổi văn bản định hướng thông báo*** Trong truyền thông dữ liệu, một giao thức được dùng cho liên lạc thư điện tử; nó tương tự với X.400. *Xem* electronic mail, protocol, X.400.

message routing ***định tuyến thông báo*** Trong truyền thông dữ liệu, quá trình chọn tuyến đường trong một hệ thống chuyển mạch thông báo. *Xem* message switching, routing.

message sequence number ***số hiệu dãy thông báo*** Trong xác thực, một số được dùng để định danh duy nhất một thông báo và để đảm bảo rằng, thông báo được quản lý theo trình tự. *Xem* replay.

message slot ***khe thông báo*** Trong truyền thông dữ liệu, một dãy bit đủ để giữ một thông báo đầy đủ được lan truyền liên tục quanh mạng cục bộ. Khe có thể rỗng hoặc đầy, và nút bất kỳ căn cứ vào việc phát hiện một khe rỗng có thể đánh dấu khe như khe đầy và đặt một thông báo vào đó. *So sánh với* daisy chain, control token. *Xem* Cambridge Ring, local area network.

message space ***không gian thông báo*** Trong mật mã, một tập tất cả các thông báo có thể mà có thể được mã hóa theo một mã pháp cho trước.

So sánh với cryptogram space, key space.

message specific random integer ***số nguyên ngẫu nhiên đặc trưng cho thông báo*** Trong xác thực, một số nguyên ngẫu nhiên được dùng với một thông báo chỉ ra và không được cố tình dùng lại cho thông báo khác bất kỳ.

message stream modification ***biến đổi dòng thông báo*** Trong an toàn liên lạc, đề cập tới những tấn công lên tính xác thực, tính toàn vẹn và/hoặc thứ tự các PDU của dòng thông báo. Tấn công lên tính xác thực có thể được thực hiện bằng cách thay đổi thông tin kiểm soát giao thức trong các PDU để chúng bị gửi sai đích, hoặc bằng cách gài các PDU (do kẻ tấn công tạo ra hoặc được quay lại từ các thông báo trước đó) vào dòng thông báo. Tương tự, tấn công lên tính toàn vẹn sẽ hướng tới việc thay đổi dữ liệu chứa trong PDU. Các tấn công lên tính trật tự sẽ xóa các PDU hoặc thay đổi trật tự thông tin trong phần kiểm soát các PDU. *So sánh với* denial of message service, spurious association initiation. *Xem* PDU.

message switching ***chuyển mạch thông báo*** Trong truyền thông dữ liệu, một kỹ thuật tăng khả năng tải của mạng bằng cách chuyển mạch tuần tự các thông báo được lưu trước đó. Không giống với chuyển mạch gói, các thông báo được chuyển đi một lần và trọn vẹn trên mạng nên hệ thống sẽ giữ trách nhiệm phân phối nó. *So sánh với* packet switching. *Xem* store and forward.

message switching center ***trung tâm chuyển mạch thông báo*** Trong truyền thông dữ liệu, một trung tâm ở đó các thông báo được định tuyến theo thông tin chứa trong chính các thông báo. *Đồng nghĩa với* relay center.

message text ***nội dung thông báo, văn bản thông báo*** Trong liên lạc dữ liệu, phần thông báo liên quan khá chặt chẽ tới bên nhận thông báo. Nội dung thông báo không chứa phần tiêu đề và phần thông tin điều khiển. *So sánh với* message heading.

message transfer agent ***bộ phận chuyển thông báo, đại lý chuyển thông báo*** Trong truyền thông dữ liệu, một thành phần trong các hệ thống gửi thư điện tử chuyển tiếp thông báo từ người gửi tới người nhận. Nếu bộ phận chuyển thông báo nhận được một thông báo từ bộ phận người dùng thì nó sẽ kiểm tra cú pháp và trả lại thông báo cùng với lời giải thích cho trạm người sử dụng nếu thông báo không hợp lệ. Nếu thông báo hợp lệ thì nhóm ký tự định danh thông báo và tem ngày tháng sẽ được dán vào nó. Sau đó thông báo được xử lý giống như các thông báo nhận được từ các trạm chuyển phát khác. Nếu thông báo được nhắm tới hộp thư địa phương thì nó sẽ được phân phát, được xếp đợi phân phối hoặc được lưu trong hộp thư; trái lại, nó sẽ được chuyển tới trạm chuyển phát thông báo tiếp theo. *So sánh với* user agent. *Xem* electronic mail, user agent, X.400.

metadata ***siêu dữ liệu*** (1) Trong tính toán, sự tham chiếu dữ liệu tới một dữ liệu khác (như các cấu trúc dữ liệu, chỉ số và con trỏ) mà được dùng để diễn giải một khái niệm trừu tượng

(chẳng hạn "quá trình", "tác vụ", "đoạn", "tệp" hoặc "ống dẫn"). (2) Trong tính toán, một cơ sở dữ liệu đặc biệt cũng được tham chiếu tới như một cuốn từ điển dữ liệu chứa các mô tả về các phần tử (chẳng hạn các quan hệ, vùng, các thực thể hay các mối tương quan).

method of advice ***phương pháp thông báo*** Trong hoạt động ngân hàng, một phương pháp thông tin đặc biệt cho nhóm thứ ba. *Xem* advice.

metropolitan area network ***mạng khu vực thủ đô, mạng khu vực trung tâm*** Trong truyền thông, một mạng liên lạc phục vụ một thành phố. *So sánh với* local area network. *Đồng nghĩa với* municipal area network.

MF keypad ***vùng phím đa tần*** Trong truyền thông, một vùng phím cung cấp các tín hiệu đa tần, những tín hiệu này có thể được dùng với những loại tổng đài điện thoại phù hợp cho cả hai mục tiêu gọi thiết lập và sau đó truyền dữ liệu tốc độ thấp, tức nhỏ hơn 600 baud.

MGTU virus ***virut MGTU*** Trong an toàn máy tính, một loại virut gây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian hoạt động, phá hoại chương trình, các tệp dữ liệu và OVL. *Xem* virus names.

MIC ***mã toàn vẹn thông báo*** *Xem* message integrity code.

Michelangelo ***virut Michelangelo*** Trong an toàn máy tính, một loại virut vùng secto khởi động chuẩn dựa trên virut Stoned. Nó thiết lập ngày hoạt động vào 6/3, tức ngày sinh của họa sĩ Michelangelo. *Xem* virus names.

MICR ***nhận dạng ký tự nhờ mực từ tính, kỹ thuật MICR*** Viết tắt của Magnetic Ink Character Recognition. Một kỹ thuật để nhận dạng các ký tự được in bằng mực chứa một ít chất liệu từ tính. MICR được dùng trong công nghiệp ngân hàng để ghi các mã được truyền đi và các số tài khoản trên các tấm séc để xử lý dữ liệu. *So sánh với* optical character recognization.

microbend loss ***tổn hao do cong nhẹ, mất mát do uốn cong vi mô*** Trong truyền thông, sự rò rỉ ánh sáng do những điểm uốn nhỏ đột ngột trong cáp sợi quang, sự cố này có thể xảy ra khi sợi thủy tinh chạm phải lớp vỏ bọc phủ lên nó. *So sánh với* macrobend loss. *Xem* fiber optics.

Microbes ***virut Microbes*** Trong an toàn máy tính, một loại virut gây chấm dứt chương trình và nằm thường trú trong bộ nhớ, gây nhiễm lên secto khởi động của đĩa mềm và đĩa cứng, phá hoại secto khởi động, tác động trong thời gian hoạt động, phá hoại các tệp dữ liệu. *Xem* virus names.

microcircuit card ***cạc vi mạch*** *Đồng nghĩa với* smart card.

microcomputer ***máy vi tính, máy tính cỡ nhỏ*** Một thuật ngữ dùng chỉ các máy tính để bàn được thiết kế cho những người yêu máy tính, các ứng dụng kinh doanh nhỏ và giáo dục, khi được so sánh với một bộ vi xử lý, là chip vi xử lý trung tâm của máy vi tính.

microdata file ***tệp dữ liệu vi mô*** Trong an toàn cơ sở dữ liệu, một tệp chứa thông tin về các cá nhân, các hộ

gia đình, các doanh nghiệp... *Xem* inference control.

micro mainframe link ***kết nối vi khối chính*** *Xem* cooperative processing.

microprocessor ***bộ vi xử lý*** Trong tính toán, một chip đơn lẻ chứa một khối xử lý trung tâm đầy đủ trong đó có khối logic, khối số học và khối điều khiển. Các loại bộ vi xử lý khác nhau có thể nhận các lệnh mã theo các từ có độ dài 8, 16, 32 và 64 bit và hoạt động như khối xử lý trung tâm hoặc như bộ đồng xử lý trong một máy vi tính.

microprocessor card ***cạc vi xử lý*** *Xem* smart card.

microwave motion detection ***phát hiện chuyển động ở dải vi ba*** *Xem* microwave sensor.

microwave sensor ***bộ cảm biến vi ba*** Trong an toàn vật lý, một thiết bị phát hiện đột nhập của người thông qua một mẫu vi sóng do một máy phát tạo ra. Sự phát hiện dựa trên hiệu ứng Doppler hay nguyên lý ngắt chùm tia. Hiệu ứng Doppler là sự thay đổi rõ ràng về tần số khi tốc độ giữa nguồn phát xạ và máy thu thay đổi. *Xem* beam break.

MID ***ký hiệu nhận dạng thông báo, bộ định danh thông báo, ký hiệu MID*** Trong hoạt động ngân hàng, viết tắt của Message IDentifier, ký hiệu nhận dạng thông báo được dùng để xác định một thông báo hay giao dịch tài chính trong tính toán MAC, trong phép thử hay trong dấu xác thực. *Xem* authenticator, MAC, test.

midnight attack ***tấn công lúc nửa đêm*** Trong quản lý khóa, một tấn công trong đó, phiên liên lạc phức hợp giữa máy chủ và thiết bị đầu cuối, có cả truyền khóa phiên (khóa này được mã bằng khóa terminal) sẽ bị nghe trộm và được ghi lại. Sau đó, một cách ẩn dụ, vào lúc nửa đêm, kẻ tấn công truy nhập được tới thiết bị đầu cuối không bị giám sát và đưa vào đó thông tin thu được giữa máy chủ và thiết bị đầu cuối, như vậy giả trang như máy chủ liên lạc với thiết bị đầu cuối. Thiết bị đầu cuối sẽ giải mã bản mã thu được bằng khóa phiên đã mã thu được. Tấn công này có thể ngăn chặn được bằng thủ tục bắt tay. *Xem* handshaking, masquerading, session key, terminal key.

migration ***(kỹ thuật) di chuyển*** Trong cơ sở dữ liệu, một kỹ thuật dùng kho chứa truy nhập nhanh được tối ưu hóa bằng cách chuyển các mục ít bị truy nhập tới thiết bị nhớ có tốc độ chậm, giá thành thấp.

military critical technology ***công nghệ quân sự quan trọng*** Những vật dụng đi kèm hoạt động, ứng dụng hoặc bí quyết bảo trì tinh vi đóng góp to lớn vào tiềm lực quân sự của nước bất kỳ hay nhiều nước liên kết và có thể chứng minh là gây hại cho an ninh của Hoa Kỳ. *Xem* know how.

Milnet ***mạng quân sự*** *Xem* Internet.

Milwauke 414 ***nhóm tin tặc Milwauke 414*** Trong an toàn máy tính, nhóm 7 thanh niên ở Milwauke, vùng Wisconsin đã đột nhập trái phép vào các máy tính trải suốt từ Mỹ tới Canada trong năm 1983. Nhóm lấy tên theo mã điện thoại vùng Milwauke. *Xem*

hacker, telephone intrusion.

mimicking *giả mạo* *Đồng nghĩa với* masquerading.

minimal cover time *thời gian bảo vệ tối thiểu* Trong mật mã, thời gian bảo vệ ngắn nhất trước tấn công có thể bất kỳ. *Xem* cover time.

minimum knowledge proof *chứng minh với tri thức tối thiểu* *Đồng nghĩa với* zero knowledge proof.

minimum weight routing *định tuyến theo trọng số tối thiểu* Trong truyền thông dữ liệu, một phương pháp tối ưu hóa cuộc truyền một thông báo bằng việc kết hợp yếu tố trọng số với mỗi kết nối trên mạng. Đường truyền được chọn là đường tối thiểu hóa tổng các trọng số của các đường mà nó dùng. Nếu các trọng số được chọn là trễ chuyển tiếp của các đường dây thì sẽ nhận được tuyến có trễ tối thiểu. *Xem* adaptive routing, directory routing.

minor change to a system of records *sửa đổi nhỏ hệ thống các bản ghi* Trong tính toán, sự sửa đổi không làm thay đổi quan trọng hệ thống; nghĩa là không ảnh hưởng tới đặc trưng hay mục đích của hệ thống và không làm ảnh hưởng tới khả năng một cá nhân truy nhập được tới bản ghi của anh ta hay bất kỳ thông tin liên quan tới anh ta trong hệ thống, chẳng hạn sự thay đổi đầu đề của bộ quản trị hệ thống.

MIPS *triệu lệnh/giây* Viết tắt của Million Instruction Per Second, một số đo năng lực tính toán. *So sánh với* LIPS.

Mirror *virut Mirror* Trong an toàn máy tính, một loại virut làm chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp EXE, tác động trong thời gian chạy và phá hoại các chương trình và các tệp OVL. *Xem* virus names.

miscellaneous common carrier *công ty truyền thông đa tạp công cộng* Trong truyền thông, các công ty truyền thông không cam kết cung cấp các dịch vụ điện thoại hay điện báo. Thường những công ty này có trách nhiệm đối với các dịch vụ truyền thanh và vô tuyến dùng các kết nối vi ba mặt đất. *Xem* common carrier.

MIX1 *virut MIX1* Trong an toàn máy tính, một loại virut làm chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COMMAND.COM, COM, EXE, tác động trong thời gian chạy và phá hoại các chương trình và các tệp OVL. *Xem* virus names.

MIX2 *virut MIX2* Trong an toàn máy tính, một loại virut làm chấm dứt chương trình và nằm thường trú, lây nhiễm tới các tệp COMMAND.COM, COM, EXE, tác động trong thời gian chạy và phá hoại các chương trình và các tệp OVL. *Xem* virus names.

MLAT *Hiệp ước hỗ trợ luật pháp lẫn nhau* *Xem* Mutual Legal Assistance Treaty.

MLS *an toàn nhiều mức; bộ sinh an toàn nhiều mức* (1) An toàn nhiều mức, *xem* multilevel secure. (2) Trong an toàn máy tính, bộ sinh an toàn nhiều mức là bộ tạo thể thức an toàn nhiều mức - một công cụ phân tích lưu lượng được phát triển tại SRI để

dùng với HDM. *Xem* HDM, security flow analysis.

MMS ***Hệ thống Thông báo Quân sự, hệ MMS*** Viết tắt của Military Message System. *Xem* Landwehr's security model for military message systems.

mocking brid ***chương trình nhái*** Trong an toàn máy tính, một chương trình hoặc quá trình máy tính bắt chước hành vi hợp pháp về một tính năng hệ thống thông thường (hay một chức năng hữu dụng tường minh khác) song thực hiện các hành động ác ý ngay khi được người dùng gọi tới. *So sánh với* Trojan Horse, virus.

MOD ***ngày khởi đầu thông báo*** Trong hoạt động ngân hàng, viết tắt của Message Origination Date, ngày mà dựa vào đó người khởi đầu giao dịch đã tính MAC, thử nghiệm hoặc dấu xác thực. *Xem* authenticator, MAC.

mode ***phương thức; chế độ; giá trị mốt; kiểu*** (1) Trong mật mã, phương thức là cách thức hoạt động của mã khối, chẳng hạn sồ mã điện tử, liên kết khối mã... *Xem* block cipher, cipher block channing, electronic codebook. (2) Trong tính toán, chế độ một nút tùy chọn trong phương pháp hoạt động, chẳng hạn, chế độ nhị phân, chế độ chữ - số... (3) Trong toán học, giá trị mốt là giá trị thường xuất hiện nhất trong một mẫu thống kê. (4) Trong truyền thông, kiểu là cách thức các chùm tia sáng truyền dọc theo cáp sợi quang. *Xem* fiber optics, mode dispersion, monomode fiber, multimode fiber.

mode dispersion ***tán sắc kiểu*** Trong truyền thông, sự tán sắc xuất hiện do các chùm ánh sáng đi qua các nhánh khác nhau trong sợi quang. Sự tán sắc này làm méo xung nhận được. *Xem* fiber optics, mode, monomode fiber, multimode fiber.

model ***mô hình*** (1) Trong an toàn dữ liệu, sự biểu thị chính sách ở dạng để hệ thống có thể tuân thủ hoặc có thể phân tích về tính hợp lý của chính sách và việc buộc tuân thủ nó. (2) Sự biểu diễn một hệ thống cụ thể ở dạng logic, chẳng hạn, thông qua phần mềm để dự báo sự cố nào đó trong tương lai.

modeling ***(sự) lập mô hình*** Trong luật pháp, việc sử dụng một máy tính để dàn cảnh một tội ác.

MODEM ***modem, bộ biến hoàn điệu, bộ điều chế-giải điều chế*** Trong truyền thông dữ liệu, viết tắt từ MOdulator-DEModulator, một thiết bị điều chế tín hiệu cần truyền đi và giải điều chế tín hiệu thu được tại trạm dữ liệu. Ví dụ, một modem được dùng để chuyển một tín hiệu số từ một máy tính thành tín hiệu tương tự để truyền trên mạng và thường được dùng để liên lạc giữa các máy vi tính trên mạng điện thoại. Một modem có thể làm việc trong chế độ song công hoặc bán song công trên mạch hai hoặc bốn dây. *Xem* four wire circuit, full duplex, half duplex, modulation, limited distance modem, security modem. *Đồng nghĩa với* data set.

mode of attack ***kiểu tấn công, phương thức tấn công*** Trong an toàn thông tin, một chuỗi những cuộc tấn công thực sự theo một nhánh tấn công chỉ ra. Điều này được thực hiện

bằng cách tấn công trực tiếp hoặc gián tiếp lên điểm yếu cụ thể của mỗi biện pháp đối phó trong nhánh đó. *Xem* attack path, information technology security evaluation criteria, vulnearability.

mod n ***phép lấy phần dư n*** Trong toán học, b (mod n) là phần dư còn lại sau phép chia số nguyên b cho n, chẳng hạn 7 (mod 3) = 1. *Xem* congruent, modulo arithmetic, residue.

modular redundancy ***dư thừa môđun, lắp dư môđun*** Trong lĩnh vực độ tin cậy, một phương pháp lắp dư mạch cứng trong đó một môđun được nhân bản và nhiều bản sao chạy song song. Các đầu ra của các môđun được so sánh với nhau và sự khác nhau giữa chúng cho thấy có sai sót. *So sánh với* structural redundancy, hardware redundancy, hybrid redundancy, NMR, triple modular redundancy.

modulated photoelectric sensor ***bộ cảm biến quang điện điều chế*** Trong an toàn vật lý, một bộ phát hiện xâm nhập dùng chùm tia đã điều chế, thường là tia tử ngoại ánh sáng đỏ. Máy thu tạo ra một tín hiệu báo động khi không có tia tới được điều chế ở tần số chỉ ra. Như vậy, hệ thống tái hoạt động cả khi chùm tia bị ngắt lẫn khi có có vật gì đó đi qua nhờ dùng một chùm ánh sáng hướng trực tiếp tới máy thu. *Xem* photoelectronic sensor.

modulating signal ***tín hiệu điều biến*** Trong truyền thông, một tín hiệu bị cưỡng bức theo sóng mang nhằm thay đổi nó theo dạng nào đó. *Xem* carrier, modulation.

modulation ***(sự) điều chế, (sự) điều biến*** Trong truyền thông, một quá trình chuyển thông tin lên sóng mang để truyền đi. Suốt quá trình đó, đặc trưng nào đó của sóng liên tục, chẳng hạn tần số hay biên độ của nó, được thay đổi theo tín hiệu điều chế như sóng tiếng nói, truyền hình hay fax. *Xem* amplitude modulation, frequency modulation, modulating signal, phase modulation, pulse modulation.

modulation rate ***tốc độ điều biến*** Trong truyền thông, đại lượng nghịch đảo của khoảng thời gian ngắn nhất giữa các thời khoảng có nghĩa kế tiếp nhau của tín hiệu được điều chế. Nếu đại lượng đo này được tính theo giây thì tốc độ điều biến tính theo baud. *Xem* baud, modulation.

modulator ***bộ điều biến, bộ điều chế*** Trong truyền thông, một thiết bị hay máy biến đổi đặc trưng nào đó của tín hiệu. *Xem* modulation.

module interface analysis ***phân tích mạch ghép nối môđun*** *Xem* static analysis.

modulo arithmetic ***số học môđulo*** Trong toán học, một dạng số học trong đó chỉ dùng những phần dư của phép chia cho số nguyên.

Nếu chia b cho n được phần dư là c thì mệnh đề này được viết như sau: $b \equiv c \pmod{n}$ hay b đồng dư với c theo môđulo n; c được gọi là phần dư của b môđulo n.

Có thể thực hiện phép cộng và nhân trực tiếp trên các phần dư, tức là nếu $b_1 \equiv c_1 \pmod{n}$ và $b_2 \equiv c_2 \pmod{n}$ thì $b_1 + b_2 \equiv c_1 + c_2 \pmod{n}$.

Tương tự với phép nhân, với các số nguyên k_1, k_2:

$b_1 \ b_2 = (k_1 n + c_1).(k_2 n + c_2)$

$= (k_1 k_2 n + c_1 k_2 + c_2 k_1) n + c_1 c_2$

Bởi vậy

$b_1 b_2 \equiv c_1 c_2 \pmod{n}$.

Một kỹ thuật số học modulo đặc biệt hữu dụng đối với phép lấy lũy thừa. Nếu một số có 200 chữ số cần được nâng lên lũy thừa bậc cao theo số học modulo thì rất có lợi nếu có thể rút gọn chính lũy thừa theo số học modulo. Xét hai trường hợp, đầu tiên hạn chế n là số nguyên tố để nó không thể chia hết cho b. Định lý của Fermat cho kết quả hữu dụng sau:

$b^{n+1} \equiv 1 \pmod{n}$; ví dụ

$2^6 = 64 \equiv 1 \pmod{7}$.

Bởi vậy, đặt hạn chế lên n và b, có thể giảm lũy thừa của b theo modulo $n - 1$. Ví dụ: $2^{16} \equiv 2^{6}.2^{6}.2^{4} \pmod{7} \equiv 1.1.2^4 \pmod{7} = 2$, vì thế trong phép tính $2^{16} \pmod{7}$, có thể giảm số mũ từ 16 xuống còn 4.

Nếu n không phải là số nguyên tố thì phải dùng phép suy rộng Euler. Trong trường hợp này, trước hết cần xác định hàm Euler $\phi(n)$, hàm này bằng số các số nguyên tố cùng nhau với n nằm trong dải $1..n - 1$, chẳng hạn $\phi(10) = 4$, (1 3 7 9). Phép suy rộng Euler phát biểu rằng:

$b^{\phi(n)} \equiv 1 \pmod{n}$.

miễn là b nguyên tố cùng nhau với n. Như vậy, với điều kiện này có thể rút gọn lũy thừa theo modulo $\phi(n)$, chẳng hạn $3^7 \pmod{10} \equiv 2187 \pmod{10} \equiv 7$, khi rút gọn lũy thừa $\phi(10) = 4 \pmod{n}$ ta sẽ được $3^7 \pmod{10} \equiv 3^3 \pmod{10} \equiv 27 \pmod{10} \equiv 7 \pmod{10}$.

Số học modulo rất quan trọng trong mật mã vì nó đưa tính ngẫu nhiên bậc cao vào các hàm số, làm cho người mã thám khó mà thu hẹp được vùng tìm kiếm. Xét hàm bậc ba $y = x^3$. Nếu biết x nằm giữa 6 và 15 thì y phải nằm trong khoảng từ 216 tới 3375. Tuy nhiên, nếu dùng số học modulo 10 thì y có thể lấy giá trị bất kỳ trong số các giá trị 6, 3, 2, 9, 0, 1, 8, 7, 4 hoặc 5. Ngoài ra, mẫu đầu ra thay đổi theo kiểu không thể dự đoán được khi đầu vào thay đổi; một sự thay đổi nhỏ của x từ 9 tới 10 sẽ tạo ra sự biến đổi của y từ 9 tới 0, tức là từ một giá trị cực trị này tới giá trị cực trị khác trong phạm vi các đầu ra có thể. *Xem* congruent, coprime, Euler's Generalization, Fermat's Theorem, RSA.

modulo n ***modulo n*** *Xem* congruent, mod N, modulo arithmetic.

modulo N check ***kiểm tra modulo N*** Trong tính toán, một biện pháp kiểm tra các giá trị của dữ liệu mà nhờ đó, một toán hạng chia cho số N và phần dư được dùng làm chữ số kiểm tra. Thường N được chọn là 11, như vậy, 81 modulo 11 = 4. *Xem* operand.

modulo 2 ***modulo 2*** Trong toán học, một phép toán tương đương với phép loại trừ - hoặc, tức là 0 + 0 = 0, 0 + 1 = 1 và 1 + 1 = 0. Nó là phép tính quan trọng trong tiêu chuẩn mã số liệu DES và được viết là $A +_2 B$. Chú ý rằng $A +_2 A = 0$. *Xem* DES, EXCLUSIVE OR, modulo arithmetic.

monitoring ***(sự) giám sát*** Trong an toàn dữ liệu, việc ghi chép lại thông tin liên quan về mỗi hoạt động của một chủ

thể trên một đối tượng, được duy trì trong vệt kiểm toán giúp cho việc phân tích sau này. *So sánh với* threat monitoring. *Xem* audit trail, automated security monitoring, object, subject.

monitoring station ***trạm giám sát*** Trong an toàn vật lý, một khu vực ở xa mà đứng tại đó, những người bảo vệ vẫn có thể giám sát các bảng tín hiệu báo hệ thống an toàn hoặc các máy thu tín hiệu báo động. *So sánh với* central station.

monoalphabetic cipher ***mã pháp đơn biểu*** Trong an toàn dữ liệu, một phép mã thay thế trong đó mỗi chữ cái của bảng chữ cái sẽ ánh xạ lên chữ cái khác với mỗi sự ghép cặp riêng được giữ cố định theo ý người mã dịch. *So sánh với* polyalphabetic cipher. *Xem* cipher cryptography, substitution cipher.

monolithic TCB ***TCB đơn khối*** Trong an toàn tính toán, một cơ sở tính toán tin cậy (TCB) chứa một tập con TCB đơn lẻ. *Xem* Blue Book, TCB subset.

monomode fiber ***sợi quang đơn kiểu*** Trong truyền thông, sợi quang có lõi rất nhỏ (2 - 10 micron); tuyến truyền duy nhất là dọc trục x, vì thế có mức tán sắc thấp. *So sánh với* multimode fiber. *Xem* fiber optics, mode, mode dispersion.

Monxla ***virut Monxla*** Trong an toàn máy tính, một loại virut lây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian hoạt động, phá hoại chương trình và các tệp OVL. *Xem* virus names.

Moriss worm ***sâu Moriss*** Trong an toàn máy tính, một loại sâu do một sinh viên tốt nghiệp tên là Robert Tappan Moriss đã tấn công lên mạng Internet của Mỹ vào tháng 11/1988.

Internet vào lúc đó là một mạng logic ở Mỹ chứa nhiều mạng vật lý nối tới 60.000 viện nghiên cứu, các máy tính nghiên cứu và máy tính quân sự. Mạng Milnet trong hệ thống này được dự bị cho liên lạc quân sự an toàn cao song không phải hầu hết là thông tin quân mật.

Chỉ trong vài giờ tràn qua mạng, sáng hôm sau, vài ngàn máy tính đã bị lây nhiễm. Mạng đã chịu tổn thất nặng và các nhà quản trị hệ thống đã phải ngắt máy tính của họ ra khỏi mạng để tránh hậu họa.

Sâu (worm) được viết bằng ngôn ngữ lập trình C và nó đã tấn công các hệ thống máy vi tính Sun 3 và các máy tính Vax (Vax là đăng ký nhãn hiệu của Phòng thí nghiệm Digital Equipment) chạy trên các kiểu hệ điều hành BSD 4 Unix (Unix là nhãn hiệu đăng ký của các Phòng thí nghiệm AT&T).

Sâu không chứa mã thực hiện các hành vi ác ý. Tác động độc hại của nó là do sự quá tải của các máy tính trên mạng bị lây nhiễm sâu, do thời gian tiêu phí vào việc kiểm tra các máy tính có thể lây nhiễm và những nỗ lực quá sức của các nhà khoa học máy tính khi phân tích sâu và chỉnh lại các hành động của nó. Như thế, sâu đã không:

- tác động tới các tệp hệ thống hoặc tệp của người dùng;
- làm thay đổi các chương trình của người dùng, giúp cho việc làm lan truyền nó;
- cài các con ngựa thành Torroa;
- ghi hoặc phát các mật khẩu do kẻ tấn

công phát ra;

- cố gắng giành quyền quản trị hệ thống, tức người sử dụng siêu đẳng, các đặc quyền.

Worm (sâu) đã được viết bằng C và nó chứa hai thành phần:

- Chương trình mồi với 99 dòng mã nguồn được viết bằng ngôn ngữ C (còn được gọi là chương trình vecto).
- Hai tệp lớn có thể định vị lại các tệp đối tượng chứa Sun 3 và Vax - những bản tương ứng phần thân chính của Worm.

Hoạt động của Worm có thể chia thành các cơ chế tấn công, bảo vệ và kiểm soát chung. Trong giai đoạn tấn công, khi đang có một tài khoản trong máy chủ, Worm sẽ cố tìm cách lây nhiễm tới các máy khác trước hết bằng cách:

- xác định địa chỉ các máy chủ ở xa;
- gài chương trình mồi lên một trong những máy đó;
- dịch và thi hành chương trình mồi trên các máy chủ đó;
- lợi dụng hoạt động của chương trình mồi để tải phần còn lại của Worm và sau đó thi hành Worm trên máy chủ mới.

Các cơ chế bảo vệ được thiết kế để tránh các cuộc phản công nhằm phát hiện và loại bỏ Worm đã gây khó khăn cho việc tìm kiếm phân tích hoạt động của Worm từ bất kỳ đoạn mã nào bắt được. Các kỹ thuật kiểm soát chung tìm cách tránh sự sinh sôi nhanh chóng tính độc hại của Worm trên máy chủ bất kỳ bằng một kỹ thuật xác định sự tồn tại của con sâu khác và sau đó tung súc sắc để xác định xem con (sâu) nào trong hai con cần tự hủy.

Bước đầu tiên khi lây nhiễm tới máy chủ mới, Worm nhận được địa chỉ của những máy chủ và tên các tài khoản được giữ trên máy chủ đó. Thông tin này được nhận từ một loạt các tệp khác nhau (có thể đọc được) của người dùng trên máy chủ đã bị nhiễm Worm. Khi đó, chúng tấn công các máy chủ ở xa nhờ lợi dụng một trong hai kẽ hở phần mềm đã biết trong các chương trình gửi thư điện tử (Sendmail) và chương trình finger hoặc lợi dụng tính kém kỷ luật về an toàn của con người.

Hệ thống gửi thư điện tử Sendmail là một chương trình phần mềm rất phức tạp, cung cấp các phương tiện gửi thư điện tử trên mạng. Người gửi thông báo làm việc trên một máy chủ sẽ tạo ra một thông báo và dán địa chỉ mạng thích hợp của người nhận lên đó. Chương trình Sendmail sẽ truyền thông báo trên mạng, có thể dùng các cổng cung cấp các nối từ một mạng cục bộ đến một mạng khác và cuối cùng Sendmail lưu thông báo trong tệp chứa thư điện tử thích hợp trên máy chủ của người nhận.

Như vậy, thư điện tử phải cung cấp một cơ chế gài dữ liệu vào máy tính khác trên mạng khi người gửi không có các đặc quyền cần thiết để đăng nhập vào máy tính. Điều này bản thân nó không thể hiện vấn đề về an toàn máy tính. Tuy nhiên, nếu người gửi theo cách nào đó, có thể gài và thực thi các chương trình trên máy tính bên nhận thì sẽ tồn tại một hở vòng cho các virut và sâu. Khả năng này có thể được gói phần mềm Sendmail cung cấp dưới tình

huống nhất định. Thông thường thư điện tử được phân phối tới (tệp) hộp thư, song Sendmail cũng cho phép người nhận mà nó nhắm tới chuyển hướng thư mới tới vào một quá trình. Ví dụ, quá trình gửi một thông báo trả lại, cho người gửi biết người nhận đang nghỉ và không thể đọc thư được.

Hở vòng trong phương tiện Sendmail do chương trình gỡ rối đưa ra. Nếu người quản trị hệ thống để cờ gỡ rối ở trạng thái mở (on) thì người gửi hay đúng hơn là người nhận thư có thể hướng thư tới một quá trình. Hở vòng này đã được phát triển một cách trong suốt để kiểm tra hoạt động của Sendmail trên mạng, song nó lại gây nên hở vòng nghiêm trọng về an toàn. Một người sử dụng trái phép có thể thực hiện các thao tác trên các máy tính nối mạng ở xa. Worm gửi một thông báo, lợi dụng kẽ hở vòng trong quá trình gỡ rối, tải chương trình mồi, dịch và thi hành nó.

Hở vòng thứ hai xuất hiện từ kẽ hở trong demon finger thuộc chương trình fingerd. Đemon là một chương trình liên tục kiểm tra các điều kiện nào đó. Nếu điều kiện được thỏa mãn, chương trình sẽ hành động. Chương trình finger cho phép người sử dụng tại chỗ nhận được thông tin về người dùng trên máy tính chính, còn chương trình demon fingerd sẽ cung cấp phương tiện này cho những người dùng ở xa. Như vậy, có thể gửi một yêu cầu hỏi xem liệu một người dùng cụ thể hiện đã nhập mạng tại máy chủ ở xa chưa. Chương trình finger bản thân nó không gây ra mối nguy hại về an toàn. Song chương trình con fingerd lại có kẽ hở về lập trình, nó đã lưu dữ liệu nhận được vào ngăn xếp mà không kiểm tra xem có đủ không gian nhớ cấp phát để điều tiết nó không.

Worm gọi chương trình fingerd với một thông báo dài được cấu trúc một cách đặc biệt làm tràn bộ nhớ đệm, ghi đè lên các phần của ngăn xếp. Trên đường ra khỏi chương trình finger, điều khiển chuyển tới mã chứa những lệnh do Worm cung cấp. Những lệnh gài sẵn này được thiết kế để chương trình mồi Worm được biên dịch và thi hành.

Tuyến lây nhiễm thứ ba không dựa vào những kẽ hở phần mềm song lại lợi dụng thói quen lỏng lẻo về an toàn về phía người dùng. Worm có một hệ thống phỏng đoán mật khẩu phức tạp, khi nó phỏng đoán một mật khẩu thì nó có cách nhập vào tài khoản của người sử dụng trên máy nội bộ. Ngoài ra, đặc quyền này có thể cũng cho phép Worm truy nhập tới các tài khoản của cùng người sử dụng trên các máy mạng khác.

Morris đã bị tuyên bố phạm tội về cuộc tấn công lên mạng Internet, đã bị phạt 10.000 đô la, bị thử thách 3 năm và 400 giờ lao động công ích. *So sánh với* Xmas tree. *Xem* debug, Internet, loophole, malicious code, virus, worm.

motion detector ***bộ phát hiện chuyển động*** Trong an toàn vật lý, một hệ thống phát hiện sự chuyển động trong khu vực bảo vệ bằng cách so sánh các trường năng lượng xung quanh, hoặc phát hiện ra những sự phản xạ hay những thay đổi theo sự phát năng lượng liên tiếp. *Xem* infrared motion detector, microwave sensor, ultrasonic

motion detector. *Đồng nghĩa với* presence detector.

MOTIS ***trao đổi văn bản định hướng thông báo, giao thức MOTIS*** *Xem* message oriented text exchange.

M out of N code ***mã N sai M bit*** Trong các loại mã, mã truyền cùng với các phương tiện phát hiện lỗi gài trong nó. Số bit chỉ ra (M) trong ký tự có N bit phải là các bit 1. Ký tự nhận được bất kỳ không chứa tất cả M bit 1 sẽ khởi đầu một thủ tục phát hiện lỗi. *Xem* error detection code. *Đồng nghĩa với* constant ratio code.

MSAR ***(các) yêu cầu bảo đảm an toàn tối thiểu, yêu cầu MSAR*** Trong an toàn máy tính, viết tắt của Minimum Security Assurance Requirements. *Xem* MFSR.

m-sequence ***dãy m*** Trong toán học, một dãy các chữ số nhị phân có độ dài n bit và có chu kì 2^{n-1} bit tạo ra từ một thanh ghi dịch có phản hồi tuyến tính. Dãy có độ phức tạp tuyến tính cực đại với chu kỳ của nó. *Xem* bit, linear complexity, linear feedback shift register.

MSFR ***(các) yêu cầu chức năng an toàn tối thiểu, yêu cầu MSFR*** Trong an toàn máy tính, viết tắt của Minimum Security Functionality Requirements, một tập các yêu cầu đối với các hệ điều hành đa dụng nhiều người sử dụng đã được phát triển như một phần của dự án FC-FIPS. Những yêu cầu này đã xây dựng dựa trên công trình trước đó của cả TCSEC (Tiêu chuẩn đánh giá hệ thống tin cậy của Mỹ) và ITSEC (Tiêu chuẩn đánh giá hệ thống thông tin của Châu Âu). Chúng đã xác định các yêu cầu cơ bản có thể áp dụng cho các trạm làm việc nhiều người sử dụng, các máy tính cỡ nhỏ và các máy tính lớn. Có thể dùng chúng như một tập các nguyên tắc chỉ đạo giúp cho những nhà thiết kế xây dựng các yêu cầu ứng dụng đặc biệt. Tài liệu đã xác định tám chức năng buộc tuân thủ tính an toàn tương tự với biện pháp của ITSEC:

- định danh và xác thực;
- kiểm soát truy nhập;
- phân định trách nhiệm;
- kiểm toán;
- dùng lại đối tượng;
- tính chính xác;
- tính tin cậy của dịch vụ;
- trao đổi dữ liệu.

Trong mỗi trường hợp, nó đưa ra các chỉ tiêu chi tiết được gắn nhãn (R) hoặc (A). "R" chỉ các chỉ tiêu thỏa mãn các nhu cầu của một doanh nghiệp thương mại điển hình hay tổ chức của chính phủ. "A" chỉ các chỉ tiêu đáng mong muốn của một doanh nghiệp thương mại điển hình hay tổ chức của chính phủ. Người ta đã nhận thấy trong tài liệu rằng, sự hiện diện của riêng những tính năng an toàn mong muốn không đủ để thiết lập giá trị tiềm tàng của một sản phẩm máy tính nhằm bảo vệ thông tin. Bởi vậy, các yêu cầu ràng buộc sự phát triển sản phẩm và các thủ tục đánh giá và chỉ ra bằng chứng đã được tạo ra như một kết quả các xử lý yêu cầu bảo đảm. Các yêu cầu bảo đảm an toàn tối thiểu (MSAR) sẽ nằm trong FC-FIPS để dùng với MSFR. Những yêu cầu bảo đảm này đại diện cho sự hội tụ của lớp C2 thuộc TCSEC và mức E2

của ITSEC. *Xem* baseline. ITSEC, FC-FIPS, FIPS, Orange Book, TCSEC.

MSM ***phép biến đổi dòng thông báo, phép biến đổi MSM*** Trong xác thực, viết tắt của Message Stream Modification, là phép biến đổi dòng thông báo. *Xem* message authentication.

MTA *Xem* message transfer agent.

MTBF *Xem* mean time between failure.

MTS ***dịch vụ chuyển thông báo, dịch vụ MTS*** Trong truyền thông dữ liệu, viết tắt của Message Transform Service, là dịch vụ chuyển thông báo theo chuẩn quản lý thông báo CCITT X.400. *So sánh với* MTA, UA. *Xem* X.400.

multicast ***truyền đa kiểu*** Trong truyền thông, sự truyền đồng thời dữ liệu hoặc các tín hiệu tới nhóm lựa chọn các trạm. *So sánh với* broadcast, point-to-point.

multidrop circuit ***mạch nhiều điểm*** Trong truyền thông dữ liệu, một mạch cho khách hàng thuê để truyền dữ liệu giữa một trạm (site) trung tâm, thường là một máy tính và một số các thiết bị đầu cuối ngoài trạm. Có thể truyền hai chiều giữa thiết bị đầu cuối bất kỳ và trạm trung tâm song không được truyền trực tiếp giữa hai thiết bị đầu cuối. *So sánh với* ponit-to-point. *Xem* circuit. *Đồng nghĩa với* multipoint circuit.

multilevel database security ***an toàn cơ sở dữ liệu nhiều mức*** Trong an toàn dữ liệu, các phương pháp được dùng để bảo vệ tính an toàn của một cơ sở dữ liệu chứa dữ liệu có nhiều mức phân loại an toàn khác nhau và phục vụ cộng đồng những người sử dụng có các mức truy nhập (clearance) an toàn khác nhau. Một người dùng hợp pháp của cơ sở dữ liệu phải được cung cấp tất cả các phương tiện của một cơ sở dữ liệu thông thường chứa thông tin trong phạm vi các bảo hộ đặc quyền của người dùng. Mặt khác, sự bảo hộ người dùng hợp pháp như vậy phải chống được cả sự truy nhập tới hoặc thậm chí tham chiếu tới thông tin nằm ngoài mức đặc quyền của họ.

Người thiết kế hệ thống cơ sở dữ liệu nhiều mức cũng phải giải quyết những vấn đề về an toàn nảy sinh từ các kênh ngầm, tức là với sự rò rỉ thông tin mật do kiểu hợp tác nào đó giữa người dùng và mã ác ý nhúng trong phần mềm máy tính. Đây là vấn đề nghiêm trọng vì phần mềm DBMS cực kỳ phức tạp và không tuân theo các phương pháp đánh giá hình thức hiện thời.

Nếu một hệ thống nhiều mức an toàn cần được đánh giá thì phải có một tuyên bố trên hệ thống cần đạt tới về tính an toàn, tức là phải tuyên bố một chính sách an toàn tường minh. Theo các thuật ngữ về kiểm soát truy nhập, có hai dạng chính sách:

- kiểm soát truy nhập tùy ý;
- kiểm soát truy nhập bắt buộc.

Trong các hệ thống cơ sở dữ liệu, một người dùng sẽ lập một câu truy vấn, có thể chứa cả tiêu chuẩn lựa chọn mở rộng được gắn với một khối lượng lớn các mục dữ liệu trong nhiều tệp. Trong trường hợp này, vấn đề gán một phân loại cho câu trả lời câu truy vấn khá phức tạp. Dĩ nhiên, để chắc ăn, hệ thống luôn có thể cho dữ liệu mức phân loại bằng với mức của tệp được phân loại

cao nhất được truy nhập tới và như vậy, từ chối truy nhập đối với nhiều yêu cầu khác. Tuy nhiên, cơ sở dữ liệu phải cung cấp dịch vụ tới những người sử dụng ở tất cả các mức truy nhập (clearance). Ở mỗi mức, người dùng sẽ được cấp các phương tiện đọc như thể cơ sở dữ liệu chỉ chứa dữ liệu có phân loại an toàn kém hơn mức truy nhập (clearance) của người dùng.

Một vấn đề nghiêm trọng khác là tính toàn vẹn của cơ sở dữ liệu; một cơ sở dữ liệu lớn sẽ là đối tượng đề gài, cập nhật và xóa liên tục, trong nhiều trường hợp, những đầu vào như vậy là của cộng đồng đông đảo người dùng. Việc duy trì tính toàn vẹn của cơ sở dữ liệu là một vấn đề cơ bản đối với những người thiết kế và quản trị cơ sở dữ liệu.

Khu vực liên quan thứ ba là kiểm soát tham chiếu. Các cơ sở dữ liệu hiện hành có phần mềm BDMS cực kỳ phức tạp. Nếu những tính năng liên quan đến an toàn đều cần được thiết kế vào DBMS thì chúng gồm có:

- thiết kế lại DBMS của hệ thống hiện tại hoặc
- bản thiết kế DBMS mới.

Ở mỗi trường hợp, rất khó bảo đảm tính hiệu quả cho các tính năng an toàn được xây dựng vào các gói phần mềm lớn, phức tạp.

Ba biện pháp giữ an toàn cho các cơ sở dữ liệu nhiều mức được mô tả:

- Với mỗi mức phân loại an toàn, các ngăn an toàn cung cấp hiệu quả các cơ sở dữ liệu tách biệt về mặt vật lý;
- khóa tính toàn vẹn, cho phép trang bị thêm bộ lọc an toàn vào DBMS hiện hành;
- mô hình quan hệ của Denning.

Các hệ thống ngăn an toàn

Các hệ thống nhiều mức đặt ra nhiều vấn đề thiết kế quan trọng hơn theo quan điểm an toàn, so với các hệ thống một mức. Trong hệ thống một mức, người dùng hoặc có mức truy nhập (clearance) cần thiết hoặc không có; những nghiên cứu an toàn chủ yếu đều liên quan tới kiểm soát truy nhập vật lý.

Bởi vậy, vấn đề về các hệ thống cơ sở dữ liệu nhiều mức có thể giải quyết bằng bản sao DBMS và dữ liệu lưu đối với mỗi mức an toàn. Hệ thống cho mức an toàn thấp nhất chỉ chứa dữ liệu ở mức đó; cơ sở dữ liệu ở mức phân loại mật cao nhất sẽ chứa dữ liệu ở tất cả các mức.

Rõ ràng, một trong những nhược điểm chính của hệ thống cơ sở dữ liệu như vậy là nó không thừa nhận quy tắc dư thừa tối thiểu dữ liệu. Nếu cần gài, cần thay đổi hay xóa một mục dữ liệu có mức phân loại thấp thì tất cả các cơ sở dữ liệu chứa mục dữ liệu đó phải được thay đổi. Chắc chắn sẽ còn tồn tại những mâu thuẫn trong các cơ sở dữ liệu vì những cập nhật như vậy không chắc sẽ xảy ra đồng thời.

Froscher đã đề xuất dùng một máy tính song song để phát triển hệ thống quản trị cơ sở dữ liệu tin cậy hiệu quả cao. Hệ thống đề xuất được minh họa trên hình 1. Các hệ thống đĩa giữ tất cả dữ liệu mà người dùng đòi hỏi với mức truy nhập (clearance) cho trước. Những đĩa không được phân loại chỉ giữ những dữ liệu không phân loại; đĩa có

mức tối mật giữ những dữ liệu ở tất cả các mức phân loại... DBMS được nhân bản cho mỗi hệ thống đĩa và mỗi bản sao được quản lý bằng một bộ kiểm soát nút tin cậy. Người dùng giao tiếp với DBMS thông qua ngoại vi tin cậy. Như vậy, các tính năng liên quan tới an toàn của hệ thống nằm trong hai hệ thống tin cậy tương đối nhỏ và không được nhúng vào DBMS phức tạp.

Chức năng của Ngoại vi Tin cậy là đảm bảo cho các câu hỏi của người dùng được hướng tới hệ thống cơ sở dữ liệu con tương ứng với mức phân loại mà người dùng được đăng nhập. Một người dùng có thể vào mạng ở mức bất kỳ tương ứng với mức truy nhập hay mức thông (clearance) của anh ta. Ngoại Tin cậy cũng đảm bảo rằng, dữ liệu do hệ thống trả về được hướng trực tiếp tới người sử dụng đúng. Không kể những cái khác, Bộ kiểm soát Nút tin cậy đảm bảo rằng, những địa chỉ của người sử dụng đúng đều được thêm vào dữ liệu trả về.

Kiến trúc đưa ra cung cấp các biện pháp bảo vệ chống lại bốn dạng tấn công cơ sở dữ liệu, tức truy nhập trực tiếp, truy nhập gián tiếp, phân phối trực tiếp con ngựa thành Torroa và sự rò rỉ con ngựa thành Torroa. Trong mỗi trường hợp, những tấn công này có thể chỉ này sinh nếu có thể lấy ra được dữ liệu ở những mức phân loại cao hơn mức đăng nhập của người dùng.

Tuy nhiên, vấn đề cập nhật lại tạo ra những bài toán phức tạp hơn. Khi một người dùng đăng nhập vào ở mức thấp, thực hiện các công việc chèn, cập nhật hoặc xóa một mục dữ liệu thì tất cả các cơ sở dữ liệu ở cùng hoặc trên mức đó đều phải được cập nhật. Những cập nhật như vậy sẽ được thực hiện một cách đồng thời để tránh sự không thống nhất về dữ liệu. Các giao thức và chuyển thông báo phải được đánh giá cẩn thận; DBMS sẽ đòi hỏi cơ chế nào đó ghi lại thông báo lỗi và những thông báo lỗi như vậy từ các hệ thống phân loại mật cao có thể tạo nên dạng kênh ngầm nào đó.

Việc nhân bản dữ liệu đề cập tới rất nhiều vấn đề về kiểm soát truy nhập bắt buộc, song dùng kiểm soát truy nhập tùy ý sẽ không thể thực hiện được. Có thể dùng Ngoại vi Tin cậy để lưu các danh sách kiểm soát truy nhập, chỉ ra những người sử dụng nào được phép truy nhập tới một quan hệ cho trước. Bộ kiểm soát Nút Tin cậy khi đó chỉ lấy ra được những dữ liệu từ một đĩa nếu truy nhập tới quan hệ đó được Ngoại vi Tin cậy chấp thuận. Tuy nhiên, sự bảo đảm DBMS không có truy nhập tới dữ liệu vượt ra ngoài sự bảo hộ đặc quyền của người dùng sẽ không áp dụng trong trường hợp kiểm soát truy nhập tùy ý. Như vậy, các kiểu tấn công khác nhau mô tả ở trên đòi hỏi xem xét cẩn thận trong mối tương quan với khả năng dữ liệu bị lộ cho người dùng và điều đó trái với các quy tắc kiểm soát truy nhập tùy ý vào thời điểm đó.

Khóa toàn vẹn

Một vấn đề quan trọng trong thiết kế một hệ thống cơ sở dữ liệu an toàn nhiều mức là "liệu có thể trang bị thêm tính an toàn vào cơ sở dữ liệu hiện có không?". Khi đưa ra một thiết kế đáng mong muốn để tạo ra, thậm chí một

DBMS mức đơn, thì điều rõ ràng là, biện pháp như vậy có thể cung cấp được giải pháp khả thi duy nhất để nâng cao tính an toàn của hệ thống hiện hành.

Người ta có thể đề xuất khái niệm về bộ lọc giao tiếp với DBMS sẽ phục vụ một chức năng tương tự với bộ kiểm soát tham chiếu, làm trung gian truy nhập giữa người dùng và dữ liệu do DBMS lấy ra. Khóa toàn vẹn đã được đề xuất cho mục tiêu này (xem hình 2). Sự tách bạch về truy nhập cơ sở dữ liệu và hệ thống kiểm tra tính an toàn hàm nghĩa rằng, việc xác minh an toàn hình thức chỉ cần áp dụng cho bộ lọc và do vậy, không cần mở rộng cho phần mềm phức tạp của DBMS.

Với khóa toàn vẹn, bộ lọc sẽ gắn một tổng kiểm tra mật mã vào mỗi mục dữ liệu mà cần được gắn nhãn bằng một phân loại an toàn. Tổng kiểm tra là một MAC đã tính sẵn hiệu quả trên một mục dữ liệu và nhãn phân loại nhờ dùng khóa mật chỉ bộ lọc biết. Bản thân dữ liệu được lưu ở dạng rõ và bởi vậy có thể được DBMS điều khiển; tuy nhiên, bất kỳ cố gắng trái phép nào nhằm thay đổi dữ liệu được lưu hoặc thay đổi phân loại an toàn của nó cũng sẽ bị bộ lọc phát hiện khi nó xem xét tính hợp lệ của tổng kiểm tra. Kỹ thuật này được đặt tên là "phun sơn" vì mỗi mục dữ liệu đều được tô màu không thể tẩy xóa được cùng với phân loại của nó.

Chức năng của bộ lọc là để:

- tính tổng kiểm tra bằng khóa mật đã lưu đối với dữ liệu vào và nhãn an toàn kết hợp, sau đó gắn các tổng kiểm tra đó vào dữ liệu;
- xem xét tính hợp lệ của các tổng kiểm tra của dữ liệu được DBMS trả về cho nó và nhãn an toàn kết hợp;
- phát hiện và ghi lại tổng kiểm tra không hợp lệ bất kỳ; tổng kiểm tra không hợp lệ sẽ chỉ ra sự thay đổi (giả mạo) bất hợp pháp nhãn an toàn kết hợp và dữ liệu, chẳng hạn những mưu toan giảm cấp nhãn an toàn;
- đảm bảo rằng, mức an toàn của câu trả lời các câu hỏi nằm trong phạm vi mức truy nhập (clearance) an toàn của người sử dụng.

Các chức năng của bộ lọc sẽ được giữ đơn giản tới mức có thể để việc xác minh hình thức tính an toàn của nó được dễ dàng. Như vậy, bộ lọc sẽ không có sự truy nhập phức tạp và các chức năng tìm kiếm của DBMS.

Mô hình quan hệ của Denning

Mô hình cơ sở dữ liệu quan hệ nhiều mức an toàn của Denning cho phép nhìn sâu vào bản chất của những vấn đề đi theo các cơ sở dữ liệu an toàn dữ liệu nhiều mức.

Mô hình xử lý cả vấn đề phân loại tính toàn vẹn lẫn tính bí mật. Trên thực tế, phân loại của đối tượng và mức truy nhập một chủ thể được mô tả bởi một thành phần an toàn (mức mật, bảng phân loại mật) và thành phần toàn vẹn (mức toàn vẹn, bảng phân loại tính toàn vẹn). Mối quan tâm chính của mô hình liên quan tới phân loại và nó sẽ làm đơn giản thảo luận nếu mức phân loại xem xét chỉ có một mức phân cấp mật đơn giản, chẳng hạn như TUYỆT MẬT v.v.

Denning đã sử dụng rộng rãi khái niệm về các khung nhìn (khung hiển thị thông tin về cơ sở dữ liệu) trong mô

hình để xử lý những vấn đề nảy sinh từ các mối quan hệ chung trong dữ liệu theo quan điểm an toàn, cũng như một cơ chế để lọc dữ liệu hiển thị cho người sử dụng.

Trong mô hình, mỗi phần tử - tức mục nhập của bảng có một mức phân loại. Phân loại không đi kèm theo bản thân dữ liệu, song lại đi kèm với mỗi vị trí trong bảng. Như vậy, một mục nhập đối với hạt nhân, địa điểm sẽ chỉ ra vị trí của một trạm hạt nhân, vị trí này có thể là mật song giá trị thực sự Litteleborough lại không mật.

Việc gán mức phân loại cho mỗi phần tử không hàm ý cần lưu nó cùng với mỗi phần tử; trong một số trường hợp, mức phân loại có thể được lưu theo thuộc tính, theo bộ hoặc thậm chí theo quan hệ. Sự phân loại dữ liệu theo phần tử cũng không hàm ý rằng, có thể cho mỗi phần tử một phân loại độc lập. Trong một số trường hợp, hệ thống làm người dùng có ấn tượng một mục dữ liệu được cất trữ khi thực tế nó được tính toán từ các mục dữ liệu được lưu trữ. Trong trường hợp như vậy, phải dùng mức phân loại của những mục này để xác định mức phân loại của mục đã tìm ra.

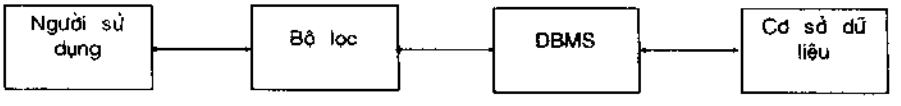
Mức phân loại của dữ liệu được trả về nhận được từ khung hiển thị thông tin (khung nhìn). Nói cách khác, phân loại của dữ liệu được trả về (trả lời) được xác định bởi khung hiển thị thông tin (trả lời các câu truy vấn), hoặc có mức phân loại cố định hoặc tính toán mức phân loại của nó dựa trên cơ sở của dữ liệu khác trong cơ sở dữ liệu. Như vậy, tất cả dữ liệu tìm thấy từ cơ sở dữ liệu đều được phân loại theo tập các khung nhìn được gọi là các điều kiện ràng buộc phân loại. Thực tế, phân loại được kết hợp với khung nhìn và phân loại có thể là một hằng hoặc một hàm số của dữ liệu mà tạo nên đầu vào cho khung nhìn.

Ưu điểm của phương pháp này là nó có thể:

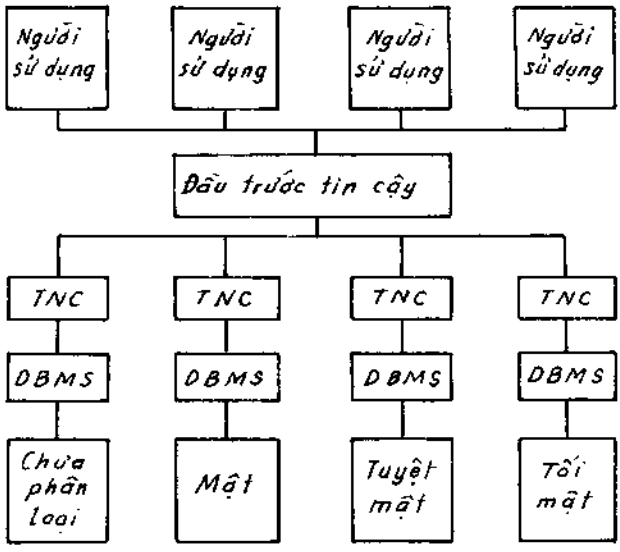
- cấp mức phân loại dựa trên cơ sở hằng số hoặc điều kiện nào đó;
- xử lý các mối quan hệ chung có thể nảy sinh giữa các phân loại của các phần tử;
- làm đơn giản dữ liệu, cho phép nó có phân loại thấp hơn phân loại được cấp theo các quy tắc;
- cấp phân loại cho dữ liệu toàn thể cao hơn phân loại được cấp theo các quy tắc thuần nhất.

Nhờ dùng kỹ thuật này, có thể nói rằng, tất cả các mục dữ liệu trong bảng xử lý vị trí những nơi đóng quân đều là mật, trừ những nơi là căn cứ tên lửa là tuyệt mật.

Nếu phân loại được áp cho các phần tử



multilevel database security: *an toàn cơ sở dữ liệu nhiều mức*. Hình 1. Dùng bộ lọc để mô phỏng bộ kiểm soát tham chiếu.



multilevel database security: *an toàn cơ sở dữ liệu nhiều mức.* Hình 2. Cơ sở dữ liệu an toàn mức bội được chia ngăn.

vốn nhận được từ những phần tử khác thì phân loại của phần tử nhận được phải bằng phân loại lớn nhất của những phần tử rút ra.

Việc sử dụng tất cả các phân loại mục dữ liệu theo các quy tắc dẫn xuất sẽ bảo vệ chống lại được tấn công truy nhập gián tiếp. Nếu dữ liệu có mức phân loại cao được dùng theo nghĩa trung gian nào đó trong câu trả lời một câu truy vấn có phân loại thấp của người dùng thì sẽ tồn tại mối nguy hiểm rằng người sử dụng có thể suy luận ra thông tin từ câu trả lời.

Trong trường hợp đơn giản hóa, có thể cho phép gán mức phân loại thấp hơn phân loại của dữ liệu từ nơi mà nó được lấy ra. Ví dụ, hóa đơn lương tổng của một tổ chức có thể cho mức phân loại thấp hơn mức phân loại lương của nhà quản lý, mặc dù các mức lương của các nhà quản lý cũng nằm trong số lương tổng cộng.

Trong trường hợp các ràng buộc phân loại dùng cho các quy tắc đơn giản hóa, mức phân loại của phần tử lấy ra phải không lớn hơn phân loại của tất cả các phần tử được dẫn xuất được dùng trong phép truy lục và phục hồi và không nhỏ hơn phân loại của tất cả các phần tử có thể suy luận được từ dữ liệu tìm được. Trong trường hợp hóa đơn lương tổng, phân loại của tổng có thể thiết lập tới:

- mức phân loại lớn nhất của mức lương cá nhân nếu số tiền lương trong câu hỏi nhỏ hơn 100;
- mức không xếp vào loại mật trong những trường hợp khác.

Lý lẽ biện minh cho phân loại thấp hơn trong trường hợp thứ hai là do không

chắc có thể suy ra mức lương của cá nhân từ tổng lương.

Mặt khác, những cơ hội nảy sinh khi tập hợp dữ liệu nhạy cảm hơn các phần dữ liệu riêng lẻ. Sự tập hợp như vậy có thể nảy sinh khi hai hay nhiều mục thông tin cá biệt có thể có mức phân loại thấp song khi kết hợp lại lại trở nên nhạy cảm hơn. Tình huống như vậy xảy ra khi một giao dịch tài chính được liên kết giữa người trả tiền và người nhận tiền. Các cặp (tên người sử dụng, giao dịch số) có thể không mật song hai cặp có cùng số giao dịch, tên người trả tiền, nhận tiền có thể rất nhạy cảm.

Nói chung, các ràng buộc phân loại có thể được xác định để kết hợp dữ liệu, tương tự với những điều kiện cho dữ liệu đơn giản hóa, trừ phi phân loại cho khung nhìn cao hơn phân loại của các mục dữ liệu riêng biệt là đầu vào của khung nhìn.

Tập hợp các ràng buộc về phân loại cho một cơ sở dữ liệu, tức là hằng số, dữ liệu được dẫn xuất, dữ liệu được đơn giản hóa và dữ liệu kết hợp phải thỏa mãn các điều kiện về tính đầy đủ và nhất quán. Yêu cầu về tính đầy đủ phát biểu rằng, tất cả dữ liệu tìm được phải được cấp một phân loại theo một ràng buộc về phân loại. Điều kiện về tính nhất quán là tập các ràng buộc phân loại chỉ tạo ra một mức phân loại cho dữ liệu được tìm ra.

Các ràng buộc phân loại cung cấp một cơ chế gán một mức phân loại cho dữ liệu trong đích của khung nhìn; tất cả dữ liệu trong đích sẽ có cùng mức phân loại, tức là được gán theo ràng buộc phân loại. Các ràng buộc phân loại đưa ra một biện pháp phân loại các mục dữ liệu được đưa ra trong câu trả lời câu truy vấn. Khía cạnh tiếp theo trong mô hình là chỉ ra các cơ chế nhờ nó người dùng có mức truy nhập cho trước sẽ được phép hoặc bị từ chối truy nhập tới dữ liệu.

Khung nhìn truy nhập là ánh xạ từ một tập các quan hệ lên một quan hệ sao cho, tất cả dữ liệu thuộc nguồn của ánh xạ có mức phân loại được đặt trội hơn phân loại của khung nhìn truy nhập. Sự hạn chế về cả dữ liệu nguồn lẫn đích của khung nhìn bảo đảm rằng, không có dữ liệu được phân loại cao hơn nào có thể suy từ dữ liệu trả về trong khung nhìn. Ngoài phân loại an toàn ra, khung nhìn cũng chỉ ra dạng truy nhập được phép theo một, tức là tìm kiếm, chèn và cập nhật v.v..

Người dùng có thể truy nhập tới dữ liệu đích của một khung nhìn truy nhập nếu các quy tắc truy nhập tùy ý và bắt buộc đều được thỏa mãn bởi được nhập mạng theo mức truy nhập (clearance) an toàn, ID của người dùng khi đăng nhập, phân loại của khung nhìn truy nhập và chế độ truy nhập. Ví dụ, người dùng có thể đọc dữ liệu nếu:

- mức phân loại an toàn của người dùng trội hơn phân loại của khung nhìn truy nhập;
- khung nhìn cho phép chế độ tìm kiếm;
- người dùng được cấp quyền truy nhập đọc tùy ý tới dữ liệu đích trong khung nhìn.

Xem aggregation, attribute, Bell-La Padula model, Biba model, Blue Book, covert channel, database security, DBMS.

direct access, discretionary access control, dominate, indirect access, integrity locking, mandatory access control, multilevel secure, polyinstantiation, reference monitor concept, relation, relational database, Trojan Horse direct release, Trojan Horse leakage, tuple, view.

multilevel device ***thiết bị nhiều mức*** Trong an toàn máy tính, một thiết bị xử lý đồng thời dữ liệu có hai hay nhiều mức an toàn mà không gây tổn thương. Để thực hiện điều này, các nhãn nhạy cảm được lưu trong cùng môi trường vật lý và có cùng dạng thức (tức người hoặc máy có thể đọc được) như dữ liệu đang được xử lý. *So sánh với* single-level device. *Xem* multilevel network subject, multilevel secure, multilevel security mode, security level, sensitivity label.

multilevel network subject ***chủ thể mạng nhiều mức*** Trong an toàn liên lạc, một chủ thể mạng làm cho thông tin chảy qua mạng ở hai mức an toàn hoặc nhiều hơn mà không bị tổn thương. Để có được điều này, các nhãn nhạy cảm đều được truyền cùng dữ liệu. *Xem* multilevel device, multilevel secure, multilevel security mode, security level, sensitivity label, subject.

multilevel secure ***an toàn nhiều mức*** Trong an toàn máy tính, một lớp hệ thống chứa thông tin có các mức nhạy cảm khác nhau cho phép những người sử dụng có các mức truy nhập (clearance) khác nhau và có nhu cầu cần biết đồng thời truy nhập tới, song lại ngăn cản được những người thiếu sự ủy quyền hay không được truy nhập tới. *Xem* multilevel device, multilevel network subject, multilevel security mode, security level, neet to know.

multilevel security mode ***chế độ an toàn nhiều mức*** (1) Trong an toàn máy tính, một chế độ hoạt động cung cấp khả năng với các mức khác nhau, các loại hình (category) và các ngăn khác nhau của dữ liệu. Dữ liệu nầy được lưu và được xử lý đồng thời trong một hệ thống tự động và cho phép những người sử dụng có các mức truy nhập (clearance) khác nhau và có nhu cầu cần biết truy nhập có lựa chọn tới một cách đồng thời. Những kiểm soát bên trong cũng như các kiểm soát về con người, vật lý và quản trị, tách bạch những người dùng và dữ liệu dựa trên cơ sở mức truy nhập an toàn. Những kiểm soát an toàn bên trong phải được chứng minh kỹ lưỡng là hiệu quả trong việc ngăn chặn truy nhập trái phép tới thông tin. (2) Trong an toàn máy tính, một chế độ hoạt động có hiệu lực khi ít nhất một số người dùng truy nhập tới hệ thống không có mức truy nhập (clearance) hay nhu cầu cần biết đối với tất cả các tài liệu đã xếp loại mật trong hệ thống thông tin. Chế độ này tạo khả năng cho những người chưa được phân mức truy nhập (clearance) và những người dùng có mức truy nhập an toàn khác nhau truy nhập đồng thời và dùng hệ thống thông tin. Việc nhận diện, sự phân tách và sự kiểm soát những người dùng và tài liệu nhạy cảm dựa trên cơ sở mức truy nhập an toàn, bảng phân loại tài liệu và nhu cầu cần biết phải là nền tảng chủ

yếu của kiểm soát tự động. Hoạt động trong chế độ này sẽ được dựa trên một chứng minh toàn diện rằng, các kiểm soát an toàn bên trong có thể ngăn chặn hiệu quả những nỗ lực ác ý đi vòng qua những kiểm soát này. (3) Trong an toàn máy tính, một chế độ hoạt động dưới hệ điều hành (chương trình thực hiện hay chương trình giám sát) cung cấp khả năng cho phép các mức khác nhau, các loại hình (category) hoặc các ngăn về tài liệu được lưu và xử lý đồng thời trong một hệ thống ADP. Trong hệ thống chia sẻ tài nguyên truy nhập từ xa, những người có các mức truy nhập (clearance) an toàn khác nhau và được phép có thể truy nhập có lựa chọn và điều khiển thông tin từ các thiết bị đầu cuối có điều khiển khác nhau. Chế độ hoạt động này có thể điều tiết việc lưu trữ và xử lý đồng thời (*a*) hai hay nhiều hơn mức dữ liệu mật, hoặc (*b*) một hoặc nhiều mức dữ liệu mật có dữ liệu chưa xếp vào loại mật tùy thuộc vào những ràng buộc trên hệ thống bởi cơ quan có thẩm quyền phê chuẩn. *Xem* Designated Approving Authority, multilevel device, multilevel network subject, multilevel secure, security mode, neet to know.

multilink ***đa liên kết*** Trong truyền thông dữ liệu, một nhánh giữa hai nút có hai hay nhiều kết nối dữ liệu. *Xem* data link.

multimode fiber ***cáp quang nhiều chế độ*** Trong truyền thông, một cáp quang có lõi đủ lớn cho phép năng lượng quang học lan truyền theo một số phương thức khác nhau. So sánh với monomode fiber. *Xem* fiber optics, mode, mode dispersion.

multipath ***đa tuyến*** Trong truyền thông, sự tán sắc dạng xung do những tia sáng đi qua cáp sợi quang có tốc độ và tuyến khác nhau. *Xem* mode dispersion.

multiple access rights terminal ***thiết bị đầu cuối cho phép truy nhập bội*** Trong kiểm soát truy nhập, một thiết bị đầu cuối cho phép nhiều lớp người sử dụng, ví dụ những người dùng có các quyền truy nhập khác nhau tới dữ liệu. *Xem* access.

multiple categories ***loại hình bội*** Trong kiểm soát truy nhập, mức truy nhập mà Bộ Quốc Phòng (Mỹ) đòi hỏi ngoài mức truy nhập tối mật dựa trên sự điều tra cơ bản đặc biệt hiện tại. *So sánh với* confidential clearance, one category, secret clearance, unclassified information, uncleared. *Xem* clearance, top secret clearance.

multiple DES encipherment ***phép mã DES bội*** Trong mật mã, độ dài hiệu quả của khóa DES có thể tăng lên theo phép mã bội. Tuy nhiên, một phép mã kép đơn giản dùng hai khóa khác nhau lại không làm tăng độ dài khóa hiệu quả từ 56 lên 112 bit.

Nếu tổ chức một cuộc tấn công biết trước bản rõ lên bản rõ được mã kép thì một lần tìm kiếm được tiến hành theo phép mã bản rõ biết trước với một dải các khóa, còn lần tìm kiếm thứ hai được tiến hành theo phép giải mã tương ứng bản mã. Các kết quả của mỗi lần tìm kiếm này được lưu riêng và được so sánh với nhau; sự đối chiếu kết quả sẽ chỉ ra cặp khóa có thể. Cuộc tìm

kiếm sẽ tạo nên một số đáng kể các cặp khóa ứng cử viên song lần tìm kiếm thứ hai bằng các khóa ứng cử viên này cùng với một cặp bản rõ-mã khác nhau sẽ để lộ cặp khóa đã dùng trong phép mã kép ban đầu. Kỹ thuật này được gọi là "tấn công gặp điểm giữa" và nó chỉ ra rằng, phép mã kép chỉ làm tăng hiệu quả độ dài khóa từ 56 lên 57 bit vì nỗ lực tìm ra một cặp khóa gần gấp hai lần so với việc xác định một khóa đơn. Một dạng thực hiện khóa bội ba gồm phép mã hóa bằng một khóa (k_1), phép giải mã bằng khóa k_2 và phép mã lần nữa bằng khóa thứ ba k_3 sẽ khắc phục được hiểm họa của kiểu tấn công gặp điểm giữa. Trong một số trường hợp, k_1 và k_3 giống nhau và như vậy chỉ còn cần hai khóa. Kỹ thuật này có ưu điểm là nó có thể tương hợp với phép mã khóa đơn ($k_1 = k_2 = k_3$). Tuy nhiên, người ta đã chỉ ra rằng, một sơ đồ như vậy, có thể vẫn còn dễ bị tổn thương trước kiểu tấn công gặp điểm giữa và bởi vậy nó đã được khuyến nghị rằng cần dùng ba khóa khác nhau.

Tuy vậy, toàn bộ vấn đề về phép mã DES bội ba hiện vẫn để lại một số vấn đề chưa trả lời được. Phép tấn công gặp ở bên trong xoay quanh việc xắp xếp và lưu 2^{56} số 64 bit và sau đó kiểm tra các mục vào trong danh sách này. Nó đưa ra một kho lưu trữ dữ liệu rất lớn và công việc truy lục còn tiêu phí thời gian và tiền của hơn nữa so với các tính toán tìm kiếm toàn diện khóa dùng các vi chip DES. Câu tuyên bố rằng phép mã khóa kép đơn giản chỉ tương đương với việc tăng độ dài khóa hiệu quả lên một bit đã lờ đi chi phí, thời gian và nỗ lực trong khía cạnh lưu trữ kể trên. *Xem* cryptographic key, DES, key-encrypting key, key management, known plaintext.

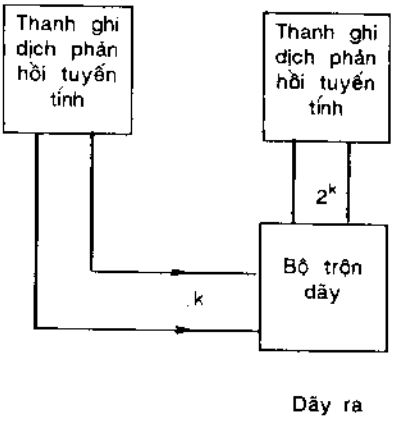
multiple key retrieval ***truy lục khóa bội, tìm kiếm khóa bội*** Trong các cơ sở dữ liệu, một kỹ thuật truy lục các bản ghi dựa trên giá trị của một vài từ khóa, một số hoặc tất cả các khóa thứ cấp. *Xem* key, record, secondary key.

multiple routing ***định tuyến bội*** Trong truyền thông dữ liệu, một phương pháp gửi thông báo tới nhiều hơn một đích, địa chỉ đích này được ghi trên phần tiêu đề của thông báo. *Xem* message heading, routing.

multiplex ***đa hợp, dồn kênh*** Trong an toàn vật lý, đề cập tới các hệ thống báo động dùng các tín hiệu đa hợp giữa các bộ cảm biến và bảng tín hiệu báo hoặc hệ thống báo động. *Xem* annunciator. *So sánh với* homerun.

multiplexer ***bộ dồn kênh, bộ đa hợp*** Trong truyền thông dữ liệu, một thiết bị lấy một số kênh và kết hợp các tín hiệu vào một kênh chung để truyền đi. Tại phía bên kia, bộ giãn kênh sẽ rút ra các tín hiệu ban đầu. *Xem* multiplexing.

multiplexing ***(sự) trộn dãy; (sự) dồn kênh, (sự) đa hợp*** (1) Trong mật mã, một kỹ thuật tạo các dãy số giả ngẫu nhiên được dùng như các chuỗi bit mã. Kỹ thuật này dùng hai thanh ghi dịch có mạch phản hồi tuyến tính có độ dài tương ứng là k và 2^k. Đầu ra của thanh ghi dịch ngắn hơn được dùng để chọn bit của thanh ghi dịch dài hơn để cho



multiplexing: *trộn dãy.* Phương pháp tạo các dãy ngẫu nhiên cho dòng bit mật mã.

ra một dãy ngẫu nhiên. *Xem* bit, cryptographic bit stream, linear feedback shift register. (2) Trong truyền thông, quá trình kết hợp một số tín hiệu để chúng có thể dùng chung một phương tiện truyền dẫn, do vậy làm tăng hiệu quả tài nguyên dùng chung. *Xem* frequency division multiplexing, time division multiplexing.

multiplex mode ***chế độ dồn kênh*** Trong truyền thông dữ liệu, một biện pháp truyền dữ liệu đi khỏi hoặc đến các thiết bị vào ra I/O tốc độ thấp trên một kênh dùng bộ dồn kênh nhờ xen kẽ các byte dữ liệu. *Xem* byte, input output device, multiplexer. *Đồng nghĩa với* byte mode.

multipoint circuit ***mạch nhiều điểm, mạch đa điểm*** *Đồng nghĩa với* multidrop circuit.

multipoint connection ***nối kết đa điểm*** Trong truyền thông dữ liệu, một nối kết nối ba trạm dữ liệu hoặc nhiều hơn với một liên kết đi từ trạm này tới trạm tiếp theo theo kiểu nối tiếp hơn là theo kiểu ngôi sao. *Xem* star.

multi-use security mode of operation ***chế độ hoạt động an toàn nhiều người sử dụng*** Trong an toàn máy tính, một chế độ hoạt động được thiết kế cho các hệ thống xử lý thông tin nhạy cảm không được xếp loại mật, trong đó những người dùng có thể không có nhu cầu cần biết đối với tất cả các thông tin đã xử lý trong hệ thống. Chế độ này cũng dành cho quá trình xử lý trên các máy vi tính những thông tin nhạy cảm không xếp vào loại mật không thể đáp ứng những yêu cầu về chế độ hoạt động độc lập. *So sánh với* multilevel security mode. *Xem* need to know.

municipal area network ***mạng thành phố*** Trong truyền thông dữ liệu, một mạng có các đặc trưng:

- rộng về mặt vật lý, khi được so sánh với mạng nội hạt thì phạm vi rộng khoảng 50 km;
- được kết nối chung nhanh chóng, cho phép những người thao tác mạng cung cấp các dịch vụ dữ liệu tốc độ cao ở trong nước cũng như quốc tế;
- hỗ trợ nhiều nhóm người sử dụng khác nhau trong khi vẫn duy trì tính an toàn giữa các nhóm;
- nhắm chủ yếu đến hoạt động của những thao tác viên mạng công cộng và được thiết kế để dùng các tuyến truyền hiện tại và tương lai của các mạng công cộng.

So sánh với local area network, wide area network. *Đồng nghĩa với*

metropolitan area network.

Murphy *virut Murphy* Trong an toàn máy tính, loại virut ngắt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COMMAND.COM, COM, EXE và OVL, tác động trong khi chạy, làm hỏng chương trình và các tệp OVL. *Xem* virus names.

Musis Bug *virut Musis Bug* Trong an toàn máy tính, loại virut ngắt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm secto khởi động của đĩa mềm và bảng phân hoạch (partition table) của đĩa cứng, làm hỏng secto khởi động, tác động trong thời gian chạy. *Xem* virus names.

mutual authentication *xác thực lẫn nhau* (1) Trong xác thực, sự xác thực ở nơi cả hai người sử dụng xác thực lẫn nhau. (2) Trong an toàn dữ liệu, cung cấp sự bảo đảm về nhau đối với danh tính của các chủ thể và/hoặc các đối tượng. Ví dụ, một hệ thống cần xác thực một người sử dụng, còn người sử dụng lại cần xác thực xem hệ thống có thật không. *Xem* authentication, object, subject.

Mutual Legal Assistance Treaty *Hiệp ước giúp tuân thủ luật pháp chung* Trong luật pháp, một hiệp ước cho phép các nhân viên hải quan và thi hành luật thuế truy nhập tới dữ liệu và bản ghi riêng tư của cá nhân ở một nước đã ký hiệp ước này. *Xem* data protection.

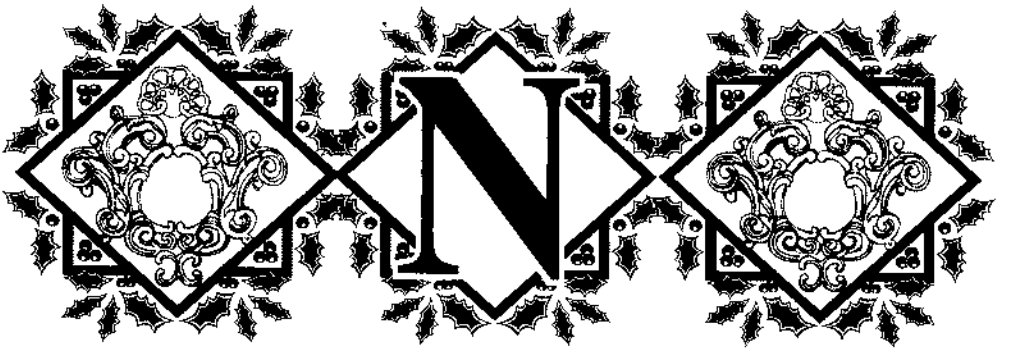
mutually prime *đồng nguyên tố, nguyên tố cùng nhau* *Đồng nghĩa với* coprime.

mutually suspicious *nghi ngờ lẫn nhau* Trong an toàn máy tính, đề cập tới tình trạng tồn tại giữa các quá trình tương tác (các hệ thống con và chương trình), mỗi quá trình đều chứa những dữ liệu nhạy cảm và được giả thiết là được thiết kế để trích dữ liệu từ quá trình khác và bảo vệ dữ liệu riêng của mình.

mutual security *an toàn tương tác* Trong an toàn liên lạc, đề cập tới phép thử các hoán vị được dùng trong phép xáo trộn (tiếng nói) theo các đoạn thời gian. Nếu hai hoán vị thực hiện sao cho, kết quả của hoán vị này được tiếp tục bởi phép đảo của hoán vị thứ hai tiến gần tới dãy các đoạn ban đầu thì một trong hai hoán vị sẽ không được dùng trong quá trình xáo trộn. Phép thử an toàn tương tác sẽ kiểm tra mỗi phép hoán vị mới (dùng trong tập hoán vị được lưu) dựa vào mỗi hoán vị có sẵn trong tập. *Xem* time element scrambler, voice scrambling.

MUX *bộ dồn kênh* *Xem* multiplexer.

MVS *hệ MVS, hệ thống phê chuẩn tính hợp lệ MAC* Trong xác thực, viết tắt của MAC validation system, tức là hệ thống phê chuẩn MAC, một hệ thống để thử tính phù hợp của các thiết bị cung cấp theo các chuẩn xác thực dữ liệu Liên bang Hoa Kỳ và thương mại. *Xem* MAC.



NAK ***báo phủ nhận*** *Xem* negative acknowledgement.

NAK attack ***tấn công báo phủ nhận*** Trong an toàn máy tính, một kiểu tấn công thâm nhập lợi dụng một điểm yếu tiềm ẩn trong hệ điều hành không điều khiển các ngắt dị bộ một cách chính xác và do vậy, dẫn tới hệ thống ở trạng thái không được bảo vệ trong suốt thời gian ngắt như vậy. *Xem* interupt, operating system, penetration.

narrow band ***dải thông hẹp, dải hẹp*** Trong truyền thông dữ liệu, nói tới kênh có dải thông nhỏ hơn dải thông của kênh truyền tiếng nói. Nó thường được dùng cho tốc độ truyền nhỏ hơn 300 bit/giây. *Xem* bandwidth, voice grade channel.

NASA *Xem* National Aeronautics and Space Agency.

National Aeronautics and Space Agency ***Cơ quan hàng không và vũ trụ Quốc gia (Hoa Kỳ)*** Một cơ quan của chính phủ Mỹ có trách nhiệm quản lý các chương trình liên lạc vệ tinh.

National Commission on Data Processing and Freedom ***Ủy ban Quốc gia về xử lý và tự do dữ liệu*** *Xem* data protection - France.

National Communications Security Directive 4 ***Chỉ thị 4 về an ninh thông tin Quốc gia*** Một chỉ thị của Mỹ có tên là "Chính sách Quốc gia về kiểm soát các nguồn phát xạ gây hại" đề xuất từ năm 1981. Nó yêu cầu các cơ quan liên bang bảo vệ thông tin đã xếp vào loại mật chống các nguồn phát xạ gây hại. *Xem* compromising emanations.

National Computer Security Center ***Trung tâm An toàn Máy tính Quốc gia*** Một trung tâm của Cơ quan An ninh Quốc gia (Hoa Kỳ) được lập ra từ chỉ thị 145 về an ninh quốc gia. Mục đích chính của Trung tâm là giúp đạt

được tính sẵn sàng cho các hệ thống máy tính tín nhiệm ở khắp nước Mỹ. Nó đã được biết đến lần đầu với tên Ban bảo vệ Trung tâm an toàn máy tính. *Xem* NSDD-145.

National Crime Information Center ***Trung tâm thông tin về tội phạm Quốc gia*** Trong luật pháp, một trung tâm của FBI đề cập tới các tin tức tình báo về tội phạm. *Xem* data protection - USA.

National institute for Science and Techology ***Viện khoa học và công nghệ Quốc gia*** Một cơ quan của Mỹ trước kia có tên là Cục Tiêu chuẩn Quốc gia. Đó là cơ quan có trách nhiệm thiết lập các tiêu chuẩn liên bang nhằm sử dụng hiệu quả và hiệu lực các hệ thống máy tính.

National Security Agency/Central Security Service ***Cơ quan an ninh Quốc gia/Dịch vụ an toàn trung tâm*** Cơ quan an ninh Quốc gia của Mỹ được thành lập năm 1952 với tư cách là một cơ quan độc lập trong Bộ quốc phòng, có nhiệm vụ đảm bảo an toàn liên lạc và tình báo tín hiệu cho Chính phủ Mỹ. Nó có sứ mệnh nữa là đảm bảo an toàn máy tính từ năm 1984. Dịch vụ An toàn Trung tâm được thành lập vào năm 1972 để tổ chức chức năng mật mã thống nhất hơn nữa trong phạm vi Bộ quốc phòng. Ba sứ mệnh chính của Cơ quan An ninh Quốc gia/Dịch vụ an toàn Trung tâm là an toàn liên lạc, an toàn máy tính và thông tin tình báo nước ngoài.

National Security Directive-42 ***Chỉ thị 42 về an ninh Quốc gia*** Trong luật pháp, một chỉ thị đòi hỏi các cơ quan liên bang tôn trọng triệt để Điều luật về An ninh Máy tính. *Xem* Computer Security Act of 1987.

native key ***khóa riêng*** Trong mật mã, một khóa mã ở dạng các bit nhị phân như thuật toán mã và giải mã đòi hỏi. *So sánh với* long key.

native mode ***chế độ riêng*** Trong mật mã, một chế độ hoạt động của DES trong đó, một hay nhiều khối bit vào 64 bit sẽ tạo ra các khối bản mã 64 bit tương ứng bằng cách đưa liên tiếp các khối vào để mã hóa. Với một khóa cho trước, DES sẽ tạo có kết quả một từ điển mã điện tử với 2^{64} mục vào của các cặp bản rõ-bản mã. Nếu các thông báo được định dạng cao thì các khối bản mã nào đó có khả năng lặp lại và điều đó rất có giá trị đối với kẻ tấn công. *So sánh với* cipher block channing, cipher feedback, output feedback. *Xem* data encryption standard. *Đồng nghĩa với* electronic codebook.

natural language ***ngôn ngữ tự nhiên*** Ngôn ngữ trong đó các quy tắc ứng với thói quen sử dụng hiện thời mà không phải tuân theo những quy định bắt buộc. Ngôn ngữ được những người sử dụng dùng trong truyền thông thông thường như khi được so sánh với ngôn ngữ hạn chế dùng cho liên lạc với các máy tính, đánh số các tài liệu... *So sánh với* program language.

navigation ***định vị thông tin*** Trong các cơ sở dữ liệu, quá trình chuyển qua một cơ sở dữ liệu, theo một tuyến đi rõ ràng từ mục dữ liệu này tới mục dữ liệu tiếp theo cho tới khi đạt tới mục

dữ liệu cần thiết.

NCC ***trung tâm NCC*** Viết tắt của UK National Computing Center (Trung tâm tính toán Quốc gia của Anh).

NCIC ***trung tâm NCIC*** *Xem* National Crime Information Center.

NCSC ***trung tâm NCSC.*** *Xem* National Computer Center.

neccesary bandwith ***dải thông cần thiết*** Trong truyền thông, độ rộng của dải thông vừa đủ để đảm bảo truyền thông tin ở tốc độ và phẩm chất cần thiết. *Xem* bandwidth.

need to know ***nhu cầu cần biết, cần thì biết*** (1) Trong an toàn dữ liệu, một quyết định do bộ xử lý thông tin nhạy cảm đưa ra để người nhận trong tương lai (vì lợi ích an ninh quốc gia), có yêu cầu truy nhập tới, để biết được hoặc sở hữu thông tin nhạy cảm nhằm thực hiện các nhiệm vụ hay các dịch vụ của cơ quan. *Xem* need to know violation. (2) Trong an toàn dữ liệu, sự cần thiết truy nhập tới, biết được hoặc sở hữu thông tin nào đó để tiến hành nhiệm vụ. Trách nhiệm đối với việc xác định xem, liệu các nhiệm vụ của cá nhân có đòi hỏi có hoặc truy nhập tới thông tin như vậy không, và liệu cá nhân có được ủy nhiệm nhận nó dựa trên cơ sở cá nhân có sở hữu, có kiến thức hoặc kiểm soát thông tin liên quan và không dựa vào người nhận trong tương lai không. *Xem* need to know violation. (3) Trong an toàn dữ liệu, một chính sách hạn chế truy nhập tới thông tin đã phân loại đối với cá nhân có nhiệm vụ yêu cầu sự truy nhập như vậy.

need to know violation ***vi phạm quy chế cần biết*** Trong an toàn dữ liệu, sự làm lộ thông tin mật hoặc thông tin bảo vệ nhạy cảm khác cho cá nhân đã được phân mức truy nhập (cleared) song không có yêu cầu cần thông tin đó để tiến hành các nhiệm vụ được giao. *Xem* need to know.

negative acknowledgement ***báo phủ nhận, báo không công nhận*** Trong truyền thông dữ liệu, một tín hiệu gửi từ máy thu tới máy phát để chỉ ra rằng, đã nhận được một thông báo có các lỗi có thể phát hiện. Khi đó máy phát sẽ phát lại thông báo. *So sánh với* affirmative acknowledgement.

negative card ***thẻ âm*** Trong hoạt động ngân hàng, một thẻ do người sử dụng hợp pháp giữ song bị hạn chế đối với các phương tiện (chẳng hạn, thẻ ghi nợ do người chủ sở hữu thẻ giữ cùng với số tiền chi trội trái phép). *So sánh với* hot card list. *Xem* debit card.

negative disclosure ***(sự) tiết lộ âm, (sự) lộ bí mật phủ nhận*** Trong an toàn cơ sở dữ liệu, một dạng tiết lộ cá nhân trong đó có thể suy luận ra rằng, cá nhân không có thuộc tính đặc biệt, chẳng hạn không bị một căn bệnh đặc biệt. *Xem* personal disclosure.

negative file ***tệp âm*** *Đồng nghĩa với* host card list.

negative safeguard ***bộ phận bảo vệ không thực*** Trong an toàn máy tính, một bộ phận bảo vệ được giả thiết là đang hoạt động song thực tế lại không.

netkey ***khóa mã đơn cho mạng*** Trong mật mã, một kỹ thuật dùng một khóa mật mã đơn lẻ cho tất cả các cuộc truyền giữa các thiết bị đầu cuối trong

mạng đã cho. *So sánh với* session key.

network *mạng* (1) Trong truyền thông dữ liệu, hai hay nhiều hệ thống được nối vào một phương tiện truyền thông có trách nhiệm chuyển thông tin từ hệ thống này tới hệ thống khác. (2) Trong truyền thông dữ liệu, một mạng gồm phương tiện truyền tin và tất cả các thành phần gắn với môi trường truyền dẫn đó có trách nhiệm truyền thông tin. Những thành phần đó có thể chứa các AIS, chuyển mạch gói, các bộ điều khiển viễn thông, các trung tâm phân phối khóa và các thiết bị điều khiển kỹ thuật. *Xem* AIS, key distribution center, packet switching. (3) Trong truyền thông dữ liệu, sự kết nối hai hay nhiều phương tiện máy tính trung tâm ADP để truyền hay chia sẻ các tài nguyên ADP. Mạng ADP chứa các phương tiện máy tính trung tâm, các thiết bị đầu cuối ở xa, các kết nối liên lạc, các bộ xử lý ngoại vi và các hệ thống viễn thông. *Xem* front end processor. (4) Một loạt các điểm được kết nối. (5) Trong truyền thông, một hệ thống gồm các phương tiện liên lạc được kết nối.

network architecture *kiến trúc mạng* Trong truyền thông dữ liệu, một tập hợp các tầng và giao thức (gồm cả các định dạng và các chuẩn cho các phần cứng/mềm khác nhau phải tuân theo nhằm đạt được các mục tiêu đề ra) xác định một mạng. *Xem* open system interconnection, protocol.

network component *thành phần mạng* Trong truyền thông dữ liệu, một hệ thống con của mạng có thể được đánh giá theo các diễn dịch mạng tin cậy liên quan tới chính sách đối với thành phần lấy từ chính sách tổng thể về mạng. *Xem* component.

network connection *(sự) nối mạng* Trong truyền thông dữ liệu, tuyến logic hoặc vật lý bất kỳ từ máy chủ này tới máy chủ khác cho phép truyền thông tin giữa chúng. Một ví dụ là kết nối TCP. Tuy nhiên, khi một máy chủ truyền một gói dữ liệu (datagram) IP mà chỉ dùng các dịch vụ có các trình biên dịch Giao thức Internet (IP) không kết nối thì với cuộc truyền này, nó cũng được xem như một kết nối giữa các máy chủ nguồn và đích. *Xem* connectionless service, datagram, TCP/IP.

network control program *chương trình kiểm soát mạng* Trong các mạng máy tính, một phần của hệ điều hành của một máy tính chủ có nhiệm vụ thiết lập và ngắt các kết nối logic. Một mặt, nó liên lạc với các quá trình của người sử dụng trong máy tính chủ, mặt khác nó liên lạc với mạng. *Xem* host computer, operating system.

network control station *trạm kiểm soát mạng* Trong truyền thông, một trạm phối hợp sắp xếp sử dụng một mạng liên lạc.

network control system *hệ thống kiểm soát mạng* Trong truyền thông dữ liệu, một hệ thống máy tính cung cấp các biện pháp thu thập và xử lý thông tin liên quan tới trạng thái của một mạng viễn thông.

network database *cơ sở dữ liệu mạng* Trong cơ sở dữ liệu, một cấu trúc cho phép liên kết mục dữ liệu này với mục dữ liệu khác. *So sánh với*

hierarchical database, relational database, tree database.

network delay ***thời gian trễ trên mạng*** Trong truyền thông dữ liệu, thời gian chuyển tiếp một gói trong mạng chuyển mạch gói. Nó được xác định là khoảng thời gian từ lúc bit cuối cùng của gói rời khỏi nút nguồn cho tới khi bit đầu tiên vào được nút đích. *Xem* computer network, packet switching.

network diagram ***biểu đồ mạng*** Một biểu đồ chỉ ra các nút và các kết nối của chúng. *Xem* node.

network discretionary access control ***kiểm soát truy nhập tùy ý mạng*** Trong an toàn liên lạc, sự kiểm soát truy nhập tùy ý áp dụng lên các thành phần của mạng ở mức giao thức 3. *Xem* discretionary access control, OSI security.

network encryption ***mật mã mạng, mã hóa mạng*** Trong an toàn liên lạc, những kỹ thuật được dùng để mã hóa bảo mật các thông báo truyền qua mạng. Liên lạc an toàn trên mạng bị phức tạp thêm bởi sự hiện diện của các nút trung gian để nhận các thông báo và định hướng lại chúng tới các kết nối ra thích hợp.

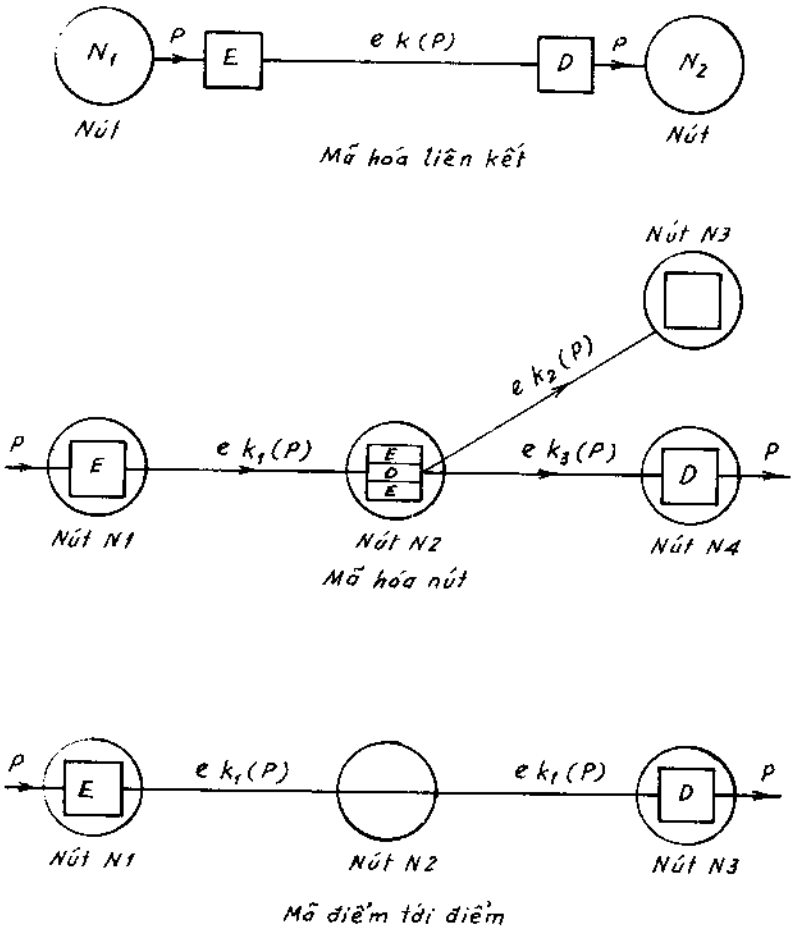
Có ba phương pháp xử lý mật mã trên mạng là mã liên kết, mã nút và mã điểm tới điểm (xem hình 1).

Mã liên kết đòi hỏi các thiết bị mật mã tại mỗi bên liên kết; các thông báo được giải mã trước khi được đưa vào nút; chúng sẽ được mã lại bằng một khóa khác sau khi rời khỏi nút và trước khi vào kết nối liên lạc tiếp sau. Mã nút mạng dùng cho phép giải mã thông báo và tái mã hóa bằng một khóa khác để truyền tới nút tiếp sau trong phạm vi các modun an toàn nằm tại nút. Mã điểm tới điểm không có modun giải mã và tái mã hóa trung gian; hai người dùng tại mỗi bên của tuyến liên lạc bởi vậy phải thỏa thuận với nhau về khóa mã cần dùng.

Mã liên kết hoàn toàn trong suốt đối với người dùng song các thông báo lại được chuyển qua các nút ở dạng rõ. Điều này không thể chấp nhận được với một số người dùng những dữ liệu đặc biệt nhạy cảm. Phép mã nút mạng cũng trong suốt đối với người dùng trong khi phép mã điểm tới điểm có thể nằm dưới sự kiểm soát của người dùng, tức là phép mã có tính cá nhân hoặc nó có thể là một phương tiện do người thao tác hệ thống cung cấp. Cũng có thể kết hợp mã điểm tới điểm và mã nút mạng hoặc mã liên kết để tạo ra phép mã kép cho các thông báo.

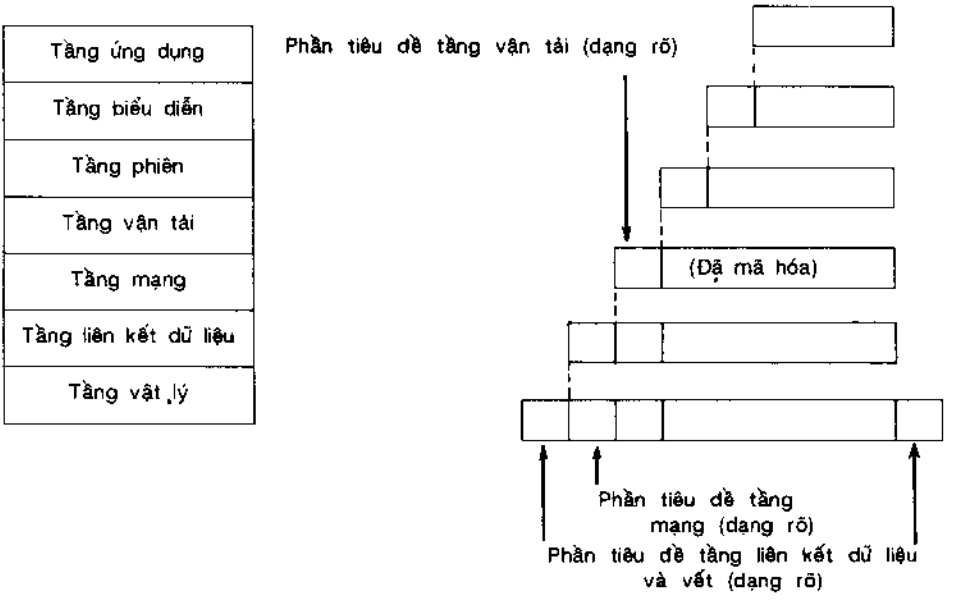
Phép mã liên kết có chi phí thiết bị mã cao nhất, nó gồm hai thiết bị trên mỗi kết nối liên lạc an toàn. Mã nút mạng cho phép tất cả các kết nối liên lạc, các nút vào và ra dùng chung một khối mã nút. Phép mã điểm tới điểm chỉ đòi hỏi các khối mã ở những nơi mà các nút đầu cuối đòi hỏi các phương tiện đó.

Mô hình Tham chiếu Các Hệ thống mở (OSI) trên hình 2 đưa ra một khung làm việc hữu dụng để so sánh mã điểm tới điểm và mã kết nối trong phạm vi các kiến trúc mạng liên lạc. Trong trường hợp mã điểm tới điểm, các quá trình mã và giải mã phải nằm ở một trong các tầng ngay trong máy, tức các tầng ứng dụng, biểu diễn, tầng phiên hoặc tầng

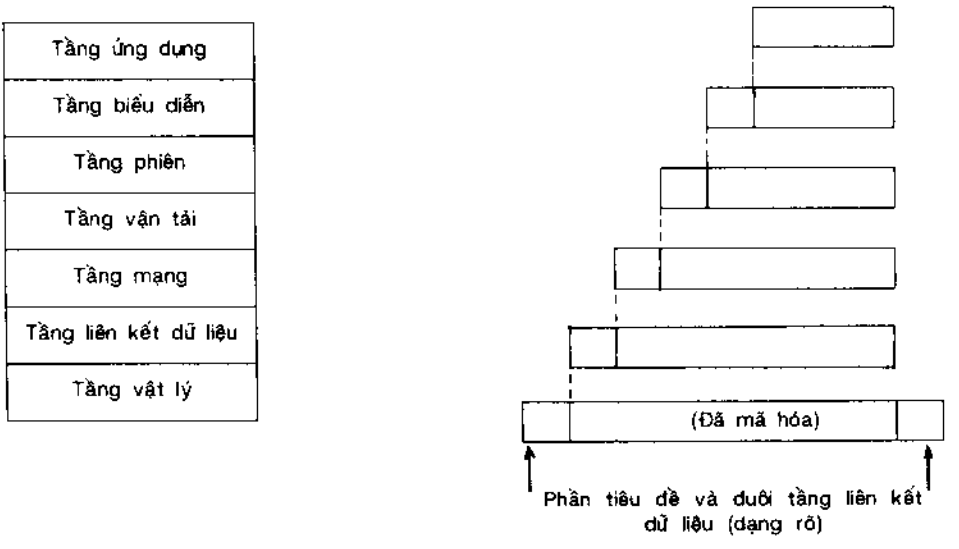


network encryption: *mật mã mạng*. Hình 1.

vận tải. Ngay khi phép mã vừa thực hiện, thông tin điều khiển do các giao thức của tầng dưới (tầng tiếp theo) được thêm vào thông báo sẽ được truyền đi qua mạng ở dạng rõ. Như vậy, trong ví dụ nêu trên hình 3, việc phá hoại các nút mạng trung gian hoặc nghe trộm các kết nối liên lạc sẽ để lộ thông tin trong phân tích lưu lượng không để lộ nội dung thực sự của thông báo. Trong trường hợp mật mã kết nối, các quá trình mã và giải mã đều được thực hiện ở tầng liên kết dữ liệu. Trong trường hợp đó (hình 3), chỉ thông tin điều khiển giao thức được thêm vào thông báo tại tầng liên kết dữ liệu mới được truyền qua điểm kết nối ở dạng rõ. Vì thế, phía nút thu ít nhất phải có khả năng giải mã thông tin điều khiển giao thức được tầng mạng thêm vào để



network encryption: *mật mã mạng*. Hình 2. mã điểm tới điểm.



network encryption: *mật mã mạng*. Hình 3. mã liên kết.

xác định xem thông báo cần được định tuyến tới nút nào. *Xem* cryptographic equipment, cryptographic key, end-to-end encryption, key management, link encryption, node encryption, OSI security, private cryptography, traffic analysis.

network guard ***phòng thủ mạng, lá chắn mạng*** Trong an toàn liên lạc, một hệ thống an toàn thực hiện kiểm soát truy nhập giữa các mạng, nơi mỗi mạng đang hoạt động ở những vùng riêng biệt. Hệ thống phòng thủ mạng cũng có thể kiểm soát dòng dữ liệu định hướng giữa các mạng theo chính sách an toàn được lập trình sẵn, chẳng hạn, kiểm soát truy nhập tùy ý, kiểm soát truy nhập bắt buộc...

network layer ***tầng mạng*** Trong truyền thông dữ liệu, một tầng trong mô hình tham chiếu các hệ thống mở của ISO. Tầng này có trách nhiệm kiểm soát hoạt động của mạng con. Nó liên quan chủ yếu tới các kỹ thuật định tuyến trong một hệ thống điểm tới điểm và những tác động của quá trình định tuyến không tốt, chẳng hạn tắc nghẽn. *So sánh với* application layer, data link layer, physical layer, presentation layer, transport layer, session layer. *Xem* open systems interconnection, routing.

network management ***quản lý mạng*** Trong truyền thông dữ liệu, các thủ tục có tính hệ thống cần thiết để lập kế hoạch, tổ chức và kiểm soát một mạng liên lạc sao cho có giá thành và hiệu suất tối ưu.

network management system ***hệ thống quản lý mạng*** Trong truyền thông dữ liệu, một hệ thống cho phép người điều hành mạng giám sát các tình trạng của mỗi kênh liên lạc, modem và thiết bị đầu cuối trong mạng và định vị những hỏng hóc. Thường thì đơn vị điều khiển sẽ giám sát mạng qua một kênh phụ tốc độ thấp tùy thuộc vào kênh dữ liệu chính. *Xem* channel, MODEM.

network operating center ***trung tâm điều hành mạng*** Trong truyền thông dữ liệu, một hệ thống máy móc cài đặt thuận tiện cho việc điều hành mạng tin cậy thông qua giám sát tình trạng mạng, kiểm soát và phối hợp điểm bảo dưỡng mạng, thu thập dữ liệu về tài khoản và sử dụng...

network redundancy ***(sự) dư thừa mạng*** Trong truyền thông dữ liệu, một thuộc tính mạng có nhiều kết nối tới các nút hơn số cần thiết và do vậy, cho phép mạng tiếp tục chức năng của mình nếu có những kết nối nào đó bị hỏng.

network reference monitor ***giám sát tham chiếu mạng*** Trong kiểm soát truy nhập, một khái niệm chỉ đến một máy trừu tượng dàn xếp tất cả các cuộc truy nhập của các chủ thể tới các đối tượng trong phạm vi mạng. *Xem* reference monitor concept.

network security ***an toàn mạng*** Trong an toàn liên lạc, sự bảo vệ các mạng và các dịch vụ của chúng khỏi sự biến đổi, phá hoại hoặc làm lộ trái phép. Cung cấp sự bảo đảm để mạng thực hiện các chức năng quan trọng của nó một cách đúng đắn và không gây những tác động phụ, kể cả độ chính xác của thông tin.

network security architecture ***kiến trúc an toàn mạng*** Trong an toàn liên lạc, một tập con kiến trúc mạng xác định rõ những vấn đề liên quan tới an toàn.

network security model ***mô hình an toàn mạng*** Trong an toàn liên lạc, một mô hình thực hiện những vấn đề về kiến trúc an toàn mạng. Sự mở rộng mô hình tham chiếu cơ bản OSI bao quát những khía cạnh an toàn vốn là những thành phần kiến trúc chung của các giao thức truyền thông. Các phần tử kiến trúc an toàn chung có thể được áp dụng thích hợp trong những tình huống đòi hỏi bảo vệ liên lạc giữa các hệ thống mở. Có thể cải thiện các chuẩn hiện có và phát triển các chuẩn mới nhờ dùng đường lối chủ đạo và các ràng buộc trong mô hình an toàn mạng. *Xem* network security architecture, OSI security.

network sponsor ***nhà bảo trợ mạng*** Trong an toàn liên lạc, một cá nhân hay tổ chức có trách nhiệm đối với việc định ra chính sách an toàn mà mạng phải tuân thủ, đối với việc thiết kế kiến trúc an toàn mạng để thi hành đúng đắn chính sách đó và bảo đảm rằng, mạng được thực hiện theo đúng chính sách. Đối với các hệ thống thương mại đóng gói sẵn, nhà bảo trợ thường là nhà cung cấp. Đối với hệ thống mạng ngoài (fielded network), nhà bảo trợ thường là nhà quản lý dự án hoặc quản trị hệ thống.

network structure ***cấu trúc mạng*** Trong tính toán, một cấu trúc trong đó nút bất kỳ có thể được nối tới nút bất kỳ khác. *So sánh với* tree structure.

network system ***hệ thống mạng*** Trong truyền thông dữ liệu, một hệ thống được thực hiện cùng với một tập các thành phần mạng được nối liền với nhau. Một hệ thống mạng được dựa trên kiến trúc và thiết kế an toàn chặt chẽ. *Xem* network security architecture.

network termination unit ***khối cuối mạng, thiết bị cuối mạng*** Trong truyền thông dữ liệu, phần thiết bị mạng nối trực tiếp với DTE, nó hoạt động giữa các đường truyền nội bộ và các mạch ghép nối của thuê bao. *Xem* DTE.

network timing ***định thời mạng*** Trong truyền thông dữ liệu, các tín hiệu định thời được chuyển từ DCE tới DTE để kiểm soát sự truyền các chữ số qua các mạch thu và phát dữ liệu. *Xem* DCE, DTE.

network topology ***cấu hình mạng, topo mạng*** Trong truyền thông, sự sắp xếp hình học các nút và các kết nối trong một mạng.

network trusted computing base ***cơ sở tính toán tin cậy mạng*** Trong an toàn liên lạc, toàn bộ cơ chế bảo vệ trong phạm vi hệ thống mạng, bao gồm phần cứng, phần mềm và phần sụn, kết hợp chúng để thi hành chính sách an toàn. *So sánh với* trusted computing base. *Xem* security policy, trusted computing base.

network user identification ***nhận diện người sử dụng mạng, định danh người dùng mạng*** Trong truyền thông dữ liệu, mã định danh được khách hàng dùng trên cổng quay số công khai để tự định danh chính mình

nhằm các mục đích kế toán. *So sánh với* user id. *Xem* network user identity, packet switching, public dial port.

network user identity ***mã định danh người sử dụng mạng*** Trong truyền thông dữ liệu, một mã được yêu cầu để quay số truy nhập tới mạng dữ liệu. *So sánh với* user id. *Xem* network user identification.

network virtual terminal ***thiết bị đầu cuối ảo trên mạng*** Trong truyền thông dữ liệu, một thiết bị đầu cuối trừu tượng cho phép các hệ thống có các thiết bị đầu cuối không tương thích nhau liên lạc chung trên một mạng. Mỗi thiết bị đầu cuối được một phần mềm phục vụ, sắp xếp các chức năng của thiết bị đầu cuối ảo mạng thành các chức năng của loại thiết bị đầu cuối cụ thể đó. *Xem* virtual terminal.

network weaving ***(sự) lách qua mạng, (sự) len lỏi qua mạng*** Trong an toàn liên lạc, một kỹ thuật dùng các mạng liên lạc khác nhau để truy nhập tới một hệ thống của tổ chức. Ví dụ, một kẻ tấn công tạo một cuộc gọi đi qua mạng của hãng AT&T, nhảy qua mạng Sprint sau đó qua MCI và tới mạng của hãng Tymnet. Mục đích nhằm tránh phát hiện và truy ngược tới nguồn gốc của cú gọi. *Xem* hacker.

new hire orientation ***định hướng thuê nhân công mới*** Trong an toàn thủ tục, nói tới các phương pháp đã được thông qua để tuyển một nhân viên mới theo các thủ tục về an toàn của một tổ chức. *Xem* computer fraud control, personal security.

New Sunday ***virut New Sunday*** Trong an toàn máy tính, một virut chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COM, EXE và OVL, tác động trong thời gian chạy, làm ngắt các tệp chương trình, dữ liệu và các tệp OVL và liên kết tệp. *Xem* virus names.

next-day funds ***quỹ ngày hôm sau*** Trong hoạt động ngân hàng, các quỹ luôn có sẵn để chuyển nhượng giữa những quỹ giống nhau và lệ thuộc vào sự thanh toán, có sẵn cho ngày hoạt động tiếp theo đối với các chuyển nhượng, hoặc cho rút tiền mặt trong cùng ngày. Kiểu các quỹ này chỉ có thể áp dụng cho các giao dịch bằng đô la Mỹ. *So sánh với* same-day funds. *Xem* funds type.

nibble ***nửa byte, nible*** Trong tính toán, một từ chứa 4 bit. *So sánh với* byte. *Xem* bit, word.

NIFTP ***giao thức NIFTP*** Trong truyền thông dữ liệu, viết tắt của Network Independent File Transfer Protocol (giao thức chuyển tệp độc lập với mạng). *Xem* file transfer.

NIIT ***mạng NIIT*** Viết tắt của National, International and Intercontinental Telecommunication network (mạng viễn thông quốc gia, quốc tế và liên lục địa).

Nina ***virut Nina*** Trong an toàn máy tính, một virut chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COMMAND.COM, COM tác động trong thời gian chạy, làm ngắt các tệp chương trình, dữ liệu và các tệp OVL. *Xem* virus names.

NIST *Xem* National Institute of Standards and Technology.

NKSR *Xem* non-kernel-security-related software.

NMR ***dư thừa N modun*** Trong lĩnh vực độ tin cậy, một dạng dư thừa modun tương tự với dư thừa modun bội ba trừ phi dùng *N* khối, *N* là một số lẻ. *So sánh với* triple modular redundancy. *Xem* modular redundancy.

no contract ***không hợp đồng*** Trong truyền thông dữ liệu, không phổ biến cho người ký hợp đồng; chỉ ra rằng, thông tin chứa trong tài liệu không được phát cho những người ký hợp đồng hay tư vấn chuyên môn

node ***nút*** (1) Trong truyền thông dữ liệu, một hệ thống máy tính được nối tới mạng liên lạc và tham gia vào việc định tuyến các thông báo trong phạm vi mạng đó. Các mạng thường được mô tả như một tập hợp các nút kết nối với nhau qua các kênh liên lạc. *Xem* network. (2) Trong truyền thông dữ liệu, một nơi có tầm quan trọng để chuyển tải dữ liệu, một điểm kết nối chung tới mạng. (3) Trong tính toán, một thực thể nằm trên hai hoặc nhiều hơn tuyến truy nhập.

node computer ***máy tính nút*** Trong truyền thông dữ liệu, một máy tính thường dùng để nối liền với máy tính chủ. Máy chủ được nối tới mạng liên lạc qua máy tính nút. *Xem* host computer.

node encryption ***mật mã nút*** Trong an toàn liên lạc, một phương pháp mã dữ liệu mạng trong đó, dữ liệu được giải mã trong phạm vi nút trung gian và được mã lại bằng một khóa khác để truyền tiếp. Phép giải mã và mã lại được thực hiện trong các modun an toàn và như vậy, bản rõ không được truyền qua nút. So sánh với end-to-end encryption. *Xem* network encryption, plaintext.

NOFORN ***không phổ biến ra nước ngoài*** Thuật ngữ này xuất xứ từ chữ NO FOReigN, chỉ thông tin chứa trong tài liệu không được phổ biến sang các nước khác.

noise ***tiếng ồn, tạp âm, nhiễu*** (1) Trong truyền thông, tín hiệu ngẫu nhiên không mong muốn. *Xem* thermal noise. (2) Trong quản lý khóa, tín hiệu ngẫu nhiên mà có thể dùng các thuộc tính ngẫu nhiên của nó để tạo ra các khóa phiên (trong mật mã). *Xem* random number, session key. (3) Trong an toàn cơ sở dữ liệu, những số ngẫu nhiên được thêm vào các mục dữ liệu theo các kỹ thuật gây nhiễu. *Xem* inference control, perturbation.

noise temperature ***nhiệt độ tiếng ồn, nhiệt độ tạp âm*** Trong điện tử học, nhiệt độ của nguồn ồn nhiệt tạo ra cùng công suất ồn tại đầu ra ở cùng dải thông như thiết bị đang được xem xét. *Xem* thermal noise.

nomenclature ***danh pháp, thuật ngữ*** Một phương pháp nhất quán để gán các tên cho các phần tử của một hệ thống.

Nomenclature ***virut Nomenclature*** Trong an toàn máy tính, một virut chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COMMAND.COM, COM, EXE và OVL. Tác động trong thời gian chạy, làm hỏng các

tệp chương trình, OVL và các tệp dữ liệu. *Xem* virus names.

nonbreak glass station ***trạm báo cháy không đập vỡ kính*** Trong an toàn vật lý, một trạm báo hỏa hoạn bằng tay không cần bẻ kính để kích hoạt tín hiệu báo. *Xem* alarm station.

nonce ***số nonce, số hiện tại*** Trong mật mã, một số ngẫu nhiên được dùng trong giao thức hỏi/đáp. *Xem* replay.

noncoded system ***hệ thống không quy tắc, hệ không mã*** Trong an toàn vật lý, một hệ thống trong đó tín hiệu báo động liên tục sẽ được tiếp âm với thời gian tối thiểu quyết định trước. Bởi vậy, tín hiệu báo cháy có thể ngừng tự động hoặc do thủ công. *So sánh với* coded system.

noncompatibility ***không tương thích*** Trong tính toán, nói tới tình huống một hệ thống không thể tìm kiếm được thông tin được lưu trữ trên máy khác hoặc chạy các chương trình phát triển trên máy khác. *So sánh với* compatibility.

nondense index ***chỉ số không trù mật*** Trong các cơ sở dữ liệu, một chỉ mục cung cấp thông tin về vị trí của một nhóm bản ghi. Ngay khi truy nhập tới nơi, các bản ghi phải được quét tuần tự cho tới khi tìm thấy bản ghi tương ứng với khóa sắp xếp phù hợp. *So sánh với* dense index. *Xem* index, record, key.

nondestructive readout ***đọc ra không xóa*** Trong tính toán, thao tác đọc không làm thay đổi dữ liệu được lưu. *So sánh với* destructive readout.

nondeterministic polynomial class ***lớp đa thức không tất định*** *Xem* NP class.

non-discretionary security ***an toàn không tùy ý*** Trong an toàn dữ liệu, một khía cạnh của chính sách an toàn của DOD (Bộ Quốc Phòng Mỹ) nhằm hạn chế truy nhập tới các mức an toàn cơ bản. Một mức an toàn gồm có một mức đọc và một hạn chế tập bảng các phân loại. Để truy nhập đọc tới một mục thông tin, người dùng phải có mức truy nhập (clearance) lớn hơn hoặc bằng phân loại của thông tin và cũng có bảng các phân loại mức truy nhập (clearance) trong đó chứa tất cả các loại truy nhập chỉ ra đối với thông tin. *So sánh với* discretionary security. *Xem* mandatory security.

noninvertibility ***tính không thể đảo ngược*** Trong mật mã, một tính chất của một thuật toán mã. Thuật toán được coi là không thể đảo ngược được nếu ta không thể xác định ra khóa mã về mặt tính toán khi cho trước bản rõ và bản mã tương ứng. *Xem* ciphertext, computationally infeasible, cryptographic algorithm, cryptographic key, plaintext.

non-kernel security-related software ***phần mềm an toàn không nhân*** Trong an toàn máy tính, một phần mềm an toàn chạy trong môi trường do nhân an toàn cung cấp chứ không phải là một phần của nhân. Các quá trình thực hiện phần mềm này có hoặc không đòi hỏi đặc quyền đặc biệt vượt lên các quy tắc an toàn mà nhân buộc tuân thủ. *Xem* security kernel.

nonoverwriting virus ***virut không***

ghi đè Trong an toàn máy tính, một virut tự gắn vào chương trình bị lây nhiễm sao cho chương trình vẫn thực hiện đúng sau khi chạy đoạn mã có virut. *So sánh với* overwriting virus. *Xem* virus.

nonprime attribute ***thuộc tính phụ*** Trong cơ sở dữ liệu, một thuộc tính không phải là thuộc tính cơ bản, tức là nó không phải là một thành viên của một khóa dự bị. *So sánh với* prime attribute. *Xem* candidate key, relational database.

nonprocedural language ***ngôn ngữ không thủ tục*** Trong tính toán, một ngôn ngữ trong đó người sử dụng chỉ ra kết quả cuối cùng chứ không phải là quá trình cần thiết để nhận được nó. Ví dụ, khi đặc tả một cây gia phả và xác định cháu trai là con của con trai hay con gái của ông bà thì người dùng có thể đưa yêu cầu về ông bà của cá nhân chỉ ra. *So sánh với* procedural language. *Đồng nghĩa với* declarative language.

nonrepudiation ***không từ chối, không chối bỏ, thừa nhận*** (1) Trong xác thực, một dịch vụ cung cấp bằng chứng về tính toàn vẹn và xuất xứ của dữ liệu, cả hai đều thuộc mối quan hệ không thể giả mạo được, điều này có thể xác minh qua một nhóm thứ ba vào bất kỳ lúc nào. (2) Trong xác thực, sự xác thực có sự bảo đảm cao có thể được khẳng định là chân thực và không thể bác bỏ được. *So sánh với* repudiation.

nonreturn to zero ***không trở về không*** Trong truyền thông dữ liệu, một phương pháp truyền dữ liệu trong đó, điện áp một cực biểu diễn bit 1 còn cực kia là bit 0. Mạch tải dữ liệu bất cứ lúc nào có thể. Nó là phương pháp chung để chuyển dữ liệu giữa máy tính và các thiết bị ngoại vi của nó.

nonsecret design ***thiết kế không mật*** Trong an toàn dữ liệu, nguyên tắc mà các khía cạnh thiết kế một hệ thống an toàn không cần giữ bí mật bởi vì tính an toàn nằm trong các khóa mật, các tham số... Ví dụ, thuật toán DES được công bố công khai còn bí mật của phép mã phụ thuộc vào các khóa mật. Nguyên tắc này cho phép hệ thống được nhiều chuyên gia nghiên cứu, tìm ra những thiếu sót trong thiết kế. Mặt khác, tính mở làm tăng thêm sự nguy hiểm của việc phát hiện ra khiếm khuyết trong thiết kế hay những cái bẫy trong hệ thống, khi những hệ thống này sử dụng rộng rãi sẽ tiềm ẩn những hậu quả cực kỳ nghiêm trọng. *Xem* DES, trapdoor.

nonstandard sector ***cung không chuẩn, secto không chuẩn*** Trong bảo vệ phần mềm, một đĩa mềm đã được định dạng theo cách không chuẩn và làm nó không thể sao chép bằng các tiện ích của hệ điều hành. *Xem* execute protection, flopy disk, formating, operating system.

nonswitched line ***đường dây không chuyển mạch*** *Đồng nghĩa với* leased circuit.

nontransparent mode ***chế độ không trong suốt, phương thức không trong suốt*** Trong truyền thông dữ liệu, sự truyền các ký tự theo một khuôn thức xác định, chẳng hạn mã ASCII, trong đó

tất cả các dãy và các ký tự điều khiển xác định đều được nhận dạng và được xử lý. *So sánh với* control character, transparent data communication code. *Xem* ASCII.

nonvolatile storage ***bộ nhớ bất biến*** Trong tính toán, phương tiện lưu trữ vẫn giữ thông tin khi nguồn điện bị ngắt. *So sánh với* volatile storage.

normal forms ***dạng chuẩn, dạng thông thường*** Trong cơ sở dữ liệu, một lớp các quan hệ trong các cơ sở dữ liệu quan hệ có các tính chất xác định trước về mối quan hệ qua lại giữa các thuộc tính. Việc dùng các dạng chuẩn trong cơ sở dữ liệu sẽ làm giảm những vấn đề về thao tác và lưu trữ dữ liệu có thể này sinh từ những mối tương quan giữa các thuộc tính. *Xem* relation, attribute, first normal form, relational database, second normal form, third normal form.

nostro account ***tài khoản nostro, tài khoản của chúng tôi*** Trong hoạt động ngân hàng, một bản ghi được giữ bởi ngân hàng người chủ tài khoản có tài khoản được ngân hàng phục vụ tài khoản phục vụ nhân danh nó. *Xem* account servicing bank.

notarization ***công chứng, chứng thực*** (1) Trong xác thực, sự đăng ký dữ liệu với nhóm thứ ba tin cậy cho phép sự bảo đảm sau đó về tính chính xác của các đặc trưng như nội dung, nơi xuất xứ, thời gian và sự phân phối. (2) Trong mật mã, một phương pháp áp dụng tính an toàn bổ sung đối với khóa nhằm tận dụng những đặc tính đồng nhất của người khởi đầu cuộc liên lạc và người nhận sau cùng. *Xem* cryptographic key. *Đồng nghĩa với* key notarization.

NP Class ***lớp NP*** Trong toán học, lớp các đa thức không tất định - một lớp bài toán trong đó thời gian xác định lời giải tăng lên theo hàm mũ theo kích thước của bài toán, song thời gian kiểm tra lời giải lại tăng tuyến tính hoặc theo thời gian đa thức. *Xem* NP complete, public key cryptography, time and space requirements.

NP complete ***NP đầy đủ*** Trong toán học, một lớp bài toán NP có tính chất rằng, nếu có một phương pháp dễ dàng thực hiện để tìm ra một lời giải tổng quát cho bất kỳ bài nào trong số chúng thì tất cả các bài toán NP đều có các phương pháp như vậy. *Xem* NP Class.

n-respondent, k%-dominance ***n-trả lời, k% lợi thế*** Trong an toàn dữ liệu, một tiêu chuẩn kiểm soát suy luận được dùng với dữ liệu điều tra dân số. Nó xác định một thống kê nhạy cảm như một thống kê mà *n* hay vài bản ghi góp hơn *k*% tổng số. *Xem* inference control, sensitive statistic, statistical database.

NRZ ***không trở về không*** *Xem* nonreturn to zero.

NSA ***Cục an ninh Quốc gia*** Viết tắt của U.S. National Security Agency (Cục an ninh Quốc gia Hoa Kỳ). *Xem* National Security Agency/Center Security Service.

NSA COMSEC module ***modun COMSEC của NSA*** Trong mật mã, dưới CCEP, NSA xác nhận hai kiểu sản

phẩm mật mã: kiểu I và kiểu II. Sản phẩm kiểu I nhằm dùng trong việc bảo vệ thông tin đã xếp loại của chính phủ Mỹ và chỉ Chính phủ Mỹ được sử dụng, còn các nhà thầu khoán cũng sẽ chịu sự kiểm soát của chính phủ Mỹ. Sản phẩm kiểu II cũng chỉ Chính phủ Mỹ và các nhà thầu khoán của họ được sử dụng, không có sẵn cho các khu vực tư nhân thương mại. Các sản phẩm kiểu I và II không được phép xuất khẩu. Chúng chứa một trong ba loại modun dạng chip bán dẫn do NSA cung cấp thông qua các nhà cung cấp modun COMSEC. Những môđun này thể hiện một thuật toán mã mật trong một chip đóng kín, chống lại được kỹ thuật đảo. Mỗi modun chứa các tính năng an toàn cơ bản và có dạng thức vào và ra chuẩn. Chúng được cung cấp cho phía người dùng tin tức về các nhà cung cấp, chẳng hạn OEM, ai sau đó sẽ sản xuất thiết bị an toàn truyền thông, kể cả những modun này.

Cả môđun kiểu I lẫn kiểu II đều có ba phương án khác nhau về kích thước, giá thành và tốc độ, được thiết kế cho tiếng nói kênh đơn, dữ liệu máy tính và dữ liệu tốc độ cao. Các modun trong phạm vi mỗi phương án riêng lẻ sẽ được thao tác chung với mỗi modun khác. *So sánh với* data encryption standard. *Xem* CCEP, COMSEC, OEM, NSA, reverse engineering.

NSD-42 *Xem* National Security Directive-42.

NSDD ***chỉ thị NSDD*** Viết tắt của U.S. National Security Decision Directive (chỉ thị quyết định an toàn quốc gia Hoa Kỳ).

NSDD-145 ***chỉ thị NSDD-145*** Viết tắt của National Security Directive (chỉ thị an toàn quốc gia Hoa Kỳ). Một chỉ thị trong đó Tổng thống Mỹ đã công nhận vấn đề an toàn và tính nhạy cảm của liên lạc khu vực tư nhân. Kết quả của chỉ thị này, NSA đã sửa lại cho phù hợp chương trình CCEP của họ, cho phép khu vực tư nhân truy nhập tới thiết bị CCEP. *Xem* CCEP, DES, NSA, NSA COMSEC module.

NSI ***thông tin an ninh Quốc gia của Mỹ*** Viết tắt của U.S. National Security Information.

NTCB *Xem* Network Trusted Computing Base.

NTCB partition ***phân hoạch NTCB*** Trong an toàn truyền thông, tổng tất cả các cơ chế trong phạm vi một thành phần mạng đơn lẻ để buộc tuân thủ chính sách mạng khi được cấp phát cho các thành phần; phần của NTCB trong phạm vi một thành phần mạng đơn lẻ. *Xem* network component, NTCB, security policy.

NTISS ***an toàn hệ thống thông tin và viễn thông Quốc gia của Mỹ*** Viết tắt của U.S. National Telecommunications and Information System Security.

NTISSC ***Ủy ban NTISSC*** Viết tắt của U.S. National Telecommunications and Information System Security Committee (Ủy ban an toàn hệ thống thông tin và viễn thông Quốc gia Hoa Kỳ).

NTISSD ***Chỉ thị về an toàn hệ thống thông tin và viễn thông Quốc gia của Mỹ*** Viết tắt của U.S. National

Telecommunications and Information System Security Directive.

NTISSP-200 ***chính sách NTISSP-200*** Viết tắt của U.S. National Telecommunications and Information System Security Policy-200 (chính sách an toàn hệ thống thông tin và viễn thông Quốc gia Hoa Kỳ), một chính sách của Mỹ đề nghị năm 1987 yêu cầu tất cả hệ thống hoạt động nhân danh chính phủ và được người dùng truy nhập ở các mức ủy nhiệm khác nhau cần được đánh giá ít nhất là theo mức C2, được định nghĩa trong Sách Da Cam. *Xem* C2, Orange Book.

n-tuple ***bộ (quan hệ) n*** Trong toán học, tập hợp *n* phần tử, thường được sắp theo thứ tự. *Xem* tuple.

nucleus ***tâm*** Trong tính toán, phần của hệ điều hành là trung tâm của mọi hoạt động điều khiển và quản lý tài nguyên. Nó xử lý việc cấp phát tài nguyên và truy nhập tới các giao diện vào/ra. Nó thường được phân biệt với nhân bởi sự pha trộn của việc lập trình thông thường với các vi lệnh (microcode). *Xem* I/O, kernel.

NUI *Xem* network user identification.

nuisance alarm ***báo động hỏng hóc*** Trong an toàn vật lý, một sự kích hoạt báo động do hỏng thiết bị hay sự cố tương tự.

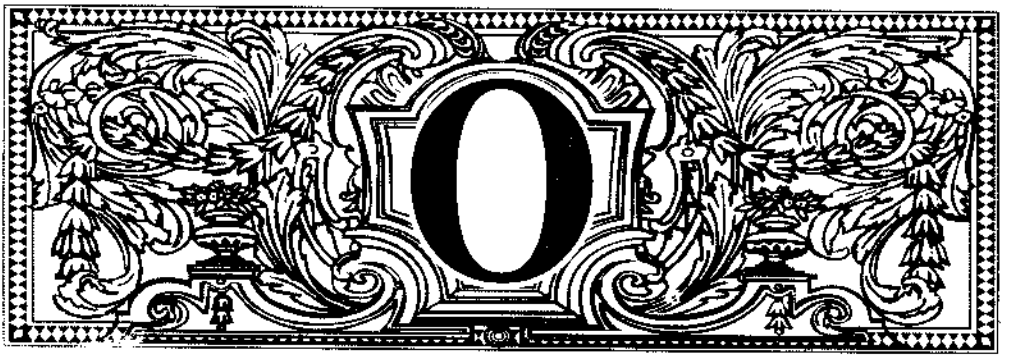
null modem ***modem trống, modem rỗng*** Trong truyền thông dữ liệu, một thiết bị được lợi dụng để nối hai hệ thống liên lạc thông thường với modem. Ví dụ, nếu hai máy tính liên lạc trực tiếp nhờ dùng mạch ghép nối RS-232C và cả hai sẽ truyền dữ liệu trên chân 2 và đợi thu dữ liệu trên chân 3. Trong trường hợp đó, modem trống sẽ đơn giản kết hợp một hệ thống chân cắm để nối chân 2 trên một máy tính với chân 3 trên máy kia và ngược lại. *Xem* MODEM, RS-232C.

null string ***xâu rỗng, chuỗi rỗng*** Trong tính toán, một chuỗi không chứa các ký tự. *Xem* string.

null suppression ***triệt ký tự rỗng, bỏ ký tự rỗng*** Trong mã hóa, bỏ không nhớ hoặc không truyền các ký tự rỗng để tiết kiệm thời gian truyền hoặc không gian nhớ. *Xem* data compression.

number ***số, số lượng*** Thực thể toán học cho biết lượng các đơn vị.

number crunching ***tốc hoạt số*** Trong tin học, các hoạt động xử lý liên quan tới một tỷ lệ cao phép toán trên dữ liệu, thường nảy sinh trong các ứng dụng khoa học. Những ứng dụng như thế sử dụng mạnh bộ xử lý trung tâm và liên quan tới tương đối ít các thao tác nhập xuất. *Xem* CPU.



OA ***tự động hóa văn phòng*** Viết tắt của Office Automation.

object ***đối tượng, đích*** (1) Trong an toàn máy tính, một thực thể thụ động để chứa hoặc nhận thông tin. Sự truy nhập tới một đối tượng có nghĩa truy nhập tới thông tin mà nó chứa. Những ví dụ về các đối tượng là: các biểu ghi, các khối, trang, đoạn, tệp, thư mục, cây thư mục và các chương trình cũng như các bit, các byte, các từ, các trường, các bộ xử lý, màn hình video, bàn phím, đồng hồ , máy in, các nút mạng... *So sánh với* subject. (2) Trong tính toán, một thực thể trong bộ nhớ máy tính mà chứa và bảo vệ một tập các dữ liệu liên quan. Các đối tượng thực hiện các tác vụ được gán cho nó thông qua liên lạc với những đối tượng khác. Ví dụ một đối tượng bộ xử lý lưu dữ liệu quan trọng cho bộ xử lý, nếu một bộ xử lý khác được thêm vào hệ thống thì nó đơn thuần thêm một đối tượng tương ứng vào bộ nhớ.

object authentication ***xác thực đối tượng*** Trong xác thực, sự xác minh xem các đối tượng, chẳng hạn các chương trình lớn có bị thay đổi trong thời gian chúng không được điều khiển trực tiếp không.

object code ***mã đối tượng*** Trong tính toán, mã của một chương trình người sử dụng sau khi nó đã được dịch. *So sánh với* source code.

object of defense ***mục tiêu bảo vệ*** Trong an toàn tính toán, các thủ tục bảo vệ an toàn đều được thiết kế nhằm đạt các mục tiêu: (*a*) ngăn chặn sự cố để lộ nhờ dựng lên các rào chắn giữa hiểm họa bất kỳ và những điểm yếu đối với nó, (*b*) tối thiểu hóa hoặc hạn chế ảnh hưởng của thiệt hại chủ yếu nhờ dùng các tầng bảo vệ kế tiếp để hạn chế tác nhân gây hiểm họa và (*c*) cực đại hóa khả năng phục hồi thiệt hại. Đưa ra các cách thức giảm thiệt hại, chẳng hạn, dùng cách sao chép dự

phòng và tái xây dựng lại các tệp. *Xem* defensive depth, threat, vulnerability.

objectivity ***tính khách quan*** Trong an toàn thông tin, một tính chất của phép thử tại đó kết quả nhận được với ý kiến hoặc đánh giá chủ quan ít nhất. *Xem* information technology security evaluation criteria, information technology security evaluation manual.

object language ***ngôn ngữ đối tượng*** Trong tính toán, một ngôn ngữ ra của một quá trình dịch. *So sánh với* source language.

object program ***chương trình đối tượng*** Trong tính toán, một chương trình viết ở dạng mã đối tượng. *Xem* object code.

object protection ***bảo vệ đối tượng*** (1) Trong kiểm soát truy nhập, những biện pháp kiểm soát được dùng để hạn chế truy nhập tới một đối tượng. *Xem* object. (2) Trong an toàn vật lý, những biện pháp dùng để bảo vệ các đối tượng có giá trị, chẳng hạn két sắt, các hồ sơ từ vùng được bảo vệ.

object reuse ***dùng lại đối tượng*** (1) Trong an toàn máy tính, sự dùng lại đối tượng nào đó có môi trường (chẳng hạn khung trang, cung từ của đĩa, băng từ) chứa một hay nhiều đối tượng. Để dùng lại một cách an toàn, các môi trường đó phải không chứa dữ liệu còn lại của đối tượng hay các đối tượng được chứa trên đó trước đấy. *Xem* object, residue, subject. (2) Trong an toàn thông tin, các chức năng kiểm soát việc sử dụng lại các đối tượng dữ liệu. *Xem* information technology security evaluation criteria.

OCD ***trường OCD*** Trong hoạt động ngân hàng, viết tắt của Other Card Data (trường dữ liệu thẻ khác), dữ liệu được ghi trên thẻ mà thông thường các nhóm không phải người phát hành hoặc đại lý của nó không thể biết được. *Xem* card key.

OCI ***cơ quan OCI*** Viết tắt của Office of Computer Information (cơ quan thông tin máy tính Hoa Kỳ) một cơ quan thuộc Bộ Thương mại Hoa Kỳ.

OCR *Xem* optical character recognition.

octal ***bát phân, cơ số 8*** Trong toán học, nói tới con số 8. Ký pháp cơ số 8 hay bát phân dùng cơ số 8 và là dạng tiện lợi để biểu diễn các số nhị phân, ví dụ số thập phân 66 = 102 theo cơ số 8 = 1 000 010 theo hệ cơ số 2. *So sánh với* hexadecimal. *Xem* binary.

octet ***octet, byte, 8 bit*** Trong tính toán, một nhóm 8 chữ số nhị phân được xử lý như một thực thể. *Xem* octal.

odd even check ***kiểm tra tính chẵn lẻ*** *Đồng nghĩa với* parity checking.

odd parity ***tính lẻ*** *Xem* parity.

odd prime ***số nguyên tố lẻ*** Trong toán học, số nguyên tố bất kỳ trừ 2. *Xem* prime number.

ODETTE ***tổ chức ODETTE*** Viết tắt của Organization for Data Exchange and Teletransmission in Europe (tổ chức trao đổi dữ liệu và truyền thông từ xa ở Châu Âu). Một tổ chức thiết lập ra các chuẩn để trình bày tài liệu sao cho có thể gửi chúng trên mạng dữ liệu và người nhận hiểu được. *Xem* electronic data interchange.

Oe ***ơstet*** *Xem* oersted.

OEM *Xem* original equipment manufacturer.

oersted *ơstet* Trong điện tử học, một đơn vị đo lực từ hóa cần thiết để tạo ra thông lượng từ tính mong muốn qua một bề mặt. *Xem* magnetic flux.

OFB *Xem* output feedback.

off line *gián tiếp, ngoại mạch, ngoại tuyến* Trong các hoạt động, nói tới thiết bị xử lý không được nối với máy tính hay với mạng, hoặc các thao tác được thực hiện trên thiết bị như vậy. *So sánh với* on line.

off line card reader *bộ đọc cục gián tiếp* Trong kiểm soát truy nhập, một bộ đọc thẻ kiểm soát truy nhập chứa đầy đủ thông tin để nhập vào hoặc cho ra các quyết định dựa trên việc đọc thông tin từ thẻ truy nhập. *So sánh với* on line card reader. *Xem* card reader. *Đồng nghĩa với* intelligent card reader.

off line crypto-operation *hoạt động mật mã ngoại tuyến* Trong an toàn liên lạc, phép mã hoặc giải mã được thực hiện như một hoạt động độc lập tách khỏi sự truyền văn bản đã mã, như bằng tay hoặc bằng máy, không nối ở dạng điện tử với dây tín hiệu. *So sánh với* on line crypto-operation. *Xem* encrypt, decrypt.

off line encryption *phép mã gián tiếp, phép mã ngoại mạch* *Xem* off line cryptosystem.

offset *dịch vị, độ lệch, khoảng lệch* (1) Trong an toàn vật lý, khoảng cách trên mặt đất, nơi kẻ đột nhập có khả năng tránh phát hiện bằng cách bò dưới bộ cảm biến khoảng cách. *Xem* span sensor. (2) Trong an toàn vật lý, phần gối lên nhau của vùng phủ sóng mở rộng của chùm tia do sự dao động của các máy thu và máy phát để tối thiểu hóa khoảng trống trong phạm vi tác động của chùm tia. (3) Trong hoạt động ngân hàng, một số liên quan về mặt toán học với mã định danh tính sẵn cho PIN được chọn của khách hàng. *Xem* PIN management and security. *Đồng nghĩa với* PIN offset. (4) Trong quản lý khóa, *đồng nghĩa với* key offset.

off site storage *cất trữ ngoài vị trí* Trong an toàn vật lý, một kỹ thuật duy trì sự sao chép dự phòng tài liệu trong vùng an toàn ngoài dinh cơ. *Xem* backup procedures.

Off Stealth *virut Off Stealth* Trong an toàn máy tính, loại virut lén lút chấm dứt chương trình và nằm thường trú trong bộ nhớ; lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, làm sai lạc các tệp chương trình, OVL và các tệp dữ liệu. *Xem* virus names.

OIS 21 *ban OIS 21* Trong an toàn dữ liệu, một ban trong Cục tiêu chuẩn Anh (BSI) đảm trách các tiêu chuẩn an toàn dữ liệu. *Xem* BSI, TC 97/SC20.

OMB *văn phòng OMB* Viết tắt của U.S. office of management and Budget (Văn phòng quản lý và ngân sách của Hoa Kỳ).

OMR *Xem* optical mark recognition.

one category *loại một, hạng một* Trong an toàn dữ liệu, một mức truy nhập của Bộ quốc phòng Hoa Kỳ cần thiết ngoài mức truy nhập tối mật dựa trên cuộc điều tra nền tảng hiện tại.

Việc cấp các quyền truy nhập do một cá nhân có trách nhiệm tiến hành. *So sánh với* confidential clearance, multiple categories, secret clearance, unclassified information, uncleared. *Xem* clearance, top secret clearance.

one end device ***thiết bị một đầu*** Trong an toàn máy tính, một thiết bị bảo vệ chống sự đột nhập bằng điện thoại, thiết bị này được cài đặt tại phía máy tính chủ, hoặc phía người dùng của đường dây điện thoại. *So sánh với* two end device. *Xem* port protection device, security modem, telephone intrusion.

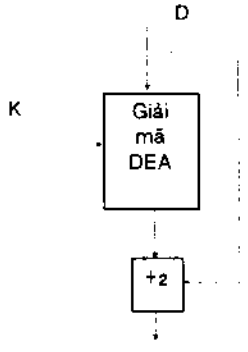
one key cryptosystem ***hệ thống mã một khóa, hệ thống mã đối xứng*** *Đồng nghĩa với* symmetric cryptosystem.

one-time pad ***mã pháp dùng khóa một lần*** Trong mật mã, một mã pháp dùng một chuỗi khóa ngẫu nhiên không lặp. Chúng là mã pháp duy nhất đạt được độ mật hoàn hảo song độ dài khóa bằng độ dài thông báo. Chúng được sử dụng chủ yếu trong liên lạc ngoại giao. *Xem* perfect secrecy, stream cipher.

one-time passwords ***(các) mật khẩu dùng một lần*** Trong kiểm soát truy nhập, những mật khẩu được thay đổi sau mỗi lần dùng và rất hữu ích khi mật khẩu không được bảo vệ đầy đủ khỏi bị hại trong thời gian đăng nhập (ví dụ, dây liên lạc bị nghi ngờ nối rẽ). *Xem* expired password, log in, password.

one-way cipher ***mã pháp một chiều*** Trong mật mã, một mã pháp là một hàm không thể lấy nghịch đảo từ bản rõ sang bản mã, tức là, không thể thực hiện được về mặt tính toán để giải mã bản mã. Kỹ thuật này có thể dùng để lưu các mật khẩu đã mã trong hệ thống máy tính. Khi người dùng nhập một mật khẩu, nó được mã hóa tương tự và được so sánh với mật khẩu mã đã lưu. Với kỹ thuật này, kẻ tấn công không thể xác định được dạng rõ của mật khẩu ngay cả khi truy nhập bất hợp pháp tới được bộ nhớ của máy tính. Tuy nhiên, anh ta có thể thu được lợi lộc từ sự truy nhập tới tệp mật khẩu mã vì có thể tiến hành gián tiếp tấn công theo kiểu liệt kê. *Xem* computationally infeasible, dictionary attack, one-way function. *Đồng nghĩa với* irreversible encryption.

one-way function ***hàm một chiều, OWF, hmc*** (1) Trong mật mã, một phép tính dựa trên hai mục dữ liệu K và D sao cho đầu ra O thoả mãn $O = dK(D) \oplus D$, ở đây, d ký hiệu phép giải mã khi dùng thuật toán DES.



đầu ra = hmc (K, D)

one-way function: *hàm một chiều.*

Cho trước một đầu vào (K hoặc D) và đầu ra O, việc xác định đầu vào kia đòi hỏi cuộc tìm kiếm kiểu vét cạn tất cả các giá trị có thể.

Trong một số trường hợp, một đầu vào

O

có thể là một giá trị biết trước. Trong trường hợp đó, nó sẽ được dùng như đầu vào khóa (K). Nếu đầu ra O và đầu vào D đều đã biết thì kẻ tấn công có thể dễ dàng tính $dK(D)$ bằng phép LOẠI TRỪ- HOẶC trên O và D.

Bây giờ kẻ tấn công phải kiểm tra hết các giá trị của K, song khi (ví dụ) anh ta tìm được một giá trị K' sao cho $eK'(D) = eK(D)$ thì cuộc tìm kiếm kết thúc. Tuy nhiên, nếu giá trị đã biết được dùng làm khóa thì kẻ tấn công phải tìm kiếm theo kiểu vét can tất cả các khối dữ liệu vào có thể. Ngoài ra, ngay khi tìm thấy được một giá trị ăn khớp, thì lại có yêu cầu tìm tiếp vì đó là bản chất của hàm một chiều là với một khóa cho trước, một số trong các khối dữ liệu có thể ánh xạ lên cùng khối ra. *So sánh với* one-way hash function. *Xem* transaction key system. (2) Trong mật mã, một hàm toán học f rất dễ tính toán song chỉ đối với giá trị y tổng quát trong khoảng nhưng lại rất khó tính toán để tìm ra giá trị x trong miền sao cho $f(x) = y$. Có thể có vài giá trị y mà với nó việc tìm ra x không khó lắm. *Xem* domain range. (3) Trong mật mã, hàm $f(x)$ dễ dàng tính được nếu biết x với x bất kỳ thuộc miền của nó song đảo của nó không thể tính được về mặt tính toán. Trong mật mã khóa công khai có thể nhân hai số nguyên tố lớn nhưng về mặt tính toán không thể tính được các thừa số của tích. *Xem* computationally infeasible, domain, password.

one-way hash function ***hàm băm một chiều, hàm hash một chiều*** Trong mật mã, một hàm $F(x)$ có các tính chất:

- F có thể áp dụng cho đối số bất kỳ có kích thước tùy ý.
- F tạo ra đầu ra có độ dài cố định.
- Khi biết trước F và x, dễ dàng tính được $F(x)$.
- Cho trước F, việc tìm cặp giá trị x và x' bất kỳ sao cho $x <> x'$ và $F(x) = F(x')$ là không thể tính toán được.

So sánh với one-way function.

onion skin architecture ***kiến trúc kiểu vỏ hành, kiến trúc phân tầng*** Trong truyền thông dữ liệu và kiến trúc, một cấu trúc phân tầng tạo thuận tiện cho việc liên lạc giữa các quá trình cùng mức, việc dùng các quá trình mức thấp hơn trong chừng mực nào đó trong suốt hơn đối với các quá trình của người sử dụng. Trong các hệ thống liên lạc, sự tiếp cận này tạo thuận lợi cho việc thiết kế và sử dụng các mạng và hệ thống phức tạp. Các quá trình nhận thông báo từ tầng trên và chuyển chúng tới các quá trình tương ứng nằm cùng mức bằng cách đầu tiên truyền chúng tới tầng thấp hơn. Những quá trình này chỉ đề cập tới sự chuyển các thông báo qua hai giao diện tầng mặc dù toàn hệ thống có thể nhiều tầng. *Xem* transparent, onion skin language, open systems interconnection.

onion skin language ***ngôn ngữ kiểu vỏ hành*** Trong các cơ sở dữ liệu, một ngôn ngữ máy tính để thực hiện phân cấp bậc cho các hệ thống. Một hệ cơ sở dữ liệu có thể được xây dựng như một tập hợp các hệ thống tăng dần về độ phức tạp sao cho hệ thống này là tập con của hệ thống tiếp sau. Một

ngôn ngữ kiểu vỏ hành sẽ chế tác hệ thống phức tạp nhất và các tập con ngôn ngữ sẽ chế tác các tập con kế tiếp của hệ thống. *Xem* onion skin architecture.

on line ***trực tuyến, trực tiếp*** Trong các hoạt động, đề cập tới việc xử lý dữ liệu và thiết bị liên lạc được nối với máy tính hoặc kênh liên lạc. *So sánh với* off line.

on line card reader ***bộ đọc thẻ trực tuyến*** Trong kiểm soát truy nhập, một bộ đọc thẻ được nối với bộ xử lý trung tâm chấp nhận kiểm soát truy nhập dữ liệu trên thẻ và ra quyết định cho truy nhập/không cho truy nhập. *So sánh với* intelligent card reader, off line card reader. *Đồng nghĩa với* system card reader.

on line crypto-operation ***hoạt động mật mã trực tuyến*** Trong an toàn liên lạc, việc sử dụng thiết bị mật mã được nối trực tiếp với đường dây liên lạc, tạo ra các quá trình liên tục mã, truyền, nhận và giải mã. *So sánh với* off line crypto-operation. *Xem* decrypt, encrypt.

on line encryption ***mã hóa trực tuyến*** *Xem* on line crypto-operation.

Ontario ***virut Ontario*** Trong an toàn máy tính, một virut tự mã hóa, làm chấm dứt chương trình và thường trú trong bộ nhớ, lây nhiễm tới các tệp COMMAND.COM, COM, EXE, tác động trong thời gian chạy, làm hỏng các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

open hot site ***trạm nóng mở, điểm nóng mở*** Trong an toàn máy tính, một địa điểm nóng được vận hành để thu lợi và tạo sự sẵn sàng cho các công ty không được liên kết với người vận hành địa điểm. *So sánh với* closed hot site. *Xem* hot site.

open position ***vị thế mở*** Trong hoạt động ngân hàng, vị thế nguy hiểm mà ngân hàng bị đặt vào khi tổng tài sản và tiền nợ theo tiền hiện hành là không cân bằng.

open security environment ***môi trường an toàn mở*** Trong an toàn máy tính, một môi trường gồm các hệ thống giữ đúng một trong những điều kiện sau: (*a*) những nhà phát triển ứng dụng (kể cả những người bảo trì) không có mức truy nhập hay cấp phép đầy đủ để cung cấp những giả định chấp nhận được rằng, họ đã không đưa ra logic ác ý. (*b*) Kiểm soát cấu hình không cung cấp sự bảo đảm đầy đủ rằng, các ứng dụng được bảo vệ chống lại logic ác ý trước và trong khi vận hành các ứng dụng hệ thống. *Xem* configuration control, malicious logic.

open shop ***phương tiện mở, dịch vụ mở*** Trong an toàn dữ liệu, phương tiện mà mỗi người dùng trực tiếp có thể thiết kế, phát triển thử và chạy các chương trình của riêng họ. *So sánh với* closed shop.

open storage ***kho lưu trữ mở, bộ nhớ mở*** Trong an toàn dữ liệu, việc lưu trữ thông tin đã phân loại không ở trong các vật chứa an toàn đã được chấp thuận mà ở trong phạm vi phương tiện được chính thức công nhận, trong khi phương tiện như vậy không phải do những cá nhân hợp pháp chiếm giữ.

O

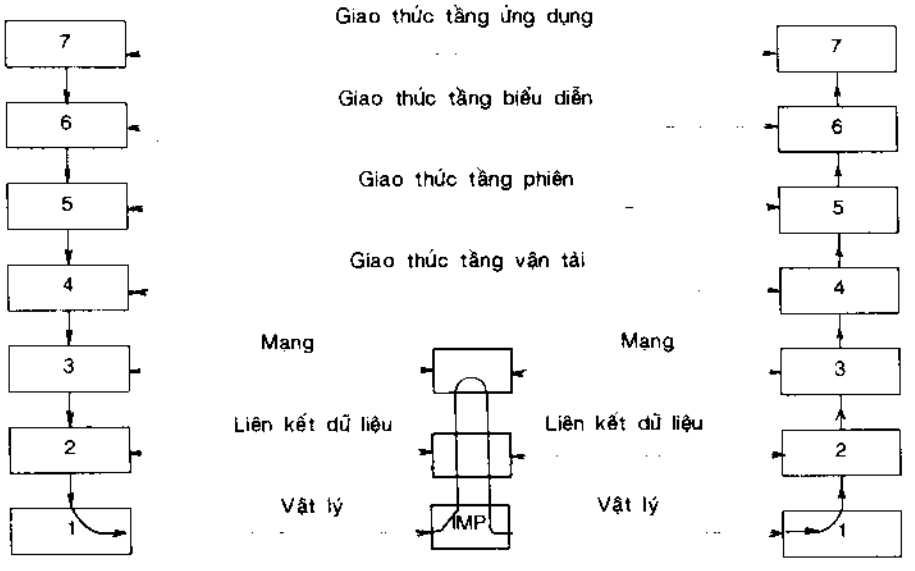
open system ***hệ mở*** Trong hoạt động ngân hàng, mạng EFTPOS trong đó các giao dịch được định tuyến trực tiếp giữa những nhà bán lẻ và cơ sở tài chính trong việc vào sổ bên có cho tài khoản các nhà bán lẻ và vào sổ bên nợ trong tài khoản các khách hàng. *So sánh với* gateway. *Xem* EFTPOS.

open systems ***(các) hệ thống mở*** Trong tính toán và liên lạc, một thuật ngữ được dùng để mô tả các hệ thống (từ các nhà cung cấp khác nhau) có thể trao đổi thông tin, hoặc các dịch vụ cho người dùng thông qua các giao diện chuẩn vận hành theo các chuẩn chung, đối lập với các hệ thống sở hữu thường chỉ cho phép nối dễ dàng giữa các hệ thống con của các nhà cung cấp. Nói chung, một hệ thống mở cần có các giao diện, các dịch vụ, các giao thức được xác định đúng đắn và những công cụ này cần luôn sẵn sàng cho các nhóm thứ ba sử dụng.

open systems interconnection ***kết nối chung các hệ thống mở, hợp mạng hệ mở*** Trong liên lạc dữ liệu, nói tới mô hình tham chiếu của ISO nhằm đến sự phối hợp phát triển các chuẩn ở tất cả các mức liên lạc. Mục tiêu là cho phép những người mua sắm các thiết bị thông tin được tự do nhiều hơn trong việc pha trộn và phối hợp thiết bị cũng như chống lại sự lỗi thời tốt hơn.

Mô hình có bảy tầng: tầng vật lý, tầng kết nối dữ liệu, tầng mạng, tầng vận tải, tầng phiên, tầng biểu diễn và tầng ứng dụng. Bảy tầng này được minh họa trên hình.

Khái niệm tầng tạo nên mức độc lập



Open systems interconnection: *kết nối các hệ thống mở.* Bảy tầng tạo sự độc lập đối với các hoạt động thông tin khác nhau.

đáng có giữa các hoạt động phong phú và phức tạp trong liên lạc dữ liệu. Một quá trình đang hoạt động ở một mức tin rằng nó đang liên lạc với tầng tương ứng tại máy chủ bên nhận. Nó nhận các thông báo từ tầng trên, cộng thêm thông tin điều khiển vào và chuyển thông báo tiếp xuống tầng dưới gần nhất. Tại phía máy nhận, quá trình diễn ra ngược lại, các thông báo được nhận từ tầng dưới nó, cởi bỏ thông tin điều khiển và chuyển tiếp thông báo lên tầng tiếp theo.

Có thể minh họa khái niệm này qua việc thông tin giữa các doanh nghiệp ở các nước khác nhau. Thương doanh *A* ở Turin chỉ quan tâm tới việc chuyển bản phân tích kinh doanh tới thương gia *B* ở Tokyo. Ông ta chuyển tiếp bản phân tích tới người phiên dịch chỉ biết tiếng Anh và tiếng Italia. Ông này dịch bản phân tích kinh doanh sang tiếng Anh gửi nó qua bưu điện để truyền đi. Bưu điện chuyển bức điện dưới dạng bức thư sang Tokyo, tại đây nó sẽ được chuyển bằng tay tới người phiên dịch địa phương, anh ta sẽ dịch lại nó từ bản tiếng Anh sang tiếng Nhật và đưa tới thương gia *B*. Mức độc lập rất rõ ràng, những người phiên dịch có thể thỏa thuận về ngôn ngữ phổ dụng khác nhau và bưu điện có thể chọn đầy đủ các loại kiểu truyền thông báo khác nhau; không cần biết các tầng khác nhau và chúng không bị tác động khi có những thay đổi.

Tầng vật lý liên quan tới sự truyền các dòng bit thô. Tầng liên kết dữ liệu dùng các mã phát hiện sai sót và điều khiển các thông báo từ máy chủ này tới máy chủ khác để chuyển đổi kênh truyền không tin cậy thành kênh tin cậy. Tầng mạng trong mạng điểm nối điểm về cơ bản phụ trách việc định tuyến và vấn đề tắc nghẽn. Tầng vận tải tạo ra sự liên lạc tin cậy giữa máy chủ và che dấu những chi tiết về mạng liên lạc với tầng phiên.

Tầng phiên đến lượt mình có trách nhiệm thiết lập, quản lý và đóng các kết nối từ quá trình này tới quá trình kia trong khi tầng biểu diễn thực hiện những biến đổi hữu ích ở dạng văn bản, chẳng hạn nén văn bản, và cho phép đối thoại với các thiết bị đầu cuối thông minh không tương thích.

Nội dung của tầng ứng dụng dành cho những người dùng và các giao thức chuẩn đối với các ngành công nghiệp đặc thù, chẳng hạn, các ngân hàng. *So sánh với* SNA. *Xem* application layer, bit, data link layer, error dectecion code, host, OSI security, physical layer, point-to-point, presentation layer, routing, session layer, text compression, transport layer.

operand ***toán hạng*** Trong toán học, đại lượng là đối tượng của một phép toán toán học. *So sánh với* operator.

operating system ***hệ điều hành*** Trong tính toán, một tập hợp các chương trình phần mềm dùng để điều khiển trực tiếp mạch cứng của máy tính (ví dụ các yêu cầu vào/ra, cấp phát tài nguyên, quản lý dữ liệu) và tất cả các chương trình khác chạy trên máy tính đều phụ thuộc vào nó. *Xem* UNIX.

operating time ***thời gian vận hành*** Trong liên lạc, toàn bộ thời gian cần

thiết để quay số, đợi thiết lập nối mạch và sau đó phối hợp giao dịch với cá nhân hay thiết bị tại bên thu.

operational date security *an toàn dữ liệu thao tác* Trong an toàn dữ liệu, sự bảo vệ dữ liệu khỏi sự cố hoặc biến đổi cố ý hay trái phép, sự phá hoại hay làm lộ trong khi nhập, xử lý hay thao tác đầu ra.

operational site security manual *sổ tay an toàn địa điểm vận hành* Sổ tay cung cấp tư liệu về các yêu cầu hoạt động, môi trường an toàn, các cấu hình cứng và mềm và các giao diện; tất cả các thủ tục an toàn, các biện pháp và các tính năng; và đối với các phương tiện máy tính là các kế hoạch bất thường để hỗ trợ tiếp trong trường hợp có tai họa tại chỗ. *Xem* contingency plans.

operational vulnerability *điểm yếu hoạt động, tính dễ tổn thương vận hành* Trong an toàn thông tin, một tính chất dễ bị tổn hại tận dụng một điểm yếu trong các biện pháp đối phó phi kỹ thuật để vi phạm tính an toàn của mục tiêu đánh giá. *So sánh với* construction vulnerability, exploitable vulnerability, potential vulnerability. *Xem* information security evaluation criteria, vulnerability.

operations security indicators *(các) chỉ báo cho các hoạt động an toàn* Trong an toàn dữ liệu, các hoạt động hoặc các thông tin đã hoặc chưa phân loại có thể nhận được từ đối phương, dẫn tới các đánh giá hiểu rõ đối phương, các kế hoạch và các hoạt động gây hại đối với các ý định thân thiện và duy trì các khả năng quân sự thân thiện. *Xem* OPSEC.

operator *người vận hành, người thao tác; toán tử* (1) Người vận hành là người được giao trách nhiệm làm cho một phần thiết bị có thể thực hiện chức năng của nó. (2) Trong toán học, toán tử là một ký tự dùng để ấn định một phép toán hay phép logic, chẳng hạn phép +.

OPM *cơ quan OPM* Viết tắt của U.S. Office of Personnel Management (cơ quan quản lý nhân sự Hoa Kỳ).

OPNAVINST *cơ quan OPNAVINST* Viết tắt của U.S. Office of Navy Operations Instruction (cơ quan hướng dẫn các hoạt động hải quân Hoa Kỳ).

OPSEC *an toàn vận hành* Viết tắt của OPerations SECurity.

optical character recognition *quang nhận dạng ký tự, nhận dạng ký tự bằng quang học* Trong tính toán, đề cập tới kỹ thuật và thiết bị đọc các ký tự in hoặc có thể là ký tự viết tay trên tài liệu và chuyển chúng thành dạng mã số để đưa vào máy tính. Ở dạng đơn giản nhất của nó, ánh sáng được chiếu qua ký tự còn ánh sáng phản chiếu được chiếu lên một ma trận các tế bào quang điện. Đầu ra của ma trận được quét và tín hiệu nhận được được đọc vào một ma trận các ô nhớ, tại đây chúng được so khớp với tập các mẫu ký tự lưu trữ. *So sánh với* optical mark recognization.

optical density card *thẻ độ đen, thẻ mật độ quang* Trong kiểm soát truy nhập, một dạng thẻ kiểm soát truy nhập trong đó thông tin số được mã bằng

chất liệu trong mờ có mật độ thay đổi kiểm soát được. Thẻ được đọc bằng cách truyền ánh sáng qua vùng được mã. Nó được dùng cho các ứng dụng an toàn cao vì thẻ tương đối khó giả mạo. *Xem* card reader. *Đồng nghĩa với* varying density holographic card.

optical digital disk ***đĩa quang số*** *So sánh với* optical disk storage.

optical disk ***đĩa quang*** Thuộc kiểu đĩa video, một đĩa trong đó thông tin được khắc ăn mòn lên bề mặt như một chuỗi các vệt lõm và được đọc bằng tia lade. *Xem* optical disk storage.

optical disk storage ***bộ nhớ đĩa quang*** Trong việc cất trữ dự phòng, việc dùng các đĩa kim loại hay chất dẻo có các vệt lõm nhỏ được gắn vào thành các rãnh tròn biểu diễn các bit được lưu. Đĩa được đọc bằng tia lade giống như các đĩa video thông thường. Đĩa quang số tương tự với đĩa video hay đĩa âm thanh compac trừ việc nó được dùng để lưu dữ liệu nhị phân chứ không phải là hình ảnh hay âm thanh. Dung tích nhớ tổng cộng của các hệ thống đĩa quang cỡ gigabyte và chi phí/bit hiện tại chỉ bằng 10% đĩa cứng. Những người dùng đĩa hiện tại chỉ có thể đọc, hoặc chỉ ghi một lần và đọc, bởi vậy các hệ thống này không linh hoạt như các thiết bị đĩa từ có thể xoá được. Ngoài ra, các hệ thống ghi/đọc rất đắt so với các thiết bị ngoại vi của máy vi tính thông thường.

optical mark recognition ***quang nhận dạng dấu hiệu, nhận dạng dấu hiệu bằng quang học*** Trong tính toán, nói tới các kỹ thuật ghi các dấu hiệu trên các tài liệu. Các dấu hiệu thường là những đoạn thẳng ngắn hay các hình vuông đặc trên các tài liệu định dạng, chẳng hạn, các câu trả lời cho các câu hỏi có nhiều lựa chọn trên các trang kiểm tra (thi), tài liệu đơn đặt hàng của khách hàng. Tài liệu được định vị và được quét bằng một tia sáng và được truyền đi hoặc được phản chiếu, được tập hợp lại nhờ các tế bào quang điện. Ý nghĩa của dữ liệu phụ thuộc vào vị trí tọa độ của nó trên tài liệu và các tín hiệu từ các tế bào quang điện được đưa vào máy tính. *So sánh với* optical character recognition.

optical memory ***bộ nhớ quang*** *Xem* optical disk storage.

optional ***tùy chọn, tùy ý*** Trong các tiêu chuẩn, một đặc tính mà một tiêu chuẩn cụ thể không đòi hỏi và cũng không cần thiết đáp ứng một điều khoản không bắt buộc của tiêu chuẩn.

Orange Book ***Sách Da Cam*** Trong an toàn máy tính, một ấn phẩm của Bộ Quốc Phòng Hoa Kỳ về "Tiêu chuẩn đánh giá hệ thống máy tính tin cậy của Bộ Quốc Phòng" phát hành vào tháng 8/1983 và được duyệt lại vào (3)1985.

Tổng quan

Trong tài liệu có ba lý do chính để phát triển tiêu chuẩn:

- Cung cấp cho những người dùng một thước đo đánh giá mức tin cậy vào các hệ thống máy tính đối với các quá trình xử lý an toàn thông tin mật và thông tin nhạy cảm khác.
- Đưa ra hướng dẫn cho các nhà máy về việc xây dựng những tính năng an toàn nào vào các sản phẩm thương

mại mới, nhằm cung cấp những hệ thống rộng rãi, sẵn có, thỏa mãn những yêu cầu về tính tin cậy cho các ứng dụng nhạy cảm.

- Cung cấp cơ sở cho việc chỉ ra các yêu cầu an toàn theo các chỉ tiêu kỹ thuật nhận được.

Sách Da Cam được chia thành hai phần, phần đầu giải quyết tiêu chuẩn về chi tiết còn phần thứ hai nêu lý do và những đường lối chủ đạo của những tiêu chuẩn đó. Cuốn sách cũng có bốn phụ lục mô tả Các quá trình Đánh giá sản phẩm Thương mại, Tóm tắt về Phân loại Tiêu chuẩn, Tóm tắt về Các lớp Tiêu chuẩn Đánh giá và Danh bạ các yêu cầu. Cuối cùng là Phần từ điển ngắn và Danh sách các Tài liệu tham khảo.

Một hệ thống máy tính nhiều mức được thiết kế nhằm xử lý một khoảng dữ liệu mật và phục vụ cộng đồng người dùng có các mức truy nhập an toàn khác nhau. Một máy tính như vậy cũng có thể chứa phần mềm có mã ác ý, làm cho dữ liệu thuộc một mức phân loại bị rò rỉ vào một tệp có phân loại thấp hơn; hoặc làm giảm cấp an toàn của dữ liệu được phân loại mật ở mức cao một cách ác ý và làm nó trở nên có sẵn cho những người dùng có mức truy nhập an toàn thấp hơn truy nhập tới được.

Một hệ thống máy tính tin cậy được định nghĩa là một hệ thống dùng các biện pháp toàn vẹn đầy đủ cho phần cứng và phần mềm, cho phép dùng nó để xử lý đồng thời một dải rộng thông tin mật hay nhạy cảm.

Sách Da Cam đề cập tới việc đánh giá các hệ thống máy tính tin cậy theo định nghĩa ở trên và nó dùng thuật ngữ cơ sở tính toán tin cậy để chỉ cơ chế tham chiếu hợp thức là cơ chế an toàn, nhân, lọc ngoại vi an toàn hay toàn bộ hệ thống máy tính được tin cậy. Cơ sở tính toán tin cậy (TCB) được định nghĩa là toàn bộ cơ chế trong phạm vi máy tính bao gồm phần cứng, phần mềm, phần sụn, sự kết hợp của chúng sẽ buộc tuân thủ một chính sách an toàn. Nó tạo nên một môi trường bảo vệ cơ bản và cung cấp các dịch vụ bổ sung cần thiết đối với một hệ thống máy tính tin cậy cho người dùng. Khả năng của cơ sở tính toán tin cậy buộc tuân thủ đúng chính sách an toàn phụ thuộc vào cơ chế trong phạm vi TCB và việc người quản trị hệ thống có đưa đúng các tham số liên quan tới chính sách an toàn hay không (ví dụ mức truy nhập của người dùng).

Tiêu chuẩn đánh giá đòi hỏi công bố chính sách an toàn cần được hệ thống máy tính tin cậy tuân thủ. Ngoài ra, những lập luận thuyết phục được trình bày để giải thích tại sao TCB thỏa mãn hai yêu cầu thiết kế đầu tiên về giám sát tham chiếu, tức là chống trộm cắp và bảo đảm để bộ giám sát được gọi tới trong mọi cuộc truy nhập.

Tiêu chuẩn giải quyết các chính sách kiểm soát truy nhập bắt buộc và tùy ý, còn việc diễn đạt tiêu chuẩn về kiểm soát truy nhập bắt buộc liên quan tới mô hình Bell-La Padula.

Tiêu chuẩn đưa ra các yêu cầu về một hệ thống máy tính an toàn, tức là các hệ thống an toàn sẽ kiểm soát hết các đặc tính an toàn đặc thù của việc truy nhập tới thông tin sao cho, chỉ những

cá nhân hợp pháp hay các quá trình hoạt động thay mặt họ mới được truy nhập đọc, ghi, tạo hay xóa thông tin.

Các yêu cầu về chức năng

Có sáu yêu cầu chức năng và chúng được nhóm lại theo các tiêu đề: Chính sách, Phân định trách nhiệm và Bảo đảm. Các yêu cầu dưới hai tiêu đề đầu tiên đề cập tới những thứ cần thiết để kiểm soát và giám sát truy nhập tới thông tin. Những yêu cầu dưới tiêu đề Bảo đảm sẽ giải quyết cách thức thông tin có thể nhận được sự bảo đảm tin được để hệ thống tin cậy thực hiện được mục tiêu an toàn.

Chính sách:

- Chính sách an toàn để hệ thống tuân thủ phải tường minh và được xác định rõ ràng.
- Các nhãn an toàn phải phù hợp với các đối tượng.

Phân định trách nhiệm:

- Các chủ thể cá biệt phải được định danh.
- Thông tin kiểm toán phải được giữ gìn một cách chọn lọc và được bảo vệ để những hoạt động tác động tới tính an toàn có thể truy nhập được tới bên có trách nhiệm.

Sự bảo đảm:

- Hệ thống máy tính phải chứa các cơ chế cứng/mềm có thể được đánh giá độc lập, đủ bảo đảm để hệ thống tuân thủ theo bốn yêu cầu nêu trên.
- Các cơ chế tin cậy buộc các yêu cầu cơ bản phải được bảo vệ liên tục chống sự giả mạo và/hoặc thay đổi trái phép.

Sự phân nhóm

Tiêu chuẩn phân chia các hệ thống máy tính tin cậy thành bốn nhóm: *A*, *B*, *C* và *D*. Nhóm cao nhất *A* dành riêng cho các hệ thống có tính an toàn toàn diện và bảo đảm nhất. Mỗi nhóm là kết quả của một quá trình cải tiến lớn độ tin cậy tổng thể được đặt vào hệ thống để bảo vệ thông tin nhạy cảm.

Hai nhóm *C* và *B* được chia tiếp thành các lớp *C*1, *C*2, *B*1, *B*2 và *B*3. Lớp *C*2 biểu diễn mức an toàn cao hơn lớp *C*1.

Bốn nhóm có thể tóm tắt lại như sau:

- Nhóm *D*: bảo vệ tối thiểu
- Nhóm *C*: Kiểm soát truy nhập tùy ý
- Nhóm *B*: Kiểm soát truy nhập bắt buộc
- Nhóm *A*: Bảo vệ có xác minh.

Trong phạm vi mỗi nhóm và lớp, tiêu chuẩn được liệt kê dưới các tiêu đề: chính sách, phân định trách nhiệm, bảo đảm và tài liệu.

Nhóm *D* được đặc trưng hóa bởi sự bảo vệ tối thiểu. Nó dành cho các hệ thống được đánh giá không đáp ứng tiêu chuẩn của các lớp cao hơn.

Nhóm *C*, tiêu chuẩn lớp *C*1 liên quan tới hệ thống kiểm soát truy nhập tùy ý cho những người dùng cộng tác. Khi người dùng hợp pháp chỉ ra các chế độ truy nhập được phép tới các đối tượng, những chủ thể có thể được xác định là những người sử dụng riêng lẻ, các thành viên của các nhóm đặc biệt hay những người dùng nói chung. Những người dùng của hệ thống phải có khả năng chứng minh danh tính của mình, ví dụ thông qua mật khẩu, còn thông tin định danh phải được bảo vệ chống sự truy nhập trái phép. Cơ chế buộc kiểm soát truy nhập phải được xác định

rõ và được bảo vệ chống giả mạo hay cản trở từ bên ngoài và nó phải kiểm tra định kỳ để xem còn làm việc đúng không.

Hệ thống được kiểm tra để đảm bảo rằng, nó thực hiện theo tài liệu và không có cách nào để hệ thống an toàn có thể bỏ qua nó.

Ngoài những thứ khác, tài liệu yêu cầu một bản mô tả các cơ chế bảo vệ, cách thức dùng và sự tương tác giữa chúng. Nó cũng đòi hỏi công bố về triết lý bảo vệ của nhà máy, cách chuyển triết lý này thành TCB; chỉ dẫn về hoạt động của hệ thống an toàn và các sơ đồ thử nghiệm...

Lớp *C*2 là lớp đánh giá cao nhất đối với các hệ thống không buộc kiểm soát truy nhập. Nó yêu cầu hệ thống có thể định danh, kiểm soát và kiểm toán những cuộc truy nhập của những người sử dụng cá biệt.

Ví dụ, yêu cầu dùng lại đối tượng chỉ ra rằng, một cung từ (secto) trên đĩa phải tẩy sạch những dữ liệu lưu trước đó trước khi trả lại nó vào tài nguyên chung để dùng lại.

Các yêu cầu về kiểm toán nghiêm ngặt hơn đối với những đối tượng thuộc lớp *C*1 và dữ liệu kiểm toán phải được bảo vệ chống làm lộ trái phép. Các thủ tục thử nghiệm kiểm tra phải tìm ra các kẽ hở đã cho phép truy nhập trái phép đến dữ liệu hay thông tin kiểm toán.

Ngoài tất cả các phương tiện kiểm soát truy nhập tùy ý của lớp *C*2, nhóm *B*, lớp *B*1 còn đưa ra các yêu cầu kiểm soát truy nhập bắt buộc. Như vậy, nó cho thấy một yêu cầu bổ sung chính vào các hệ thống nhóm *C*. Kiểm soát truy nhập bắt buộc đòi hỏi tất cả các tệp lưu trữ... được phân loại an toàn trước. Nếu thông tin bất kỳ được nhận vào hệ thống thì nó phải được người sử dụng hợp pháp gắn nhãn đúng và nó phải có khả năng ghi lại (kiểm toán) được hành động đó. Tương tự, khi dữ liệu ra khỏi hệ thống, nó cũng phải được gắn nhãn đúng.

Kiểm soát truy nhập bắt buộc yêu cầu phân loại an toàn được dựa trên cả mức an toàn lẫn tập bảng phân loại (category). Các yêu cầu của mô hình Bell-La Padula về điều kiện an toàn đơn giản đối với truy nhập đọc và thuộc tính * đối với truy nhập ghi đều được đặt ra. Nhà phát triển phải cung cấp mô hình an toàn trên mô hình mà TCB đã dựa vào đó và phải chứng tỏ đã thực hiện giám sát tham chiếu.

TCB được đòi hỏi để duy trì dữ liệu định danh và xác thực mỗi người dùng riêng biệt và phân loại an toàn của họ. Cần phải thực hiện thử nghiệm mở rộng đối với các kẽ hở an toàn và nếu tìm thấy những kẽ hở như vậy, phải loại bỏ hiệu quả hoặc vô hiệu hóa chúng và hệ thống được kiểm chứng lại. Cần phải có một lập luận thuyết phục để chứng tỏ rằng TCB tuân thủ mô hình an toàn.

Các hệ thống lớp *B*2 có thể được chia loại mục như sự trình bày sự bảo vệ có cấu trúc. TCB được dựa trên chính sách an toàn hình thức đã được xác định rõ và lập tài liệu. Chính sách này đòi hỏi rằng, kiểm soát truy nhập tùy ý và bắt buộc được mở rộng tới tất cả các chủ thể và các đối tượng trong các hệ thống ADP. Hệ thống phải cung cấp

một tuyến tin cậy giữa người dùng và TCB để đăng nhập mạng và để xác thực. Điều này hàm ý rằng, không có phần mềm không đáng tin nào có thể giả mạo TCB trước người dùng, chẳng hạn đối với mục tiêu thu thập các mật khẩu. Các kênh ngầm được xác định, nếu không loại trừ được kênh ngầm thì về cơ bản, sự rò rỉ thông tin tiềm ẩn bất kỳ không thể kiểm toán được sẽ được thể hiện ở mức thấp chấp nhận được. Những yêu cầu đặc biệt về thiết kế TCB phải được cấu trúc thành các yếu tố bảo vệ quan trọng và không quan trọng. Các giao diện TCB với người sử dụng phải được xác định tốt và TCB được modun hóa để nó có thể chịu sự kiểm định kỹ lưỡng hơn và nhìn nhận khắt khe hơn. Việc thực hiện phải thể hiện phù hợp với phép Đặc tả Mức cao. Hệ thống phải tương đối kháng được sự thâm lậu và có sự kiểm soát quản lý cấu hình chặt chẽ.

Trong các hệ thống *B3*, nhà phát triển phải chứng tỏ chúng thích hợp với khái niệm giám sát tham chiếu và do vậy, đảm bảo chống được trộm cắp và đủ nhỏ để có thể phân tích mở rộng và kiểm định; như vậy, TCB cần được cấu trúc để loại trừ mã không cốt yếu đối với việc bảo vệ. Hệ thống được đòi hỏi phải chống được sự thâm lậu; phải mở rộng các yêu cầu về kiểm toán để nếu một số tình huống về an toàn vượt quá giá trị ngưỡng nào đó, cho thấy sự vi phạm về chính sách an toàn sắp xảy ra thì người quản trị sẽ biết được.

Điểm quan trọng nhất đối với các hệ thống *A1* là chúng không có chức năng an toàn cao hơn các hệ thống lớp *B3*. Tuy nhiên, chúng lại cho mức bảo đảm để đáp ứng cao hơn chính sách an toàn của mình.

Sách Da Cam là cột mốc lịch sử quan trọng trong thế giới an toàn máy tính, lần đầu tiên, nó cung cấp một thước đo về an toàn cho hệ thống máy tính. Sự phát triển này được tiếp nối bởi Tiêu chuẩn Đánh giá Công nghệ An toàn Thông tin và FC-FIPS. *So sánh với* FC-FIPS, information technology security evaluation criteria. *Xem* A1, Bell-La Padula model, B1, B2, B3, covert channel, C1, C2, D, descriptive top-level specification, discretionary access control, formal security policy model, front-end security filter, malicious code, mandatory access control, multilevel device, object, object reuse, reference monitor, simple security property, star security property, security kernel, subject, tamperproof, trusted computer system, trusted computing base, trusted path. *Đồng nghĩa với* trusted computer security evaluation criteria.

ORCON ***được kiểm soát bởi người khởi đầu*** Trong an toàn dữ liệu, viết tắt của ORiginator CONtrolled, một chỉ dẫn mà tài liệu mang dấu hiệu do người khởi đầu kiểm soát. Sự tái tạo lại hay sự phân phối lại đòi hỏi sự cho phép của người khởi đầu.

order ***bậc*** Trong toán học, một tính chất của các số nguyên trong số học modulo. Nếu số nguyên m là nguyên tố cùng nhau với số n thì trong số học modulo, bậc của m là số nguyên thấp nhất sao cho $m^p \pmod{n} \equiv 1$. Giá trị cực đại của p là n -1 nếu p nhỏ hơn n - 1 thì nó phải là số chia của n - 1.

Xem coprime, Fermat's theorem, modulo arithmetic.

order control *(sự) kiểm soát thứ tự* Trong an toàn cơ sở dữ liệu, một dạng kiểm soát giới hạn dạng bảng nhằm hạn chế mức của các bảng trong mô hình giàn. Nếu ngưỡng được lập là *d* thì câu truy vấn chứa nhiều hơn *d* thuộc tính sẽ không được phép. *Xem* lattice model, table restriction.

ordinal *số thứ tự* Trong toán học, một số nguyên không dấu. Khi được lưu ở dạng 8 bit, các số thứ tự có thể mang những giá trị trong khoảng từ 0 đến 255, còn nếu được lưu ở dạng 16 bit thì chúng mang các giá trị từ 0 - 65.535. *So sánh với* integer. *Xem* bit.

orientation *(sự) định hướng* Trong an toàn máy tính, những cuộc trình bày và thảo luận không hình thức và hình thức cùng với trách nhiệm của người có thẩm quyền đối với hệ thống ADP nhằm bổ sung thông tin về kiểm định và yêu cầu đánh giá an toàn ban đầu, cung cấp cho những người đánh giá hệ thống một giới thiệu về môi trường hoạt động, các kỹ thuật được dùng nhằm đảm bảo tính an toàn cho hệ thống, đặc tính và vị trí tài liệu mô tả việc thực hiện các biện pháp an toàn hệ thống (ví dụ các biến đổi O/S...) và các kỹ thuật có sẵn để chứng minh tính hiệu quả của các biện pháp đó trong việc đáp ứng các yêu cầu của Chỉ dẫn 5200.28 của DOD. *Xem* ST&E.

original equipment manufacturer *nhà sản xuất thiết bị gốc* Trong tính toán, nhà sản xuất mua thiết bị, tăng giá trị cho nó chẳng hạn bằng cách nâng cao các khả năng của nó hoặc làm nó phù hợp với một ứng dụng đặc biệt và lại bán nó đi.

originator *người khởi đầu, người phát, đơn vị khởi đầu* (1) Trong liên lạc dữ liệu, cá nhân, viện nghiên cứu hay thực thể khác có trách nhiệm hoặc được ủy quyền để khởi đầu một thông báo. *So sánh với* recipient. *Xem* message. (2) Trong hoạt động ngân hàng, người bắt đầu các lệnh chuyển khoản. *Đồng nghĩa với* initiator. (3) Trong hoạt động ngân hàng, nhóm có trách nhiệm khởi đầu một thông báo dịch vụ mật mã. *So sánh với* recipient. *Xem* cryptographic service message.

originator's bank *ngân hàng của người khởi đầu* Trong hoạt động ngân hàng, hoạt động ngân hàng đối với người khởi đầu giao dịch chuyển khoản. *Xem* originator.

Oropax *virut Oropax* Trong an toàn máy tính, một loại virut làm chấm dứt chương trình và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COM, phá hoại các tệp chương trình và OVL, tác động trong thời gian chạy. *Xem* virus names.

OSI *Xem* open systems interconnection.

OSI security *an toàn kết nối các hệ thống mở* Trong an toàn liên lạc, an toàn kết nối các hệ thống mở cung cấp các công cụ cho hoạt động liên mạng an toàn của các hệ thống mở.

Tổng quan

Các chuẩn an toàn trong OSI đang nổi lên nhanh chóng (xem hình). Kiến trúc an toàn được mô tả trong ISO 7498-2 - Các hệ thống Xử lý Thông tin - Các Hệ

Mô hình tham chiếu

Kiến trúc an toàn 7498-2

Các sườn

Tổng quan	10181-1
Xác thực	10181-2
Kiểm soát truy nhập	10181-3
Không chối bỏ	10181-4
Tính bí mật	10181-5
Toàn vẹn	10181-6
Kiểm toán	10181-7
Quản lý khóa	

Các mô hình tầng/các hướng dẫn

Mô hình tầng cao hơn 107-45
Mô hình tầng thấp hơn/hướng dẫn

Các giao thức và các thủ tục

Các tính năng an toàn thư mục
Các tính năng quản lý thông báo an toàn
Xác thực ACSE
Trao đổi ASE an toàn
Giao thức an toàn tầng vận tải
Giao thức an toàn tầng mạng
Các giao thức an toàn tầng liên kết dữ liệu
Giao thức an toàn tầng vật lý
Vv...

OSI security: *an toàn OSI.*

thống kết nối mở - Mô hình tham chiếu cơ bản, phần II: phần Kiến trúc an toàn, CCITT đã công bố Kiến trúc an toàn trong X.800 vào năm 1992. Kiến trúc này được hỗ trợ bởi một số cơ cấu tổ chức, ví dụ ISO 10181, hiện đã phát triển. Một mô hình an toàn tầng cao hơn sẽ đưa ra chi tiết hơn dựa trên sự cung ứng các dịch vụ an toàn theo các giao thức ở các tầng 6 và 7 và một mô hình tầng thấp hơn được đề xuất tương tự cho các tầng từ 1 - 5. Một số trong các dịch vụ do các giao thức tầng ứng dụng cung cấp, bao gồm:

- thư mục;
- các hệ thống quản lý thông báo;
- các modun CASE.

Kiến trúc an toàn ISO mở rộng lĩnh vực ứng dụng của chuẩn ISO 7498 tới các cuộc liên lạc an toàn giữa các hệ thống mở. Chuẩn đề cập tới những khía cạnh có thể nhìn thấy của tuyến liên lạc. Tuyến liên lạc này cho phép các hệ thống cuối chuyển thông tin an toàn giữa chúng song không có các biện pháp an toàn cần thiết tại các hệ thống cuối, các cài đặt và các tổ chức, trừ khi chúng có các hàm ý về sự lựa chọn và về vị trí của các dịch vụ an toàn trong ISO.

Các cơ chế và các dịch vụ

Chuẩn phân biệt các dịch vụ an toàn với các cơ chế cần thiết để thực hiện các dịch vụ đó. Các dịch vụ an toàn đã xét được liệt kê dưới đây.

Xác thực:

- xác thực đối tượng ngang hàng;
- xác thực về xuất xứ dữ liệu.

Kiểm soát truy nhập

Giữ bí mật dữ liệu:

- giữ bí mật nối;
- giữ bí mật không nối;
- giữ bí mật trường lựa chọn;
- giữ kín lưu lượng.

Tính toàn vẹn dữ liệu:

- toàn vẹn trong kết nối có khôi phục được;

O

- toàn vẹn kết nối không khôi phục được;
- toàn vẹn kết nối trường lựa chọn;
- toàn vẹn khi không kết nối;
- toàn vẹn không kết nối trường lựa chọn.

Không chối bỏ:

- không chối bỏ có bằng chứng về xuất xứ;
- không chối bỏ có bằng chứng về phân phối.

Xác thực thực thể ngang hàng là dịch vụ do tầng N cung cấp cho tầng $N + 1$ để chứng thực rằng, thực thể ngang hàng là thực thể tầng $N + 1$ được yêu cầu. Trong trường hợp kết nối, vào lúc bắt đầu cuộc nối, xác thực thực thể ngang hàng được kết hợp với các dịch vụ toàn vẹn dữ liệu (trong thời gian nối) có thể sẽ cùng cung cấp sự bảo đảm về nguồn của tất cả các khối dữ liệu đã chuyển đi, và tính toàn vẹn của các khối dữ liệu riêng lẻ. Xác thực thực thể ngang hàng cũng có thể (ví dụ) dùng các số hiệu dãy chống lại các khối dữ liệu đúp.

Trong trường hợp dịch vụ toàn vẹn khi không kết nối, dịch vụ tầng N sẽ cung cấp tin tức cho tầng $N + 1$ về sự thay đổi bất kỳ theo Khối Dữ liệu Phục vụ không nối đơn lẻ (SDU); ngoài ra, nó có thể cho phép một dạng phát hiện hạn chế khi quay lại.

Các dịch vụ giữ bí mật và toàn vẹn trường lựa chọn cung cấp cho các dịch vụ an toàn hạn chế đối với những mục dữ liệu chọn trước trong phạm vi thông báo. Dịch vụ không chối bỏ có bằng chứng về xuất xứ sẽ ngăn chặn người gửi khỏi từ chối thông báo; tương tự, dịch vụ không từ chối có bằng chứng về phân phối sẽ ngăn chặn được người nhận khỏi từ chối rằng mình đã không nhận được thông báo.

Các cơ chế an toàn cung cấp các dịch vụ an toàn nêu trên đều được phân loại theo đặc trưng và theo sự tỏa khắp. Những cơ chế theo đặc trưng được kết hợp chặt chẽ vào tầng N thích hợp để cung cấp dịch vụ an toàn, trong khi các cơ chế theo tỏa khắp lại không chỉ ra dịch vụ cụ thể nào hay tầng cụ thể nào. Các cơ chế an toàn được liệt kê dưới đây:

Các cơ chế an toàn theo đặc trưng:

- mã hóa (mã mật);
- các cơ chế chữ ký số;
- các cơ chế kiểm soát truy nhập;
- các cơ chế toàn vẹn dữ liệu;
- cơ chế trao đổi xác thực;
- cơ chế san bằng lưu lượng;
- cơ chế kiểm soát định tuyến;
- cơ chế về công chứng viên.

Các cơ chế an toàn tỏa khắp:

- chức năng tin cậy;
- nhãn an toàn;
- phát hiện tình huống (sự kiện);
- vệt kiểm toán an toàn;
- khôi phục tính an toàn.

Các cơ chế kiểm soát truy nhập có thể được áp dụng hoặc tại cuối tuyến liên lạc, hoặc tại điểm trung gian nào đó. Nếu sự chuyển dữ liệu không nối được thực hiện thì cần phải biết các cơ chế kiểm soát truy nhập mức ngang hàng vào lúc bắt đầu và phải ghi vào Cơ sở Thông tin Quản lý An toàn.

Các yêu cầu về tính toàn vẹn dữ liệu sẽ khác nếu cơ chế được áp dụng vào

một lớp các khối dữ liệu, hoặc các trường trong các khối dữ liệu, mặc dù kiểu dịch vụ đầu tiên không thể cung cấp được mà không có kiểu thứ hai. Việc bảo vệ một dãy các khối dữ liệu, chẳng hạn chống sự mất thứ tự, sự nhân bản, mất mát, quay lại, chèn thêm hay biến đổi sẽ đòi hỏi dạng nào đó như lấy số hiệu dãy, dán nhãn thời gian, liên kết mật mã... Trong trường hợp dịch vụ không nối, có thể dùng nhãn thời gian để bảo vệ hạn chế chống sự quay lại.

Các cơ chế trao đổi xác thực có thể được dựa trên thông tin xác thực như mật khẩu, các kỹ thuật mật mã hay các đặc trưng/thẻ bài do thực thể có.

Các cơ chế kiểm soát định tuyến có thể chọn linh động các tuyến hay sự sắp đặt trước để chỉ có thể dùng những mạng con, các kết nối hay các chuyển tiếp an toàn về mặt vật lý. Dữ liệu chứa các nhãn nào đó có thể bị cấm, theo chính sách an toàn đi qua các mạng con, các kết nối hay chuyển tiếp nào đó. Khi một nối được thiết lập, hay một khối dữ liệu không nối được truyền đi, người gửi cũng có thể chỉ ra những mạng con, những kết nối hay chuyển tiếp nhất định cần tránh.

Các cơ chế an toàn tỏa khắp có thể được xem như những khía cạnh của quản lý an toàn. Các nhãn an toàn có thể là dữ liệu thêm vào kèm theo các khối dữ liệu trong chuyển tiếp, trong trường hợp đó, chúng phải có khả năng nhận diện rõ ràng để có thể kiểm tra được chúng ở tầng thích hợp; chúng cũng phải được quy định giới hạn an toàn đối với khối dữ liệu của mình. Các nhãn cũng có thể ẩn chứa trong việc dùng một khóa mã chỉ ra hoặc trong nội dung của dữ liệu như nguồn hoặc tuyến của nó.

Việc ghi lại kết quả của các sự cố liên quan tới an toàn như các vi phạm an toàn đặc thù, các sự cố được chọn chỉ ra hay sự tràn máy tính có thể gây bởi một trong các hành động sau:

- báo cáo cục bộ về một sự cố;
- ghi lại từ xa một sự cố;
- bản ghi một sự kiện;
- hoạt động khôi phục.

Sự khôi phục lại an toàn đáp lại các yêu cầu từ phía các cơ chế an toàn, ví dụ các chức năng quản lý và điều khiển sự kiện và tiến hành các hoạt động khôi phục thích hợp, các hoạt động này có thể là:

- ngay lập tức;
- tạm thời;
- trong thời gian dài.

Hoạt động khôi phục tức thì có thể gây bỏ dở các thao tác, ví dụ ngắt nối; các hoạt động tạm thời có thể tạo ra tính không hợp thức tạm thời của thực thể, còn các hoạt động khôi phục thời gian dài có thể đặt một thực thể vào danh sách đen hoặc thay đổi một khóa mã.

Một minh họa mối quan hệ giữa các dịch vụ an toàn và các cơ chế an toàn được chỉ ra như ở dưới

Dịch vụ	*Cơ chế*
Xác thực thực thể ngang hàng	D, DS, AE
Xác thực nguồn gốc dữ liệu	E, DS
Dịch vụ kiểm soát truy nhập	AC
Giữ bí mật nối	E, RC
Giữ bí mật không nối	E, RC

Giữ bí mật trường lựa chọn	E
Giữ bí mật lưu lượng	E, TP, RC
Toàn vẹn nối có khôi phục	E, DI
Toàn vẹn nối không khôi phục	E, DI
Toàn vẹn nối trường lựa chọn	E, DI
Toàn vẹn không nối	E, DS, DI
Toàn vẹn không nối trường lựa chọn	E, DS, DI
Không chối bỏ, xuất xứ	DS, DI, N
Không chối bỏ, phân phối	DS, DI, N

Trong đó E: mã hoá, DS: chữ ký số, AC: kiểm soát truy nhập, DI: toàn vẹn dữ liệu , AE: trao đổi xác thực, TP: san bằng lưu lượng, RC: kiểm soát định tuyến, N: công chứng.

Vị trí các dịch vụ trên các tầng

Việc quyết định vị trí các dịch vụ an toàn cho các tầng và sắp theo các cơ chế an toàn được dựa trên các nguyên tắc sau:

- số các cách lựa chọn để nhận được dịch vụ là tối thiểu;
- chấp nhận việc xây dựng các hệ thống an toàn bằng cách cung cấp các dịch vụ an toàn ở một hay nhiều tầng;
- chức năng bổ sung tính an toàn không dẫn tới nhân đôi các chức năng OSI hiện hành;
- cần tránh sự vi phạm tính độc lập của các tầng;
- cần tối thiểu hóa số lượng chức năng tín nhiệm;
- ở nơi mà một thực thể phụ thuộc vào cơ chế an toàn do một thực thể ở tầng thấp hơn cung cấp thì cần xây dựng tầng ở giữa bất kỳ để không xảy ra vi phạm về an toàn;
- bất cứ nơi nào có thể, các chức năng an toàn bổ sung thêm cho một tầng cần được xác định sao cho việc thực hiện các mođun độc lập không bị cản trở;
- kiến trúc an toàn được giả thiết là áp dụng cho các hệ thống mở gồm các hệ thống cuối có tất cả 7 tầng và các hệ thống chuyển tiếp.

Các yêu cầu về dịch vụ an toàn có thể gửi từ tầng $N + 1$ tới tầng N hoặc có thể do chính tầng $N + 1$ cung cấp. Việc thiết lập và sự hoạt động của dịch vụ đối với nối hay ngắt nối liên lạc sẽ khác nhau. Việc gọi tới và sự hoạt động của một dịch vụ an toàn liên quan tới sự đối thoại với một cơ sở dữ liệu chứa các tham số an toàn thích hợp cho cả hai nhóm theo các quy tắc kết nối do các chính sách an toàn và thông tin liên quan tới quản lý an toàn đưa ra. Cơ sở dữ liệu khái niệm này được đặt tên là Cơ sở Quản lý Thông tin an toàn (SMIB).

Nếu các dịch vụ an toàn cho tầng $N + 1$ do tầng N cung cấp thì tầng N sẽ tiến hành dàn xếp với SMIB. Các dịch vụ an toàn được đưa ra có thể do yêu cầu của tầng $N + 1$ và những yêu cầu như thế có thể bị tầng N từ chối nếu chúng xung đột với các yêu cầu quản trị cho tầng $N + 1$ được lưu trong SMIB. Một cách lựa chọn, tầng N có thể bổ sung thêm sự bảo vệ cần thiết qua các dịch vụ an toàn bất kỳ bắt buộc trong SMIB cho tầng $N + 1$. Nếu tầng $N + 1$ không chỉ ra sự bảo vệ an toàn đích thì tầng N vẫn tiếp tục liên lạc bằng biện pháp bảo vệ an toàn ngầm định được chỉ ra trong SMIB cho tầng $N + 1$.

Khi tầng N đã xác định mục tiêu bảo vệ đòi hỏi, nó sẽ cố cung cấp hoặc trực tiếp từ tầng N, hoặc bằng cách chuyển tiếp yêu cầu tới tầng N - 1. Nếu không thể đạt được bảo vệ đích thì không có cuộc liên lạc nào được thực hiện.

Một tầng có thể cung cấp các dịch vụ an toàn của chính nó sẽ tương phản với tầng dựa vào các dịch vụ của tầng trực tiếp dưới nó. Trong trường hợp này, tầng liên lạc trực tiếp với SMIB. Các báo cáo về các cuộc tấn công chủ động sẽ được cung cấp bất kỳ lúc nào ghi lại được một sự thay đổi dữ liệu đối với dịch vụ toàn vẹn nối không khôi phục, tức là tầng phải quyết định dựa vào các hoạt động khôi phục của nó.

Không phải tất cả các dịch vụ an toàn có sẵn trên giao thức định hướng nối đều có sẵn trên các giao thức không nối. Ví dụ, sự bảo vệ chống quay lại, chèn và xóa phải được các tầng định hướng nối cao hơn cung cấp. Người khởi đầu của SDU không nối phải đảm bảo rằng, nó chứa tất cả thông tin để đích có thể chấp nhận được.

Việc sắp xếp các dịch vụ an toàn ở các tầng khác nhau được mô tả dưới đây.

Tầng vật lý:

- giữ bí mật cuộc nối;
- giữ bí mật lưu lượng.

Tầng liên kết dữ liệu:

- giữ bí mật cuộc nối;
- giữ bí mật không nối.

Tầng mạng:

- xác thực thực thể ngang hàng;
- xác thực nguồn gốc dữ liệu;
- dịch vụ kiểm soát truy nhập;
- giữ bí mật nối;
- giữ bí mật không nối;
- giữ bí mật lưu lượng;
- toàn vẹn nối không khôi phục;
- toàn vẹn không nối.

Tầng vận tải:

- xác thực thực thể ngang hàng;
- xác thực nguồn gốc dữ liệu;
- dịch vụ kiểm soát truy nhập;
- giữ bí mật nối;
- giữ bí mật không nối;
- giữ bí mật lưu lượng;
- toàn vẹn nối có khôi phục;
- toàn vẹn nối không khôi phục;
- toàn vẹn không nối.

Tầng phiên:

- không dùng dịch vụ an toàn nào.

Tầng biểu diễn:

các phương tiện sẽ được cung cấp:

- giữ bí mật nối;
- giữ bí mật không nối;
- giữ bí mật trường lựa chọn.

các phương tiện có thể cung cấp:

- giữ bí mật lưu lượng;
- xác thực thực thể ngang hàng;
- xác thực nguồn gốc dữ liệu;
- toàn vẹn nối có khôi phục;
- toàn vẹn nối không khôi phục;
- toàn vẹn nối trường lựa chọn;
- toàn vẹn không nối;
- toàn vẹn không nối trường lựa chọn;
- không chối bỏ có bằng chứng về nguồn gốc;
- không chối bỏ có bằng chứng về phân phối.

Tầng ứng dụng:

- xác thực thực thể ngang hàng;
- xác thực nguồn gốc dữ liệu;

- dịch vụ kiểm soát truy nhập;
- giữ bí mật nốt;
- giữ bí mật không nối;
- giữ bí mật trường lựa chọn;
- giữ bí mật lưu lượng;
- toàn vẹn nối có khôi phục;
- toàn vẹn nối không khôi phục;
- toàn vẹn nối trường lựa chọn;
- toàn vẹn không nối;
- toàn vẹn không nối trường kựa chọn;
- không chối bỏ có bằng chứng về nguồn gốc;
- không chối bỏ có bằng chứng về phân phối.

Quản lý an toàn

Quản lý an toàn theo tiêu chuẩn liên quan tới cả hai khía cạnh quản lý an toàn đối với OSI và tính an toàn của quản lý OSI. Quản lý các dịch vụ và các cơ chế an toàn OSI bao gồm sự phân phối các thông tin quản lý đối với các dịch vụ và các cơ chế này, cộng thêm sự thu thập thông tin liên quan tới hoạt động của các dịch vụ và cơ chế đó. Tuy nhiên, nó không đề cập tới việc chuyển thông tin thích hợp với an toàn vào các giao thức, ví dụ, các tham số trong các yêu cầu nối. Nơi chứa khái niệm về thông tin liên quan tới an toàn này là Cơ sở quản lý an toàn thông tin (SMIB). Sự trao đổi thông tin giữa các hệ thống và SMIB phải được bảo vệ an toàn.

Nhiều nhà quản trị hệ thống khác nhau sẽ cần trao đổi thông tin liên quan tới an toàn để thiết lập và mở rộng SMIB. Những cuộc liên lạc như vậy có thể diễn ra trong hoặc ngoài phạm vi các nhánh liên lạc của OSI.

Ba loại quản lý an toàn OSI là:

- quản lý an toàn hệ thống;
- quản lý dịch vụ an toàn;
- quản lý cơ chế an toàn.

Quản lý an toàn hệ thống liên quan tới sự quản lý các khía cạnh an toàn của toàn thể môi trường OSI gồm:

- quản lý chính sách an toàn tổng thể, kể cả cập nhật và duy trì tính nhất quán;
- tương tác với các chức năng quản lý OSI khác;
- tương tác với quản lý dịch vụ an toàn và quản lý cơ chế an toàn;
- quản lý mục xử lý biến cố;
- quản lý kiểm toán an toàn;
- quản lý việc khôi phục an toàn.

Quản lý dịch vụ an toàn đề cập tới quản lý các dịch vụ an toàn cụ thể. Điển hình: các hành động kèm theo việc quyết định và chỉ định bảo vệ đích an toàn cho dịch vụ, các quy tắc lựa chọn đối với các cơ chế an toàn chỉ ra, dàn xếp những cơ chế bất kỳ cần các thỏa thuận trước, gọi tới các cơ chế an toàn cụ thể và tương tác với các chức năng quản lý cơ chế và các dịch vụ an toàn khác.

Quản lý cơ chế an toàn điển hình có thể gồm các chủ đề như quản lý khóa, quản lý phép mã hóa, quản lý chữ ký số, quản lý kiểm soát truy nhập , quản lý tính toàn vẹn dữ liệu, quản lý xác thực, quản lý san bằng lưu lượng, quản lý kiểm soát quá trình định tuyến và quản lý công chứng.

Trong quản lý tính an toàn của OSI, các dịch vụ và cơ chế an toàn thích hợp sẽ được dùng nhằm bảo vệ thỏa đáng các giao thức và thông tin quản lý OSI.

Các khung an toàn

Các khung an toàn (xem hình) đưa ra sự an toàn OSI ở mức chi tiết hơn nữa. Chúng gồm có:

- Khái quát chung 1018-1;
- Xác thực 10181-2;
- Kiểm soát truy nhập 10181-3;
- Không chối bỏ 10181-4;
- Bí mật 10181-5;
- Toàn vẹn 10181-6;
- Kiểm toán 10181-7;
- Quản lý khóa.

Những khung công việc này sẽ mô tả các mô hình đa dụng, các cơ chế, các phần tử dữ liệu và dãy các thao tác có thể dùng cho các dịch vụ an toàn cụ thể.

Mô hình tầng cao hơn sẽ xác định các phát triển giao thức và cung cấp các dịch vụ an toàn ở mức chi tiết hơn nữa trong các tầng 6 và 7. Mô hình tầng thấp hơn cũng xác định tương tự cùng những vấn đề đối với các tầng từ 1-5.

Người dùng và các ứng dụng người dùng có thể đòi hỏi mức an toàn riêng của mình, hoặc dùng các dịch vụ an toàn do các giao thức của tầng ứng dụng cung cấp. Những dịch vụ như vậy gồm Thư mục, Quản lý thông báo và các modun Case.

Dịch vụ Thư mục được mô tả trong X.500 của CCITT và ISO 9594 cho phép xác thực mạnh và đơn giản đối với các truy nhập mức thư mục. Xác thực đơn giản được dựa trên mật khẩu trong khi xác thực mạnh lại dùng mật mã khóa công khai, các chữ ký số và chứng thực. Các phương pháp chữ ký số cũng được dùng để bảo vệ tính toàn vẹn dữ liệu được trao đổi với Thư mục. Dịch vụ Thư mục cũng giữ thông tin an toàn chẳng hạn như các chứng chỉ và bởi vậy có khả năng hỗ trợ các cơ chế an toàn của các ứng dụng khác.

Hệ thống quản mục thông báo được chuẩn hóa theo xeri chuẩn X.400 của CCITT và được xếp ngang hàng với chuẩn 10021 của ISO. Các dịch vụ do Hệ thống quản mục thông báo cung cấp bao gồm:

- xác thực xuất xứ của thông báo, đưa ra bằng chứng phân phối và xác thực thực thể ngang hàng;
- không chối bỏ được xuất xứ của thông báo phân phối hay đưa ra (submission);
- toàn vẹn nội dung và toàn vẹn trình tự thông báo;
- giữ bí mật thông báo và dòng thông báo;
- gán nhãn an toàn thông báo;
- các dịch vụ quản lý nhằm trao đổi các giấy ủy nhiệm và các nhãn cho phép đăng ký an toàn.

Các modun CASE (các thành phần dịch vụ ứng dụng chung) cung cấp các dịch vụ chung cho các ứng dụng như Thư mục và MHS. Các modun dưới phát triển cũng cho phép trao đổi thông tin giữa hai thực thể ứng dụng để hỗ trợ xác thực, kiểm soát truy nhập, giữ bí mật, chống chối bỏ và toàn vẹn... *Xem* application layer, authentication, certificate, connectionless service, data integrity, data link layer, encipherment, key, network layer, notarization, open systems interconnection, pervasive security mechanism, physical layer, presentation layer, relay, replay, SDU.

security audit trail, session layer, SMIB, time stamp, traffic padding, transport layer, trusted functionality, X.400, X.500.

OSN ***số hiệu dãy ra*** Viết tắt của Output Sequence Number. Trong hoạt động ngân hàng, một số hiệu dãy kế tiếp cho phép kiểm soát thông báo ra giữa ngân hàng phục vụ và ngân hàng nhận. *So sánh với* ISN.

other card data ***trường dữ liệu thẻ khác*** Trong hoạt động ngân hàng, một trường đặc biệt trên thẻ sọc từ của khách hàng được dùng trong hệ thống khóa giao dịch. *Xem* transaction key system.

OTP ***cơ quan OTP*** Trong liên lạc, viết tắt của Office of Telecommunications Policy (Văn phòng chính sách viễn thông), thuộc Vụ hành pháp của Tổng thống Mỹ. Một cơ quan phát triển và khuyến nghị chính sách thuộc lĩnh vực viễn thông của Mỹ.

OUSD&E ***văn phòng OUSD&E*** Viết tắt của Office of the Under Secretary of Defense for Research and Engineering (Văn phòng Thứ trưởng bảo vệ nghiên cứu và kỹ thuật).

outage ***giai đoạn ngừng (hoạt động)*** Trong lĩnh vực độ tin cậy, thời gian hệ thống không hoạt động do nguồn điện bị hỏng.

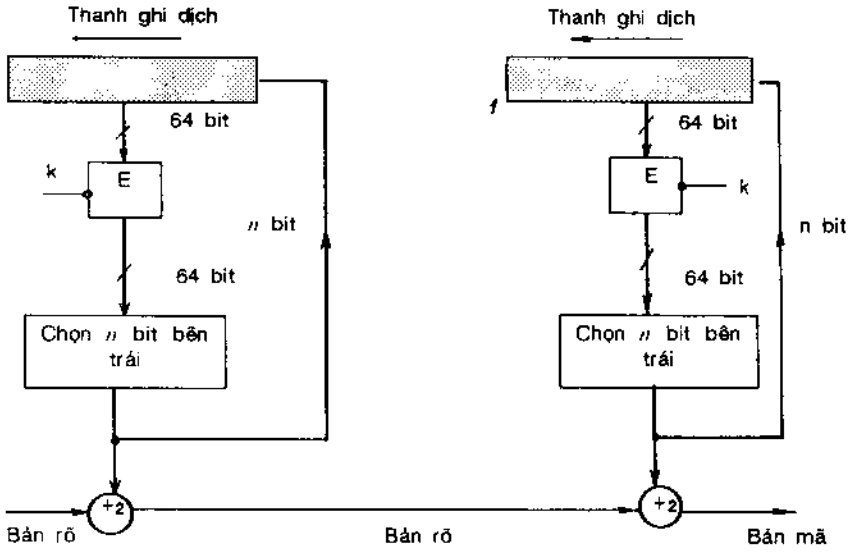
output ***tín hiệu ra, đầu ra*** Trong an toàn máy tính, thông tin do TCB xuất ra. *Xem* TCB.

output feedback ***hồi tiếp xuất, phản hồi đầu ra*** Trong mật mã, một chế độ hoạt động của mã DES. Trong chế độ phản hồi đầu ra, dòng bit mã được cộng "loại trừ- hoặc" với bản rõ, tạo ra bản mã ở phía máy phát. Một hệ thống tương tự tại phía máy thu cũng được cấp cùng khóa mã sẽ tạo ra cùng dòng bit mã, dòng bit mã này được cộng "loại trừ-hoặc" với bản mã và từ đó thu được bản rõ ban đầu.

Dòng bit mã có thể tạo ra các khối 1 bit, một byte... được cộng "loại trừ-hoặc" với các khối tương ứng trong bản rõ. Khối dòng bit mã cũng được đưa ngược trở về thanh ghi dịch tạo nên đầu vào cho bộ phận mã DES, tại đây, nó được mã hóa và tạo ra một khối đầu ra 64 bit, đoạn bên trái nhất của nó được chọn cho khối bit mã tiếp sau.

Các thanh ghi dịch phát được khởi động bằng cùng vectơ khởi đầu IV. IV đó được truyền đi ở dạng rõ từ máy phát tới máy thu như phần mở đầu của thông báo. Với mục đích này, nó không cần truyền đủ khối 64 bit; nó có thể được sắp xếp sao cho cả hai thanh ghi dịch đều có thiết lập ban đầu bằng 0 còn 8 bit được truyền để thiết lập IV. Tuy nhiên, những phần mở đầu ngắn bị xem là xấu nếu truyền các thông báo có định dạng ở mức cao.

Ưu điểm chính của mạch hồi tiếp đầu ra so với hồi tiếp bản mã là nó không bị lan rộng sai số. Một bit sai trong bản mã sẽ chỉ tạo ra một bit sai tương ứng trong bản rõ ở phía máy thu. Sự không lan truyền sai số này rất có lợi trong các ứng dụng như xáo trộn tiếng nói, nơi bản rõ có độ dư cao; có thể bỏ qua một bit sai trong khi một số khối bị cắt xén sẽ tạo ra một nhiễu kích thích tại đầu ra. Mặt khác, sự không lan truyền sai số lại cho phép kẻ tấn công đưa ra



output feedback: *hồi tiếp đầu ra.*

những thay đổi có kế hoạch và không bị phát hiện trong bản rõ nhận được. Sự mất mát hoặc bổ sung sai một khối trong dòng bản mã sẽ gây nên mất đồng bộ giữa các dòng dữ liệu phát và thu và bản rõ nhận được tại máy thu sau đó sẽ bị cắt xén. *So sánh với* cipher block chaining, cipher feedback, electronic codebook. *Xem* ciphertext, cryptographic bit stream, cryptographic key, DES, error extension, plaintext, shift register, stream EXLCUSIVE OR, IV, cipher.

output protection ***bảo vệ đầu ra*** Trong an toàn dữ liệu, nói tới các thủ tục đã được chấp nhận và thông qua đối với an toàn thông tin do các hệ thống tự động tạo ra.

outsourcing ***nguồn ngoài*** Trong tính toán, bài thực hành kiếm được từ các nguồn của các chuyên gia bên ngoài hơn là từ sự phát triển các hệ thống ứng dụng, chẳng hạn như trong chính phạm vi của tổ chức.

overhead bit ***bit nội dịch, bit bổ sung*** Trong các mã, một bit không truyền thông tin song được tính đến để điều khiển hay kiểm tra sai số. *Xem* parity checking.

overlap control ***kiểm soát chống lặp*** Trong an toàn cơ sở dữ liệu, một dạng hạn chế ô dùng vệt kiểm toán để hạn chế số các bản ghi giống nhau trên tập các câu hỏi. *So sánh với* audit expert, cell suppression, implied queries control, query set size control. *Xem* audit trail, cell restriction, query set.

overlay network ***mạng phủ, mạng xếp chồng*** Trong liên lạc, một mạng có các kết nối truyền và các trung tâm chuyển mạch được chồng lên trên mạng khác và được liên thông với nó tại những điểm cụ thể.

overt channel ***kênh công khai*** Trong an toàn liên lạc, một tuyến trong phạm vi một hệ thống được thiết kế để chuyển dữ liệu hợp pháp. *Xem* covert channel.

overwrite cycle ***chu trình ghi đè*** Trong an toàn máy tính, một phương pháp khử dữ liệu an toàn khỏi bộ nhớ từ hay điện tử. Một mẫu bit hoặc ký tự được ghi lên mỗi vị trí hay secto có thể lập địa chỉ được. Khi đó phần bù của mẫu hay ký tự được ghi vào mỗi vị trí hay cung từ có khả năng lập địa chỉ. *Xem* object reuse, overwrite procedure, residue.

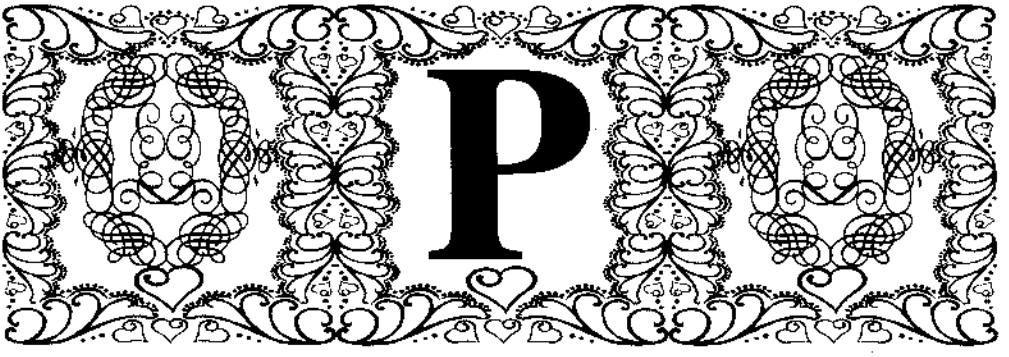
overwrite procedure ***thủ tục ghi đè*** Trong an toàn máy tính, một thủ tục chuyển hoặc hủy dữ liệu được ghi trên phương tiện lưu trữ từ ADP bằng cách ghi các mẫu dữ liệu không mật lên trên hoặc trên đỉnh của dữ liệu lưu trên phương tiện. *Xem* object reuse, overwrite cycle, overwriting.

overwriting ***(sự) ghi đè*** Trong an toàn máy tính, sự tẩy dữ liệu đã ghi bằng cách ghi dữ liệu khác lên cùng bề mặt. *Xem* overwrite procedure.

overwriting virus ***virut ghi đè*** Trong an toàn máy tính, một loại virut ghi đè lên phần đầu tiên của chương trình bị lây nhiễm làm hỏng nó sau khi virut thi hành. *So sánh với* nonoverwriting virus. *Xem* virus.

OWF *Xem* one-way function.

ownership ***quyền sở hữu*** Trong an toàn dữ liệu, quyền của những người sử dụng đối với các đặc quyền phân phối và thu hồi đối với những đối tượng mà họ sở hữu, chẳng hạn truy nhập tới các chương trình và các bộ dữ liệu. *Xem* access control, data set.



P1 ***giao thức P1; virut P1*** (1) Trong truyền dữ liệu, giao thức *P*1 là giao thức chuyển tiếp trong chuẩn xử lý thông báo X.400 của CCITT. (2) Trong an toàn máy tính, virut *P*1 là một loại virut mã hóa chính bản thân nó, kết thúc và thường trú, lây nhiễm các tệp COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu và liên kết tệp. *Xem* virus names.

P2 ***giao thức P2*** Trong truyền dữ liệu, giao thức trong chuẩn xử lý thông báo X.400 của CCITT. Nó định nghĩa phần đầu của thông báo, và các phần khác nhau của thông báo. *So sánh với* P1, P3. *Xem* X.400.

P3 ***giao thức P3*** Trong truyền thông dữ liệu, giao thức đệ trình của chuẩn điều khiển thông báo CCITT X.400. *So sánh với* P1, P2. *Xem* X.400.

PABX *Xem* private automatic branch exchange.

pacing ***thu điều khiển phát, điều khiển tốc độ, dẫn tốc độ*** Trong truyền thông dữ liệu, phương pháp mà nhờ nó một trạm nhận điều khiển tốc độ truyền để tránh mất mát dữ liệu.

packet ***gói tin, bó tin*** Trong truyền thông dữ liệu, thành phần độc lập của thông báo bao gồm địa chỉ, các tín hiệu điều khiển và dữ liệu và có thể được truyền như một thực thể trong mạng dữ liệu. *Xem* packet switching.

packet assembler/disassembler ***lắp/gỡ gói tin*** Trong truyền thông dữ liệu, đơn vị được cài đặt bởi nhân viên thao tác mạng để thực hiện giao tiếp giữa mạng chuyển mạch gói với thiết bị đầu cuối của người sử dụng. Đơn vị này thực hiện lắp ráp các thông báo dưới dạng dòng ký tự từ thiết bị đầu cuối thành các gói để truyền trên mạng và tách các gói đến từ mạng. *Xem* packet switching network.

packet interleaving ***chèn gói, chen***

gói Trong truyền thông dữ liệu, dạng ghép kênh trong mạng chuyển gói trong đó các gói từ các kênh phụ được chèn vào kênh chính. *Xem* multiplexing, packet, packet switching.

packet radio ***mạng vô tuyến gói*** Trong truyền thông dữ liệu, mạng với các liên kết vô tuyến nhờ đó một gói có thể được nhận bởi nhiều hơn một trạm. *Xem* packet switching.

packet sequencing ***lập trình tự gói, sắp thứ tự gói*** Trong truyền thông dữ liệu, một phương pháp đảm bảo các gói đến trạm nhận theo đúng thứ tự như chúng đã được gửi. *So sánh với* datagram service. *Xem* packet, packet switching.

packet switching ***chuyển mạch gói*** Trong truyền thông dữ liệu, một phương pháp truyền thông báo trong đó mỗi thông báo đầy đủ được lắp ráp thành một hoặc nhiều gói mà có thể chuyển qua mạng và tập hợp lại và sau đó được lắp ráp lại thành thông báo ban đầu tại trạm đích. Các gói riêng biệt không nhất thiết được gửi theo cùng một đường. Với phương pháp chuyển mạch gói, các kênh truyền thông chỉ bị chiếm trong khi truyền gói không giống như chuyển mạch thoại, kết nối được thiết lập và duy trì cho đến khi hoàn tất việc chuyển thông báo. *So sánh với* circuit switching, message switching. *Xem* computer network, datagram service, packet.

packet-switching exchange ***tổng đài chuyển mạch gói*** Trong truyền thông dữ liệu, hệ thống máy tính cung cấp một giao diện giữa những người sử dụng và mạng chuyển mạch gói nút tới nút. Các chức năng trao đổi bao gồm giao thức, lập trình tự gói và định tuyến. *Xem* packet, packet-switching network, protocol, routing.

packet-switching network ***mạng chuyển mạch gói*** Trong truyền thông dữ liệu, mạng các thiết bị truyền thông với nhau bằng chuyển các gói đã được đánh địa chỉ tới các đích riêng biệt. *Xem* packet switching.

packet switch node ***nút chuyển mạch gói*** Trong truyền thông dữ liệu, nút chuyển mạch trong mạng chuyển mạch gói. Các nút chuyển mạch gói là các máy tính mạnh hơn vốn có khuynh hướng thay thế các bộ xử lý thông báo giao diện, trong khi thực hiện cùng loại chức năng. *Xem* interface message processor, packet-switching network.

packet terminal ***thiết bị đầu cuối chuyển theo gói*** Trong truyền thông dữ liệu, một thiết bị đầu cuối trong mạng chuyển mạch gói có thể tạo gói và tương tác với một đầu cuối ký tự của mạng. *So sánh với* character terminal. *Xem* packet, packet switching.

packing density ***mật độ nén*** Trong tính toán, đó là số các bit có thể được lưu trên mỗi đơn vị thiết bị ghi chẳng hạn như băng từ. *Xem* magnetic tape.

PACX ***tổng đài máy tính tự động dành riêng, hệ PACX*** Trong truyền thông dữ liệu, viết tắt của Private Automatic Computer Exchange, là hệ thống chuyển mạch và tranh chấp cho phép sắp xếp các thiết bị đầu cuối với các tốc độ khác nhau, giao tiếp thông

qua một số cổng ra, liên lạc với một vài thiết bị khác chẳng hạn như máy tính. *Xem* contention, port.

PAD *Xem* packet assembler/disassembler.

padding ***đệm*** Trong mật mã, những ký tự thêm vào trong thông báo rõ để đảm bảo chiều dài của nó là một số nguyên các khối mã phù hợp với mã khối. *Xem* block cipher, pading indicator.

padding indicator ***bộ chỉ thị đệm ký tự*** Trong mật mã, một bộ chỉ thị được dùng trong chế độ liên kết các khối mã của thao tác DES. Nó được sử dụng để chỉ số các ký tự thêm vào trong khối 64 bit cuối cùng của bản rõ khi dòng thông báo không bao gồm một số nguyên các khối 64 bit. *Xem* cipher block chaining.

page ***trang nhớ*** Trong tính toán, một vùng không gian lưu giữ. *Xem* memory organization.

page frame ***khung trang*** Trong tính toán, một vùng nhớ có thể nhớ được một trang. *Xem* page.

page mode terminal ***thiết bị đầu cuối ở chế độ trang*** Trong truyền thông dữ liệu, một thiết bị đầu cuối cung cấp một thiết bị hiển thị trang mà tiêu biểu là loại 25 dòng 80 ký tự và cho phép con trỏ di chuyển trên màn hình để thay đổi màn hình hiển thị. *So sánh với* form mode terminal, scroll mode terminal.

palindromic key ***khóa đối ngẫu*** Trong mật mã, khóa của DES trong đó khóa con 1 = khóa con 16, khóa con 2 = khóa con 15 v.v.. Chỉ có những khóa yếu của DES mới có tính chất này. *So sánh với* cryptographic key, data encrytion standard, sub-key, weak key.

palmprint analysis ***phân tích in dấu tay*** Trong kiểm soát truy nhập, một kỹ thuật định danh; in dấu tay giống như những vân tay là duy nhất đối với mỗi cá thể. Những nếp gấp, đặc điểm chung của da, những hình xoáy có thể được phát hiện bởi camera; tín hiệu ra được số hóa từ camera được so sánh với hình ảnh tương ứng với số hiệu người sử dụng được lưu giữ trong một cơ sở dữ liệu kiểm soát truy nhập. Thời gian truy nhập nhanh có thể được cung cấp với tỷ lệ loại bỏ sai nhỏ hơn một phần trăm và đặc biệt tỷ lệ chấp nhận sai thấp. *So sánh với* fingerprint analysis, hand geometry analysis. *Xem* biometrics, user id.

PAM *Xem* pulse amplitude modulation.

PAN *So sánh với* PIN. *Xem* primary account number.

parallel communication ***liên lạc song song*** *Xem* parallel transmission.

parallel computer ***máy tính song song, truyền thông song song*** Trong tính toán, một máy tính có nhiều đơn vị logic hoặc số học cho phép nó thực hiện các phép toán song song hoặc xử lý song song. *So sánh với* serial computer. *Xem* parallel processing.

parallel messages ***thông báo song song*** Trong mật mã, các thông báo được mã hóa với cùng dòng bit mã hoa. *Xem* cryptographic bit stream.

parallel operation ***hoạt động song song*** Sự thực hiện những hành động đồng thời và thông thường là những

hành động cùng loại trên một tập những đầu vào có quan hệ với nhau. *Xem* parallel processing, parallel transmission.

parallel processing ***xử lý song song*** Trong tính toán, khái niệm này gắn liền với một hệ thống trong đó có hơn một tiến trình hoạt động tại một thời điểm cho trước. Thuật ngữ này thông thường được áp dụng cho các hệ thống có nhiều hơn một bộ xử lý nhưng tại bất kỳ thời điểm nào cũng chỉ có một bộ xử lý nào đó hoạt động. *So sánh với* serial computer.

parallel simulation ***mô phỏng song song*** Trong kiểm toán, một kỹ thuật trong đó người kiểm toán đưa ra một trình mô phỏng, để thực hiện xử lý đồng nhất một chương trình của một tổ chức để xem xét lại. *Xem* computer-audit packages.

parallel transmission ***truyền song song*** Trong truyền dữ liệu, sự truyền đồng thời các phần tử tạo nên cùng một mã, tức là mỗi bit của một từ được truyền đồng thời trên một đường riêng biệt. Phương pháp này có tốc độ truyền cao hơn truyền tuần tự nhưng yêu cầu 8 đường để truyền những byte riêng biệt và do vậy chủ yếu được sử dụng để truyền trên những khoảng cách ngắn, chẳng hạn trên những bus trong máy tính. *So sánh với* serial transmission. *Xem* bit rate.

parameter ***tham số*** (1) Một con số hoặc một tập con xác định một hệ thống hoặc một tiến trình. (2) Biến xác định của một hệ thống hoặc một tiến trình tạm thời có những tính chất của một hằng.

parent ***mức cha, phần tử cha*** Trong tính toán, một phần tử trong một hệ thống phân cấp ở ngay trên phần tử đang được bàn đến, chẳng hạn trong cấu trúc cây đó là nút trỏ đến nút đang bàn đến. *Xem* tree structure.

Paris ***virut Paris*** Trong an toàn máy tính, một loại virut lây nhiễm vào các tệp COMMAND.COM, COM, EXE và OVL, làm ảnh hưởng đến thao tác khi chạy, làm hỏng chương trình, các tệp OVL, các tệp dữ liệu và liên kết tệp. *Xem* virus names.

parity ***tính chẵn lẻ*** Trong các mã, khái niệm này liên quan tới điều kiện trong đó một số các phần tử trong nhóm là lẻ hoặc chẵn. *Xem* parity checking.

Parity ***virut Parity*** Trong an toàn máy tính, một loại virus lây nhiễm các tệp COMMAND.COM, COM, ảnh hưởng đến thao tác khi chạy, làm hỏng các tệp chương trình, OVL và dữ liệu. *Xem* virus names.

parity bit ***bit chẵn lẻ*** Trong các mã, bit được thêm vào nhóm bit khi cần thiết để đưa ra bit kiểm tra chẵn lẻ. *Xem* parity checking, parity.

parity checking ***kiểm tra tính chẵn lẻ*** Trong các mã, dạng kiểm tra độ dư thừa. Khi cờ chẵn hoặc lẻ được lựa chọn, số bit 1 trong nhóm được đếm và một bit chẵn lẻ được thiết lập là 0 hoặc 1 để tạo ra cờ chẵn lẻ với quy ước đã chọn, tức là một số lẻ hoặc chẵn các bit 1. Dựa vào việc nhận các bit được kiểm tra và lỗi được thông báo nếu như một cờ chẵn lẻ đã lựa chọn không tìm thấy.

Kiểm tra chẵn lẻ sẽ phát hiện ra sự mất mát hoặc thêm vào không mong muốn của một số lẻ các bit. *Xem* parity, parity bit, redundancy checking. *Đồng nghĩa với* odd even check.

passband ***dải thông*** Trong truyền thông, phạm vi tần số của dãy tín hiệu có thể được truyền đi trên một kênh cho trước. Ví dụ, dải thông qua trên các kênh tiếng nói có dải tần từ 300-3000 Hz. *Xem* Hz.

passive ***thụ động*** (1) Trong an toàn truyền thông, đó là một thuộc tính của một đối tượng hoặc đối tượng của mạng mà thiếu tính logic hoặc khả năng tính toán và không có khả năng thay đổi thông tin mà nó chứa đựng. *Xem* object. (2) Trong an toàn truyền thông, những hiểm họa đối với độ tin cậy của dữ liệu nếu xảy ra sẽ dẫn tới sự thay đổi bất hợp pháp về trạng thái của các hệ thống truyền thông công cộng (ví dụ, giám sát và/hoặc ghi dữ liệu).

passive attack ***tấn công thụ động*** Trong an toàn dữ liệu, sự tấn công trong đó dữ liệu bị chặn sẽ được ghi lại và phân tích sau đó. *So sánh với* active attack. *Xem* midnight attack, passive wiretapping.

passive electronic card ***thẻ điện tử thụ động*** *Xem* proximity card reader.

passive sensor ***bộ cảm biến thụ động*** Trong an toàn vật lý, một cảm biến không thể sinh ra hoặc truyền một tín hiệu nhưng nó có thể phát hiện mọi sự thay đổi đối với các mẫu phóng xạ, các mẫu phóng xạ này được tạo ra bởi một sự nhiễu loạn ở bức xạ xung quanh hoặc từ một nguồn phóng xạ.

passive threat ***hiểm họa bị động*** (1) Trong việc quản lý rủi ro, hiểm họa khám phá thông tin không được phép mà không làm thay đổi tình trạng của hệ thống. *So sánh với* active threat. *Xem* threat. (2) Trong an toàn máy tính, một vi phạm an toàn tiềm ẩn xảy ra mà không thay đổi tình trạng của hệ thống. Phần cứng, phần mềm, dữ liệu... sẽ không bị thay đổi. Một hiểm họa như vậy có thể xảy ra từ việc đọc các tệp không được phép hoặc sử dụng hệ thống máy tính cho một ứng dụng không được phép. *So sánh với* accidental threat, active threat, deliberate threat, logical threat, physical threat. *Xem* threat.

passive wiretapping ***nghe trộm thụ động*** Trong an toàn máy tính, việc giám sát và/hoặc ghi dữ liệu trong khi dữ liệu đang được truyền đi trên một liên kết truyền thông (FIPS). *So sánh với* active wiretapping. *Xem* passive attack.

passphrase ***câu mật khẩu, mật khẩu dài*** Trong điều khiển truy nhập, một chuỗi ký tự liên tiếp, dài hơn độ dài cho phép của một mật khẩu, nó được chuyển đổi bởi một hệ thống mật khẩu thành mật khẩu ảo có độ dài có thể chấp nhận. *Xem* password, virtual password.

password ***mật khẩu*** (1) Trong xác thực, một thông tin mật được xác thực là đúng, thông thường bao gồm một chuỗi các ký tự. (2) Trong điều khiển truy nhập, một chuỗi các ký tự bí mật được sử dụng để xác thực một danh tính. *Xem* authenticate. (3) Trong điều khiển truy nhập. một hình thức thông dụng để kiểm tra. Một mật khẩu là một

chuỗi dữ liệu chữ-số hoặc một cụm từ phải được nhập vào một hệ thống để được phép truy nhập tới một vùng vật lý hoặc một tài nguyên.

Thông thường một mật khẩu được kết hợp với một định danh của người sử dụng, người sử dụng nhập user id (số hiệu nhận diện người dùng) và sau đó mới đáp ứng yêu cầu đối với mật khẩu. Thông thường, user id có thể được truyền đi tường minh tới một máy chủ nhưng mật khẩu có thể được bảo vệ trong khi truyền.

Sử dụng và lạm dụng mật khẩu hiện nay là thông thường và việc quản lý thông qua giới hạn hợp lý để đảm bảo chắc chắn rằng chúng cung cấp mức độ an toàn thích hợp. Đặc biệt, mật khẩu phải phù hợp với mức độ an toàn được yêu cầu. Các yếu tố ảnh hưởng đến việc quản lý mật khẩu được liệt kê dưới đây.

- Người sử dụng phải được đào tạo và có động cơ để đảm bảo chắc chắn hiệu quả của việc truy nhập mật khẩu. Đặc biệt họ phải lường trước được hậu quả để bảo vệ mật khẩu của mình và phát hiện ra việc thiếu an toàn mật khẩu, ví dụ, bằng cách kiểm soát truy nhập.
- Mật khẩu phải dễ nhớ, nhờ vậy người sử dụng không phải ghi lại.
- Mật khẩu phải được thay đổi thường xuyên.
- Bản ghi mật khẩu hệ thống phải được bảo vệ, ví dụ, bằng cách mã hóa.
- Hệ thống phải chống lại mọi cố gắng để đoán ra mật khẩu bằng một loạt các lần thử liên tiếp.
- Mật khẩu không được hiển thị trên thiết bị đầu cuối trong suốt quá trình nhập mạng.

Có thể có một vài dạng thức thiết kế các mật khẩu tiện dụng mà không dựa vào các bản ghi được ghi lại. Nói chung độ dài của một mật khẩu phù hợp với mức độ an toàn yêu cầu; để tránh truy cập vào những thông tin tối mật, đòi hỏi độ dài mật khẩu hợp lý nhưng các hệ thống đã thiết kế để giảm ảnh hưởng trò chơi máy tính không nên bắt người sử dụng hợp pháp nhớ các con số dài tới 20 chữ số.

Một số hệ thống cho phép người sử dụng chọn lựa mật khẩu của mình; điều này làm cho người sử dụng có khả năng chọn một vài chuỗi ký tự hoặc số dễ nhớ nhưng nó cũng dẫn đến việc các mật khẩu quá ngắn, dễ đoán ra được từ những thông tin về tên vợ hoặc con gái người sử dụng. Các cụm từ dễ nhớ nhưng làm tăng đáng kể cả thời gian gõ chúng vào từ bàn phím lẫn khả năng gõ lỗi nhưng điều này lại làm cho việc tấn công khó khăn hơn.

Các mật khẩu ngữ âm có thể vừa ngắn và dễ nhớ, ví dụ, "joglin" dễ nhớ hơn "zxdswv". Bộ tạo mật khẩu ngữ âm có thể sinh ra các mật khẩu ngẫu nhiên. Việc quản lý các mật khẩu phải được thiết kế để đảm bảo rằng:

- Chúng bị vô hiệu hóa ngay sau khi chúng được biết là đã bị tổn thương, hoặc ngay sau khi một người làm công xin thôi việc, nghỉ hưu, bị chuyển công tác khác, đặc biệt là lòng trung thành bị thay đổi, ví dụ, người làm công bị sa thải.
- Mật khẩu phải được thay đổi định kỳ, những thay đổi như vậy sẽ giảm tối

đa sự tổn hại và cũng đảm bảo sự thông báo thường xuyên về các thay đổi trong những người sử dụng.

- Người sử dụng phải được khuyến khích thay đổi các mật khẩu nếu như họ tin chúng có thể bị tổn hại hoặc nếu như họ gặp khó khăn trong việc ghi nhớ. *Xem* access control, dynamic password, expired password, one-way function, one-time passwords, passphrase, personal password, time-dependent password, user id, valid password, virtual password. *Đồng nghĩa với* keyword.

password based encryption algorithm ***thuật toán mã dựa trên mật khẩu*** Trong mật mã, một thuật toán khóa bí mật trong đó khóa được lấy từ một người sử dụng được cung cấp mật khẩu. *Xem* secret key algorithm.

password dialogue ***đối thoại bằng mật khẩu*** *Đồng nghĩa với* handshaking procedure.

password system ***hệ mật khẩu*** (1) Trong kiểm soát truy nhập, một phần của hệ thống ADP, được sử dụng để xác thực danh tính của một người sử dụng. Việc đảm bảo sự chính xác của danh tính dựa vào khả năng của người sử dụng khi nhập vào một mật khẩu cá nhân mà không ai có thể biết. *Xem* password. (2) Trong kiểm soát truy nhập, một hệ thống mà sử dụng một mật khẩu hoặc câu mật khẩu để xác thực một định danh của người, hoặc cho phép một người truy nhập tới dữ liệu và nó gồm có một hay nhiều thao tác mật khẩu sau: sinh, phân bố, nhập, cất giữ, xác nhận, thay đổi, mã và, hoặc giải mã các mật khẩu. *Xem* passphrase, password.

patch ***đắp vá, sửa tạm*** *Xem* program patch.

path ***đường dẫn*** Trong tính toán, một giải pháp để định rõ một tệp trên một thư mục được cấu trúc cây. Việc chỉ ra đầy đủ một tệp bao gồm tên của toàn bộ các thư mục con trên đường dẫn từ gốc tới lá mà có chứa tệp. Ví dụ, \ADMIN\ACCOUNT\COMP-B\RESULTS. Tệp cần được định rõ trong phạm vi của đường dẫn từ thư mục con hiện thời. Ví dụ, nếu thư mục con hiện thời là ACCOUNT thì tệp được chỉ rõ như sau \COMP-B\RESULTS. *Xem* directory, tree structured directory.

path scrutiny ***kiểm soát theo tuyến*** Trong an toàn vật lý, việc dùng nhân viên an ninh để đi tuần khu vực làm việc, đặc biệt là thời gian ngoài giờ làm việc thông thường, để phát hiện việc xâm nhập và sử dụng trái phép các thiết bị đầu cuối, để kiểm tra mọi vi phạm an toàn, ví dụ: các tài liệu hoặc mật khẩu đã được phân loại để lại trên bàn làm việc.

pattern directed analysis ***phân tích trực tiếp mẫu*** Trong an toàn máy tính, một phương pháp phân tích tĩnh trong đó các mẫu chỉ lệnh liên quan đến dòng an toàn, được yêu cầu và cố gắng đạt tới trong phần mềm. Ví dụ, một số các thủ tục không xóa các thanh ghi và bộ nhớ đệm sau khi sử dụng. *Xem* static analysis.

pattern sensitive fault ***sai hỏng nhạy mẫu, lỗi phụ thuộc mẫu*** Trong lĩnh vực độ tin cậy, một lỗi xảy

ra trong việc đáp ứng một mẫu dữ liệu cá biệt.

pause retry ***ngừng thử lại*** Trong truyền thông dữ liệu, một tùy chọn chương trình kiểm soát mạng cho phép một người sử dụng chỉ rõ số lần mà một thông báo sẽ được truyền đi khi xảy ra các lỗi truyền, và khoảng thời gian trì hoãn giữa mỗi lần thử.

pay date ***ngày trả tiền, ngày thanh toán*** Trong hoạt động ngân hàng, ngày mà các quỹ thu được hoa lợi từ việc rút tiền mặt. *So sánh với* value date. *Xem* beneficiary.

Payday ***virut Payday*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào các tệp COM, EXE, và OVL, làm hỏng các các tệp chương trình và OVL. *Xem* virus names.

payment ***(sự) thanh toán*** Trong hoạt động ngân hàng, đây là sự chuyển nhượng các quỹ theo bất kỳ hình thức nào giữa hai thành viên.

payment cycle ***chu trình thanh toán*** *Đồng nghĩa với* banking cycle.

payment message ***thông báo thanh toán, thông báo trả tiền*** *Xem* transaction/payment message.

payment order ***trình tự thanh toán*** Trong hoạt động ngân hàng, một chỉ dẫn để xác định việc chuyển nhượng các quỹ.

payment service ***dịch vụ trả tiền, dịch vụ thanh toán*** Trong hoạt động ngân hàng, một dịch vụ trao đổi các thông báo giữa những người đóng góp và cũng có tác dụng giải quyết các thông báo này để thiết lập các hoạt động chuyển nhượng các quỹ. *Xem* funds transfer transaction.

P box ***hộp P*** Trong mật mã, một hộp hoán vị, là thành phần của một thuật toán mã hóa mà áp dụng mã pháp hoán vị trên tín hiệu đầu vào. *So sánh với* S box. *Xem* data encryption standard, transposition cipher.

PC *Xem* personal computer.

P Class ***lớp P*** Trong lý thuyết độ phức tạp, một lớp các bài toán có thể giải được trong thời gian đa thức. *So sánh với* NP class. *Xem* time and space requirements.

PCM *Xem* pulse code modulation.

PCS *Xem* physical control space.

PCD *Xem* permanent data call.

PDM *Xem* pulse duration modulation.

PDN *Xem* public data network.

PDS *Xem* protected distribution system.

PDU *Xem* protocol data unit.

peer entity ***thực thể ngang hàng*** Trong truyền dữ liệu, một thực thể trên một tầng tương ứng của mô hình bảy tầng OSI. *Xem* open systems interconnection.

peer entity authentication ***xác thực thực thể ngang hàng*** (1) Trong xác thực, sự chứng thực rằng, một thực thể ngang hàng là một thực thể được khai báo trong một kết hợp. (2) Trong an toàn truyền thông, điều này gắn liền với hoạt động của các bộ phận truyền thông tìm kiếm để xác minh mọi định danh khác. *Xem* authentication, masquerading.

PEM. *Xem* privacy enhanced mail.

penetration ***(sự) thâm nhập, (sự) đột nhập*** (1) Trong an toàn máy tính, một truy nhập không được phép tới một hệ thống ADP mà thành công. *Xem* access. (2) Trong an toàn dữ liệu, một tấn công vào sự an toàn của hệ thống máy tính, đảm nhận kiểm tra hiệu lực của sự an toàn và vạch ra vùng các điểm yếu bất kỳ. *Xem* penetration testing, threat team. (3) Trong an toàn dữ liệu, một vi phạm thành công vào một hệ thống được bảo vệ.

penetration profile ***hồ sơ thâm nhập*** Trong an toàn máy tính, một bản mô tả về các hành động cần thiết làm cho một sự thâm nhập có hiệu lực. *Xem* penetration.

penetration signature ***dấu hiệu thâm nhập*** (1) Trong an toàn máy tính, sự mô tả một tình trạng hoặc một tập các điều kiện mà một sự thâm nhập có thể xảy ra. (2) Sự mô tả các biến cố thường xuyên và không thường xuyên của hệ thống và chúng hết hợp với nhau để chỉ ra sự hiện diện của một sự thâm nhập đang xảy ra. *Xem* penetration.

penetration study ***nghiên cứu thâm nhập*** Trong an toàn máy tính, một kỹ thuật định lượng tĩnh trong đó các cá nhân bị thử thách để tìm ra những điểm yếu chưa được biết đến trong việc kiểm soát an toàn. *So sánh với* code review, source code analyzer. *Xem* static evaluation.

penetration testing ***kiểm định thâm nhập, kiểm tra thâm nhập*** (1) Trong an toàn máy tính, một phần của việc kiểm tra an toàn trong đó những người thâm nhập thử phá vỡ các đặc trưng an toàn của một hệ thống. Những người thâm nhập này có thể được sử dụng tất cả các tài liệu về thiết kế và thực thi của hệ thống, chúng có thể chứa các danh sách mã nguồn, tài liệu, và các sơ đồ mạch của hệ thống. Những người thâm nhập này làm việc mà không có sự ràng buộc nào ngoại trừ họ có quyền như những người sử dụng bình thường. *Xem* tiger team. (2) Trong an toàn máy tính, công việc của các nhóm những người lập trình viên/phân tích viên thử thâm nhập vào một hệ thống với mục đích phát hiện ra bất kỳ các điểm yếu nào trong an toàn. *Xem* penetration, tiger team.

Pentagon ***virut Pentagon*** Trong an toàn máy tính, một virut lây nhiễm vào cung khởi động của đĩa mềm và làm hỏng cung khởi động. *Xem* virus names.

percentage supervision ***giám sát tính phần trăm*** Trong an toàn vật lý, tỷ lệ giá trị thay đổi về điện trở hoặc dòng điện trên giá trị điện trở hoặc dòng điện ở chế độ hoạt động bình thường trên một đường truyền được giám sát, cần thiết để đưa ra một tín hiệu báo động. *Xem* alarm signal, supervised line.

percent denial ***phần trăm từ chối*** Trong truyền thông, tỷ lệ phần trăm trung bình của các cuộc gọi cố tình, trong lúc bận, chúng bị chắn lại vì mạng quá tải. Đại lượng đo cấp dịch vụ trên một nhóm khép kín truy nhập quay số. *Xem* dial access.

perfect secrecy ***độ mật hoàn thiện***

Trong mật mã học, một điều kiện được định nghĩa bởi trường hợp trong đó, xác suất có điều kiện để điện rõ P đã được gửi đi nếu đã nhận điện mã C, bằng xác suất điện rõ P đã truyền đi. Việc nhận điện mã này không cung cấp thêm thông tin cho kẻ tấn công so với điện rõ nguyên thủy. Điều kiện cần và đủ đối với hệ mật hoàn thiện là với mọi điện rõ P, xác suất có điều kiện để nhận được bản mã C, tương ứng với P đã được truyền đi bằng xác suất không điều kiện để nhận lại bản mã C. *Xem* Information theory, key equivocation.

performance standard ***chuẩn thực hiện*** Tiêu chuẩn thiết kế chung xác định kết quả mong muốn mà không cần chỉ rõ phương pháp để đạt được kết quả đó. *So sánh với* design standard.

Perfume ***virut Perfume*** Trong an toàn máy tính, một virut máy tính làm hỏng các tệp COM, các tệp chương trình và OVL. *Xem* virus names.

perimeter ***vành đai (bảo vệ)*** Trong an toàn máy tính, một ranh giới trong đó, các kiểm soát an toàn được áp dụng để bảo vệ những gì thuộc quyền sở hữu. Một vành đai an toàn thường gồm nhân an toàn, một số phương tiện mã tin cậy, phần cứng và một số kênh truyền thông có thể. *Xem* channel, security kernel, trusted.

perimeter barrier ***rào chắn ngoại vi, rào chắn vành đai*** Trong an toàn vật lý, một rào chắn vật lý được thiết kế để bổ sung thêm vào việc bảo vệ một vành đai bên trong hay bên ngoài. *Xem* inside perimeter, outside perimeter.

periodic audit ***kiểm toán định kỳ*** Trong tính toán, việc kiểm chứng một tệp hoặc một giai đoạn xử lý. Việc kiểm tra có chủ định để tìm ra những vấn đề này sinh và khuyến khích việc thực hiện đúng các thủ tục kiểm soát về sau này.

periods processing ***(các) giai đoạn xử lý*** Trong an toàn máy tính, các khoảng thời gian trong khi các môi trường an toàn được thiết lập tạm thời để xử lý thông tin. Ví dụ, một hệ thống tự động có thể xử lý tối mật trong chế độ an toàn thuần nhất ở giai đoạn 1, xử lý mật và tuyệt mật trong chế độ an toàn có kiểm soát ở giai đoạn 2, và chỉ có an toàn mức thấp nhất (chưa phân loại mật) ở giai đoạn 3. Hệ thống thanh lọc toàn bộ thông tin và đạt được trạng thái an toàn khi chuyển tiếp từ giai đoạn này sang giai đoạn kế tiếp. Trong suốt giai đoạn mới, người sử dụng không có mức truy nhập và nhu cầu cần biết đối với thông tin đã xử lý trong giai đoạn trước. *So sánh với* multilevel secure. *Xem* controlled security mode, dedicated security mode, isolation enforcement, need to know. *Đồng nghĩa với* temporal separation.

peripheral ***ngoại vi*** Trong tính toán, một thiết bị thực hiện một hoạt động phụ trợ trong hệ thống, ví dụ vào/ra, lưu giữ. *Xem* backing storage.

permanent data call ***gọi dữ liệu thường xuyên*** *Đồng nghĩa với* permanent virtual circuit.

permanent virtual circuit ***mạch ảo thường trực*** Trong truyền dữ liệu,

một loại dịch vụ gọi ảo đặc trưng trong đó, các liên kết logic giữa các thiết bị đầu cuối chỉ ra được thiết lập thường trực, nhờ vậy cuộc gọi được thiết lập và các thủ tục giải phóng bị loại ra. *Đồng nghĩa với* permanent data call.

permissions ***(các) quyền truy nhập cho phép, (sự) cho phép*** Trong an toàn máy tính, mô tả về loại các tác động qua lại được phép mà một đối tượng có thể có với một đối tượng. Các quyền bao gồm: đọc, ghi, thực hiện, thêm, sửa, xóa. *Đồng nghĩa với* access mode.

permutation ***hoán vị*** Trong toán học, một trong toàn bộ số các sắp xếp vị trí có thể trong một nhóm.

persistent object ***đối tượng ổn định*** Trong an toàn máy tính, một kỹ thuật trong đó một tài nguyên được gán cho một tên bí mật, chỉ các chương trình có thể sử dụng nó biết. Các chương trình này tham chiếu tới tài nguyên và sau đó làm cho tài nguyên này trở thành một thành phần không thể truy nhập được của các đối tượng khả thi sử dụng tài nguyên đó. Ví dụ, một tệp được gán cho một cái tên và tên này có trong mã nguồn của các chương trình ứng dụng được phép truy nhập nó. Các chương trình ứng dụng chỉ tồn tại ở dạng được biên dịch trên máy tính và tên của tệp bị xóa đi sau đó. Nguồn tài nguyên được che giấu khỏi tất cả các chương trình trừ khi chúng biết tên bí mật của nó. *Xem* application program, source code.

personal authentication ***xác thực cá nhân*** *Xem* personal verification.

personal computer ***máy tính cá nhân*** Trong tính toán, một máy vi tính và các thiết bị ngoại vi được thiết kế để cung cấp các công cụ tính toán cho những người sử dụng riêng lẻ. *Xem* microcomputer. *Đồng nghĩa với* home computer.

personal computer security ***an toàn máy tính cá nhân*** Việc bảo vệ dữ liệu được lưu trữ và được xử lý trên một máy tính cá nhân, chống lại việc lộ và sửa chữa không được phép, bảo vệ phần cứng, phương tiện lưu trữ tránh mất mát, sửa chữa hoặc làm hỏng.

Giới thiệu

Các máy tính cá nhân và các hệ thống nhỏ khác có duy nhất các vấn đề về an toàn mà phải được tìm hiểu nếu các biện pháp an toàn có hiệu lực được thiết lập. Mặc dù về cơ bản, các máy tính cá nhân cung cấp cùng chức năng như các hệ thống lớn, nghĩa là chúng cho phép thao tác nhanh và kiểm soát số lượng lớn văn bản và dữ liệu, song ở đây có vài đặc trưng chỉ ra các vấn đề an toàn đặc thù. Nói chung, sự khác biệt nằm trong các vùng sau đây:

- các khả năng truy nhập vật lý;
- các cơ chế an toàn kèm theo;
- bản chất của dữ liệu;
- những người sử dụng.

Việc bảo vệ vật lý cơ bản một hệ thống máy tính được yêu cầu để đảm bảo hoạt động tin cậy và tính toàn vẹn cơ bản của phần cứng và phần mềm. Các cơ chế an toàn khác, ví dụ, các cơ chế được thiết lập trong các hệ thống phần cứng và phần mềm đều dựa vào mức bảo vệ cơ bản.

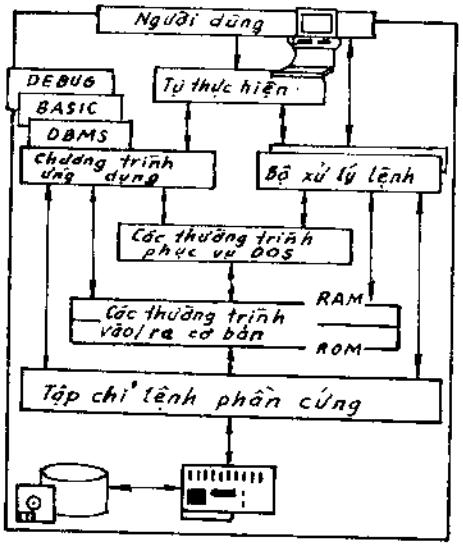
Với các máy tính cá nhân, khả năng truy nhập vật lý không dễ dàng kiểm soát, thực tế, khả năng truy nhập vốn gắn liền với khái niệm một máy tính "cá nhân". Hiếm khi có thể thực hiện được việc xây dựng một "vỏ bọc" xung quanh một máy tính cá nhân. Điều này có nghĩa là, việc bảo vệ chống lại hiểm họa, việc sửa đổi phần cứng, hoặc truy nhập trái phép gặp khó khăn thực sự.

Nhiều cơ chế an toàn kỹ thuật, ví dụ, phần mềm kiểm soát truy nhập và các thủ tục mật mã thường phụ thuộc vào tính toàn vẹn của phần cứng và phần mềm, các cơ chế an toàn này không cung cấp lâu dài mức độ an toàn mong muốn.

Vấn đề an toàn thứ hai với hầu hết các máy tính cá nhân là sự thiếu các cơ chế phần mềm đi kèm, được dùng để tách rời những người sử dụng khỏi các chức năng nhạy cảm, liên quan tới an toàn của hệ thống. Ví dụ, máy tính cá nhân thông thường không hỗ trợ các cơ chế an toàn quan trọng sau đây, song có hiệu lực trên các hệ thống lớn:

- các trạng thái đa bộ xử lý, cho phép tách rời những vùng dành cho người sử dụng và các xử lý của hệ thống;
- các lệnh đặc quyền, giới hạn truy nhập vào các chức năng nhất định, ví dụ như đọc và ghi lên đĩa, vào các xử lý của hệ thống tin cậy;
- các đặc tính bảo vệ bộ nhớ, ngăn chặn việc truy nhập trái phép vào các vùng nhạy cảm của hệ thống.

Không có các đặc tính phần cứng như vậy, không thể ngăn những chương trình của người sử dụng khỏi việc truy



personal computer security: *an toàn máy tính cá nhân.* Hình 1. Các nhánh truy nhập nội bộ trong máy tính cá nhân. DEBUG = gỡ rối; BASIC = cơ sở; DBMS = hệ quản trị cơ sở dữ liệu

nhập hoặc sửa chữa các phần của hệ điều hành và thông qua cách đó phá vỡ các cơ chế an toàn định trước.

Hình 1 trình bày nhiều giao diện bên trong, tồn tại trong một hệ thống máy tính cá nhân. Bản thân việc giữ an toàn hiệu quả trong máy tính đòi hỏi rằng, các đường dẫn thông qua nó những người sử dụng có thể truy nhập dữ liệu và các chức năng của hệ thống cần được giới hạn và kiểm soát chặt chẽ. Các cơ chế phần cứng đề cập ở trên được thiết kế để giới hạn và kiểm soát các đường dẫn này.

Có thể được nhìn thấy từ hình minh họa, các cơ chế kiểm soát được thiết lập ở một mức cho trước (ví dụ, trong một chương trình ứng dụng hoặc thậm

chí trong một hệ điều hành) có thể bị phá vỡ bởi việc sử dụng một trong các đường dẫn xen kẽ nhau. Mặc dù, nó chỉ đưa ra một mức nhất định về khả năng kỹ thuật để lợi dụng các điểm yếu như vậy, nhiều người sử dụng máy tính cá nhân có kinh nghiệm vẫn đạt được các kỹ năng như vậy.

Thông tin được xử lý và lưu giữ trên các hệ thống máy tính cá nhân thường là nhạy cảm và dễ truy nhập hơn là trên các hệ thống lớn, nhiều người sử dụng. Tình trạng này phát sinh bởi vì thông tin trên một máy cho trước thường có liên quan đến một người hoặc một nhóm xác định. Thông tin này có thể ở dạng ghi nhớ, các báo cáo, các bàn tính, hoặc các danh sách đơn giản, nó dễ truy nhập hơn bằng cách sử dụng các công cụ phần mềm thân thiện với những người sử dụng máy tính cá nhân. Cuối cùng, dữ liệu như vậy có xu hướng ở dạng "không thể thay đổi", hơn là một khối dữ liệu khó phân tích và xử lý. Tất cả điều này có thể làm cho công việc tìm kiếm thông tin chỉ ra dễ dàng hơn trên một hệ thống lớn.

Bảo vệ phần cứng

Để ngăn chặn ăn cắp máy tính cá nhân, và thiết bị văn phòng khác, có thể dùng một vài loại thiết bị khóa các thiết bị. Chúng có thể được sử dụng để ghép thiết bị vào một cái bàn hoặc đối tượng cố định khác; một số thiết bị cũng ngăn chặn truy nhập vào công tắc nguồn của hệ thống. Điều này trở nên quan trọng hơn trong việc tự ngăn chặn truy nhập bất hợp pháp vào bên trong thiết bị PC, để đảm bảo việc bảo vệ thành phần và kiểm soát cấu hình. Nhiều hệ thống có chứa các bảng mở rộng, ví dụ, bộ nhớ phụ, các modem, các giao diện đồ họa, chúng trở thành một mục tiêu ăn cắp phổ biến.

Hơn nữa, các cơ chế an toàn hệ thống, ví dụ như mật mã, có thể phụ thuộc vào các thành phần nhất định và tính toàn vẹn của các thành phần này phải được bảo vệ. Thiết bị khóa thiết bị thường cung cấp thêm để bảo vệ chống lại truy nhập vào bên trong của thiết bị. Một cách lựa chọn, các thiết bị có thể được sử dụng trong một số hệ thống, nó khóa dễ dàng vỏ thiết bị.

Các máy tính cá nhân được thiết kế để hoạt động trong một môi trường văn phòng đặc trưng, nghĩa là không cần điều kiện không gian đặc biệt, kiểm soát chất lượng nguồn điện, hoặc các kiểm soát nhiễm bẩn không khí. Nói chung, có thể cho rằng, "nếu con người thấy thoải mái thì máy tính cũng vậy". Tuy nhiên, sự quan tâm đặc biệt cần được nêu ra để tối giảm các mạo hiểm môi trường khi thiết bị này không được bảo vệ.

Cần quan tâm đặc biệt tới việc bảo vệ phương tiện từ. Nó không chỉ là nơi lưu giữ chủ yếu thông tin của mỗi người sử dụng, mà có thể là thành phần của hệ thống dễ bị tấn công nhất từ đó gây ra thiệt hại. Các đĩa cố định hoặc đĩa cứng thường được bảo vệ tốt khỏi ô nhiễm môi trường. Tuy nhiên, phải quan tâm khi vận chuyển các đơn vị này, vì mối nguy hiểm gây hại tới các đầu đọc/ghi và các thành phần bên trong khác.

Hầu như mọi hệ thống máy tính cá nhân đều có ít nhất một ổ đĩa mềm.

Các đĩa linh hoạt là phương tiện phổ biến nhất để phân phối phần mềm và dữ liệu, và việc xử lý đĩa là một phần trong việc sử dụng hầu hết PC bất kỳ. Đĩa từ hiện tại được chứa trong một vỏ bọc bảo vệ. Tuy nhiên, phải có các lỗ ở vỏ bọc để truy nhập thông qua các đầu đọc/ghi của ổ đĩa. Các mặt ngoài này là điểm yếu đặc biệt nguy hiểm. Các vỉ đĩa mềm sử dụng một vỏ nhựa cứng với một vỏ bọc truy nhập có thể co vào, điều này làm giảm khả năng dễ bị tấn công đối với việc xử lý và các chất gây ô nhiễm. Những người sử dụng PC thường không để ý nhiều tới việc xử lý phương tiện từ, và nhà quản lý có trách nhiệm cung cấp đào tạo nghiêm túc trong lĩnh vực này.

Hệ thống máy tính cá nhân và kiểm soát truy nhập dữ liệu

Có 3 hướng để đưa truy nhập được kiểm soát vào các hệ thống và thông tin:

- cấp quyền - thiết lập các quy tắc quyết định người nào có thể truy nhập vào các hệ thống và thông tin nào đó;
- định danh tính - của những người sử dụng và các hệ thống hoặc dữ liệu mà họ được phép truy nhập;
- kiểm soát truy nhập - buộc tuân theo các quy tắc cấp phép chỉ ra.

Quá trình kiểm soát truy nhập bao gồm một số quy tắc tồn tại để xác định những người sử dụng nào được quyền truy nhập vào tài nguyên, các chương trình thông thường hoặc dữ liệu của hệ thống nào đó. Các quy tắc này phải được thiết lập bởi "những người chủ sở hữu" của các nguồn tài nguyên cần kiểm soát. Các quy tắc cấp phép có thể không nhiều hơn một tuyên bố rằng, chỉ các thành viên của một nhóm hoặc bộ phận cho trước được phép truy nhập vào một máy tính hoặc hệ thống ứng dụng cho trước. Nói cách khác, các quy tắc này gồm nhiều định nghĩa hình thức về các phân loại thông tin và các quy tắc để truy nhập vào từng loại. Kiểu quy tắc cấp phép được thông qua sẽ dựa vào nhu cầu của mỗi tổ chức. Tuy nhiên, điều quan trọng là kiểu xử lý cấp phép. Các quy tắc cấp phép là bắt buộc. Điều cần thiết là những người sử dụng và các nguồn tài nguyên thường là dữ liệu sẽ được nhận dạng. Trong một môi trường máy tính cá nhân, định danh của người sử dụng có thể ẩn hoặc tường minh. Trong một trường hợp điển hình, một người sử dụng thiết lập "quyền" để sử dụng hệ thống chỉ đơn giản bằng việc có khả năng bật máy. Nếu định danh hàm ý như vậy có nghĩa là chẳng định danh gì thì hệ thống phải là một "con người" thực sự, nghĩa là một người sử dụng đơn lẻ hệ thống và ở đây phải có các kiểm soát vật lý thích hợp để đảm bảo rằng chỉ có những người sử dụng hợp pháp được phép truy nhập.

Các hàng rào của các văn phòng hoặc thiết bị được khóa cho một mức độ an toàn nào đó trong khu vực này. Nếu một hệ thống được chia sẻ thì các thủ tục định danh đơn giản có thể không thích hợp.

Đối với hầu hết tình huống mà các PC được chia xẻ, danh tính của người sử dụng phải được xác thực theo một cách nào đó. Điều này đòi hỏi sự tương tác

rõ ràng giữa hệ thống và người sử dụng. Điều này phải được thực hiện bằng kiểu xử lý "đăng nhập" hệ thống nào đó, trong đó người sử dụng cung cấp một ký tự nhận dạng không cần bí mật, ví dụ, tên hoặc số tài khoản, và một số bằng chứng khác để xác thực một yêu cầu bắt buộc, ví dụ như mật khẩu. Xác thực đăng nhập của người sử dụng phải xuất hiện bất cứ lúc nào hệ thống được cấp nguồn, hoặc một người sử dụng mới truy nhập vào hệ thống. Thêm vào đó là việc nhận dạng người sử dụng, ở đây phải có một số cách nhận dạng các tài nguyên cần bảo vệ. Những tài nguyên này thường là chứa dữ liệu hoặc các chương trình.

Thực hiện gán nhãn lên các tài liệu nhạy cảm và các tư liệu khác với các chỉ dẫn bên ngoài rõ ràng được chấp nhận từ lâu. Đặc biệt, bìa phía trước, và thường mỗi trang, của các tài liệu như vậy phải có một nhãn chuẩn để chỉ ra sự phân loại và các yêu cầu xử lý. Mặc dù, việc gán nhãn này không phải luôn dễ dàng như việc thực hiện với một loạt dạng phương tiện từ được sử dụng kèm theo các máy tính cá nhân, nó không khó khăn đối với các đĩa mềm, dạng phổ biến nhất của phương tiện lưu giữ dữ liệu. Các đĩa chứa đựng thông tin nhạy cảm có thể được gán nhãn với các nhãn đặc biệt hoặc vỏ bọc được tô màu sáng. Điều này cho phép cá nhân nhận dạng rõ ràng các tư liệu được yêu cầu bảo vệ đặc biệt. Điều này cũng làm các tài liệu nhạy cảm tường minh đối với một kẻ trộm, nên nó phải được giả thiết là những người sử dụng sẽ đưa ra sự bảo vệ thích hợp cho tất cả những tư liệu như vậy.

Hai biện pháp cơ bản có giá trị để bảo vệ dữ liệu. Kiểu đầu tiên là ngăn chặn những người không được phép truy nhập; cách tiếp cận thứ hai là từ chối hiệu quả việc sử dụng thông tin ngay cả khi đã truy nhập được. Các kiểm soát truy nhập logic cung cấp kiểu truy nhập đầu tiên, mật mã cung cấp kiểu thứ hai. Thông thường nên kết hợp cả hai kiểu bảo vệ này.

Các vấn đề về kiểm soát truy nhập logic là khác nhau đối với dữ liệu được lưu giữ trên phương tiện không cố định và dữ liệu được lưu giữ trên phương tiện cố định. Nếu dữ liệu nằm trên phương tiện không cố định, thì biện pháp "ồ và chìa" đơn giản có thể sẽ cung cấp các giải pháp có lợi. Nếu các đĩa chứa các dữ liệu nhạy cảm không thể được bảo vệ theo cách này, ví dụ, trong quá trình gửi thì phép mã hóa có thể thích hợp. Nếu dữ liệu nằm trên một phương tiện cố định, ví dụ như đĩa cứng, thì việc kiểm soát truy nhập dữ liệu sẽ đòi hỏi trước tiên là việc kiểm soát truy nhập lên chính định danh của người sử dụng, và sau đó là dữ liệu có giá trị đối với người sử dụng.

Mật mã cung cấp bảo vệ chống lại việc làm lộ không được phép. Nó cũng đảm bảo việc phát hiện ra các sửa đổi thông tin không cho phép vì sự thay đổi bất kỳ đối với dữ liệu đã được mã hóa mà không có khóa mã cần thiết, sẽ được nêu ra bởi sự có mặt của các đoạn bị trích ra trong bản rõ sau đó. Tuy nhiên, rõ ràng là, mật mã không ngăn chặn được sự sửa đổi hoặc phá hủy; đơn giản nó chỉ đảm bảo việc phát hiện những

P

sự cố như vậy. Vì vậy, dữ liệu quan trọng không thể được bảo vệ chỉ bằng mã hóa.

Có một số sản phẩm phần mềm và phần cứng có giá trị thương mại, cung cấp cho người sử dụng máy tính cá nhân các khả năng mã hóa. Nói chung, những sản phẩm này cho phép người sử dụng thực hiện các chức năng mã hóa sau đây:

- nhập vào hoặc thay đổi các khóa mã;
- mã một khối dữ liệu;
- giải mã một khối dữ liệu.

Trong một số trường hợp, các phương tiện được cung cấp nhằm tạo và quản lý các khóa. Tuy nhiên, thông thường, điều này thường để mặc cho người sử dụng. Thực tế, điều này là một trong những vấn đề chính trong việc sử dụng hiệu quả mật mã, vì bí mật các khóa là cốt yếu trong việc bảo vệ được cung cấp thông qua mật mã.

Cách thông thường trong mật mã được sử dụng trong một môi trường máy tính cá nhân là mã hóa và giải mã toàn bộ các tệp. Đặc biệt, một người sử dụng chuẩn bị một tệp và sau đó chạy một tiện ích mã hóa để đưa ra một bản văn bản mã của tệp. Sau đó, tệp nguyên thủy phải bị ghi đè lên. Chương trình tiện ích phải được sử dụng lại để giải mã và đưa ra một phiên bản bản rõ của tệp.

Người sử dụng có trách nhiệm trong việc lựa chọn, nhập vào và ghi nhớ khóa mà được sử dụng trong các quá trình mã hóa và giải mã. Các sản phẩm mật mã mang tính chất thương mại thường cung cấp các chương trình tiện ích để mã hóa và giải mã các tệp lớn cũng như một tiện ích để ghi đè lên các tệp cũ.

Các vấn đề nảy sinh trong việc mã hóa và giải mã các tệp dữ liệu lớn là sự cần thiết ghi đè lên các tệp bản rõ, và việc đào tạo con người là cần thiết. Một lựa chọn đối với quá trình mã hóa tệp nêu trên là sử dụng một phương tiện mật mã, nó tích hợp với hệ thống vào/ra tệp thứ cấp. Về cơ bản, mỗi khối dữ liệu được ghi lên đĩa đầu tiên được mã hóa, và mỗi khối được đọc từ đĩa được giải mã trước khi chuyển đi tới một chương trình yêu cầu. Điều này làm toàn bộ quá trình mật mã hầu như trong suốt đối với người sử dụng và loại trừ sự phiền phức và nguy hiểm liên quan đến các thủ tục của tệp lớn. Những người sử dụng có chuyên môn kỹ thuật cao có thể tự thực hiện khả năng như vậy. Thêm vào đó, có một số sản phẩm phần mềm và phần cứng có giá trị có tính thương mại cao.

Một khía cạnh khác của kiểm soát truy nhập, mà thường được giám sát thường xuyên, là "phần còn lại" của dữ liệu bỏ quên trên trên đĩa hoặc trên bộ nhớ. Đây là dữ liệu được lưu giữ trên các vùng của đĩa hoặc bộ nhớ đã được giải phóng để dùng lại. Thông tin như vậy có thể bị những người sử dụng sau đó đọc được. Một ví dụ phổ biến về vấn đề "phần còn lại" trên đĩa được kết hợp với việc xóa các tệp trên đĩa (ví dụ, với các lệnh Erase và Delete). Quá trình này thường chỉ dẫn tới việc thiết lập bộ chỉ báo rằng đã xóa một tệp trong thư mục tệp, chứ không xóa bỏ vật lý hoặc ghi đè lên dữ liệu thực. Vấn đề này có thể được giải quyết bằng cách sử dụng một

chương trình để "làm sạch", tức là ghi đè lên toàn bộ dữ liệu có trên tệp như một phần của quá trình xóa. Mặc dù các chương trình như vậy tương đối dễ viết nhưng chúng thường không được cung cấp thường xuyên như các đặc tính chuẩn của các hệ điều hành của máy tính cá nhân. Vì vậy, chúng phải được yêu cầu hoặc ghi thông qua người sử dụng.

Lập kế hoạch dự phòng và ngẫu nhiên

Vấn đề lập kế hoạch dự phòng và ngẫu nhiên trên một môi trường máy tính cá nhân về bản chất giống như các hoạt động xử lý dữ liệu khác. Thực chất, đối với các tổ chức có cả các máy tính cá nhân lẫn các hệ thống cỡ lớn, việc lập kế hoạch dự phòng và ngẫu nhiên phải là một quá trình thống nhất. Tuy nhiên, có một vài lưu ý đặc biệt dành cho các máy tính cá nhân, trước tiên là việc phân phối thiết bị rộng lớn và số lượng con người bao hàm trong đó.

Lập kế hoạch ngẫu nhiên bao gồm các hoạt động đảm nhận việc dự đoán trước các biến cố tiềm ẩn, là nguyên nhân gây ra các ảnh hưởng bất lợi nghiêm trọng. Tất nhiên, điều này có thể áp dụng cho những người sử dụng cá nhân và các ứng dụng của họ cũng như cho các tổ chức. Trong một môi trường máy tính cá nhân, một trong các yếu tố chủ yếu trong quá trình lên kế hoạch ngẫu nhiên là người sử dụng cá nhân, vì ở đây không có nhân viên trung tâm để thực hiện nhiều chức năng quan trọng. Các kế hoạch ngẫu nhiên nên bao gồm các thủ tục khẩn cấp, nguồn tài nguyên, nghĩa là phần cứng, phần mềm, dữ liệu, các chuẩn bị dự phòng và các kế hoạch hoạt động dự phòng. Thêm vào đó, các kế hoạch ngẫu nhiên có thể nhận thức được sẽ bao gồm các thủ tục khôi phục và kiểm tra. Với một máy tính cá nhân, hiển nhiên là cần khuyến khích sao chép dự phòng các tệp thường xuyên và có hệ thống, vì việc dự phòng như vậy có thể được thực hiện không còn tập trung và có hệ thống như trong trường hợp với một hệ thống cỡ lớn. Giải pháp và tần suất sao chép dự phòng phải do người sử dụng quyết định, dựa vào phương tiện lưu giữ và tính dễ bị thay đổi của dữ liệu được chứa trong đó.

Hầu hết phương tiện dự phòng phổ biến là đĩa mềm vì hầu như mỗi máy tính cá nhân đều có một ổ đĩa mềm. Tuy nhiên, đối với các hệ thống có các đĩa cứng, một dự phòng tệp đầy đủ có thể yêu cầu nhiều hơn 20 đĩa. Như các hệ thống dự phòng hộp băng từ liên tục cần được xem xét nếu như các bản sao chép dự phòng vào các đĩa ngày càng lớn càng trở nên khó khăn hoặc tiêu tốn thời gian.

Điều quan trọng đối với những người sử dụng là hiểu các mối hiểm họa được địa chỉ hóa bởi các thủ tục dự phòng. Lý do dễ nhận thấy đối với việc dự phòng các tệp là cho phép khôi phục dữ liệu sau khi bị mất, do các vấn đề hoặc các sự cố về phương tiện và phần cứng, ví dụ, không chủ định xóa các tệp. Điều này khuyến khích những người sử dụng lưu giữ dự phòng các bản sao tại một vị trí thích hợp, không xa. Tuy nhiên, một hiểm họa khác liên quan là sự mất mát do hỏa hoạn, trộm cắp, lũ lụt,, nó có thể bao gồm toàn bộ một

văn phòng hoặc tòa nhà. Trong các tình huống này, các bản sao dự phòng được lưu giữ cục bộ sẽ bị mất kèm theo các bản gốc. Cần khôn ngoan để lưu giữ hai bản sao dự phòng. Nếu dữ liệu nguyên thủy bị mất thì sự thiệt hại chỉ riêng đối với bản sao dự phòng trong quá trình truyền hoặc tải cũng thật tai hại.

Các virut

Máy tính cá nhân bị tấn công bởi nhiều loại virut khác nhau. Sự phức tạp và tác động của các virut này tăng đáng kể trong vài năm gần đây và các virut là một yếu tố đơn lẻ đáng kể nhất trong an toàn máy tính. Nguy cơ hiểm họa của virut đã bắt buộc những người sử dụng máy tính cá nhân thực hiện an toàn máy tính cẩn thận và chấp nhận các thủ tục hợp lý, ví dụ như dự phòng.

Có các chương trình phần mềm đa dạng được thiết kế để giúp những người sử dụng ngăn chặn hệ thống của họ khỏi virut và nhiều tổ chức có các đơn vị tập trung cung cấp các công cụ chống virut. Đặc biệt, các tổ chức lớn thực hiện các thủ tục giảm tối thiểu thiệt hại của việc sử dụng trái phép các máy tính cá nhân, đưa ra các phần mềm bất hợp pháp và không được kiểm tra ...

Các yếu tố phụ

Người điều hành các ứng dụng quan trọng trên các hệ thống nhỏ và lớn, sẽ yêu cầu các vết kiểm toán tin cậy; các tổ chức cũng mong muốn giám sát việc sử dụng máy tính cá nhân của những người làm công. Một máy tính cá nhân của một người sử dụng đơn lẻ có thể cần các phương tiện kiểm toán đặc biệt như một bản ghi lịch sử và như một phương tiện trợ giúp trong việc khôi phục từ các lỗi. Tuy nhiên, việc thay thế và sử dụng các vết kiểm toán trong các hệ thống máy tính cá nhân đòi hỏi các nghiên cứu đặc biệt. Các tổ chức với sự đầu tư đáng kể vào thiết bị máy tính cá nhân mong muốn giám sát việc sử dụng thiết bị này.

Các kiểu biến cố có thể được quan tâm gồm:

- khởi động lại hệ thống;
- bắt đầu và kết thúc phiên của người sử dụng;
- bắt đầu và kết thúc chương trình;
- truy nhập vào các tệp dữ liệu xác định.

Trong hầu hết các tổ chức, máy tính cá nhân là một trong vài loại thiết bị xử lý dữ liệu được sử dụng. Ngày càng tăng nhu cầu kết nối các máy tính cá nhân như các thiết bị đầu cuối vào các hệ thống máy chủ lớn hoặc kết nối hai hoặc nhiều hơn các máy tính cá nhân thành các mạng. Các vấn đề an toàn trong mỗi trường hợp này về cơ bản giống như trên các hệ thống máy chủ nhiều người sử dụng và các mạng truyền thông dữ liệu. Tuy nhiên, ở đây có một số vấn đề đáng chú ý cần được người quản lý xác định.

Khi một máy tính cá nhân được sử dụng như một thiết bị đầu cuối tới một hệ thống máy chủ, các yêu cầu cơ bản về an toàn và kiểm soát truy nhập giữ nguyên với máy chủ. Đối với máy chủ, nó chỉ là một thiết bị đầu cuối khác. Tuy nhiên, nó phải được nhận dạng để máy tính cá nhân có khả năng tải lên và lấy về số lượng lớn dữ liệu mà tốc

độ thường vượt quá khả năng với các thiết bị đầu cuối thông thường.

Phần mềm truyền thông dành cho các máy tính cá nhân thường cung cấp phương tiện lưu giữ các số điện thoại và các dãy đăng nhập cho các hệ thống máy chủ thường được gọi. Một vấn đề tiềm ẩn quan trọng tồn tại khi những người sử dụng lưu giữ các mật khẩu hoặc thông tin nhạy cảm khác theo cách này. Thực tế, hiện nay an toàn của máy chủ phụ thuộc vào an toàn vật lý được cung cấp qua máy tính cá nhân và các tệp của nó. Những người sử dụng cần được chỉ dẫn không nên lưu giữ các mật khẩu của hệ thống máy chủ hoặc thông tin nhạy cảm khác trên các tệp kiểm soát phần mềm truyền thông. Tất cả các thiết bị điện tử đều phát ra các tín hiệu điện từ (hình 2). Với thiết bị nào đó, ví dụ, các máy tính, các đường truyền thông, các thiết bị đầu cuối dữ liệu, những tín hiệu phát xạ của chúng có thể mang thông tin, có thể được phát hiện thông qua các thiết bị giám sát được đặt thích hợp. Các biện pháp an toàn chống lại vấn đề này được biết đến như các kiểm soát "Tempest". Ở Mỹ, các ứng dụng chứa dữ liệu được xếp vào loại mật (an toàn quốc gia) phải được xử lý bình thường trên thiết bị đã được che chắn hoặc thay đổi để giảm đến tối thiểu các phát xạ điện từ.

Quản lý

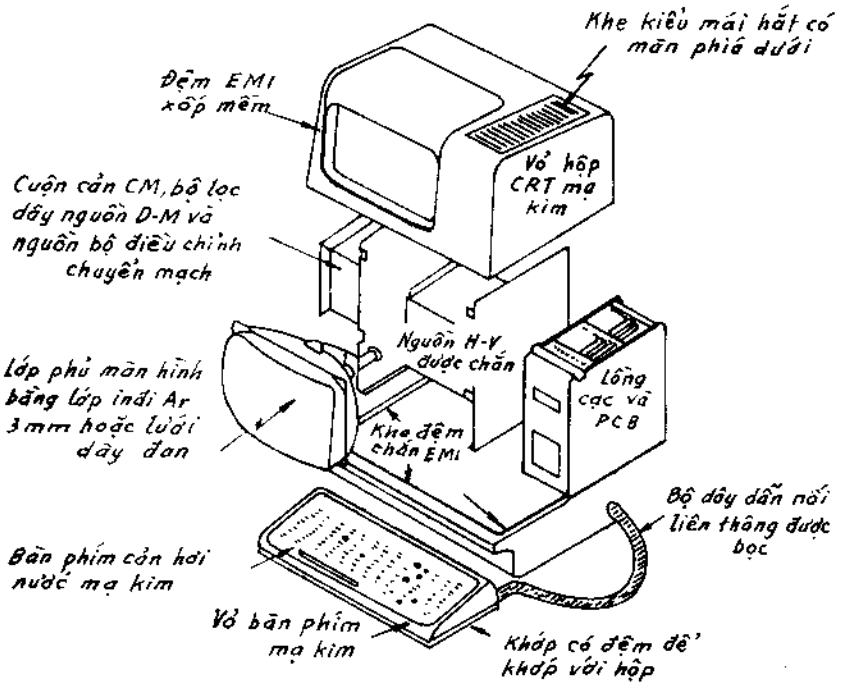
Các mục trên đã trình bày bản chất các tiết lộ an toàn đặt trước những người sử dụng các hệ thống máy tính cá nhân và một số biện pháp kiểm soát xác định mà có thể được sử dụng để giảm việc làm lộ bí mật. Mục này cung cấp một quản lý có triển vọng đối với vấn đề này và một hướng để quản lý an toàn thông tin trong một môi trường máy tính cá nhân. Có 3 chiến lược cơ bản để bảo vệ các nguồn tài nguyên thông tin khỏi các hiểm họa được đề cập gần đây:

- ngăn chặn các mối hiểm họa từ việc tấn công;
- phát hiện những mối hiểm họa tấn công này;
- khôi phục lại từ các ảnh hưởng của thiệt hại.

Một biện pháp an toàn cho trước sẽ thuộc một hoặc nhiều chiến lược cơ bản này. Mục tiêu của việc quản lý an toàn là chọn lựa các biện pháp kiểm soát, bao gồm tất cả các chiến lược bảo vệ nói trên. Để tách bạch, các chiến lược này không có giá trị đối với một người quản lý hoặc người sử dụng quan tâm đến việc bảo vệ thông tin.

Cần có một hướng có tính hệ thống để nhận dạng và thực hiện các yêu cầu an toàn. Nói chung, một hướng như vậy nên bao hàm các hoạt động sau đây:

- Nhận dạng tài sản - nhận dạng và phân loại thông tin và các tài sản khác cần bảo vệ.
- Ước lượng rủi ro - nhận dạng và ước lượng các mối hiểm họa, các điểm yếu dễ bị tấn công, và mức độ lộ bí mật.
- Lựa chọn và thực hiện kiểm soát - chọn lựa các biện pháp kiểm soát, mang lại hiệu quả trong việc giảm khả năng bị lộ bí mật.
- Kiểm toán và đánh giá - tiến hành các hoạt động để xem xét các kiểm soát liên tục có hiệu quả và thích hợp.



personal computer security: *an toàn máy tính cá nhân.* Hình 2. Các biện pháp kiểm soát bức xạ.

Mục đích của các hoạt động này là việc lựa chọn và thực hiện các biện pháp kiểm soát hiệu quả. Với các nguồn tài nguyên không bị hạn chế, có thể đạt được thực sự mức an toàn bất kỳ. Tuy nhiên, không có tổ chức nào lại giao phó các nguồn tài nguyên trong khi có quá nhiều rủi ro đi kèm. Vì vậy, vấn đề chủ yếu là quản lý rủi ro.

Khi phân tích rủi ro, điều quan trọng là nhìn nhận vấn đề như một vấn đề về an toàn thông tin, không phải là một vấn đề về an toàn máy tính. Điều này đặc biệt đúng khi máy tính cá nhân trở thành một công cụ văn phòng khác như máy chữ, máy đọc chính tả, hoặc điện thoại. Các rủi ro liên quan trước hết tới thông tin, sau đó mới tới các thiết bị vật lý mà thông tin có thể được lưu giữ hoặc xử lý trên đó.

Về mặt lý tưởng, ở đây nên có một chỉ định hình thức về quyền và trách nhiệm đối với việc quản lý an toàn thông tin đối với toàn bộ tổ chức. Điều này áp dụng cho thông tin ở dạng bất kỳ, bất cứ khi nào nó tồn tại trên một máy tính cá nhân, một hệ thống máy tính lớn, hoặc trên một trang giấy. Tuy nhiên, trách nhiệm hoạt động cơ bản nên trao cho cá nhân, người "sở hữu" thông tin, có động cơ thúc đẩy bảo vệ thông tin, và có quyền và các nguồn tài nguyên cần thiết, nghĩa là các tổ chức của người sử dụng. Vì vậy, ngoại trừ

việc phát triển chính sách và sự hướng dẫn thì một trách nhiệm đơn lẻ đối với an toàn máy tính cá nhân có thể không hoàn toàn thích hợp.

Sau cùng, nhiều kiểm soát an toàn phụ thuộc vào sự tin cậy của các cá nhân. Vì vậy, phải có một cách thức nào đó để bảo vệ cá nhân, người được quyền truy nhập vào các hệ thống thông tin nhạy cảm. Việc quản lý nên thiết lập các thủ tục kiểm soát hình thức lên trên việc phát triển và sử dụng các hệ thống thông tin. Điều này dễ dàng thực hiện được khi các hệ thống thông tin này được cấu trúc tương đối tốt và riêng biệt.

Cần có các đánh giá hình thức định kỳ đối với các hiểm họa và rủi ro liên quan tới các hệ thống thông tin nhạy cảm. Điều này được yêu cầu như một cơ sở để lựa chọn các biện pháp kiểm soát sinh lợi đối với các hệ thống này.

Các hệ thống, các tổ chức, và các môi trường sẽ thay đổi. Điều này thường dẫn tới những thay đổi về các rủi ro xảy ra đối với một hệ thống thông tin. Cần có một chương trình kiểm toán và đánh giá thường xuyên các hệ thống nhạy cảm để đảm bảo tính thỏa đáng liên tục, tính hiệu quả, tính thích hợp của các biện pháp an toàn.

Các yếu tố liệt kê ở trên không tự đảm bảo việc bảo vệ thích hợp. Đúng ra, chúng cung cấp một sườn công việc thích hợp để xây dựng bên trong nó một chương trình an toàn thông tin hiệu quả.

Giống như trường hợp đối với chương trình an toàn bất kỳ, đó là trách nhiệm của nhà quản lý để cung cấp chỉ dẫn đảm bảo an toàn cho các hệ thống máy tính cá nhân. Hướng chỉ điều này quan trọng vì sự phát triển số lượng người trong các tổ chức, những người sẽ sớm được tính đến trong việc sử dụng các hệ thống như vậy. Việc quản lý cần tập trung vào:

- bảo vệ thông tin, chứ không phải là các máy tính;
- tập trung vào việc sử dụng một biện pháp quản lý rủi ro để ra quyết định bảo vệ;
- ấn định trách nhiệm và quyền cần thiết về an toàn cho "những người sở hữu" thực sự và những người sử dụng các nguồn tài nguyên thông tin.

Xem access control, audit trail, back/up restore, contingency plans, cryptographic key, cryptography, directoty, download, floopy disk, hard disk, information security, log on, MODEM, ownership, password, plaintext, purging, residues problems, risk analysis, risk management, software protection, software tool, spreadsheet, tape streamer, Tempest proofing, van Eck phenomenon.

personal computing ***tính toán cá nhân*** Trong các ứng dụng, quá trình tính toán được thực hiện bởi người sử dụng phía một máy tính cá nhân, bao gồm thao tác trên máy và thường là xử lý văn bản, bảng tính và các ứng dụng cơ sở dữ liệu. Việc tính toán cá nhân được đặc trưng bởi các tiếp cận phi hình thức, các thủ tục đơn giản hóa và đòi hỏi độ sẵn sàng, trái ngược với quá trình xử lý dữ liệu điện tử quy ước. *Xem* data base, end user computing, electronic data processing, spreadsheet.

personal data ***dữ liệu cá nhân*** (1) Theo luật, dữ liệu bất kỳ duy nhất được sử dụng trong hệ thống hồ sơ để cất hoặc lấy ra một hồ sơ cá nhân. Thông tin phải tuân theo sự kiểm soát của Đạo luật về tính riêng tư năm 1974. (2) Dữ liệu về một cá nhân không bị giới hạn, bao gồm các hoạt động học vấn, giao dịch tài chính, tiền sử bệnh tật, trình độ chuyên môn, dữ liệu dịch vụ, tiền sử phạm tội hoặc nghề nghiệp, nó gắn dữ liệu với tên cá nhân, hoặc số định danh, ký hiệu, hoặc định dạng khác được ấn định cho cá nhân cụ thể, như dấu vân tay hoặc giọng nói hoặc một bức ảnh. *Xem* fingerprint, voice print. (3) Theo luật, như trong Đạo luật bảo vệ dữ liệu năm 1984 của Anh đã định nghĩa, dữ liệu chứa thông tin có liên quan đến một cá nhân đang sống, người mà có thể nhận dạng được thông qua thông tin này. Dữ liệu đó chứa cả phát biểu ý kiến bất kỳ về cá nhân song không chỉ ra bất kỳ ý định nào của người dùng dữ liệu đối với cá nhân đó. *Xem* data, data protection.

personal disclosure ***(sự) lộ bí mật cá nhân*** Trong an toàn cơ sở dữ liệu, một trường hợp trong đó một người sử dụng có thể suy diễn dữ liệu thống kê nhạy cảm chưa được biết đến trước đó liên quan đến một cá nhân. Như vậy, dữ liệu làm lộ có thể gần đúng, khẳng định hoặc phủ định. *Xem* data protection, disclosure risk, negative disclosure, sensitive statistic. *Đồng nghĩa với* compromise.

personal identification ***nhận dạng cá nhân*** *Xem* personal verification.

personal identification number ***số nhận dạng cá nhân*** *Xem* PIN.

personal identifier ***ký hiệu nhận dạng cá nhân*** Trong an toàn dữ liệu, một mục dữ liệu liên quan đến một cá nhân cụ thể, nó miêu tả danh tính của cá nhân này và các cá nhân khác có thể được biết.

personal password ***mật khẩu cá nhân*** Trong kiểm soát truy nhập, một mật khẩu chỉ duy nhất một người biết và được sử dụng để xác thực danh tính của người này. *Xem* password, valid password.

personal verification ***thẩm tra cá nhân, kiểm tra tư cách cá nhân*** Trong hoạt động ngân hàng, việc phê chuẩn các con số bí mật mà một người sử dụng cung cấp để thiết lập quyền của anh ta khi tiến hành một hoạt động giao dịch. *Xem* PIN validation.

personnel security ***an toàn cá nhân, an toàn nhân sự*** Trong an toàn máy tính, các thủ tục được thiết lập để đảm bảo rằng, tất cả những người đã truy nhập vào thông tin nhạy cảm bất kỳ đều có các quyền cần thiết cũng như các mức truy nhập dữ liệu nhạy cảm thích hợp. *Xem* access, sensitive information.

perturbation ***(sự) gây nhiễu*** Trong an toàn cơ sở dữ liệu, một kỹ thuật kiểm soát suy luận đối với các cơ sở dữ liệu thống kê trong đó hoặc:

- dữ liệu ngẫu nhiên được thêm vào các mục riêng biệt của dữ liệu tìm được, dữ liệu này đã dùng trong tính toán các thống kê được yêu cầu;

hoặc:

- thống kê được tính toán và được đưa

ra chỉ đưa vào một trong số tất cả các mẫu bản ghi thích hợp;

hoặc:

- các thống kê được đưa ra đều được làm tròn.

Ảnh hưởng của dữ liệu ngẫu nhiên có thể không đáng kể trong việc xác định thống kê nhưng có thể đưa ra dữ liệu bị suy đoán sai khá lớn. Ví dụ, nếu lương của một cá nhân có thể bị suy đoán bởi việc điều tra tổng số lương của toàn bộ các thành viên trong một bộ phận lớn và tổng số tất cả các thành viên của bộ phận này, thì kết quả thu được sau đó có thể được sử dụng để suy đoán ra lương của nhân viên thuộc bộ phận.

Các kỹ thuật gây nhiễu thêm các số ngẫu nhiên vào mỗi tổng số sẽ làm cho lương được suy đoán, hiệu số của hai số lớn trở nên sai hoàn toàn. *So sánh với* cell restriction, table restriction. *Xem* inference control, record based perturbation, result based perturbation, statistical database.

pervasive sercurity mechanism ***cơ chế an toàn tỏa khắp*** Trong an toàn truyền thông, một thuật ngữ được sử dụng trong an toàn OSI. Nó không đặc trưng cho một dịch vụ an toàn đặc biệt nào hoặc được kết hợp với một tầng đặc biệt nào. *Xem* OSI security.

Phantom ***virut Phantom*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy các tệp chương trình và các tệp OVL. *Xem* virus names.

phase delay ***trễ pha*** Trong truyền thông, trễ thời gian được đặc trưng bởi sự thay đổi pha của một sóng hình sin đi qua giữa hai điểm trên một đường truyền.

phase modulation ***điều pha, điều biến pha*** Trong truyền thông, một phương pháp điều biến trong đó pha của sóng mang hình sin được thay đổi để phù hợp với tín hiệu điều biến. *So sánh với* amplitude modulation, frequency modulation, pulse modulation. *Xem* carrier.

phase shift keying ***điều biến dịch pha*** Trong truyền dữ liệu, một phương pháp thay đổi pha của tín hiệu hình sin để biểu diễn cho dữ liệu nhị phân. Nếu chỉ có hai pha rời rạc được dùng thì mỗi pha sẽ tương ứng với một bit nhị phân 1 hoặc 0. Nếu dùng 4 lần dịch pha thì mỗi pha có thể tương ứng với một nhóm hai bit. *Xem* dibit, phase modulation, quadrature amplitude modulation.

phone phreaking ***(sự) xì mê điện thoại*** *Xem* phreak.

photoelectric beam smoke detector ***thiết bị phát hiện khói bằng tín hiệu quang điện*** Trong an toàn vật lý, một bộ phát hiện khói được kích hoạt bởi việc giảm cường độ của một nguồn ánh sáng nhận được do tác động của khói giữa một nguồn ánh và một tế bào quang điện. *Xem* photoelectric sensor.

photoelectric sensor ***bộ cảm biến quang điện*** Trong an toàn vật lý, một bộ cảm biến sử dụng sự thay đổi của cường độ ánh sáng tại một bộ nhận để tạo ra một tín hiệu điện kích hoạt

một chuông báo động. Các cảm biến quang điện có thể hoạt động với ánh sáng có thể nhìn thấy được hoặc với tia hồng ngoại.

photosensor ***cảm biến quang*** Trong an toàn vật lý, một thiết bị nhận một tín hiệu ánh sáng và tạo ra một tín hiệu điện tương ứng.

phracker ***phracơ, kẻ lạm dụng điện thoại - máy tính*** Trong an toàn máy tính, thuật ngữ kết hợp của từ "PHReaking" và "hACking" để chỉ kẻ kết hợp phá điện thoại bằng máy tính. Bọn này thường dùng máy tính tìm cách thọc sâu vào các tổng đài điện thoại, nhằm gian lận cước điện thoại đường dài *Xem* hacker, phreak.

phreak ***kẻ lạm dụng điện thoại*** Trong an toàn truyền thông, thuật ngữ kết hợp của PHone fREAK, một người bị mạng điện thoại làm si mê. Thông thường, một cá nhân sử dụng hiểu biết của mình về mạng điện thoại để thực hiện các cuộc gọi do người khác trả tiền phí tổn. *So sánh với* hacker. *Xem* phracker, telephone intrusion.

physical barrier ***rào chắn vật lý*** Trong an toàn vật lý, một hình thức vật lý bất kỳ, ví dụ như các hàng rào, sông, bức tường, vách đá, được thiết kế để làm chậm trễ hoặc ngăn chặn sự xâm phạm vào vùng được bảo vệ.

physical control space ***không gian kiểm soát vật lý*** Trong an toàn vật lý, khoảng hình cầu bao quanh thiết bị điện được sử dụng để xử lý thông tin nằm dưới kiểm soát vật lý để ngăn chặn các phát xạ gây hại. Nó thường được tính theo mét và có thể được kiểm soát bằng hàng rào, người gác, đi tuần, các bức tường... Phương pháp an toàn đúng đắn cho không gian kiểm soát vật lý (PCS) có thể thay đổi phụ thuộc vào mức sẵn sàng của các tài nguyên trên. *Xem* compromising emanations, Tempest, van Eck phenomenon.

physical database ***cơ sở dữ liệu vật lý*** Trong các cơ sở dữ liệu, một hình thức trong đó cơ sở dữ liệu được cất giữ trong các kho gồm cả các con trỏ bất kỳ mà nó có thể chứa. Số các cơ sở dữ liệu logic khác nhau có thể được dựa trên cùng một cơ sở dữ liệu vật lý. *So sánh với* logical database.

physical data independence ***độc lập dữ liệu vật lý*** Trong cơ sở dữ liệu, nói tới sự cấu thành của các cơ sở dữ liệu, cho phép cấu trúc lưu giữ vật lý có thể bị thay đổi mà không ảnh hưởng đến cấu trúc logic. *So sánh với* logical data independence. *Xem* data independence.

physical layer ***tầng vật lý*** Trong truyền thông dữ liệu, tầng cuối cùng của mô hình tham chiếu kết nối các hệ thống mở ISO (ISO Open Systems Interconnection Reference model). Đây là tầng liên quan đến việc truyền dòng bit chưa xử lý. *So sánh với* application layer, data link layer, network layer, presentation layer, session layer, transport layer. *Xem* bit stream, open systems interconnection.

physical record ***bản ghi vật lý*** (1) Trong tính toán, đây là một bản ghi đi kèm với một vùng lưu giữ vật lý xác định. (2) Trong tính toán, một đơn vị dữ liệu lớn nhất có thể được truyền đi

theo một thao tác đọc hoặc ghi đơn lẻ. *So sánh với* logical record.

physical security ***an toàn vật lý*** (1) Trong việc quản lý các rủi ro, các biện pháp được sử dụng để bảo vệ vật lý cho các tài nguyên tránh khỏi các hiểm họa cố tình và ngẫu nhiên. *So sánh với* logical security. (2) Việc sử dụng các khóa, người canh gác, và các biện pháp hành chính tương tự để kiểm soát truy nhập vào máy tính và thiết bị liên quan. *Xem* access. (3) Trong an toàn máy tính, một biện pháp cần thiết để bảo vệ các kiến trúc sắp xếp máy tính, các thiết bị liên quan và các nội dung của chúng tránh khỏi sự thiệt hại do tai nạn, hỏa hoạn, và thảm họa môi trường.

physical threat ***hiểm họa vật lý*** Trong an toàn máy tính, một mối hiểm họa tiềm ẩn ảnh hưởng đến sự tồn tại thực sự và điều kiện vật lý của các thiết bị máy tính, ví dụ như nạn ăn cắp trang thiết bị, hỏa hoạn, tấn công khủng bố. *So sánh với* accidental threat, active threat, deliberate threat, logical threat, passive threat. *Xem* threat.

PI *Xem* padding indicator.

PIC ***mã nhận dạng cá nhân*** Trong kiểm soát truy nhập, viết tắt của Personal Identification Code, là một mã chữ - số duy nhất được sử dụng để nhận dạng một cá nhân, thông thường được kết hợp với một thẻ vật lý, như thẻ vạch từ. Thẻ được đưa vào một máy tính thích hợp/thiết bị truyền thông để thực hiện một giao tác. *Xem* magnetic stripe card, PIN.

piezoelectric detector ***bộ phát hiện áp điện*** Trong an toàn vật lý, một bộ phát hiện làm việc nhờ dòng điện được sinh ra khi tinh thể áp điện chịu một ứng suất cơ học.

piggyback ***dịu thêm, cõng thêm*** *Xem* between- the-lines entry, electronic piggybacking, piggyback entry, piggybacking.

piggyback entry ***vào cổng sau*** Trong điều khiển truy nhập, một truy nhập không được phép vào một hệ thống ADP qua kết nối bất hợp pháp của người sử dụng khác.

piggybacking ***(sự) cõng thêm, (sự) dịu thêm*** (1) Trong truyền dữ liệu, một phương pháp gửi các báo nhận bằng cách đưa ra các thông báo, ví dụ, trong các thông báo HDLC từ *A* tới *B* chứa thông tin về các khung mà *A* nhận từ *B*. *Xem* HDLC, acknowledgement, frame. (2) Trong an toàn máy tính, *đồng nghĩa với* tailgating.

PIN ***số hiệu nhận dạng cá nhân, số hiệu PIN*** (1) Trong kiểm soát truy nhập, viết tắt của Personal Identification Number, số hiệu cá nhân duy nhất này phải được một người sử dụng nhập vào trước khi sử dụng một thiết bị đầu cuối từ xa, hoặc điểm bán hàng đầu cuối, để truyền thông tin hoặc thực hiện một giao tác. *So sánh với* password. *Xem* point of sale terminal, PIN management and security. (2) Trong hoạt động ngân hàng, một mã chữ-số hoặc mật khẩu từ 4 đến 12 vị trí mà khách hàng sở hữu để xác thực. *So sánh với* PAN. *Xem* PIN management and security.

PIN assignment ***quy định PIN*** Trong hoạt động ngân hàng, một quá trình thiết lập mối liên hệ giữa xác thực

khách hàng và dữ liệu định danh. *Xem* PIN, PIN management and security.

Ping Pong-B ***virut Ping Pong-B*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào đĩa mềm và cung khởi động của đĩa cứng, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy cung khởi động. *Xem* virus names.

PIN issuance ***(sự) phát hành PIN*** Trong hoạt động ngân hàng, một hoạt động chuyển thông tin PIN cho một khách hàng. *Xem* PIN, PIN management and security.

PIN mailer ***bưu phẩm PIN*** Trong hoạt động ngân hàng, một tài liệu chứa một PIN ở dạng rõ ràng. Tài liệu phải được in ra dưới các điều kiện an toàn cao để đảm bảo rằng người làm công không thể mở, đọc hoặc xem xét tài liệu. Bưu phẩm thường được tạo ra như một khuôn dạng đã được nhiều nhóm đóng dấu, vì vậy PIN chỉ có thể được đọc bằng cách bỏ đóng dấu khuôn dạng. *Xem* PIN, PIN management and security.

PIN management and security ***quản lý và an toàn PIN*** Trong ngân hàng và an toàn dữ liệu, việc thiết lập các quá trình bao gồm: tạo ra, gán, chuyển giao, phát hành, lưu trữ, nhập, kiểm tra, chuyển, khử kích hoạt và phá hủy các PIN.

PIN có thể được dùng trong 2 loại môi trường:

- một tổ chức nơi những người làm công hoặc các thành viên được lựa chọn sử dụng các PIN để truy nhập vào các phương tiện của tổ chức, ví dụ, các hệ thống máy tính, các cơ sở dữ liệu;
- một mạng EFT hoặc EFTPOS phục vụ một hay nhiều tổ chức tài chính và một cơ sở khách hàng lớn và phổ biến.

Các quy tắc chung trong việc quản lý và an toàn PIN là phổ biến với cả hai vùng ứng dụng nhưng chúng khác biệt hoàn toàn về số lượng người sử dụng, mối quan hệ giữa người sử dụng và hệ thống, và mối hiểm họa tiềm ẩn do việc quản lý và an toàn PIN không đầy đủ. Tầm quan trọng của nhiệm vụ và sự phức tạp của môi trường là rất lớn trên cả hai hệ thống EFT và EFTPOS, việc quản lý và an toàn PIN sẽ được thảo luận theo khía cạnh này.

Một hệ thống EFT hoặc EFTPOS phải đảm bảo được sự an toàn cho các danh tính của khách hàng và tính toàn vẹn trong hoạt động giao dịch duy nhất của khách hàng, từ khách hàng tới bộ phận phát hành thẻ cho khách hàng, không kể đến việc xác định vị trí của thiết bị đầu cuối mà khách hàng sử dụng. Thông thường các thiết bị đầu cuối này sẽ không bị giám sát, và trong trường hợp đối với hệ thống EFTPOS, chúng dễ bị những thương nhân không trung thực hoặc nhân viên của họ sửa đổi và lạm dụng.

Các rủi ro đi kèm theo với việc lộ bí mật các PIN bị những người không được phép làm lộ, có thể xảy ra do:

- lạm dụng thẻ bị mất hoặc bị đánh cắp;
- gian lận lớn do việc sản xuất và lạm dụng thẻ giả.

Các thiệt hại tiềm ẩn xảy ra do việc lạm dụng các thẻ bị mất hoặc bị đánh cắp

sẽ được hạn chế trong khoảng thời gian từ lúc mất tới lúc trình báo mất cho người phát hành thẻ, và giá trị cho phép tối đa của các hoạt động giao dịch hàng ngày. Hơn nữa, nhiều thẻ thu được bất hợp pháp sẽ có ít khả năng xác định các PIN của chúng.

Tuy nhiên, vấn đề cần quan tâm chính là việc gian lận lớn có thể xảy ra nếu các thẻ giả được sản xuất, và các PIN tương ứng được sinh ra hoặc nhân được. Việc lạm dụng một thẻ sẽ không được báo cho người phát hành thẻ cho đến khi khách hàng kiểm tra bản kê (ghi các khoản nhập và xuất tại ngân hàng) hàng tháng và trình báo có giao dịch gian lận. Người phát hành thẻ sẽ phải đối mặt với những vấn đề sau:

- Các chi phí hành chính chủ yếu trong việc sửa các tác động của các hoạt động giao dịch gian lận cá nhân.
- Vấn đề trình báo của các khách hàng đối với các hoạt động giao dịch bất hợp pháp như gian lận, bởi vì họ đã coi nhẹ hoạt động giao dịch hoặc đã gian lận lợi dụng tình trạng này.
- Làm mất lòng tin của khách hàng.

Như vậy, điều quan trọng là các quá trình bao gồm: tạo ra, gán, chuyển giao, phát hành, lưu trữ, nhập, kiểm tra, chuyển đi, khử kích hoạt và phá hủy các PIN phải ngăn ngừa được các khả năng làm lộ bí mật các PIN.

Tạo ra các PIN

Các PIN có thể được dùng trong một hệ thống trao đổi giao dịch trong đó, các khách hàng nhập danh tính của họ và các chi tiết xác thực, khi các hoạt động giao dịch bắt đầu tại các thiết bị đầu cuối được kết nối với mạng. Các chi tiết thông báo được chuyển cho người phát hành thẻ, người này chịu trách nhiệm xác thực khách hàng và cho phép hoạt động giao dịch. Các PIN có thể được sử dụng trong một mạng cá nhân, ở đó việc xác thực các khách hàng và cho phép hoạt động giao dịch được thực hiện toàn bộ bên trong mạng.

Các PIN có thể được sinh ra là các PIN suy dẫn, các PIN được sinh ra ngẫu nhiên hoặc các PIN được khách hàng lựa chọn. Một PIN suy dẫn là một hàm số số tài khoản của khách hàng hoặc một số thông tin nhận dạng khác không cần bí mật; do vậy, các PIN suy dẫn có thể được xác minh thông qua việc áp dụng cùng thuật toán lên thông tin nhận dạng của khách hàng, được sử dụng để nhận được PIN, và so sánh kết quả với trị số PIN được khách hàng nhập vào tại thiết bị đầu cuối.

Rõ ràng, khả năng tính toán PIN chắc sẽ bị hạn chế đối với người phát hành PIN, ví dụ thuật toán mã hóa DES có thể được sử dụng và việc giữ bí mật khóa được duy trì. Các PIN có thể được xác minh tại thiết bị đầu cuối vì vậy có thể truy nhập vào khóa được sử dụng trong thuật toán suy dẫn, không cần phải lưu giữ PIN trên thẻ. Kỹ thuật tạo ra PIN nên được tự động hóa hoàn toàn và các kết quả được in lên một bưu phẩm PIN để ngăn chặn những người làm công cố tình truy nhập vào các PIN của khách hàng. Các PIN suy dẫn như vậy phải được mã hóa trước khi lưu giữ.

Vấn đề này sinh đối với PIN suy dẫn là PIN được xác định bởi số tài khoản hoặc thông tin nhận dạng và khóa mã

hóa được sử dụng. Như vậy, những khó khăn này sinh nếu PIN bị nghi ngờ có sự thỏa hiệp, hoặc nó phải được thay đổi ngay sau khi ngân hàng bị thiệt hại hoặc khách hàng mất thẻ tín dụng. Tương tự, nếu như ngân hàng muốn thay đổi khóa mật mã, nó phải thông báo cho tất cả các khách hàng về PIN suy dẫn mới.

Các độ lệch PIN có thể được sử dụng để khắc phục những vấn đề này. Các PIN suy dẫn được tính toán và sau đó khách hàng có thể chọn lựa trên cơ sở ngẫu nhiên; độ lệch PIN là một số mà liên kết PIN suy dẫn tới PIN thực. Ví dụ, độ lệch có thể được thêm vào PIN thực để tạo ra PIN suy dẫn. Độ lệch PIN không cần phải là một số bí mật, do vậy có thể để trong dữ liệu vạch từ. PIN có thể bị kiểm tra cục bộ, thiết bị đầu cuối đọc số tài khoản hoặc dữ liệu nhận dạng, và tính toán các PIN suy dẫn. PIN được khách hàng nhập vào, độ lệch PIN được đọc từ thẻ, cộng với PIN nhập vào và được so sánh với PIN suy dẫn.

Một PIN được ấn định ngẫu nhiên do một quá trình ngẫu nhiên tạo ra sao cho sự hiểu biết về một dãy bất kỳ các PIN được sinh ra thì cũng không có khả năng xác định PIN khác bất kỳ. Các PIN được sinh ra phải nằm trong tập các PIN được phép, theo tập ký tự và độ dài của PIN. Các PIN được ấn định ngẫu nhiên có thể khó nhớ và do đó làm tăng nguy cơ các khách hàng sẽ tạo các bản ghi nhớ, nó có thể bị mất hoặc đánh cắp cùng với thẻ. Các phương pháp tạo ra các chuỗi ký tự dễ nhớ là rất sẵn, nhưng kỹ thuật này làm giảm đáng kể tập các PIN ấn định với độ dài của một PIN cho trước, do đó đòi hỏi các PIN dài hơn. Việc sinh ra các PIN như vậy đòi hỏi các biện pháp phòng ngừa an toàn chặt chẽ để tránh người làm công của bộ phận phát hành thẻ cố tình truy nhập bất hợp pháp vào thông tin PIN kết hợp với nhận dạng khách hàng.

Các PIN khách hàng chọn lựa cũng tương tự như vậy, chúng dễ nhớ nhưng lại tồn tại nhiều khả năng là chúng tạo một mối quan hệ có thể suy luận được các chi tiết cá nhân của khách hàng: tên con, ngày sinh, số đăng ký xe... Vì các khách hàng hướng tới việc loại bỏ số lớn các khả năng, trong dãy PIN, nên độ dài tối thiểu của một PIN phải đủ để cung cấp một dãy lớn các PIN cần cho sử dụng.

Việc kiểm tra cục bộ đối với các PIN do khách hàng chọn lựa và PIN ấn định ngẫu nhiên có thể sử dụng kỹ thuật độ lệch PIN. Độ lệch PIN được tính bằng hiệu của PIN và PIN suy dẫn. Điều quan trọng là tổ hợp PIN và độ lệch PIN cho PIN suy dẫn không được để lộ. Với thông tin như vậy, một kẻ tấn công có thể tạo ra một thẻ giả có chứa dữ liệu tài khoản của khách hàng, chọn một PIN ngẫu nhiên, tính độ lệch PIN và lưu giữ nó trên thẻ giả. Thẻ giả này cùng với PIN liên quan sẽ được các thiết bị đầu cuối cục bộ chấp nhận, thậm chí còn không bị phát hiện cho dù khách hàng sử dụng PIN.

Một kỹ thuật khác dùng các PVV (các giá trị kiểm tra PIN). PVV được tạo ra bằng cách mã hóa tổ hợp của số tài khoản và PIN của khách hàng; sau đó,

PVV 4 chữ số nhận được từ 16 ký tự hex của bản mã, ví dụ, chọn các ký tự hex tương ứng với các chữ số thập phân. Các thủ tục đặc biệt được sử dụng nếu có ít hơn 4 số thập phân trong bản mã hóa. PVV được cất giữ trên thẻ vạch từ và được sử dụng trong khi kiểm tra PIN một cách tương tự như đối với các độ lệch PIN. Trong trường hợp này, các PIN nhập vào được tổ hợp với dữ liệu tài khoản và PVV đã được tính toán, sau đó so sánh PVV đã được tính toán với giá trị được lưu giữ.

Chuyển giao các PIN

Cơ chế chuyển giao đối với một PIN phải sao cho sau khi chuyển giao, nó không xuất hiện ở dạng rõ tại nơi nó có thể được liên kết với nhận dạng của khách hàng. Các PIN phải không được gửi đi trên cùng phong bì thư như các thẻ tín dụng hoặc thẻ ngân hàng tương ứng, còn địa chỉ trả lại trên phong bì thư phải khác với địa chỉ được sử dụng với thẻ. Các PIN sẽ được in ra theo cách mà chỉ có khách hàng nhìn thấy được. Nếu một khách hàng có nhiều hơn một thẻ thì thông tin đi kèm theo PIN phải đầy đủ để khách hàng liên hệ PIN và thẻ tương ứng nhưng không đủ làm tổn hại đến PIN nếu nó bị chặn bắt. Những người phát hành thẻ phải trang bị an toàn đầy đủ để bảo vệ các PIN trong khi xử lý các tài liệu chứa PIN, các phong bì được trả lại, các tài liệu không dùng đến...

Báo cáo của khách hàng về một PIN được khách hàng lựa chọn, không kéo theo việc để lộ PIN này cho nhân viên phát hành thẻ; nếu một nhân viên được một khách hàng ủy quyền bắt đầu nhập một PIN, sau đó danh tính của nhân viên phải được ghi vào bản ghi giao dịch. Các khách hàng có thể đích thân hoặc thông qua chuyển thư hoặc hệ thống điện thoại báo cho người phát hành thẻ về PIN của họ.

Khách hàng đích thân nhập vào một PIN, sẽ yêu cầu

- nhân viên phát hành thẻ, được ủy quyền bắt đầu nhập, phải kiểm tra danh tính của khách hàng;
- danh tính của nhân viên phải được hệ thống kiểm tra và xác thực;
- quá trình nhập PIN phải được nhân viên bắt đầu và bị vô hiệu hóa ngay sau khi nhập PIN.

Đối với việc nhập các PIN do khách hàng chọn lựa thông qua chuyển thư hoặc hệ thống điện thoại, các thủ tục được chấp thuận phải đảm bảo rằng, bất kỳ cá nhân nào muốn chặn thư của khách hàng hoặc nghe trộm cuộc điện thoại thì không có khả năng để liên kết PIN với các thông tin tài khoản của khách hàng. Trong việc chuyển thư, khách hàng cần được thông báo rằng, phiếu được trả lại có chứa số PIN, và phong bì thư liên quan phải không chứa tên của khách hàng, địa chỉ hoặc thông tin nhận dạng tài khoản. Phiếu cần chứa một số hiệu kiểm soát giúp cho người phát hành thẻ liên hệ PIN và số tài khoản của khách hàng; ví dụ, số hiệu kiểm soát này là một dạng mã của số tài khoản.

Các đầu vào thông qua hệ thống điện thoại phải là một đáp ứng âm thanh hoặc hệ thống ghi để tránh khả năng khách hàng tình cờ, hoặc đáp lại một

lời mới làm một điều gì đó, làm lộ bí mật tên hoặc địa chỉ.

Ngay khi được phát ra, các PIN có thể cần được thay đổi, hoặc các khách hàng muốn được nhắc lại các PIN bị quên. Trong trường hợp này, các sắp xếp an toàn không được ít hơn những sắp xếp để phát hành và chuyển giao các PIN mới. Các khách hàng phải được thông báo qua thư về các PIN đã bị thay đổi của họ. Thư này không nên chứa PIN nhưng phải chứa các chỉ dẫn để lập tức thông báo cho người phát hành thẻ nếu như khách hàng không có yêu cầu thay đổi. Nếu khách hàng bắt đầu thay đổi tại một thiết bị đầu cuối không được giám sát thì phải nhập PIN cũ vào; một dạng định danh thêm nào đó, ví dụ, một thẻ cho phép thay đổi PIN nạp một lần (one-shot PIN) có thể được yêu cầu. Sự thay thế một PIN bị lộ có thể đòi hỏi các sắp xếp an toàn đặc biệt mà tùy thuộc vào PIN được suy dẫn, sẽ được gán ngẫu nhiên hoặc do khách hàng lựa chọn. Ví dụ, nếu như một PIN suy dẫn bị lộ thì một yếu tố dữ liệu nào đó đã được dùng trong khi sinh ra PIN, chẳng hạn như độ lệch, phải được thay đổi.

Lưu giữ các PIN

Các PIN phải thường xuyên được mã hóa trước khi lưu giữ, và phép mã hóa này hoặc có thể đảo được hoặc không. Phép mã hóa có thể đảo được cho phép phôi phục được PIN ban đầu và được mã hóa lại với một khóa mới. Tuy nhiên, nếu khóa mã bị tổn hại thì phải xem là tất cả các PIN đã mã hóa bằng khóa đó đều bị tổn hại và việc bảo vệ bằng cách mã hóa lại bằng một khóa mới sẽ quá muộn.

Phép mã không đảo được bảo đảm rằng PIN nguyên thủy không thể bị lộ, nhưng các PIN có độ dài giới hạn có thể được xác định bằng tìm kiếm kiểu vét cạn, tức là trong dãy PIN hạn chế, mọi PIN đều qua thuật toán mã hóa không đảo được và được so sánh với các giá trị mã hóa được lưu giữ. Các khóa không đảo được không thể giải mã và mã hóa lại dưới các khóa mới, tuy nhiên, đối với việc lưu trữ, sự tiện lợi này của PIN đã mã không đảo được có thể đạt được bằng phép mã hóa đảo được. Tất cả các PIN phải được kết hợp với các thông tin có liên quan đến số tài khoản của khách hàng, trước khi mã hóa, để ngăn chặn những kẻ tấn công sửa chữa các giá trị PIN được lưu trữ. Các PIN được ghi lên thẻ vạch từ của một khách hàng phải được mã hóa theo cách đảo được hoặc không. Một lần nữa, thông tin nhận dạng tài khoản phải được kết hợp với PIN trước khi mã hóa, trong trường hợp kẻ tấn công có các phương tiện xóa bỏ hoặc ghi đè lên nội dung của vạch.

Khách hàng và người sử dụng có trách nhiệm đối với sự bí mật PIN của họ; tuy nhiên, sau khi nhập vào hệ thống, người nhận thẻ có trách nhiệm đối với các PIN trong quá trình truyền, lưu giữ hoặc xử lý. Tại nơi nhận, trách nhiệm của khách hàng và người nhận thẻ chồng chéo nhau. Khách hàng nên đảm bảo để những người đang xem không có khả năng quan sát trình tự nhập khóa và việc thiết kế các thiết bị đầu cuối phải ngăn chặn được quá trình hiển thị hoặc in ra các PIN đã nhập vào.

Kiểm chứng các PIN

Việc kiểm tra các PIN là trách nhiệm của người phát hành thẻ hoặc người được ủy quyền. Các PIN có thể được kiểm tra bằng cách so sánh dữ liệu nhận được và PIN, lấy từ kho lưu trữ, nó tương ứng với số tài khoản của khách hàng. Việc kiểm chứng có thể gồm một thuật toán thực hiện trên một PIN được nhập vào và so sánh với một giá trị được mã của PIN được lưu giữ trên thẻ, hoặc gồm một thuật toán được thực hiện trên dữ liệu tài khoản và so sánh với PIN được nhập vào. Thuật toán kiểm chứng như vậy có thể được thực hiện tại một trạm ở xa, trực tuyến và không trực tuyến, miễn là các khóa mã cần thiết có sẵn tại trạm này.

PIN có thể chứa một chữ số kiểm tra để kiểm tra tính hợp lý của PIN được nhập vào, điều này thuận tiện cho việc phát hiện một PIN không được mã nhưng các chữ số kiểm tra như vậy không xác thực được dữ liệu PIN.

Các PIN được mã hóa cả trong khi truyền lẫn khi lưu trữ, các khóa mã khác nhau được sử dụng cho các quá trình này. Mã hóa trong khi truyền là đảo được nhưng các giá trị được lưu trữ có thể được mã bằng phép mã đảo được hoặc mã hóa không đảo được. Với phép mã đảo được, trong cả truyền và lưu trữ, có thể thực hiện so sánh cả hai khóa truyền và lưu trữ bằng giải mã và so sánh các giá trị của bản rõ. Tất nhiên, các phép so sánh giải mã phải được thực hiện trong một môi trường an toàn. Một cách khác, một PIN có thể được giải mã và sau đó mã hóa lại bằng khóa thứ hai để so sánh các giá trị được mã.

Đối với các hệ thống lưu không đảo được, song quá trình truyền có sử dụng mã hóa đảo được, PIN được truyền đi phải được giải mã, sau đó áp dụng quá trình mã hóa không đảo được để so sánh với các giá trị đã lưu giữ.

Việc bảo vệ các PIN trong khi truyền có thể đạt được nhờ tính an toàn vật lý của môi trường truyền hoặc bằng mã hóa. Độ an toàn vật lý của môi trường truyền bao gồm việc giám sát các kết nối bất hợp pháp và biện pháp bảo vệ vật lý có thể, chẳng hạn, ống dẫn kim loại liên tục, các cảm biến áp lực trong một ống điều áp... Sự bảo vệ vật lý như vậy cũng có thể bao gồm cả việc chắn bức xạ điện từ, dẫn đến phức tạp và đắt tiền. Các kỹ thuật mã hóa đòi hỏi các modun an toàn để lưu giữ các khóa mã chủ chốt và các quá trình mã hóa/giải mã.

Các PIN bị khử kích hoạt khi một tài khoản của khách hàng bị đóng hoặc một PIN bị tổn thương. Khử kích hoạt có chủ tâm như vậy sẽ gồm sự phá hoại vật lý các bản ghi ghi nhớ, xóa bỏ phương tiện lưu giữ điện tử... Các biện pháp ngăn ngừa phải chống lại được các rủi ro hoặc việc hủy bỏ có tính toán đối với các PIN được lưu giữ và các bản sao dự phòng được lưu giữ tại các trạm an toàn phải đặt cùng mức an toàn mật mã như dữ liệu nguyên thủy. *Xem* ANSI X9.8 - 1992, derived PIN, irreversible encrytion, PIN assignment, PIN issuance, PIN mailer, PVV, offset, reference PIN, shoulder surfing.

PIN offset ***độ lệch PIN*** Trong hoạt động ngân hàng, một giá trị liên hệ một PIN suy dẫn với PIN thực. Các PIN suy

PIN management and security: *quản lý và an toàn PIN.* Việc cân bằng các yếu tố khác nhau trong lựa chọn các kỹ thuật tạo PIN. Bảng sau đây được in với sự cho phép của Hội các chủ ngân hàng Mỹ.

	Gán các PIN dẫn xuất	*Gán các PIN ngẫu nhiên*	*Các PIN được khách hàng chọn*
Ghi nhớ	– Khó nhớ hơn một giá trị tùy ý	– Khó nhớ hơn một giá trị tùy ý	+ Dễ nhớ
Dùng không gian số hiệu PIN	+ Nếu dùng kỹ thuật dẫn xuất tốt hơn, phân bố sẽ phẳng trên không gian số hiệu PIN	+ Các giá trị có thể được gán để cho phân bố phẳng trên không gian số hiệu PIN	– Nếu không được khuyến khích, khách hàng chắc sẽ chọn các giá trị dễ phỏng đoán (ví dụ ngày sinh nhật và tên) và phân bố các giá trị trên không gian số hiệu PIN là phẳng
Phân phối	– Yêu cầu cơ chế phân phối (thường là bưu phẩm PIN)	– Yêu cầu cơ chế phân phối (thường là bưu phẩm PIN)	+ Yêu cầu có mặt tại các chỗ của người phát hành
Xác thực ban đầu	– Phân phối thư (nếu được dùng) thiếu sự xác thực dích thân ban đầu	– Phân phối thư (nếu được dùng) thiếu sự xác thực dích thân ban đầu	+ Sự tự lựa chọn cho phép người của bộ phận phát hành xác thực thủ công
Điểm yếu trong phân phối	– Sự phân phối làm PIN dễ bị chặn bắt	– Sự phân phối làm PIN dễ bị chặn bắt	+ PIN có thể không bị chặn bắt nếu khách hàng nhập vào giá trị lựa chọn.
Các PIN bị bỏ quên	+ Sự tạo lại cùng giá trị PIN làm khách hàng dễ nhớ	- Sự gán lại cùng giá trị PIN (để khách hàng dễ nhớ) đòi hỏi lưu PIN ở dạng mã đảo được	– Khôi phục lại giá trị giống nhâu nếu bị quên (thường ít khả năng hơn là các PIN được ấn định) đòi hỏi lưu trữ PIN ở dạng mã đảo được.
Các kiểm soát tính khôi phục lại được	– Khả năng tạo lại được cùng giá trị PIN làm người của bộ phận phát hành có khả năng tìm lại (khôi phục lại) được	+ PIN có thể được lưu, được mã ở dạng không đảo được (nếu được thiết kế) để ngăn cản việc khôi phục lại	+ PIN có thể được lưu, được mã ở dạng không đảo được (nếu được thiết kế) để ngăncản việc khôi phục lại
Lưu giữ giá trị kiểm chứng PIN	+ Không đòi hỏi lưu các giá trị kiểm chứng PIN	– Đòi hỏi lưu các giá trị kiểm chứng PIN	– Đòi hỏi lưu các giá trị kiểm chứng PIN tại bộ phân phát hành

PIN management and security: *quản lý và an toàn PIN.* (tiếp theo)

Kiểm chứng không có bộ phận phát hành	+ Cho phép kiểm chứng PIN qua các hệ thống được nơi phát hành ủy quyền phân phối các khóa dẫn xuất (miễn là sự phân phối, sử dụng khóa trong các hệ thống không có bộ phận phát hành có thể được phòng vệ đầy đủ)	– Sự kiểm chứng PIN tại các hệ thống không có bộ phận phát hành đòi hỏi chuyển các giá trị kiểm chứng PIN mà điều này thường bị cấm	– Sự kiểm chứng PIN tại hệ thống không có bộ phận phát hành đòi hỏi chuyển các giá trị kiểm chứng mà điều này là bị cấm
Các PIN bị lộ	– Việc làm lộ chắc chắn PIN đòi hỏi sự phát hành lại hoặc mã lại thẻ PAN và làm trễ thời gian dùng thẻ	– Việc làm lộ chắc chắn PIN đòi hỏi tạo và phân phối giá trị mới, lvô hiệu hóa giá trị cũ và làm trễ thời gian sử dụng	+ PIN có thể thay đổi dễ dàng bởi chính khách hàng tại nơi phát hành thẻ nếu được tin là đã bị lộ, không có sự chậm trễ trong sử dụng thẻ
Phát hành lại thẻ	- Sự phát hành lại thẻ với PAN mới (chẳng hạn, thay đổi mức phát ra) sẽ buộc phải phân phối một PIN mới	+ Sự phát hành lại thẻ với PAN mới có thể giữ lại cùng PIN (không phải phân phối PIN) nếu không được mã bằng phép mã đảo được với PAN	+ Sự phát hành lại thẻ với PAN mới có thẻ giữ lại cũng giá trị PIN đó (khách hàng không cần chọn lại)
Làm lộ khoá	– Việc làm lộ khóa dùng trong dẫn xuất PIN sẽ bộc lộ các giá trị PIN trong tất cả các thẻ mà không cần dữ liệu nào khác.	+ Để làm lộ PIN phải làm lộ cả khóa mã lưu trữ của PIN lẫn các giá trị kiểm chứng được lưu (điều này có thể giảm nhẹ đi hơn nữa bằng việc dùng phép mã không đảo được)	+ Để làm lộ tất cả PIN phải làm lộ cả khóa mã lưu trữ của PIN lẫn các giá trị kiểm chứng được lưu (điều này có thể giảm nhẹ đi hơn nữa bằng việc dùng phép mã không đảo được)
Tác động lên các giá trị PIN	+ Không thể tác động các giá trị dẫn xuất mà vẫn giữ nguyên chức năng đúng của chúng	– Việc giả mạo bằng cách tạo số ngẫu nhiên có thể tạo ra một dải các giá trị định sẵn cần được hạn chế chặt chẽ và gây tác động. Điều này có thể gây khó khăn cho việc phát hiện	+ Người dùng được tự do chọn giá trị của riêng họ – Người của bộ phận phát hành có thể đưa ra các ý kiến có ảnh hưởng lớn đến phạm vi và khả năng lựa chọn của họ

+ ưu điểm tương đối

– nhược điểm tương đối

P

dẫn có nhược điểm là PIN bị ghép chặt bởi số tài khoản của khách hàng và khóa mã được sử dụng trong tính toán PIN suy dẫn. Một độ lệch PIN là một giá trị tuỳ ý, liên kết PIN thực với PIN suy dẫn, như vậy PIN thực có thể bị thay đổi bằng cách tạo ra một sự thay đổi tương ứng với độ lệch. Một giá trị độ lệch không cần thiết phải bí mật và chúng có thể được lưu giữ trên thẻ của khách hàng. PIN được khách hàng nhập vào sẽ được kết hợp với một giá trị độ lệch được đọc từ thẻ và được so sánh với giá trị PIN suy dẫn được tính để kiểm tra cục bộ PIN. *Xem* derived PIN, PIN management and security. *Đồng nghĩa với* offset.

PIN pad ***bộ đệm PIN*** Trong kiểm soát truy nhập, một đơn vị chống giả mạo được sử dụng trong việc nhập PIN tại các thiết bị đầu cuối của khách hàng. Thông thường, bộ đệm PIN bao gồm một lớp đệm khóa và một màn hình hiển thị các chỉ dẫn cho khách hàng, nó chứa các khóa để mã hóa cục bộ các PIN. *Xem* cryptographic key, PIN.

PIN validation ***phê chuẩn PIN*** Trong hoạt động ngân hàng, một thẩm tra cá nhân dựa vào một PIN. *Xem* personal verification, PIN.

PIN verification ***thẩm tra PIN*** Trong hoạt động ngân hàng, việc kiểm tra tính xác thực của khách hàng do người phát hành tiến hành. *Xem* issuer, PIN management and security.

PIN verification value ***giá trị kiểm chứng PIN*** Trong kiểm soát truy nhập, một số thập phân được gán giá trị của một PIN. Một khối bản rõ, dựa vào sự móc nối PIN và số tài khoản tương ứng của nó, được mã hóa bằng thuật toán DES bằng một khóa bí mật độ dài kép.

4 bit đầu tiên của bản mã thường được kiểm tra, nếu bộ này tương ứng với một số thập phân có giá trị từ 0-9 thì nó được chấp nhận, nếu nó tương ứng với số hex giá trị từ A-F thì nó bị loại. Quá trình này được tiếp tục với các giá trị 4 bit liên tiếp cho đến khi thu được số các chữ số thập phân cần thiết. Nếu quá trình này không đưa ra đủ số lượng các chữ số thập phân thì việc kiểm tra được lặp lại và các giá trị hex từ A-F bị trừ đi 10. Một cách khác, có thể sử dụng bảng đổi sang hệ thập phân. Giá trị PIN có thể sử dụng trong việc kiểm tra giá trị của một PIN được nhập vào. Nếu giá trị kiểm chứng PIN được lưu giữ trên một thẻ vạch từ thì PIN nhập vào có thể bị kiểm tra ngoại tuyến bởi một ATM được trang bị khóa độ dài kép đã sử dụng trong việc xác định giá trị kiểm chứng PIN và so sánh với các PVV được lưu giữ và tính toán. Một PIN có thể được truyền đi an toàn tới một trạm trung tâm và sau đó được kiểm tra dựa vào các giá trị kiểm chứng PIN được lưu giữ, một quá trình mang lại rủi ro hơn là lưu trữ các PIN tại trạm trung tâm. *So sánh với* card verification value. *Xem* ATM, encryption standard, decimalization table, multiple DES encipherment, PIN, PIN management and security.

pipeline cipher ***mã pháp dạng ống*** Trong mật mã, một mã pháp mà có thể lợi dụng kiến trúc máy tính dạng ống. Một khối bản rõ được đưa vào một đơn

vị xử lý và giai đoạn đầu tiên của quá trình mã hóa được thực hiện, khi quá trình này hoàn thành, khối thứ hai của bản rõ được đưa vào đơn vị xử lý và giai đoạn đầu tiên của quá trình mã hóa được thực hiện đối với khối thứ hai này trong khi khối bản rõ đầu tiên đang tiến hành giai đoạn mã hóa thứ hai v.v..

pipelining ***tạo ống dẫn, xử lý ống dẫn*** Trong truyền thông dữ liệu, một kỹ thuật được dùng trong các hệ thống truyền thông trong đó người gửi đòi hỏi một báo nhận từ người nhận về việc nhận chính xác các khung, và thời gian truyền bị kéo dài. Người gửi truyền *n* khung dữ liệu trong một chu kỳ, bằng với thời gian cần thiết để một khung tới được người gửi và một tín hiệu nhận tới được người nhận. Sau đó, người gửi sẽ truyền khung *m* bất cứ khi nào nhận được tín hiệu báo nhận cho khung *m* - *n*. *Xem* frame, go back *n*, selective repeat.

PIR ***(cảm biến) tia hồng ngoại thụ động*** Trong an toàn vật lý, viết tắt của Passive InfraRed sensor, một bộ cảm biến tia hồng ngoại thụ động. *Xem* infra red motion detector, passive sensor.

piracy ***vi phạm bản quyền, sao chép bất hợp pháp*** Trong phần mềm, việc sao chép và phân phối phần mềm bất hợp pháp, thường để nhận được lợi ích về tài chính. *So sánh với* software creep.

PKC *Xem* public key cryptography.

PKI ***cơ sở hạ tầng khóa công khai*** Viết tắt của Public Key Intrastructure, là tất cả cơ sở công nghệ và dịch vụ nền tảng dựa trên thuật toán mã khóa công khai, đảm bảo liên lạc thương mại điện tử cũng như hệ thống thông tin khác được an toàn tin cậy. Cụ thể hơn, PKI bao gồm một hệ thống dịch vụ mật mã khóa công khai, chữ ký số, cơ quan cấp chứng chỉ (Certification Authority - CA) và danh sách hủy bỏ chứng thực.

Một ví dụ minh họa, ta hãy hình dung một khía cạnh về các cuộc mua bán "ảo" trên mạng: người mua, người bán, các hợp đồng, giai dịch mua bán, chuyển tiền... với các chữ ký của hai bên... cuộc mua bán này khá phức tạp. Liệu đối tác phía bên kia đường dây của mình có đúng là người mà họ tư nhận không; các tài liệu (hóa đơn, chứng từ có kèm chữ ký) giao dịch mua bán có toàn vẹn (không bị sửa đổi hay bị giả mạo) trong quá trình chuyển tới đầu nối bên kia không? Và còn nữa, tính bí mật của cuộc mua bán có đảm bảo trước đối thủ cạnh tranh hay không?... để hiểu rõ về PKI, ta xem xét từng thành phần một.

Mật mã công khai

Ta đã biết rằng, mật mã truyền thống dùng một cặp khóa mã giống nhau cho hai bên để mã hóa tài liệu (nên còn gọi là hệ mã đối xứng). Hệ mã này không thể triển khai trên mạng bởi tính phức tạp của quá trình phân phối khóa. Khoa học mã khóa công khai bắt đầu từ 1976. Nó đã được phát triển để khắc phục những thiếu sót của các kỹ thuật mã hóa trước đây - đó là yêu cầu về phân phối khóa mật trước đó để các nhóm có cùng khóa mã. Với mật mã khóa công khai, mỗi thành viên có hai khóa: một khóa công khai và một khóa riêng bí mật. Văn bản bất kỳ được mã bằng khóa công khai có thể được giải mã bằng khóa riêng. Khóa riêng này chỉ

người nhận có và không thể suy được khóa riêng về mặt tính toán từ khóa công khai. Nếu *A* muốn gửi thông báo bí mật cho *B*, anh ta lấy khóa công khai của *B* mã thông báo đó. Chỉ có *B* có khóa riêng của mình mới giải mã được thông báo và nhận được văn bản gốc. Đặc điểm quan trọng nhất của mật mã khóa công khai là không cần giữ bí mật khóa công khai (do đó giảm nhẹ vấn đề phân phối khóa). Tuy nhiên, thời gian thực hiện mật mã khóa công khai so với mật mã đối xứng rất lớn nên hai hệ thống này thường được kết hợp với nhau, trong đó hệ mật mã khóa công khai thường được đảm trách công việc phân phối khóa mã, nhận có và không thể suy được

Chữ ký điện tử

Chữ ký điện tử hay chữ ký số là thành phần quan trọng trong thương mại điện tử. Thực chất nó là một khối ký tự gắn kèm theo bản thông báo cần gửi đi. Nhờ có nó, người nhận sẽ biết và có thể chứng minh được thông báo đó do ai gửi đi và anh ta có thể chắc chắn về tính toàn vẹn của nó song anh ta không thể làm giả được bản thông báo đã ký. Với khả năng này, chữ ký điện tử, (khi được luật pháp thừa nhận) sẽ là phương tiện hữu hiệu đảm bảo về mặt pháp lý cho các hợp đồng, các giao dịch trên mạng. Một phương án tạo chữ ký điện tử là dựa trên mật mã khóa công khai. Nó cho phép tạo ra các chữ ký số không thể giả mạo được. Chúng là sự đảo ngược thông minh sơ đồ mã/giải mã bằng khóa công khai. Các thông báo dữ liệu mã hóa bằng khóa riêng và chúng chỉ có thể giải mã được bằng khóa công khai.

Chứng chỉ và cơ quan cấp chứng chỉ (CA)

Trong thế giới có hàng ngàn máy chủ Web và hàng triệu người sử dụng, ta không thể biết khóa công khai của tất cả mọi người trong cơ sở dữ liệu trên đĩa cứng. Ta không thể hỏi người nhận về khóa công khai của họ trước khi gửi thông điệp an toàn vì không có gì bảo đảm rằng người ở đầu nối bên kia là ai và đó có đúng là người mà ta nghĩ không. Một giải pháp cho vấn đề này là đưa vào cơ quan có thẩm quyền chứng thực (Certifying Authorities - viết tắt là CA) hay cơ quan cấp chứng chỉ (nhóm thứ ba tín nhiệm). Cơ quan này có nhiệm vụ bảo đảm chứng thực danh tính của các cá nhân và các tổ chức.

Thay vì giữ các khóa công khai của mọi người trên đĩa cứng, bạn giữ các khóa công khai của một vài CA tín nhiệm hoặc nổi tiếng. Trước khi gửi thông báo tới ai đó, ta yêu cầu họ đưa cho mình "chứng chỉ" hay chứng nhận số được CA ký nhận. Nội dung của chứng nhận số gồm danh tính của người chủ sở hữu khóa công khai, bản thân khóa công khai cùng thời hạn của khóa đó. Toàn bộ thông tin này lại được ký nhận bởi khóa mật của chính CA. Nhờ CA, bạn có thể xác minh danh tính của người nhận và tìm được khóa công khai của người đó.

Chứng nhận số không thể giả mạo và làm giả được. Hệ thống làm việc như sau:

- Tạo một cặp khóa công khai/khóa riêng.
- Giữ khóa riêng và gửi khóa công khai

tới CA cùng với thông tin về danh tính ở dạng "yêu cầu chứng thực".

- Trả tiền lệ phí cho CA.
- CA lúc đó sẽ xác minh xem bạn có đúng là người mà bạn khai báo không
- Nếu mọi thứ đã được kiểm tra, CA sẽ tạo ra một chứng thực chứa khóa công khai của bạn cùng với thông tin về danh tính. Nếu là chứng thực dùng trên bộ trình duyệt Web, nó sẽ chứa tên, địa chỉ thư điện tử của bạn. Chứng thực dùng bởi Web Server sẽ chứa home URL của Web Site.
- CA sẽ tạo ra một bản tóm lược thông báo từ chứng thực và ký hiệu hàm băm cùng với khóa riêng, tạo nên một chứng thực đã ký. Lúc đó họ sẽ trả chứng thực đã ký cho bạn.

Trước khi bạn gửi cho ai đó một bản thông báo mật, bạn yêu cầu họ gửi chứng thực đã ký. Bạn giải mã cùng với khóa công khai của CA để xác minh rằng, khóa công khai, tên và các thông tin định danh khác đã không bị sửa đổi từ khi chứng thực được ký. Bạn có thể dùng khóa công khai để gửi thông báo với sự tin cậy rằng nó là khóa đúng.

CA và các chứng thực đã ký là thành phần cơ bản của hệ thống phân phối khóa công khai hay cơ sở hạ tầng khóa công khai. Rất nhiều chứng thực được dùng với các mục đích khác nhau: xác thực Web Server được gọi là chứng thực site, để xác thực cá nhân người dùng gọi là chứng thực cá nhân, những cái được các công ty phần mềm sử dụng để ký những phần mềm thực hiện gọi là "chứng thực phát hành phần mềm". Dĩ nhiên, có những chứng thực nắm giữ các khóa công khai của CA gọi là "xác nhận chứng thực của người có thẩm quyền". Tuy có các mục tiêu sử dụng khác nhau nhưng tất cả chúng đều có chung khuôn dạng theo chuẩn X.509.

Thời hạn chứng thực và thu hồi chứng thực

Các khóa công khai không tồn tại mãi. Có một số tình huống làm mất giá trị của cặp khóa công khai/khóa riêng: bao gồm sự mất mát hay hỏng khóa riêng, sự thay đổi về thông tin danh tính chứa trong chứng thực và sự thỏa hiệp (dễ tổn thương) của chính bản thân khóa riêng của CA. Khi bất kỳ sự cố nào kể trên xảy ra, chứng thực bị tác động sẽ được hủy bỏ để không sử dụng nó nữa. Một thành phần cơ bản nữa của hạ tầng cơ sở khóa công khai là "danh sách hủy bỏ chứng thực" (certification revocation list - CRL), một cơ sở dữ liệu sắp xếp giữ các số hiệu nhận diện cá nhân (ID) của tất cả các chứng thực đã mất hiệu lực. Về lý thuyết, bất kỳ ai muốn gửi một thông báo cần kiểm tra khóa công khai của người nhận trong CRL trước khi gửi thông báo.

Thực tế, điều này không xảy ra trên Internet vì tính không thực tiễn của việc giữ cơ sở dữ liệu CRL. Với sự loại bỏ các chứng thực công bố phần mềm và một số intranet, không ai giữ CRL có thể truy nhập tới. Thay vào đó, tất cả các chứng thực đều có thời hạn, điển hình khoảng một năm từ ngày được phát hành. Nếu ai đó đưa ra một chứng thực đã hết hiệu lực, phần mềm sẽ kiểm tra tính hợp lệ của nó và sẽ biết điều đó. Như vậy, trách nhiệm chính của CRL là theo dõi các chứng chỉ/khóa đã được

phát hành...

Trên thực tế, các hạ tầng công nghệ và các dịch vụ do các cơ quan có thẩm quyền xây dựng, cung cấp và quản lý. Phía người dùng chỉ cần biết tới các cơ quan cấp chứng chỉ (CA), sau khi đăng ký và được cấp chứng chỉ, họ sẽ sử dụng các dịch vụ (mật mã, chữ ký số...) dựa trên các thông số có trên chứng chỉ đó để phục vụ cho công việc của mình... *Xem* public key cryptography, digital signature, CA.

Plague ***virut Plague*** Trong an toàn máy tính, một virut lây nhiễm vào các tệp COM và EXE. *Xem* virus names.

plaintext ***bản rõ, bản gốc*** (1) Trong mật mã, một thông tin không được mã hóa. *So sánh với* ciphertext. (2) Trong mật mã, văn bản hiểu được hoặc các ký hiệu có nghĩa và có thể được đọc mà không cần áp dụng sự giải mã bất kỳ. *Xem* decrypt. *Đồng nghĩa với* clear data, cleartext.

plaintext ciphertext avalanche ***thác rõ mã*** Trong mật mã, một đặc tính của một mã pháp trong đó sự thay đổi của một bit trong bản rõ sẽ gây ra một thay đổi toàn bộ trong bản mã tương ứng. *So sánh với* key ciphertext avalanche. *Xem* ciphertext, cryptographic key, plaintext.

planted record ***bản ghi cắm*** Trong an toàn cơ sở dữ liệu, một kiểu tấn công trong đó, các bản ghi bản rõ được thêm vào một cơ sở dữ liệu được mã hóa và các thay đổi xảy ra sau đó trong các nội dung cơ sở dữ liệu sẽ cung cấp các chi tiết về cặp bản rõ - mã. *Xem* chosen plaintext.

Plastique ***virut Plastique*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào các tệp COMMAND.COM và COM, EXE và OVL, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy các tệp chương trình, các tệp dữ liệu và OVL. *Xem* virus names.

plug compatible manufacturer ***nhà sản xuất tương hợp giắc cắm, nhà sản xuất tương thích phích cắm*** Một nhà sản xuất cung cấp thiết bị có thể hoạt động kết hợp với thiết bị của người sản xuất khác khi được kết nối bằng ổ cắm và dây cáp. Đây là một thuật ngữ được sử dụng phổ biến trong kết nối với thiết bị IBM.

POB ***điểm thanh toán ngân hàng, điểm POB*** Viết tắt của Point of Bank. *So sánh với* POS.

pocket banking ***thẻ ngân hàng, ngân hàng bỏ túi*** *Xem* supersmart card.

Pohlig-Hellman cipher ***mã pháp Pohlig-Hellman*** Trong mật mã, một mã pháp có sự tương tự với RSA nhưng không thích hợp cho mật mã khóa công khai vì khóa giải mã có thể dễ dàng tính được từ khóa mã.

Với mã pháp này, một số nguyên tố lớn n được chọn và phép toán số học được thực hiện trong trường Galois $GF(n)$. Một khóa mã E được chọn sao cho nó nhỏ hơn n. Phép mã hóa được thực hiện theo một cách tương tự như RSA, nghĩa là, bản mã C được tạo ra bằng cách lấy mũ một khối thông báo rõ M:

$C \equiv M^E \pmod{n}$.

So sánh với RSA. *Xem* Euler's generalization, Euler totient function,

Galois field, known plaintext, prime number, public key cryptography.

pointer *con trỏ* Trong tính toán, một biến lưu giữ địa chỉ của một mục dữ liệu. Trong một danh sánh móc nối đơn giản, một con trỏ sẽ lưu giữ địa chỉ của mục kế tiếp trong danh sách.

point of sale *điểm cuối bán hàng, điểm trả tiền* Trong hoạt động ngân hàng, một vị trí tại đó một khách hàng thanh toán các hóa đơn hoặc các dịch vụ. *Xem* point-of-sale terminal.

point-of-sale terminal *thiết bị đầu cuối tại điểm trả tiền, đầu cuối POS* Trong hoạt động ngân hàng, một thiết bị đầu cuối được sử dụng tại nơi thực hiện hoạt động giao dịch của khách hàng, và được thiết kế riêng các chức năng đầu vào đặc biệt. Trong nhiều trường hợp, chúng được điều hành bởi nhân viên không thông thạo thao tác và có các phương tiện để đọc dữ liệu trực tiếp, ví dụ như tự động đọc các nhãn hàng hóa được mã hoặc các mã vạch. Các thiết bị đầu cuối phức tạp hơn có thể được liên kết với ngân hàng của khách hàng để tự động thanh toán khoản nợ. *Xem* electronic funds transfer point of sale.

point protection *bảo vệ theo điểm, điểm bảo vệ* Trong an toàn vật lý, điều này gắn liền với một cảm biến hoặc một nhóm các cảm biến được sử dụng để giám sát, hoặc phát hiện sự xâm nhập vào một vùng nhỏ. *So sánh với* line sensor.

point-to-point *điểm tới điểm, điểm nối điểm* (1) Trong quản lý khóa, một sắp xếp trong đó một cặp truyền thông chia sẻ một khóa mã khóa, hoặc một khóa để mã một cặp khóa, có khả năng trao đổi các khóa dữ liệu hoặc khóa mã khóa sau nữa. Ít nhất một trong số các bên phải có khả năng tạo ra hoặc thu được các khóa. *So sánh với* key distribution center, key translation center. *Xem* ANSI X9.17 - 1985, communicating pair, cryptographic key, data key, key encrypting key, key encrypting key pair, point-to-point environment. (2) Trong truyền thông, nói tới sự kết nối giữa hai, và chỉ hai thiết bị đầu cuối được cài đặt. Việc kết nối có thể gồm cả các thiết bị chuyển mạch. *So sánh với* broadcast, multicast, multidrop circuit.

point-to-point environment *môi trường điểm tới điểm* Trong việc quản lý khóa, môi trường điểm tới điểm tồn tại khi mỗi thành viên của một cặp truyền thông có một khóa công khai cùng với khóa bí mật kết hợp của nó, và giấy chứng thực khóa công khai này do một người có thẩm quyền chứng nhận đưa ra, vì vậy có thể trao đổi các khóa dữ liệu đối xứng. Ít nhất một thành viên cặp truyền thông cần có các khả năng tạo ra hoặc bằng cách khác thu được các khóa đối xứng. *Xem* certificate, certification authority, point-to-point, public key, secret key, symmetric key system.

Poisson distribution *phân bố Poisson* Trong toán học, một phân phối xác suất thích hợp với các dòng lưu lượng trong các hệ thống tính toán và truyền thông. Nó được sử dụng để ước lượng kích cỡ và thời gian chờ đợi của các hàng đợi các hệ thống dịch vụ

trong đó, các tỷ lệ đến và tỷ lệ dịch vụ có đặc tính thống kê nhất định nào đó. *So sánh với* Gaussian distribution.

polarized return to zero ***trả về số không có phân cực*** Trong truyền thông, một phương pháp báo hiệu với 3 trạng thái, các tín hiệu dương và âm biểu diễn mỗi một trạng thái nhị phân còn trạng thái nằm ngang trả về điện áp 0 giữa các tín hiệu. *Xem* bit.

police connect ***nối tới cảnh sát*** Trong an toàn vật lý, nói tới một hệ thống báo động được nối với một trạm cảnh sát. *Xem* central station.

police station unit ***thiết bị trạm cảnh sát*** Trong an toàn vật lý, một bộ nhận báo động có thể cài đặt tại một trạm cảnh sát để nhận tín hiệu báo động từ một vùng được bảo vệ. *Xem* police connect.

policy ***chính sách, quy tắc*** Trong an toàn thông tin, một ngôn ngữ tự nhiên chung chung, phi hình thức mô tả hành vi của hệ thống mong muốn. Các chính sách có thể được xác định cho các yêu cầu đặc biệt như an toàn, tính toàn vẹn và tính sẵn sàng. *So sánh với* corporate security policy. *Xem* security policy.

Polimer ***virut Polimer*** Trong an toàn máy tính, một virut lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy các tệp chương trình và các tệp OVL và tệp dữ liệu. *Xem* virus names.

Polish-2 ***virut Polish 2*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy các tệp chương trình và các tệp OVL và tệp dữ liệu. *Xem* virus names.

Polish 217 ***virut Polish 217*** Trong an toàn máy tính, một virut lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng thao tác trong thời điểm thực hiện, phá hủy các tệp chương trình và các tệp OVL và tệp dữ liệu. *Xem* virus names.

polling ***kiểm soát hỏi vòng*** Trong truyền thông dữ liệu, một phương pháp kiểm soát các thiết bị đầu cuối trên một mạng đa điểm hoặc mạng dữ liệu nhóm, tại đây mỗi thiết bị đầu cuối được máy tính hỏi quay vòng để quyết định khi nào thì sẵn sàng nhận hoặc gửi dữ liệu. Việc truyền dữ liệu chỉ được bắt đầu bởi máy tính. *Xem* cluster, hub polling, multidrop circuit, roll call polling.

polling list ***danh sách hỏi vòng, danh sách hỏi lần lượt*** Trong tính toán, một danh sách xác định trình tự của các thiết bị đầu cuối sẽ được hỏi vòng. *Xem* polling.

polling overhead ***thời gian tốn thêm cho hỏi vòng*** Trong tin học, thời gian máy tính tốn cho việc hỏi vòng các thiết bị đầu cuối. *Xem* polling.

polyalphabetic cipher ***mã đa biểu*** Trong mật mã, đây là một mã pháp thay thế, mã này dùng một nhóm các mã trong bảng chữ cái đơn. Một khóa mật mã được ghi lặp trên bản rõ và chữ cái khóa sẽ chỉ ra mã đơn biểu cụ thể nào được dùng để mã hóa chữ cái tương ứng trong bản rõ. *So sánh với* monoalphabetic cipher. *Xem* cipher,

cryptography, substitution cipher.

polyinstantiation ***nhiều thể hiện*** Trong an toàn dữ liệu, sự tồn tại đồng thời nhiều đối tượng dữ liệu có cùng một tên, dẫn đến phân biệt chúng bằng cách phân loại. Nhiều thể hiện có thể nảy sinh trong các cơ sở dữ liệu quan hệ nhiều mức. Nếu một mục vào trong một bảng có phân loại tối mật, và một người sử dụng với mức an toàn mật truy nhập bảng này, thì sẽ nhận lại được một bảng nhập trống (NULL) đối lập với mục tối mật. Người sử dụng không có cách nào để phân biệt giữa một mục vào có giá trị NULL thực với một mục vào được sinh ra từ sự hiện diện của một mục vào được phân loại cao hơn. Như vậy, nếu người sử dụng đang nói tới quyết định chèn thêm mục được phân loại mật vào vị trí đó trong bảng, thì mục nhập vào phải được và phải được người dùng tìm thấy trong các truy nhập sau đó. Một người sử dụng có mức truy nhập tối mật sẽ tìm ra được sau đó 2 mục tương phản với mục vào của bảng đó, một là mật và một là tối mật. *Xem* multilevel database security, relational database.

polynomial code ***mã đa thức*** Trong các mã, một mã phát hiện lỗi trong đó một phép toán học được thực hiện trên dữ liệu cần gửi đi và được lặp lại tại điểm nhận cuối; sau đó một kiểm tra được thực hiện để phát hiện bất kỳ sự sai lạc dữ liệu nào trong khi truyền hoặc di chuyển. Đặc biệt, tổng số thu được từ phép tính tổng các số nhị phân, tương ứng với các mẫu bit của các ký tự được truyền, được chia cho một hằng số xác định mã. Số dư được truyền đi như một ký tự kiểm tra theo chu kỳ ở cuối thông báo. Tại trạm nhận, tổng số sau đó được tính toán như trên cùng với ký tự kiểm tra theo chu kỳ được thêm vào. Nếu phép chia cho cùng một hằng số (được lựa chọn tùy ý) được thực hiện và phần dư là 0, thì thông báo coi như hủy bỏ. *Xem* cyclic redundancy check, error detection code.

polynomial time ***thời gian đa thức*** *Xem* time and space requirement.

port ***cổng*** Trong tính toán, một đơn vị chức năng của một nút qua nó dữ liệu có thể ra khỏi hoặc nhập vào một mạng dữ liệu hoặc một máy tính. *Xem* node, port protection device.

portability ***tính cơ động, tính linh hoạt, tính khả chuyển*** Trong tính toán, nói tới các chương trình ở dạng mà có thể cho phép chúng được chạy trên nhiều hơn một hệ thống máy tính.

portable detector system ***hệ thống phát hiện cơ động*** Trong an toàn vật lý, một hệ thống phát hiện đầy đủ có thể chuyển dịch dễ dàng, thường có các dự phòng một thiết bị báo động cục bộ, các đường dây báo động và các bộ phận điều chỉnh tự động hoặc thủ công. *Xem* alarm line.

portable duress sensor ***bộ cảm biến (bắt buộc) xách tay*** Trong an toàn vật lý, một cảm biến được một cá nhân mang theo, nó được kích hoạt bằng tay hoặc tự động trong trường hợp khẩn cấp hoặc ép buộc. Hoạt động tự động này có thể được khởi đầu bởi cảm biến ở vị trí nằm ngang nhiều hơn một khoảng thời gian xác định. Cảm biến mang một tần số vô tuyến hoặc đầu

phát siêu âm báo hiệu cho một trạm giám sát báo động trung tâm thông qua một máy thu cục bộ. *Xem* duress alarm.

portfolio ***danh mục đầu tư*** Trong hoạt động ngân hàng, một nhóm các sản phẩm thuộc nhóm các bên đối tác, được mở rộng bởi ngân hàng hoặc bộ phận ngân hàng. *Xem* counterparty, counterparty group, product.

port protection device ***thiết bị bảo vệ cổng*** Trong an toàn máy tính, một thiết bị được kết nối với các cổng truyền thông của một máy chủ, nó có chức năng cho phép người sử dụng truy nhập vào cổng.

Thiết bị bảo vệ cổng (PPD) có thể hoạt động giữa máy chủ và modem, hoặc giữa modem và máy điện thoại. Các PPD có tới 4 tính năng điển hình:

- các bảng mật khẩu;
- gọi lại cho người bắt đầu;
- ngụy trang;
- chống lại đánh dấu và đăng nhập.

Tất cả các PPD yêu cầu người sử dụng nhập các mật khẩu để truy nhập vào cổng quay số. Các mật khẩu này được bổ sung để tự đăng nhập vào chính máy tính, các PPD hạn chế số lần thử mật khẩu trên mỗi kết nối qua điện thoại. Với đặc tính gọi lại cho người bắt đầu, người sử dụng được yêu cầu nhập vào một mật khẩu, một bảng PPD được tìm kiếm để xác định số điện thoại của người sử dụng tương ứng với mật khẩu được nhập vào, cuộc gọi bị hủy kết nối và PPD gọi lại cho người sử dụng. Tuy nhiên, phương tiện này có thể bị tấn công: nếu một kẻ xâm nhập trái phép có thể lừa PPD rơi vào tình huống ngắt đường dây thì cuộc gọi sẽ bị cản trở. Hơn nữa, nếu PPD dự phòng một tập hợp các đường chỉ dành riêng cho cuộc gọi lại, thì một kẻ thâm nhập có thể giữ trước (cuộc gọi khi đường dây đang bận) một trong các đường một cách đơn giản, với một tín hiệu chuông thích hợp, và chặn lấy cuộc gọi lại dành cho một người sử dụng hợp lệ.

Nếu PPD được kết nối giữa máy điện thoại và modem thì nó có thể ngụy trang máy tính bằng cách đáp lại các cuộc gọi bằng một tiếng nói tổng hợp của con người (nhân tạo). Với một PPD được kết nối giữa modem và máy tính thì việc ngụy trang được tạo ra bằng một màn hình, khác hoàn toàn với màn hình máy tính. Các phương tiện báo tấn công và đăng nhập tạo ra các tín hiệu báo động và các bản ghi về các cuộc thử tấn công quay số. *Xem* attack signalling, call back, telephone intrusion.

POS ***điểm POS*** *So sánh với* POB. *Xem* point-of-sale terminal.

positive noninterfering and succession coded station ***trạm báo hỏa được mã liên tiếp và không can thiệp*** Trong an toàn vật lý, một trạm báo hỏa mà khi được kích hoạt, nó sẽ phát đi ít nhất 3 lượt các tín hiệu báo động đã được mã mà không có sự can thiệp nào từ phía các trạm khác trên một vòng khép kín. Một hoặc nhiều trạm này, nếu bị kích hoạt sau đó, sẽ phát đi ít nhất 3 lượt tín hiệu được mã hóa của chúng mà không có sự can thiệp nào từ phía các trạm khác và từ phía trạm bị kích hoạt đầu tiên. *Xem* coded system, alarm station, local noninterfering coded station.

positive response ***đáp ứng xác thực, đáp ứng dữ liệu đã nhận đủ*** Trong truyền dữ liệu, một đáp ứng chỉ ra rằng, một thông báo đã được nhận thành công. *Xem* acknowledgement.

postcondition ***điều kiện sau*** Trong tính toán, một sự xác nhận, được biểu thị theo các giá trị của các biến chương trình, hoặc mối quan hệ giữa chúng, nó đặc trưng hóa trạng thái của một chương trình ngay sau khi thi hành một tập các lệnh cho trước. Một chương trình được cho là đúng hoàn toàn nếu nó khởi đầu trong một trạng thái tương ứng với điều kiện trước và chấm dứt trong một trạng thái tương ứng với điều kiện sau. *So sánh với* precondition. *Xem* proof of program correctness.

posting date ***ngày chuyển*** *Đồng nghĩa với* entry date.

Post Telegraph and Telephone ***công ty bưu điện, điện thoại và điện báo, công ty bưu chính viễn thông*** Một công ty truyền thông công cộng chịu sự điều khiển của nhà nước bên ngoài USA. *Xem* common carrier.

postulated threat ***hiểm họa giả định*** Trong an toàn máy tính, các cách mà thông qua chúng các khả năng hoặc ý định theo giả thiết, được suy luận ra từ các điều kiện liên quan hoặc bằng cớ, hiểm họa ảnh hưởng bất lợi cho một hệ thống trang thiết bị, hoặc các thao tác tự động hóa. *Xem* threat.

potential vulnerability ***điểm yếu tiềm ẩn, khả năng bị tấn công tiềm ẩn*** Trong an toàn thông tin, một điểm dễ bị tấn công bị nghi ngờ có thể được sử dụng để làm hỏng mục tiêu an toàn của một đích đánh giá, nhưng khả năng bị lợi dụng hay sự tồn tại của nó vẫn chưa chứng minh được. *So sánh với* construction vulnerability, exploitable vulnerability, operational vulnerability. *xem* information technology security evaluation criteria, vulnerability.

power ***lũy thừa*** Trong toán học, số lần mà một đại lượng được nhân với chính nó. *Xem* exponent.

power restart ***khởi động lại nguồn*** Trong lĩnh vực độ tin cậy, một phương tiện phát hiện sự giảm sút trong điện áp nguồn và bắt đầu một thủ tục ngắt cho phép máy tính tự chuẩn bị cho sự mất nguồn. Chương trình có thể được bắt đầu lại mà không bị lỗi khi nguồn được phục hồi lại.

PPD *Xem* port protection device.

PPL *Xem* preferred products list.

PPM *Xem* pulse position modulation.

pre-alarm ***báo động trước*** (1) Trong an toàn vật lý, một báo động nghe thấy được kích hoạt trong các hệ thống có các mạch trễ vào/ra để cảnh báo cho người sử dụng biết rằng, báo động phải được tháo gỡ trong một khoảng thời gian xác định. Nếu báo động không được tháo gỡ thì một tín hiệu sẽ được gửi đến một trạm trung tâm. *Xem* delay circuit. (2) Trong an toàn máy tính, một báo động dùng để cảnh báo cho nhân viên an ninh về một trang thiết bị hư hỏng.

precondition ***điều kiện trước, điều kiện dẫn*** Trong tính toán, một sự xác nhận, được biểu diễn theo các giá trị của các biến chương trình, hoặc mối

quan hệ giữa chúng, mà đặc trưng hóa cho trạng thái của một chương trình ngay trước khi thi hành một tập các lệnh cho trước. Một chương trình được cho là đúng hoàn toàn nếu nó khởi đầu trong một trạng thái tương ứng với điều kiện trước và chấm dứt trong một trạng thái tương ứng với điều kiện sau. *So sánh với* postcondition. *Xem* proof of program correctness.

predicate ***(câu lệnh) vị ngữ*** (1) Trong toán học, một câu lệnh logic được thực hiện đối với một trạng thái nào đó, nghĩa là nó chỉ có thể thừa nhận các giá trị đúng hoặc sai. (2) Trong các cơ sở dữ liệu, một số hạng của một biểu thức tính quan hệ chỉ rõ điều kiện cần được thỏa mãn bởi các số hạng trong tập hợp được tìm kiếm. *Xem* relational calculus, relational database.

predicate transformer ***trình biến đổi vị ngữ*** Trong tính toán, một tập các lệnh làm biến đổi điều kiện trước thành điều kiện sau. *Xem* postcondition, precondition, proof of program correctness.

Preferred Products List ***danh sách sản phẩm ưu tiên*** Một danh sách do Hoa Kỳ đưa ra bao gồm các hệ thống viễn thông, hệ thống xử lý thông tin và các trang thiết bị phù hợp với dạng trước đó chấp thuận đo theo chuẩn tiêu chuẩn quốc gia Tempest. *So sánh với* Endorsed Tempest Products List, Evaluated Produces List. *Xem* Tempest.

prefix ***mã tiền tố*** Trong truyền thông, một mã tại điểm bắt đầu của một thông báo.

presence detector ***bộ phát hiện sự có mặt*** *Đồng nghĩa với* motion detector.

presentation layer ***tầng biểu diễn*** Trong truyền thông dữ liệu, một tầng trong mô hình tham chiếu kết nối các hệ thống mở ISO. Không giống như các tầng thấp hơn, tầng này quan tâm đến cú pháp và ngữ nghĩa của các thông báo được điều khiển. Nó bao gồm các dịch vụ thường được yêu cầu bởi hàng loạt những người sử dụng và do đó có thể làm giảm bớt những người sử dụng này trong việc cung cấp các dịch vụ có tính riêng tư. Như vậy, nó thực hiện các chuyển đổi hữu ích nói chung, chẳng hạn như nén văn bản. *So sánh với* application layer, data link layer, network layer, physical layer, session layer, transport layer. *Xem* intelligent terminal, open systems interconnection, text compression.

presignal system ***hệ thống báo trước*** Trong an toàn vật lý, một hệ thống trong đó nhân viên then chốt được thông báo khi hoạt động đầu tiên của trạm báo hỏa nhân công hoặc một bộ phát hiện báo động tự động chỉ kích hoạt một nhóm xác định trước các bộ chỉ báo báo động. *Xem* chime, alarm station.

preventive maintenance ***bảo trì phòng ngừa*** Trong lĩnh vực độ tin cậy, đây là một thủ tục kiểm tra thường xuyên trang thiết bị và thay thế các phần phụ để giảm tối thiểu các khả năng hỏng hóc xảy ra cho trang thiết bị. *So sánh với* corrective maintenance.

primary account information ***thông tin về tài khoản gốc*** Trong hoạt

động ngân hàng, dữ liệu tại một cơ quan tài chính, dùng để nhận dạng một cá nhân và gắn kết cá nhân này với các tài khoản. *Xem* financial institution, primary account number.

primary account number ***số tài khoản gốc, PAN*** Trong hoạt động ngân hàng, PAN gồm số định danh của bộ phận phát hành và nhận dạng bộ phận phát hành mã giao dịch cần chuyển tới. Tiếp theo là số tài khoản, nó nhận dạng người cần được thực hiện giao dịch. Phần tử cuối cùng là một chữ số kiểm tra.

primary key ***khóa chính*** (1) Trong các cơ sở dữ liệu, một khóa nhận dạng duy nhất một thực thể. *So sánh với* secondary key. *Xem* entity, candidate key. (2) Trong việc quản lý khóa, một khóa được sử dụng trong mã hóa/giải mã dữ liệu. *So sánh với* secondary key. *Đồng nghĩa với* data-encrypting key.

primary station ***trạm chính*** Trong truyền thông dữ liệu, một trạm trên một liên kết dữ liệu có quyền chọn lựa trạm thứ hai để gửi một thông báo. Tại một thời điểm bất kỳ chỉ có một trạm chính trên một liên kết dữ liệu. Trạng thái này chỉ tạm thời, nó được cấp cho một trạm để có thể gửi một thông báo. *So sánh với* secondary station.

prime attribute ***thuộc tính cơ sở*** Trong các cơ sở dữ liệu, một thuộc tính của một cơ sở dữ liệu quan hệ, là một thành phần có ít nhất một khóa dự bị. *Xem* attribute, candidate key, relational database.

prime number ***số nguyên tố*** Trong toán học, một số không thể được tạo ra bằng cách nhân các số nguyên (trừ chính số đó và 1). Việc nghiên cứu những số này rất quan trọng trong một số khía cạnh của mật mã khóa công khai. *Xem* public key cryptography, RSA.

primitive ***đơn vị nguyên thủy*** Một đơn vị cơ bản hoặc chủ yếu.

primitive root ***căn nguyên thủy*** Trong toán học, một số nguyên m trong số học modulo n mà bậc của m bằng $n - 1$. *Xem* modulo arithmetic, order.

principal ***chủ sự*** Trong an toàn thông tin, một người hoặc hệ thống có thể được phép truy nhập các đối tượng hoặc có thể thực hiện các lệnh tác động đến các quyết định kiểm soát truy nhập. *Đồng nghĩa với* subject.

principle of closed environment ***nguyên tắc môi trường kín*** *Xem* closed environment, principles of secure systems.

principle of complete mediation ***nguyên tắc dàn xếp hoàn toàn*** *Xem* principles of secure systems.

principle of least common mechanism ***nguyên tắc cơ chế chung tối thiểu*** *Xem* principles of secure systems.

principle of least privilege ***nguyên tắc đặc quyền tối thiểu*** (1) Trong an toàn máy tính, nguyên tắc yêu cầu mỗi chủ thể trong một hệ thống được cung cấp tập hạn chế nhất các nguyên tắc (hoặc mức truy nhập thấp nhất) để thực thi các nhiệm vụ cho phép. Việc ứng dụng nguyên tắc này hạn chế được thiệt hại do ngẫu nhiên, do lỗi hoặc sử dụng bất hợp pháp. *Xem* principles of

secure systems, subject. (2) Trong an toàn máy tính, việc cung cấp quyền truy nhập tối thiểu cần thiết để thực thi các nhiệm vụ được yêu cầu. *Xem* access, authorization, need to know, principles of secure systems.

principle of secure systems ***nguyên tắc về các hệ thống an toàn*** Trong an toàn máy tính, Saltzer và Schroeder đã đề ra các nguyên tắc của hệ thống an toàn được liệt kê dưới đây:

- Tính đơn giản - tính đúng đắn của các biện pháp an toàn, được kết hợp trong phần cứng và phần mềm, có thể được kiểm tra dễ dàng hơn nếu các biện pháp này đơn giản và nhỏ gọn.
- Dự phòng an toàn - các sự cố truy nhập cần yêu cầu quyền cho phép một cách dứt khoát, nghĩa là trạng thái ngầm định là không truy nhập.
- Dàn xếp hoàn toàn - việc kiểm tra truy nhập dựa vào thông tin kiểm soát truy nhập, phải được thực hiện dưới tất cả các trường hợp bao gồm hoạt động bình thường, duy trì, khôi phục...
- Tách bạch đặc quyền - triết lý hai khóa, với mỗi một khóa được đặt tại một bộ phận riêng rẽ, sẽ đảm bảo rằng một sự cố đơn lẻ không dẫn đến việc mất an toàn.
- Đặc quyền tối thiểu - mọi quá trình cần hoạt động ở mức đặc quyền tối thiểu cần thiết để thực hiện nhiệm vụ đòi hỏi.
- Cơ chế ít chung nhất - việc sử dụng các cơ chế được chia sẻ giữa những người sử dụng cần được hạn chế tối thiểu vì an toàn chung của họ.
- Chấp nhận được đối với người dùng - các biện pháp an toàn không được gây trở ngại quá mức cho công việc của người sử dụng, tất nhiên, song vẫn đáp ứng tất cả các ràng buộc cần thiết về an toàn.
- Kiểm soát công khai - các biện pháp an toàn cần sẵn sàng để các chuyên gia xem xét lại, ví dụ, các thuật toán mã hóa có thể được phổ biến rộng rãi, độ an toàn của chúng chỉ phụ thuộc vào độ mật của khóa mã.

Xem complete mediation, cryptographic key, fail safe, least common mechanism, nonsecret design, least privilege, separation of privilege, simplicity, user acceptability.

printed circuit board ***bo mạch in*** Trong tính toán, một bảng làm bằng chất dẻo nhờ đó các thành phần điện như các điện trở, các tụ điện, và các mạch tích hợp được lắp ghép và được liên thông qua đường dẫn bằng lá được mạ kim loại hoặc khắc ăn mòn. Các bảng mạch in được sử dụng như các modun được cắm vào trong các máy vi tính. *Xem* expansion card, integrated circuit. *Đồng nghĩa với* circuit board.

Print Screen ***virut Print Screen*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào đĩa mềm và cung khởi động của đĩa cứng, làm hỏng cung khởi động và các tệp dữ liệu, ảnh hưởng thao tác trong thời điểm thực hiện. *Xem* virus names.

print suppress ***chặn in*** Trong an toàn máy tính, để loại trừ việc in ra các ký tự để bảo đảm tính bí mật chúng; ví dụ, các ký tự trong một mật khẩu

khi nó được khóa bởi một người sử dụng nhập vào tại một thiết bị đầu cuối đầu vào. *Xem* password.

priority ***độ ưu tiên, thứ tự ưu tiên*** Trong tính toán, thứ hạng gắn liền với một tác vụ, quyết định quyền ưu tiên của nó trong việc nhận các nguồn tài nguyên của hệ thống.

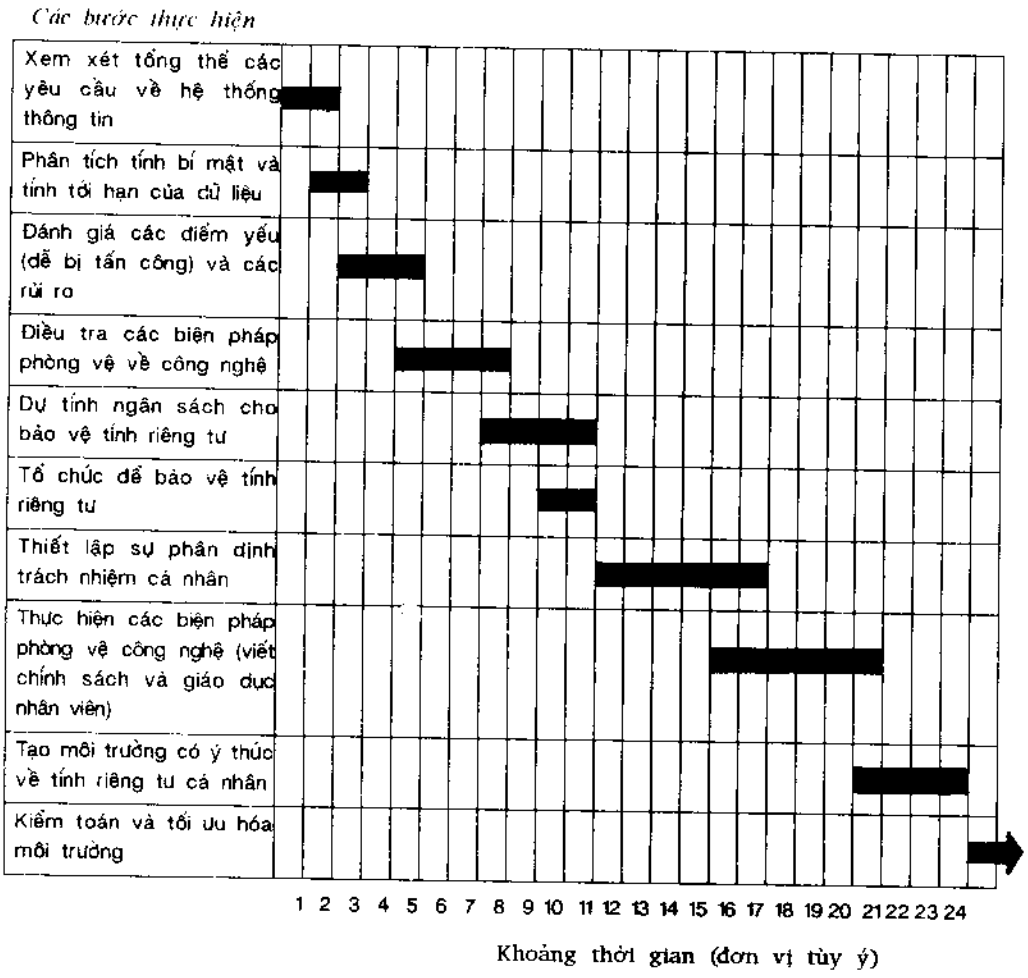
priority processing ***xử lý ưu tiên*** Trong tính toán, một phương pháp điều khiển một hệ thống máy tính, để trình tự các chương trình được xử lý được xác định hoàn toàn bởi một hệ thống các ưu tiên.

priority scheduler ***bộ lập biểu ưu tiên, bộ sắp hàng ưu tiên*** Trong tính toán, một hệ thống mà sử dụng hàng đợi vào và ra trong lập lịch công việc của mình để cải thiện hiệu năng tổng thể.

privacy ***(sự) riêng tư, (sự) bảo mật*** (1) Trong luật pháp, quyền của các cá nhân kiểm soát hoặc chi phối thông tin liên quan đến họ, thông tin này có thể được chọn lựa, lưu giữ và nó có thể bị lộ do họ và đến họ. *Xem* data protection. (2) Trong an toàn dữ liệu, quyền để quyết định tính an toàn thích hợp và định rõ những người sử dụng có quyền đối với thông tin hoặc các hệ thống. (3) Quyền tự quyết của một cá nhân về mức độ muốn chia sẻ thông tin về chính mình với các cá nhân khác, thông tin này có thể bị tổn thương bởi sự trao đổi không cho phép của các cá nhân hoặc các tổ chức khác. *Xem* compromise, data protection. (4) Quyền của các cá nhân và các tổ chức được kiểm soát việc thu thập, lưu giữ, và phổ biến các thông tin của họ hoặc thông tin về bản thân họ. (5) Trong an toàn dữ liệu, quyền của một cá nhân để thực hiện một dạng kiểm soát nào đó trên thông tin được lưu giữ về anh ta hoặc cô ta cũng như những nhân viên được phép truy nhập vào thông tin này. Nguyên nhân của sự quan tâm sâu sắc của nhiều cộng đồng, đặc biệt là do sự phát triển công nghệ tạo thuận tiện cho việc thu thập, liên kết và phân phối thông tin cá nhân nhạy cảm. Việc quản lý về mặt pháp lý đối với các hoạt động trên thay đổi đáng kể từ quốc gia này sang quốc gia khác. *Xem* data protection, privacy protection.

privacy Act 1974 ***đạo luật 1974 về tính riêng tư*** Trong luật pháp, một luật của Hoa Kỳ cho các cá nhân có được kiểm soát hoặc chi phối ở mức độ nào đó trong việc việc chọn lựa, lưu giữ và phổ biến dữ liệu cá nhân của họ. *Xem* personal data.

privacy enhanced mail ***dịch vụ thư điện tử an toàn*** Trong an toàn truyền thông, một dịch vụ tùy chọn tin cậy và toàn vẹn để chuyển thư tín điện tử trên mạng Internet. Theo X.400, dịch vụ là một phần của bộ phận người dùng (user agent) và trong suốt đối với hệ thống chuyển thông báo (MTS). Dịch vụ PEM gồm việc thêm phần tiêu đề vào thông báo người dùng, nó được MTS xử lý như phần khác của thông báo. Dịch vụ PEM kết hợp việc quản lý khóa tự động và sự toàn vẹn thông báo đầy đủ nhờ sử dụng các mã pháp đối xứng và không đối xứng và một cách tùy chọn, mã hóa chọn lựa sử dụng một mã pháp đối xứng. *Xem* asymmetric



privacy protection: *bảo vệ tính riêng tư.* Một kế hoạch bảo vệ tính riêng tư một cách tổng quát. Giống như tất cả các mục tiêu của tổ chức, tính riêng tư về thông tin không thể đạt được mà không có sự ủy quyền quản lý cao nhất đối với kế hoạch hành động xác định trước, với sự hỗ trợ của các nguồn tài nguyên thích hợp.

cipher, electronic mail security, key management, symmetric cipher, user agent, X.400.

privacy protection ***bảo vệ mật***

Trong an toàn máy tính, sự thiết lập các biện pháp bảo vệ hành chính, kỹ thuật, vật lý thích hợp để đảm bảo độ an toàn và tính bí mật của các bản ghi dữ liệu và để bảo vệ tính an toàn và sự bí mật khỏi các mối hiểm họa hoặc mối nguy hiểm bất kỳ được dự đoán trước mà có thể dẫn đến mối nguy hiểm to lớn, rắc rối, phiền phức hoặc sự bất công cho bất kỳ cá nhân nào mà những thông tin về họ được duy trì.

Xem confidentiality, data protection, security.

privacy transformation ***phép biến đổi mật*** *Đồng nghĩa với* encryption algorithm.

private address space ***không gian địa chỉ riêng*** Trong tính toán, một vùng địa chỉ của máy tính được gán cho một người sử dụng cụ thể. *Xem* address.

private automatic branch exchange ***tổng đài nhánh tự động riêng, tổng đài tự động nội bộ*** Trong truyền thông, một tổng đài điện tử nhánh tự động riêng.

private cryptography ***mật mã riêng*** Trong an toàn truyền thông, việc cung cấp mật mã không trong suốt đối với người sử dụng. Phép mã liên kết và mã nút trong suốt đối với người sử dụng, còn phép mã điểm tới điểm có thể trong suốt nếu nó được cung cấp tự động như dịch vụ hệ thống. *Xem* end-to-end encryption, link encryption, network encryption, node encryption, transparent.

private dial port ***cổng chọn số riêng*** Trong truyền dữ liệu, một cổng quay số của một mạng chuyển mạch gói, cung cấp một cổng truy nhập cho một khách hàng, với một số điện thoại không được liệt kê. *So sánh với* public dial port. *Xem* packet switching.

private key ***khóa riêng*** Trong mật mã, một khóa mã được sử dụng để giải mã, ký các thông báo trong mật mã khóa công khai. Khóa này được người sở hữu khóa giữ bí mật. *So sánh với* public key. *Xem* ciphertext, cryptographic key, digital signature, public key cryptography.

private key encryption ***phép mã khóa riêng*** *Đồng nghĩa với* secret key encryption.

private line ***đường dây riêng*** *Xem* leased circuit.

privilege ***đặc quyền*** Trong tính toán, nói tới một chương trình hoặc người sử dụng và kiểu thao tác mà có thể được thực hiện. Những người sử dụng hoặc chương trình có đặc quyền có thể thực hiện các thao tác mà thường được xem như vùng của hệ điều hành và nó có thể ảnh hưởng đến hiệu năng của hệ thống. *Xem* operating system.

privileged data ***dữ liệu đặc quyền*** Trong an toàn dữ liệu, dữ liệu không lệ thuộc vào các quy tắc thông thường vì một tình huống đặc biệt nào đó. Ví dụ, các tệp giáo sĩ, luật pháp, y học.

privilege instructions ***lệnh đặc quyền, chỉ thị đặc quyền*** (1) Trong an toàn máy tính, một tập các lệnh nói chung chỉ được thi hành khi hệ thống ADP đang hoạt động ở trạng thái thi hành; ví dụ, xử lý các ngắt. *Xem* executive state. (2) Trong an toàn máy tính, các lệnh máy tính đặc biệt được thiết kế để điều khiển việc bảo vệ các tính năng của một hệ thống ADP; ví dụ, các tính năng bảo vệ bộ nhớ.

privileged process ***xử lý đặc quyền*** Trong an toàn máy tính, một quá trình được cấp (bởi nhân) một số đặc quyền mà các đặc quyền này không được cấp cho các quá trình của người sử dụng bình thường. Một đặc quyền điển hình là khả năng giành quyền đối với thuộc

tính * an toàn. Các quá trình đặc quyền đều được tín nhiệm. *Xem* security kernel, star property.

privilege profile ***hồ sơ đặc quyền, tệp lược tả đặc quyền*** Trong an toàn máy tính, một bản ghi được lưu giữ trong máy tính, nó chỉ ra các nguồn tài nguyên được phép một cách rõ ràng mà một người sử dụng, một trình hoặc máy tính xác định có thể truy nhập tới.

privity ***thao tác riêng*** Trong an toàn máy tính, một chế độ thao tác đặc quyền cho sự kiểm soát hệ thống hoàn thiện và không bị giới hạn, tại đó tất cả các lệnh đều hoạt động.

procedural language ***ngôn ngữ thủ tục*** Trong tính toán, một ngôn ngữ quy ước bậc cao trong đó người lập trình viên định rõ các hoạt động cần thiết để đạt được kết quả mong muốn. *So sánh với* nonprocedural language.

procedural security ***an toàn thủ tục*** *Đồng nghĩa với* administrative security.

procedure ***thủ tục*** (1) Trong tính toán, tiến trình được tiến hành để giải quyết một vấn đề. (2) Trong tính toán, chỉ một chương trình con. *Xem* subroutine.

procedure oriented language ***ngôn ngữ định hướng thủ tục*** Trong tính toán, một ngôn ngữ bậc cao định hướng tới một lớp các thủ tục cho trước.

procedures ***(các) thủ tục*** *Xem* backup procedures, handshaking procedure, recovery procedures, system integrity procedures.

process ***quá trình, tiến trình*** (1) Trong tính toán, một thực thể hệ thống có hiệu lực nhờ nó các chương trình chạy được. Thực thể trong một hệ thống máy tính được cấp các quyền; như vậy nó là một đơn vị có trách nhiệm trong một hệ thống máy tính. Một tiến trình bao gồm một không gian địa chỉ duy nhất chứa dữ liệu và mã chương trình có thể truy cập được, một vị trí chương trình để thực hiện lệnh hiện thời, và truy nhập định kỳ vào bộ xử lý để tiếp tục. (2) Trong tính toán, một chương trình trong quá trình thi hành. Nó được đặc trưng hóa đầy đủ bởi một điểm thi hành đơn lẻ hiện thời (được biểu thị bằng một trạng thái máy) và không gian địa chỉ. (3) Một tiến trình gồm các biến cố xảy ra theo đúng mục đích hoặc tác động nhắm tới. (4) Trong tính toán, một chương trình là một đoạn mã tĩnh và một tiến trình là sự thi hành mã này. Khi một chương trình được nạp vào bộ nhớ, một tiến trình được tạo ra. (5) Trong tính toán, một tính toán độc lập, với chương trình và dữ liệu của riêng nó, có thể liên hệ với các tiến trình cạnh tranh khác.

processing ***xử lý, gia công*** Theo luật pháp, xử lý được Đạo luật về bảo vệ dữ liệu của Anh năm 1984 định nghĩa, liên quan đến việc sửa đổi, tăng thêm, xóa bỏ hoặc sắp xếp lại dữ liệu hoặc trích ra thông tin tạo thành dữ liệu, và trong trường hợp dữ liệu cá nhân, thì việc xử lý có nghĩa là thực hiện một trong bất kỳ các thao tác trên bằng các tham chiếu tới chủ thể dữ liệu. *Xem* data, data subject, Data Protection Act 1984, data protection - U.K., personal data.

processing priority ***ưu tiên xử lý***

Trong hoạt động ngân hàng, một mức khẩn cấp do người gửi yêu cầu dành cho người nhận khi xử lý thông báo.

processor ***bộ xử lý*** Trong tính toán, một thiết bị hoặc hệ thống có khả năng thực hiện các thao tác trên dữ liệu. Một bộ xử lý trung tâm là một bộ xử lý phần cứng, một bộ biên dịch là một bộ xử lý ngôn ngữ. *Xem* central processing unit, compiler, hardware.

processor utilization ***(sự) tận dụng bộ xử lý*** Trong tính toán, việc cân đối thời gian của bộ xử lý được dùng trong việc thực hiện những tác vụ có ích và cần thiết trong mối tương quan với tổng thời gian có thể sử dụng.

product ***sản phẩm*** Trong hoạt động ngân hàng, tên của một sản phẩm được nhà băng đưa ra, ví dụ, dịch vụ hoặc phương tiện.

product cipher ***mã tích*** Trong mật mã, một mã pháp được tạo ra bởi sự hợp thành của một số các mã pháp thay thế và chuyển vị. *Xem* DES, Feistel cipher, substitution cipher, transposition cipher.

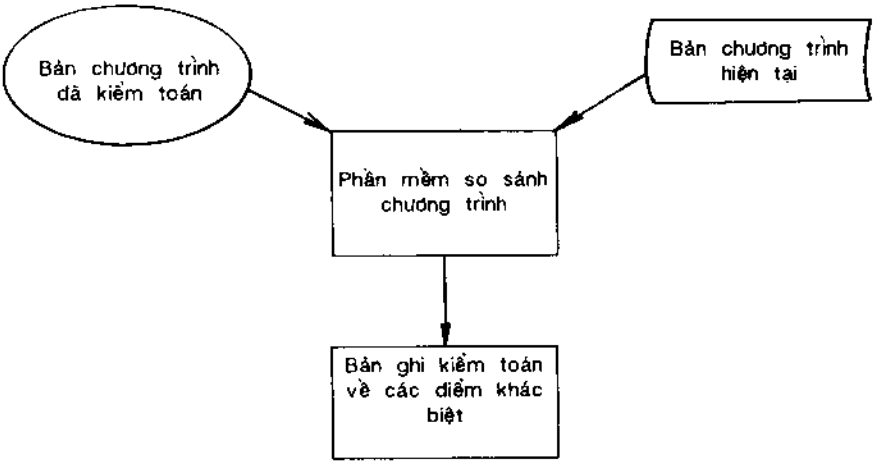
production run ***chạy (chương trình) tạo sản phẩm*** Trong tính toán, việc thi hành thủ tục (chương trình con) của một chương trình được sử dụng phổ biến, ví dụ, việc tính toán chi trả các hóa đơn.

product type ***kiểu sản phẩm*** *Đồng nghĩa với* facility type.

profile ***lược tả*** Trong hoạt động ngân hàng, sự xuất trình dữ liệu trong một khoảng thời gian, phân biệt với thời điểm cụ thể.

profiles ***hồ sơ lược tả*** Trong an toàn máy tính, một mô tả an toàn chi tiết về cấu trúc vật lý, các thành phần thiết bị, các vị trí và mối quan hệ của thiết bị, và môi trường hoạt động chung của hệ thống tự động.

program ***chương trình*** Trong tính toán, một loạt các định nghĩa và lệnh



program comparison utilities: *các tiện ích so sánh chương trình.*

đầy đủ phù hợp với cú pháp của một ngôn ngữ máy cho trước, để khi được thi hành trên một máy tính, nó sẽ thực hiện một tác vụ được yêu cầu. *Xem* source program, object program, programming, syntax.

program analyzer ***bộ phân tích chương trình, trình phân tích chương trình*** Trong an toàn máy tính, một công cụ phần mềm được sử dụng trong việc kiểm tra động; bộ phân tích thu thập dữ liệu trong chương trình để kiểm tra trong suốt quá trình thực hiện của nó. Bộ phân tích có thể được sử dụng để ước lượng mức độ dữ liệu được thực hiện trong chương trình và để nhận dạng ra mã lạ bắt nguồn từ bên ngoài mà có thể gây ra một sự sửa đổi trái phép. *So sánh với* flaw hypothesis. *Xem* dynamic testing.

program comparison utilities ***(các) tiện ích so sánh chương trình*** Trong kiểm toán, một tiện ích phần mềm mà cho phép một kiểm toán viên kiểm tra một chương trình hoạt động tới hạn dựa vào một phiên bản cho phép. *Xem* computer audit packages.

program language ***ngôn ngữ chương trình*** Trong tính toán, một bộ các quy tắc hình thức để xác định cách thức trong đó cấu trúc dữ liệu được lập theo hệ thống, còn các lệnh xử lý thì được ghi lại và được tổ chức. *Xem* high-level language, low-level language, programming.

programming ***lập trình*** Một tiến trình nhờ đó có thể làm cho một máy tính thực hiện một nhiệm vụ xác định. Nó bao gồm việc tạo ra một chuỗi hình thức các lệnh mà máy có thể nhận biết và thực hiện được. Các chỉ dẫn này (chương trình) là một thực thể tĩnh, nhưng khi được thi hành, chúng dẫn tới một tiến trình xử lý thông tin hữu ích. Tất cả mọi chương trình đều liên quan, hoặc gián tiếp hoặc trực tiếp tới luồng thông tin. Dữ liệu, hoặc được đưa ra một cách tường minh, hoặc được tạo ra như một thành phần bên trong của chương trình, được sử dụng như một đầu vào, sau đó mới được xử lý, hoặc tính toán, để đưa ra một đầu ra. Tất cả các chức năng được thực hiện bằng máy tính đều phụ thuộc vào một chương trình tại giai đoạn nào đó.

programming standards ***(các) chuẩn lập trình*** Trong tính toán, một bộ các quy tắc được một tổ chức đưa ra để áp đặt một nguyên tắc trong việc tạo ra các chương trình. Các quy tắc này có thể bao gồm từ các quy tắc xử lý phân tích các chương trình lớn thành các modun riêng biệt, tới các quy tắc sử dụng các cấu trúc chương trình riêng, chẳng hạn các vòng lặp. *Xem* loop.

program patch ***đoạn mã sửa chương trình*** (1) Trong tính toán, một đoạn mã phần mềm được chèn vào một chương trình để hiệu chỉnh các lỗi hoặc sửa đổi chương trình. (2) Trong an toàn máy tính, một đoạn mã được thêm vào mã của đối tượng và do vậy không ảnh hưởng đến mã nguồn. Như vậy, các mã bổ sung này có thể bỏ qua các thủ tục kiểm soát thông thường và có thể được sử dụng trong việc sửa đổi chương trình bất hợp pháp. *Xem* object code, source code.

program specification *(bản) đặc tả chương trình* Trong tính toán, một tài liệu cung cấp các chi tiết đầy đủ của một chương trình, đưa ra các chức năng của nó, các tệp được truy nhập, các yêu cầu vào/ra v.v..

program statement *(câu) lệnh chương trình* Trong tính toán, một biểu thức hoặc một chỉ lệnh được tổng quát hóa theo một ngôn ngữ nguồn. *Xem* source language.

projection *phép chiếu* Trong các cơ sở dữ liệu, một phép toán trong đại số quan hệ. Một phép chiếu trên một quan hệ cho trước, chỉ rõ các thuộc tính của quan hệ đó, đưa ra quan hệ thứ hai chỉ chứa một tập các ±bộ≥ với các thuộc tính được xác định, và với tất cả các bản sao bị loại bỏ. *So sánh với* division, join, selection. *Xem* relational algebra, relational database.

PROM *bộ nhớ PROM, bộ nhớ chỉ đọc lập trình được* Trong tính toán, viết tắt của Programmable Read Only Memory, bộ nhớ chỉ đọc lập trình được, là một hình thức của bộ nhớ ROM mà có thể được lập trình thông qua một người sử dụng. Các vi mạch nhớ trống được mua về và dữ liệu cần thiết được đưa vào vi mạch trong một thiết bị đặc biệt (lập trình viên PROM). *Xem* ROM.

proof of program correctness *chứng minh tính đúng đắn của chương trình* Trong lập trình, một chứng minh toán học hình thức rằng, các ngữ nghĩa của chương trình trùng khớp với bản đặc tả cho chương trình đó.

Phương pháp kiểm tra truyền thống các chương trình bằng cách thử dữ liệu không tin cậy, không hiệu quả và không cung cấp hướng dẫn trong việc phát triển các chương trình không có lỗi.

Kết quả của các lần chạy thử không đáng tin cậy bởi vì không có phương pháp chính xác trong việc lựa chọn dữ liệu thử để đảm bảo rằng, tất cả các nhánh có thể xuyên suốt chương trình đều được kiểm tra. Phương pháp không hiệu quả vì cần các bộ dữ liệu kiểm tra lớn và nếu với dữ liệu bất kỳ, chương trình bị lỗi, thì chương trình phải được sửa đổi và chạy thử lại từ đầu, để đảm bảo không có các lỗi nào nữa được chèn vào bởi sự sửa đổi.

Tuy nhiên, thiếu sót nghiêm trọng nhất của kỹ thuật này là nó không cung cấp hướng bắt buộc cho việc phát triển chương trình; thực tế, các sửa đổi liên tiếp đối với chương trình nhằm sửa chữa các thiếu sót, được chỉ ra bằng dữ liệu thử, có thể dẫn tới các chương trình cuối cùng cực kỳ khó duy trì hoặc cập nhật.

Trước hết, các phương pháp kiểm chứng hình thức tính chính xác phụ thuộc vào mệnh đề toán học, hoặc vào điều khẳng định toán học vốn trình bày một cách chính xác và rõ ràng kết quả mong muốn của chương trình theo dữ liệu đầu vào và các trạng thái. Nó là một nhiệm vụ khó khăn đối với các chương trình quan trọng nhưng điều đáng lưu ý là, đây là hình thức lập trình đối với ngôn ngữ phi thủ tục. Việc xác nhận trên dữ liệu hoặc các trạng thái đầu ra của chương trình được gọi là điều kiện sau. Điều kiện trước là một xác nhận trên dữ liệu hoặc các trạng thái đầu vào trước khi thực hiện

chương trình. Một chương trình được cho là đúng nếu nó thi hành, bắt đầu với các trạng thái tương ứng với điều kiện trước, tạo ra một tập các trạng thái thỏa mãn điều kiện sau. Việc kiểm chứng sự chính xác của toàn bộ chương trình đòi hỏi cả điều kiện sau đúng nếu chương trình kết thúc (được biết đến như việc kiểm chứng tính chính xác từng phần) và cả việc kiểm chứng rằng chương trình quả thực đã kết thúc.

Việc chứng minh rằng, một chương trình cho trước sẽ đảm bảo kết thúc theo điều kiện sau chỉ ra, là một nhiệm vụ khó khăn đối với các chương trình lớn. Tuy nhiên, ý nghĩa của các kỹ thuật hình thức đó không nằm trong kiểm chứng chính xác về lỗi logic mà nằm trong hướng tiếp cận buộc tuân thủ do chúng cung cấp để tạo ra các chương trình không có lỗi.

Mỗi modun nằm trong một chương trình lớn có thể được phát triển theo một kiểu không có lỗi bằng cách sử dụng liên tiếp điều kiện trước và sau; trong một chương trình có tính tuần tự, điều kiện sau của một đoạn trở thành điều kiện trước của đoạn kế tiếp. Cách tiếp cận này có thể làm nổi bật các lỗi đặc trưng tiềm ẩn, ví dụ, chia cho 0, các thao tác chuỗi trên các chuỗi rỗng. Các lệnh nhảy có điều kiện trong một chương trình bao gồm một số các nhánh có thể và điều kiện trước phải bao trùm cả các trạng thái điều kiện trước cho mỗi tuyến và điều kiện cần thiết cho tuyến được lựa chọn đó.

Các chương trình chứa các các vòng lặp là nguồn tiềm ẩn các lỗi, đặc biệt các vòng lặp vô tận xuất hiện trong các điều kiện nhất định hoặc vòng lặp không kết thúc với một tập các trạng thái đầu ra được yêu cầu. Các kỹ thuật hình thức cung cấp một hướng bắt buộc để thiết kế các vòng lặp, chúng đòi hỏi lập trình viên đảm bảo rằng, vòng lặp khởi đầu với điều kiện cần ban đầu và rằng, vòng lặp này sẽ kết thúc, còn khi nó chạy, điều kiện cần sau được đáp ứng. Một khái niệm quan trọng là trạng thái bất biến của một vòng lặp. Trạng thái này có giá trị đúng trước và sau mỗi lần thi hành các lệnh trong vòng lặp. Việc lựa chọn tính bất biến của vòng lặp đưa ra một cách nhìn mới về hành vi của các vòng lặp chương trình. Hướng hình thức đảm bảo rằng, vòng lặp kết thúc sau một số hữu hạn lần lặp và rằng, điều kiện sau được thỏa mãn vào lúc kết thúc. *Xem* bug, loop, postcondition, precondition, predicate transformer.

PROPIN ***thông tin PROPIN*** Trong an toàn dữ liệu, thông tin cảnh báo - thuộc quyền sở hữu có liên quan. *Xem* proprietary data.

proprietary data ***dữ liệu sở hữu, dữ liệu riêng*** Dữ liệu do các cá nhân có các quyền hợp pháp tạo ra, sử dụng và tiêu thụ. *Xem* software protection.

proprietary fire alarm system ***hệ thống báo hỏa riêng*** Trong an toàn vật lý, một hệ thống bao gồm một trạm giám sát trung tâm và trang thiết bị cho phép người điều hành duy trì, kiểm tra và thao tác hệ thống và nắm được các hoạt động cần thiết dựa vào một tín hiệu báo động nhận được.

protected distribution system ***hệ***

thống phân tán có bảo vệ (1) Trong an toàn truyền thông, các hệ thống viễn thông được phê chuẩn được áp dụng các bảo vệ an toàn điện từ và vật lý để cho phép truyền điện an toàn các thông tin nhạy cảm không được mã hóa. (2) Trong an toàn truyền thông, một hệ thống truyền thông áp dụng các bảo vệ an toàn âm thanh, điện, điện từ và vật lý cho phép sử dụng nó để truyền dưới dạng điện hoặc quang đối với các thông tin đã được phân loại không được mã hóa hoặc thông tin nhạy cảm không được mã hóa. *Xem* fiber optics.

protected subsystem ***hệ thống con được bảo vệ*** (1) Trong an toàn truyền thông, người sử dụng được cung cấp (tầng 7) các chương trình để kiểm soát truy nhập vào các đối tượng ở "mức hạt" mịn hơn sự kiểm soát truy nhập do nhân cung cấp. *Xem* kernel, open systems interconnection. (2) Trong an toàn dữ liệu, một tập hợp các thủ tục và các đối tượng dữ liệu được gói gọn trong một vùng mà nó sở hữu, vì vậy cấu trúc bên trong của đối tượng dữ liệu chỉ có thể truy cập được tới các thủ tục của hệ thống thứ cấp được bảo vệ. Các thủ tục có thể chỉ được gọi tại các điểm vào của vùng được chỉ định và chỉ bị gọi bởi các chủ thể được chỉ định. *Xem* domain subject. (3) Trong an toàn máy tính, một chương trình hoặc một hệ thống thứ cấp có thể hoạt động như một chủ thể. *Xem* subject.

protected wireline distribution system ***hệ thống phân tán nối dây có bảo vệ*** Trong an toàn dữ liệu, một hệ thống viễn thông được phê chuẩn bởi một người có thẩm quyền được chỉ định hợp pháp. Nó được áp dụng các biện pháp bảo vệ an toàn điện từ và vật lý để cho phép truyền dưới dạng điện đối với các thông tin nhạy cảm không được mã hóa. *Xem* sensitive information. *Đồng nghĩa với* approved circuit.

protection ***(sự) bảo vệ*** Trong kiểm soát truy nhập, nói tới các thiết bị và cơ chế kiểm soát truy nhập vào thông tin được lưu giữ. *Xem* data-dependent protection, data protection, fetch protection, lock-and-key protection system, privacy protection.

protection-critical portions of the TCB ***(các) phần bảo vệ trọng yếu của TCB*** Trong an toàn máy tính, các phần của TCB mà chức năng thông thường của chúng là xem xét sự kiểm soát truy nhập giữa các chủ thể và các đối tượng. *Xem* access, object, subject, TCB.

protection pattern ***khu vực bảo vệ*** Trong an toàn vật lý, một vùng bảo vệ được bao phủ bởi một thiết bị cảm ứng.

protection philosophy ***triết lý bảo vệ*** Trong an toàn máy tính, một mô tả phi hình thức về toàn bộ thiết kế của một hệ thống mà phác họa một cơ chế bảo vệ được sử dụng. Sự phối hợp (tương ứng với một lớp đánh giá) của các kỹ thuật hình thức và phi hình thức được sử dụng để chỉ ra rằng, các kỹ thuật đủ để buộc tuân thủ chính sánh an toàn. *Xem* security policy.

protection ring ***vành bảo vệ*** Trong an toàn máy tính, một phân cấp các chế độ đặc quyền của một hệ thống ADP mà đưa ra các quyền truy nhập nào đó

cho những người sử dụng, các chương trình, và các quá trình xử lý được phép hoạt động trong một chế độ đã cho.

protective redundancy ***dư thừa bảo vệ*** Trong lĩnh vực độ tin cậy, việc sử dụng các modun được nhân bản về phần cứng hoặc phần mềm, hoặc việc sử dụng các mã hiệu chỉnh lỗi để đưa ra khả năng kháng lỗi của một hệ thống. *Xem* error correction code, fault tolerance, redundancy. *Đồng nghĩa với* spacial redundancy.

protocol ***giao thức*** (1) Trong truyền thông dữ liệu, một tập các quy tắc xác định ý nghĩa và khuôn thức của các khung, các gói hoặc các thông báo được trao đổi giữa các thực thể ngang hàng trên một tầng của mô hình tham chiếu kết nối các hệ thống mở. *Xem* open systems interconnection. (2) Trong truyền dữ liệu, một tập các quy ước được định rõ, một cách hình thức, chi phối khuôn thức và điều khiển các đầu vào và đầu ra giữa hai hệ thống truyền thông.

protocol converter ***bộ đổi giao thức, bộ đổi quy cách*** Trong truyền dữ liệu, một thiết bị ghép nối hai hệ thống truyền thông làm việc theo các giao thức khác nhau. Ví dụ, một bộ đổi giao thức có thể ghép với một máy vi tính, thông qua cổng nối tiếp không đồng bộ RS-232C, và tới một mạng đồng bộ IBM SNA/SDLC. Tất cả các quy ước mã EBCDIC/ASCII đều được thực hiện, như xác định vị trí con trỏ, đặt vào bộ nhớ đệm của màn hình và xử lý lỗi. *So sánh với* software protocol converter. *Xem* ASCII, asynchronous transmission, code conversion, EBCDIC code, protocol, RS-232C, SDLC, SNA.

protocol data unit ***đơn vị dữ liệu giao thức*** Trong truyền thông, một đoạn đơn vị dữ liệu dịch vụ cộng với phần tiêu đề điều khiển. Khi một tầng trong mô hình tham chiếu kết nối các hệ thống mở chuyển một đơn vị dữ liệu dịch vụ, nó có thể cắt thành nhiều đoạn và cho mỗi đoạn một phần tiêu đề khi truyền, chúng tạo thành một gói đơn vị dữ liệu giao thức. *So sánh với* interface data unit, service data unit. *Xem* open systems interconnection.

protocol standards ***(các) chuẩn giao thức*** Trong truyền dữ liệu, các giao thức được định nghĩa thuận tiện cho việc liên lạc giữa một nhóm những người sử dụng rộng rãi và khác nhau. Ban đầu các giao thức được cung cấp chỉ đơn thuần để kết nối các thiết bị giống nhau còn mạng Arpanet là một ngoại lệ, nó cho phép kết nối hai hệ thống truyền thông bất kỳ. Một số giao thức trước đây, ví dụ, BISYNC, trở thành các chuẩn không theo thể thức khi chúng được nhiều nhà sản xuất khác nhau chấp nhận. Có hai tổ chức quốc tế quan tâm đến các chuẩn giao thức - CCITT và ISO. CCITT chịu trách nhiệm về các chuẩn trong lĩnh vực các dịch vụ truyền thông công cộng. Đây là một ủy ban thường trực của ITU. Các khuyến nghị được biết đến nhiều nhất của nó là các khuyến nghị xeri V và xeri X dành cho truyền dữ liệu tương tự và số. ISO có một số lượng lớn các tổ chức thành viên, nằm ở các quốc gia riêng biệt - BSI tại Anh, ANSI tại Hoa Kỳ, AFNOR tại Pháp. Các tổ chức khác như CCITT và ACMA cũng được đại diện. Hội nghị của Châu Âu về quản trị

bưu chính và viễn thông đảm trách sự chuẩn hóa trong lĩnh vực mở rộng hệ thống điện thoại vào các phương tiện khác được các PTT cung cấp, ví dụ, các mạng dữ liệu số. Các tổ chức quốc gia như IEEE công bố các chuẩn, ví dụ RS-232C, tương đương với chuẩn V.24 của CCITT và một chuẩn mạng cục bộ IEEE 802. *Xem* AFNOR, ANSI, ARPA, BISYNC, BSI, CCITT, ECMA, IEEE, IEEE 802, ISO, ITU local area network, PTT, RS-232, V, X.

protocol suite ***bộ giao thức*** Trong an toàn truyền thông, một tập hợp các thiết lập hợp thức các giao thức (nhưng trong thực tiễn không phải luôn như vậy) dựa vào một mô hình chuẩn giao thức. *Xem* protocol.

provisions ***(các) điều khoản*** Trong hoạt động ngân hàng, các mục được phép dựa vào các lợi nhuận trong mối quan hệ thực tiễn hoặc ngầm định đoán trước.

proximity card reader ***bộ đọc thẻ gần*** Trong điều khiển truy nhập, một thiết bị đọc thẻ không cần gài thẻ vào trong thiết bị. Thẻ có chứa các mạch điều hưởng tần số vô tuyến, tương tác với các tín hiệu do bộ đọc tạo ra. Những thay đổi bất thường về tần số xảy ra sau đó được thiết bị này phát hiện và được giải thích bằng sơ đồ mạch thông dịch để xác định phép mã trên thẻ. *Xem* card reader, smart card, transmitter.

pseudo-flaw ***kẽ hở giả*** Trong an toàn máy tính, một lỗ hổng vòng lặp được gài một cách thận trọng vào trong một chương trình của hệ điều hành như một cái bẫy cho những kẻ xâm nhập. *Xem* entrapment, loophole.

pseudorandom number ***số giả ngẫu nhiên*** Trong tính toán, một số được sinh ra từ một thuật toán xác định xấp xỉ với một số ngẫu nhiên. Các thuật toán như vậy được thiết kế để đưa ra các số có các thuộc tính thống kê xác định. *Xem* random numbers.

PSK *Xem* phase shift keying.

PSN *Xem* packet switch node, packet-switching network.

PSOS ***hệ PSOS, hệ điều hành an toàn chứng minh được*** Trong an toàn máy tính, viết tắt của Provably Secure Operating System, một hệ điều hành tin cậy có thể chứng minh được. Một hệ điều hành dựa trên năng lực, được cấu trúc như một hệ thống phân bậc của các máy trừu tượng được xếp lồng nhau. PSOS đã được thiết kế tại SRI và thiết kế hệ thống sử dụng các công cụ SPECIAL và MLS. *Xem* capability, MLS, Special.

PTT *Xem* post telegraph and telephone.

public data network ***mạng dữ liệu công cộng*** Trong truyền dữ liệu, một mạng cung cấp một dịch vụ truyền dữ liệu cho công cộng, do một cơ quan có thẩm quyền chung hoặc hãng hoạt động cá nhân được công nhận cung cấp.

public dial port ***cổng chọn số công cộng*** Trong truyền dữ liệu, một cổng quay số cung cấp truy nhập vào một mạng chuyển mạch gói từ một thiết bị đầu cuối được kết nối với hệ thống điện thoại công cộng. *Xem* private dial port.

public domain ***tư liệu khu vực công cộng*** Theo luật, một tài liệu mà

không có bản quyền hoặc bản quyền hết hiệu lực. *Xem* copyright.

public key ***khóa công khai*** (1) Trong mật mã, một khóa (trong một hệ thống mật mã không đối xứng hoặc mã khóa công khai) trong một bộ khóa của người sử dụng mà những người sử dụng khác cũng biết. *So sánh với* secret key. *Xem* asymmetric algorithm, public key cryptography. (2) Trong mật mã, một khóa mã được sử dụng để mã các thông báo, hoặc kiểm tra các chữ ký trong mật mã khóa công khai. Khóa này được người nhận bản mã hóa hoặc chữ ký làm sẵn trước. *So sánh với* private key. *Xem* ciphertext, cryptographic key, digital signature, public key cryptography.

public key cryptography ***mật mã khóa công khai*** Trong mật mã, một hệ thống mật mã không đối xứng, có nghĩa là một hệ thống trong đó các khóa mã và giải mã là khác nhau và không thể tính toán một khóa từ khóa kia khi cho trước thuật toán mã hóa. Trong mật mã khóa công khai, khóa mã hóa được đưa ra công khai nhưng khóa giải mã được giữ bí mật, nó có các ưu điểm so với các mã pháp đối xứng, thí dụ DES, trong các lĩnh vực:

- giữ an toàn của các thông báo, từ sự đa dạng của các nguồn, tác động trực tiếp tới một tổ chức cá nhân;
- quản lý khóa;
- các chữ ký số.

Nếu một số các cá nhân muốn gửi thông tin bí mật tới một tổ chức trung tâm thì các mã pháp đối xứng đòi hỏi tạo ra các sắp xếp ban đầu cho cá nhân và tổ chức để chia sẻ một khóa bí mật duy nhất. Trong khi đó, mật mã khóa công khai cho phép tổ chức công bố một khóa mã đơn lẻ khác, có thể ở trong một thư mục công cộng, và những người gửi thông báo chỉ cần truy nhập vào thư mục này, mã hóa thông báo của họ bằng khóa công khai và thuật toán đã thỏa thuận, và gửi nó tới tổ chức. Như vậy, những người gửi sẽ không có khả năng giải mã các thông báo, do các cá nhân khác gửi nếu sử dụng cùng một khóa, bởi vì các khóa giải mã được giữ bí mật và chỉ có tổ chức đang nói tới giữ nó.

Việc bí mật khóa công khai là không yêu cầu nhưng điều cơ bản là tính toàn vẹn của khóa trong thư mục công cộng được đảm bảo. Nếu một kẻ tấn công có thể thay thế khóa công khai của một tổ chức bằng một khóa mã do anh ta tự đưa ra thì anh ta cũng sẽ nắm được khóa giải mã tương ứng. Khi đó, thông tin bí mật dành riêng cho tổ chức sẽ trở thành thứ anh ta có thể dùng được. Điều quan trọng là những người sử dụng không dùng các thông báo đã định dạng ở mức độ cao bởi vì một kẻ tấn công có một sự lựa chọn hoàn toàn tự do trong các tấn công bản rõ đã chọn. Như vậy kẻ tấn công này có thể thông minh đoán ra ý nghĩa của các khối rõ nhất định bị lặp đi lặp lại trong các bản mã được mã bằng khóa công khai cho trước. Sau đó kẻ tấn công sẽ kiểm tra các phỏng đoán này bằng việc mã hóa chúng bằng khóa công khai, và so sánh kết quả với các khối bản mã.

Quản lý khóa là một lĩnh vực khác trong đó, mật mã khóa công khai có khả năng thực hiện các xâm nhập đáng kể.

Vì không cần trao đổi khóa bí mật trước khi thiết lập các truyền thông an toàn, nên mật mã khóa công khai có thể được sử dụng để truyền khóa để mã các khóa và các khóa dữ liệu. Kỹ thuật này có các lợi thế nhờ việc sử dụng mật mã khóa công khai để mã hóa dữ liệu thông báo, vì các mã đối xứng, ví dụ DES, đòi hỏi tính toán ít hơn so với các phương pháp mã hóa khóa công khai hiện tại.

Một số thuật toán mã khóa công khai đưa ra các kỹ thuật chữ ký số tinh tế. Nếu có thể dùng khóa giải mã để mã hóa, và ngược lại, thì người nhận có thể giải mã một thông báo bằng cách sử dụng khóa công khai, và anh ta được đảm bảo rằng, thông báo nhận được chỉ có thể được mã hóa bởi người nắm giữ khóa giải mã bí mật.

Diffie và Hellman là người đầu tiên công bố một bài báo, giới thiệu các khái niệm về mật mã khóa công khai và cuốn "New Directions in Cryptography" (Những hướng đi mới trong mật mã) xuất bản năm 1976. Ý tưởng về một khóa mã không mật là một tiến bộ quan trọng trong mật mã; nó ngụ ý rằng, ở đây không có đòi hỏi nào về một kênh an toàn giữa người gửi và người nhận các thông báo. Không có mật mã, thì một kênh an toàn là yếu tố chủ yếu để duy trì toàn bộ sự bí mật của thông báo trước đối phương; với mật mã thông thường thì yêu cầu về một kênh an toàn sẽ được giảm đi để dành cho sự truyền khóa mật mã.

Mật mã khóa công khai cho phép một người gửi truy nhập một khóa mã, ví dụ, từ một thư mục công khai, mã hóa một thông báo và gửi nó tới người nhận, người này phải giữ khóa giải mã riêng; không lúc nào đòi hỏi một kênh an toàn.

Như vậy, mật mã có thể được xem là đã phát triển theo 3 giai đoạn. Giai đoạn đầu, thuật toán mã hóa và các khóa liên quan bất kỳ được giữ bí mật. Giai đoạn thứ hai, các thuật toán mã hóa được để công khai nhưng các khóa mã và giải mã có thể đồng nhất hoặc không đồng nhất không được để lộ ra. Với mã hóa khóa công khai, cả phương pháp mã hóa lẫn các khóa mã hóa được công khai, sự bí mật của mã pháp phụ thuộc vào sự an toàn của khóa giải mã riêng. Cả 3 giai đoạn phát triển cho thấy các yêu cầu về thuật toán mã hóa ngày càng tăng, nó có thể được biểu diễn như sau:

$C = f(M, E)$

Trong đó, C là bản mã, M là bản rõ, E là khóa mã, f là thủ tục mã hóa. Nếu cả thuật toán mã hóa (f) lẫn khóa mã E được giữ bí mật, thì nhà phân tích mã (nhà mã thám) không được cung cấp chút thông tin nào trừ việc bản mã là một thông báo có ý nghĩa theo một ngôn ngữ tự nhiên cho trước, thủ tục mật mã trong những trường hợp đó khá đơn giản. Khi thuật toán mã hóa (f) là kiến thức công khai và khóa mã E được giữ bí mật thì các yêu cầu đối với thủ tục mật mã phụ thuộc vào độ dài của khóa.

Nếu khóa là ngẫu nhiên, và có cùng độ dài với thông báo, thì thủ tục có thể khá đơn giản bởi vì nhà mã thám không có đủ thông tin để khôi phục lại bản rõ. Tuy nhiên, nếu khóa tương đối

ngắn. khi so với thông báo, thì các kỹ thuật về lý thuyết thông tin chỉ ra rằng, độ dư thừa của các ngôn ngữ tự nhiên cung cấp cho nhà mã thám đủ thông tin để giải mã bản mã. Về mặt toán học, nhà phân tích mã phải cố gắng tính toán một hàm ngược lại: $E = h(M, C)$. Độ phức tạp của thủ tục mã hóa phải sao cho quá trình này là không thể về mặt tính toán.

Với mật mã khóa công khai, về lý thuyết, nhà phân tích mã được cung cấp đầy đủ thông tin để giải mã thông báo mà không cần bất kỳ sự nhờ cậy nào vào việc nghiên cứu độ dư thừa của ngôn ngữ bản rõ. Cả thuật toán mã hóa lẫn khóa mã hóa đều để công khai, sự phân tích toán học sẽ chỉ ra mối liên hệ giữa khóa giải mã chưa biết, khóa mã và thuật toán đã biết. Như vậy, thuật toán mật mã phải sao cho không thể tính toán để thực hiện hàm ngược: $M = p(C, E)$. Về mặt toán học, điều này chỉ ra rằng thuật toán mã hóa, f, phải là hàm một chiều.

Tuy nhiên, người lập khóa công khai có một nhiệm vụ lớn hơn là việc chỉ đơn thuần đưa ra một hàm một chiều hiệu quả; trong khi phải ngăn chặn nhà mã thám khỏi tính toán hàm $M = p(C, E)$, thì rõ ràng điều quan trọng là người nhân hợp pháp cần có khả năng thu được bản rõ với khả năng tính toán hợp lý. Như vậy, giới hạn nữa đối với $f(M, E)$ là hàm này là một hàm cửa sập một chiều, có nghĩa là người sử dụng hợp pháp, được trang bị một khóa giải mã riêng (D), có thể dễ dàng tính toán hàm $M = g(C, D)$.

Lý thuyết độ phức tạp cung cấp một lớp các bài toán, được biết đến như đa thức không tất định, hoặc các bài toán NP, là các ứng cử viên cho các hàm cửa sập một chiều. Các bài toán NP có thuộc tính là thời gian giải chúng tăng kiểu hàm mũ theo kích thước của bài toán, nhưng thời gian kiểm tra một lời giải chỉ tăng theo hàm đa thức của kích thước.

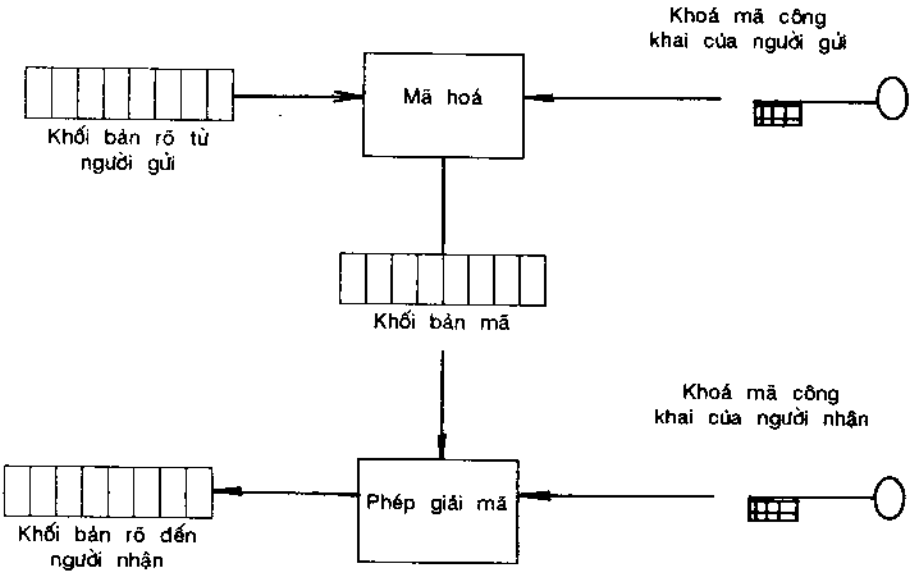
Các yêu cầu của mật mã khóa công khai được liệt kê dưới đây:

- Có một cặp thuật toán mã và giải mã $C = f(M, E_k)$, $M = g(C, D_k)$ trong đó các bản rõ và bản mã, M và C là phần tử của một tập hữu hạn các thông báo.
- Các thuật toán, f và g, dễ dàng tính toán với mọi giá trị M, E_k, C, D_k.
- Với mọi giá trị của k, không tính toán được D_k từ E_k.
- Với mọi giá trị của k, không thể tính toán được các cặp đảo, E_k và D_k.

Các hệ thống mã chỉ ra có thể đặt các điều kiện ràng buộc thêm cho f và g. Ví dụ, các ứng dụng chữ ký số yêu cầu: $C = f(M, D_k)$, $M = g(C, E_k)$.

Một lớp phổ biến mật mã khóa công khai dựa vào mã pháp lũy thừa. Kỹ thuật Diffie-Hellman, mã Pohlig-Hellman, RSA và bài poke trí tuệ đều là mã lũy thừa, nghĩa là nếu cho trước M, E và n, có khả năng tính toán được $M^E \pmod n$, M, E và n có thể là các số với hàng trăm chữ số thập phân. Tuy nhiên, không có khả năng tính toán được M nếu cho trước $M^E \pmod n$, E và n.

Kỹ thuật Diffie-Hellman có thể được sử dụng để trao đổi các khóa riêng trên các kênh không an toàn. Mã pháp Pohlig-Hellman không đáp ứng được



public key cryptography: *mật mã khóa công khai.*

yêu cầu chính của mật mã khóa công khai vì nó dễ dàng tính được khóa giải mã từ những hiểu biết về khóa mã hóa và thuật toán. RSA là một mã lũy thừa dựa vào tính không thể thực hiện được về mặt tính toán phép phân tích nhân tử các số nguyên tố lớn. Bài poke trí tuệ là một mã lũy thừa, nó có thể được sử dụng, ví dụ, bởi hai thành viên chơi bài poke qua điện thoại.

Lớp thứ hai của mật mã khóa công khai được dựa trên các mã pháp ba lô (knapsack). Bài toán ba lô xoay quanh việc lựa chọn một tập nhỏ các số nguyên mà tổng của chúng bằng một giá trị xác định. Tính dễ bị tấn công của các mã ba lô là một chủ đề của các tranh luận lớn và Shamir đã trình bày một phương pháp phá bài toán ba lô cơ bản của Merkle-Hellman vào năm 1982.

Kỹ thuật thứ 3 dành cho mật mã khóa công khai cũng đã được mô tả, nó dựa vào kỹ thuật của các mã hiệu chỉnh lỗi. Trong truyền dữ liệu thông thường, thông báo có thể được biến đổi bằng việc đưa thêm các bit dư hiệu chỉnh lỗi; trong suốt quá trình truyền, toàn bộ thông báo, nghĩa là dữ liệu và các bit hiệu chỉnh lỗi có thể bị thay đổi bởi nhiễu. Bên nhận thực hiện phép biến đổi dựa trên thông báo để trích ra dữ liệu nguyên thủy từ thông báo bị sửa đổi. Một kỹ thuật mật mã khóa công khai được đề xuất trong đó, ma trận chuyển đổi thông báo sẽ gồm một khóa mã công khai. Đầu tiên người gửi biến đổi thông báo với ma trận này, làm biến đổi và mở rộng thông báo bằng các bit dữ liệu thêm vào. Sau đó, một số xác định các bit được thay đổi một cách

P

ngẫu nhiên. Bên nhận khống chế ma trận chuyển đổi thông báo bí mật và tìm lại được dữ liệu nguyên thủy; các bit dư thừa đầy đủ được thêm vào thông báo nguyên thủy để cho phép người nhận lọc ra được các nhiễu được người gửi đưa ra một cách thận trọng. *Xem* asymmetric cryptosystem, authentication, DES, Differ-Hellman technique, digital signature, ElGamal cipher, error correction code, information theory, key management, knapsack cipher, mental poker, Pohlig-Hellman cipher, RSA, symmetric cryptosystem, trapdoor one-way function.

public key distribution ***phân phối khóa công khai*** Trong mật mã, một phương pháp trao đổi các khóa bí mật giữa các bên truyền thông mà không đòi hỏi một kênh an toàn. *Xem* Diffie-Hellman technique, keyless cryptography, key management, public key cryptography.

public switched network ***mạng chuyển mạch công cộng*** Trong truyền thông, hệ thống chuyển mạch cung cấp các phương tiện truyền chuyển mạch cho các khách hàng.

pull station ***trạm kéo*** Trong an toàn vật lý, một hệ thống báo động thủ công, được thiết kế dành cho các thành viên công cộng sử dụng. Nó bao gồm một chuyển mạch bằng tay đặt trong một hộp thiết bị công suất lớn. Sau đó, tín hiệu báo động này có thể được mã và chuyển tới một trạm trung tâm.

pulse amplitude modulation ***điều biến biên độ xung, điều biên xung*** Trong truyền thông, một phương pháp điều biến xung trong đó biên độ của một dãy xung được điều chỉnh phù hợp với biên độ tín hiệu vào. *So sánh với* pulse code modulation, pulse duration modulation, pulse position modulation. *Xem* modulation, pulse modulation.

pulse code modulation ***điều biến mã xung, điều chế mã xung*** Trong truyền thông, một kỹ thuật truyền thông tin tương tự ở dạng số. Tín hiệu tương tự được lấy mẫu và giá trị lấy mẫu được biểu diễn bằng số nhị phân có độ dài cố định. Sau đó số này được truyền đi như một khối các xung tương ứng. Trong điện thoại, tốc độ lấy mẫu là 8000/giây. *So sánh với* pulse amplitude modulation, pulse duration modulation, pulse position modulation. *Xem* sampling, pulse modulation.

pulse duration modulation ***điều biến thời khoảng xung*** Trong truyền thông, một kỹ thuật điều biến xung trong đó, độ rộng của xung, trên một dãy xung, được điều chỉnh phù hợp với tín hiệu vào. *So sánh với* pulse amplitude modulation, pulse code modulation, pulse position modulation. *Xem* pulse modulation. *Đồng nghĩa với* pulse width modulation.

pulse modulation ***điều biến xung, điều chế xung*** Trong truyền thông, một hệ thống truyền tín hiệu trong đó nội dung thông tin được đưa vào một dãy xung bằng cách điều chỉnh hoặc biên độ xung (PAM), thời hạn xung (PDM), hoặc vị trí xung (PPM), hoặc bằng các mã nhị phân dựa vào sự có mặt hoặc vắng mặt các xung (PCM). *Xem* pulse amplitude modulation, pulse duration modulation, pulse position

modulation, pulse code modulation.

pulse position modulation ***điều biến vị trí xung*** Trong truyền thông, một kỹ thuật điều biến xung trong đó việc định thời các xung riêng biệt, trên một dãy xung, phụ thuộc vào tín hiệu điều biến. *So sánh với* pulse amplitude modulation, pulse code modulation, pulse duration modulation. *Xem* pulse modulation.

pulse repetition rate ***tốc độ lặp xung*** Trong điện tử học, số các xung trên đơn vị thời gian.

pulse train ***chuỗi xung, loạt xung*** Trong truyền dữ liệu, một loạt các xung có các đặc tính giống nhau. Một phương pháp chuyển tải thông tin nhị phân trong đó sự có mặt, hoặc vắng mặt của một xung biểu diễn bằng một số nhị phân 1 hoặc 0 tương ứng.

pulse width modulation ***điều biến độ rộng xung*** *So sánh với* pulse duration modulation.

purging ***dọn dẹp, làm sạch*** (1) Trong tính toán, việc xem xét có thứ tự việc lưu giữ và loại bỏ các tệp dữ liệu không hoạt động hoặc quá hạn. (2) Trong an toàn máy tính, sự loại bỏ dữ liệu quá hạn bằng cách xóa, ghi đè lên vùng lưu trữ, hoặc thiết lập lại trạng thái các thanh ghi. *Xem* overwritng, personal computer security.

PVC *Xem* permanent virtual circuit.

PVV *Xem* pin verification value.

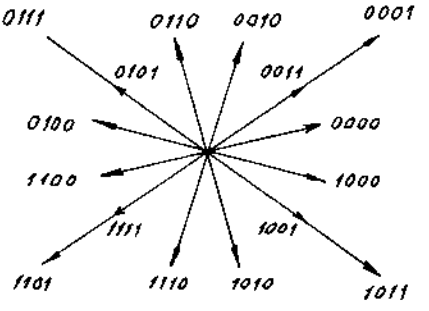


Q

QAM *Xem* quadrature amplitude modulation.

quadratic residue ***thặng dư bậc hai*** Trong toán học, một thuộc tính của một vài số nguyên trong một phép số học modulo cho trước. Số c là phần dư bậc hai modulo với n, nếu nó nguyên tố cùng nhau với n và ở đây tồn tại một số x khác sao cho: $x^2 = c \pmod{n}$. Nói cách khác, phần dư bậc hai có một căn bình phương số nguyên modulo n. *Xem* co-prime, mental poker, modulo arithmetic.

quadrature amplitude modulation ***điều biến biên độ vuông góc, điều biên vuông góc*** Trong truyền dữ liệu, một phương pháp biến đổi các tín hiệu số thành các tín hiệu tương tự sử dụng để truyền trên một mạng điện thoại. Nó kết hợp các kỹ thuật điều biến biên độ và điều biến pha. Khi cho trước 16 trạng thái sóng mang, có thể thu được một cấu trúc tín hiệu 16 điểm bằng cách kết hợp 12 góc pha và 4 pha điều biến biên độ. 4 pha được điều biến biên độ có hai mức biên độ có thể. *So sánh với* amplitude modulation, frequency shift keying, phase modulation. *Xem* analog signal, carrier, digital signal.



quadrature amplitude modulation: *điều biên vuông góc.*

qualitative risk analysis ***phân tích rủi ro định tính*** *So sánh với* quantitative risk analysis. *Xem* matrix methodology, risk analysis methodologies.

quantitative risk analysis ***phân tích rủi ro định lượng*** Trong việc quản lý rủi ro, phương pháp học phân tích rủi ro nhằm định lượng điểm số rủi ro, thường xảy ra trong các lĩnh vực tài chính. Mục tiêu của biện pháp này là cho phép quản lý để cân bằng chi phí của các biện pháp đối phó an toàn được đề xuất, dựa vào việc ước lượng thực tế tác động của rủi ro. Biện pháp này bao gồm các bước cơ bản sau: nhận dạng tài sản sở hữu, tính toán rủi ro và đánh giá các biện pháp đối phó.

Giai đoạn nhận dạng tài sản sở hữu được hướng dẫn để đưa ra một ước lượng thực tế về các khả năng có thể xảy ra và phí tổn liên quan đến các mối hiểm họa được nhận dạng đối với hệ thống. Nó bao gồm 3 phạm vi sau: các tài sản sở hữu, các mối hiểm họa và các khảo sát an toàn.

Các tài nguyên cần bảo vệ được nhận dạng và định giá đầu tiên. Trong an toàn máy tính, các nguồn tài nguyên này có thể là:

- trang thiết bị và nguồn cung cấp;
- tài sản thuộc trí óc (dữ liệu và các chương trình);
- các dịch vụ và xử lý trên máy tính.

Các giá trị tài chính có thể được thay thế không khó khăn gì dựa vào phần cứng và phần mềm thuộc quyền sở hữu. Tuy nhiên, chi phí liên quan đến việc thay đổi dữ liệu và các chương trình hoặc mất mát dịch vụ của một máy tính có thể bao gồm ít nhất một sự ước lượng về chi phí cho việc tái tạo lại dữ liệu từ các tài liệu nguồn hoặc chi phí của việc di chuyển tạm thời các xử lý nội bộ ra bên ngoài.

Tuy nhiên, nói chung các yêu cầu trực tiếp đối với việc cấp phát một giá trị tiền tệ cho các tập hợp riêng dữ liệu trong một tổ chức lớn cũng tương tự như việc đưa ra các câu trả lời, chúng rất chủ quan và đã được xử lý với "thái độ hoài nghi" đáng xem xét.

Việc quyết định các ước lượng liên quan đến các mối hiểm họa khó giải quyết hơn ngay cả khi sử dụng cách tiếp cận nhất quán, có phương pháp và có cấu trúc để khuyến khích nhân viên tập trung vào các vấn đề xác định và vì thế, nhận dạng được các khoảng giá trị hợp lý.

Các hiểm họa phổ biến đối với hệ thống máy tính có thể được liệt kê như sau:

- các thảm họa tự nhiên;
- sự phá ngầm;
- sự phá hoại;
- gian lận;
- ăn trộm;
- sự cố tiện ích công cộng;
- lỗi phần cứng;
- lỗi do con người.

Dữ liệu lịch sử được sử dụng phổ biến trong ngành bảo hiểm để giúp cho việc đánh giá như vậy, nhưng sự non trẻ và đa dạng đồ sộ của ngành công nghệ thông tin làm giảm nhẹ cách tiếp cận này.

Những hiểm họa tượng trưng cho các thực thể trên nó vốn đã tồn tại. Mức độ mà chúng sẽ thực sự gây ra một tác động có hại trên một tổ chức phụ thuộc vào điểm yếu của tổ chức trước những hiểm họa đó. Như vậy, bất kỳ việc xây dựng nào cũng là đối tượng của một hiểm họa hỏa hoạn; việc xây dựng bằng

gỗ trong một vùng công nghiệp là một điểm yếu vô cùng cho một hiểm họa hơn là việc xây dựng bằng bê tông trên các khu đất sở hữu. Đánh giá khả năng có thể xảy ra một hiểm họa đặc biệt và sau đó gây ra một tác động nghiêm trọng trong một môi trường đặc biệt là một vấn đề phức tạp.

Khảo sát an toàn được tiến hành trong giai đoạn nhận dạng tài sản sở hữu, vì vậy, sẽ bao gồm việc xem xét tới các nhân tố được liệt kê dưới đây:

- Sự tồn tại các hệ thống phần cứng và phần mềm: tài liệu, các kiểm soát truy nhập, các khả năng hoạt động.
- Các ứng dụng xử lý dữ liệu: các chuẩn, tài liệu.
- Các hoạt động: các chuẩn, phổ biến thông tin, các thủ tục, các thư viện, lên kế hoạch ngẫu nhiên, lưu giữ tài liệu.
- Môi trường vật lý: độ tin cậy của các tiện ích chung, môi trường lân cận, kiểm soát truy nhập, tính an toàn của tòa nhà, các thủ tục bảo trì.
- Truyền dữ liệu: các đường truyền, các lắp đặt cáp, phân phối và phê chuẩn thông báo.
- Cá nhân: việc sử dụng các thủ tục, đào tạo, giám sát, phát triển nghề nghiệp.

Giai đoạn nhận dạng tài sản sở hữu được tiếp theo giai đoạn tính toán các rủi ro. Giai đoạn này mang lại cho những nhà quản lý một tập hợp ngắn gọn dữ liệu mà sau đó sẽ được sử dụng, làm cho việc đánh giá các biện pháp đối phó trở nên thuận tiện. Các hiểm họa được xem xét theo các chi phí ước đoán gắn liền với các tác động và tần số xuất hiện của chúng. Các ước đoán như vậy có thể được đưa ra theo các mức độ quan trọng và do đó, một tập hợp các giá trị được lượng tử hóa được xác định cả về chi phí tác động lẫn tần số xuất hiện. Làm việc theo khái niệm i (tác động) và f (tần số) với các giá trị thực tế và các tần số xuất hiện (xem bảng 1) sẽ thuận tiện hơn.

Bảng 1

i	Tác động (I)	f	Tần số xuất hiện (F)
1	10	1	Một lần trong 300 năm
2	100	2	Một lần trong 30 năm
3	1.000	3	Một lần trong 3 năm
4	10.000	4	Một lần trong 100 ngày
5	100.000	5	Một lần trong 10 ngày
6	1.000.000	6	Một lần trong 1 ngày

Sự mất mát dự tính có thể được tính toán từ:

Mất mát dự tính = Mất mát gắn liền với biến cố (I) x xác suất của biến cố (F).

Thang đo loga được sử dụng trong bảng này cung cấp các biến liên quan $I = 10^i$ và $F = (10^{(f-3)})/3$. Điều này dẫn tới giá trị dự tính mất mát hàng năm (Annual Loss Expectancy):

$ALE = I.F = (10^{(f+i-3)})/3$.

Ví dụ, một mất mát ước tính là \$10.000 xảy ra với một tần số là 3 năm một lần cho ALE là \$3.000, được làm tròn xuống là \$1.000. Việc tính toán ALE được đơn giản hóa nhờ phép lượng tử hóa được đưa ra như trên; một bảng ALE với các giá trị khác nhau của i và f sẽ làm giảm đi các tính toán. Việc ghép cặp của các tác động và các tần số xuất hiện phải được xử lý có

phương pháp; các khuôn dạng được in ra sẽ giúp cho việc ghi dữ liệu và tính toán các ALE liên quan, và một số lượng các các bộ phần mềm cũng có thể dùng được dành cho mục đích này.

Nếu một tài nguyên đặc biệt phải chịu các hiểm họa khác nhau thì nó phải được ghép cặp với mỗi một hiểm họa tương ứng, do đó ALE được tính toán. Một tổng liên tục ALE đối với mỗi tài nguyên bị tác động bởi một hiểm họa xác định, cần phải được phát triển theo cách đó.

Các tính toán ALE cung cấp sự quản lý với một danh sách ưu tiên các hiểm họa tiềm ẩn. Giai đoạn tiếp theo của việc phân tích rủi ro là xem xét các biện pháp đối phó an toàn khác nhau và các chi phí liên quan của chúng. Lợi ích của biện pháp đối phó được đánh giá từ sự khác biệt giữa tổng số ALE của hiểm họa với chi phí của biện pháp an toàn. Nếu nhà quản lý quyết định rằng, việc phân tích rủi ro đã cách ly một hiểm họa nghiêm trọng và biện pháp đối phó an toàn không thể thực hiện được trong tương lai gần thì việc phân tích rủi ro sẽ cung cấp một đại lượng đo thực tế về lượng tiền bảo hiểm cần đặt cho giai đoạn chuyển tiếp. *So sánh với* qualitative risk analysis. *Xem* FIPS Pub 65, risk analysis, risk analysis methodologies.

quantize ***lượng tử hóa*** Trong truyền thông, gán một giá trị trong một tập hợp cố định các giá trị vào một tín hiệu tương tự như một phần của quá trình chuyển đổi tương tự - số, ví dụ, trong điều biến mã xung, một tín hiệu tương tự được lấy mẫu, được lượng tử hóa, và một tập hợp tương ứng các xung nhị phân được tạo ra. *Xem* pulse code modulation.

quantizing noise ***tạp âm lượng tử hóa*** Trong truyền thông, nhiễu xuất hiện từ các quá trình chuyển đổi tương tự sang số và sau đó chuyển đổi số sang tương tự. Quá trình lượng tử hóa gây ra sai lệch trong các tín hiệu tương tự đầu vào và đầu ra. *Xem* quantize.

query language ***ngôn ngữ truy vấn*** Trong các cơ sở dữ liệu, một phần của hệ quản trị cơ sở dữ liệu mà cung cấp các công cụ cho truy vấn dữ liệu. Sự phức tạp của các phương tiện truy vấn thay đổi từ ngôn ngữ này tới ngôn ngữ khác. Các ngôn ngữ truy vấn cũng thường cung cấp một số phương tiện cho việc sửa đổi và cập nhật cơ sở dữ liệu. *Xem* database management system, relational database.

query modification ***sửa đổi câu truy vấn*** Trong an toàn cơ sở dữ liệu, một kỹ thuật trong đó các câu hỏi người sử dụng được sửa đổi để thích hợp với các quyền truy nhập của người sử dụng. Ví dụ, nếu một người sử dụng chỉ được phép truy nhập vào các bản ghi cá nhân dành cho một bộ phận xác định, và câu hỏi đầu vào dành cho tất cả các đối tượng là nữ giới trong tổ chức, thì câu hỏi sẽ được sửa đổi để thông tin được trả lại sẽ chỉ liên quan đến đối tượng là nữ giới trong bộ phận đã nói trên.

query set ***tập hợp câu truy vấn*** Trong an toàn cơ sở dữ liệu, một tập hợp các bản ghi được lựa chọn theo tiêu chuẩn chọn lựa của một câu hỏi

riêng biệt.

query set size control ***kiểm soát kích thước tập câu truy vấn*** Trong an toàn cơ sở dữ liệu, một dạng hạn chế ô mà giới hạn các câu hỏi dựa vào một tập hợp vô cùng nhỏ hoặc vô cùng lớn các bản ghi. Nếu một câu hỏi dựa vào một số ít bản ghi thì có thể suy luận ra các thống kê liên quan đến một cá nhân có thể cuối cùng. Nếu gộp một tập hợp vô cùng lớn các bản ghi (P) thì có thể được sử dụng các thống kê được phát ra, được ghép lại với các thống kê cho tập toàn bộ của các bản ghi (N) để suy luận ra dữ liệu trên tập hợp nhỏ ($N - P$) tập hợp các bản ghi. *So sánh với* audit expert, cell suppression, grouping, implied queries control, overlap control. *Xem* cell restriction, inference control.

queue ***hàng đợi*** (1) Trong các cấu trúc dữ liệu, một danh sách trong đó các mục được thêm vào tại điểm cuối và bị lấy ra từ điểm kia. (2) Trong các cấu trúc dữ liệu, các tiến trình hoặc các mục đợi dịch vụ theo nguyên tắc FIFO (vào trước ra trước). *So sánh với* stack. *Xem* list, FIFO.

queuing time ***thời gian hàng đợi*** Trong truyền thông, thời gian chờ đợi để gửi đi hoặc nhận lại một thông báo tránh tranh chấp.



Rabin signature ***chữ ký Rabin*** Trong xác thực, một phương pháp chữ ký số sử dụng trong phép mã DES. Người gửi tạo ra 36 khóa DES (k_1, k_2, ..., k_{36}) và 36 số ngẫu nhiên (x_1, x_2,..., x_{36}). Chúng là các khối đầu vào 64 bit để mã hóa DES. Thêm 36 số (y_1, y_2,... y_{36}) được tạo ra bằng việc mã hóa các giá trị x với các khóa DES tương ứng, nghĩa là $y_i = ek_i(x_i)$. Sau đó, các giá trị x và y được công bố như các khóa công khai cho chữ ký, cùng với một hàm (f).

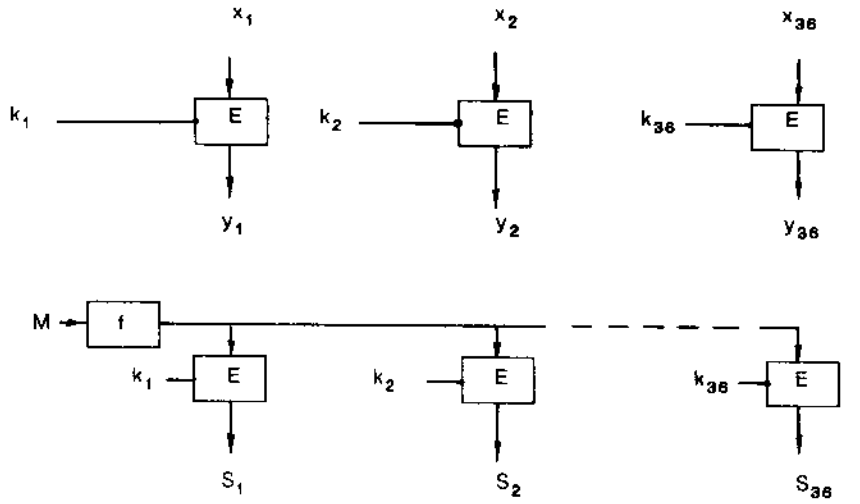
Người gửi tạo ra một chữ ký của một thông báo (M) bằng cách thao tác nó với thuật toán (f) đưa ra một đầu ra 64 bit. Đầu ra ($f(M)$) này được sử dụng như một đầu vào dành cho 36 phép tính DES với các khóa (k_1, k_2, ..., k_{36}). 36 đầu ra của các phép mã (S_1, S_2,... S_{35}) đó với $S_1 = ek_i(f(M))$, sẽ tạo ra một chữ ký số cho thông báo (M).

Người nhận phê chuẩn chữ ký này bằng cách yêu cầu 18 khóa được chọn từ người gửi, nghĩa là người nhận chọn ngẫu nhiên 18 số nguyên trong phạm vi từ 1-36. Người gửi cung cấp các khóa yêu cầu và sau đó người nhận kiểm tra từng khóa một:

$S_i = ek_i(f(M))$.

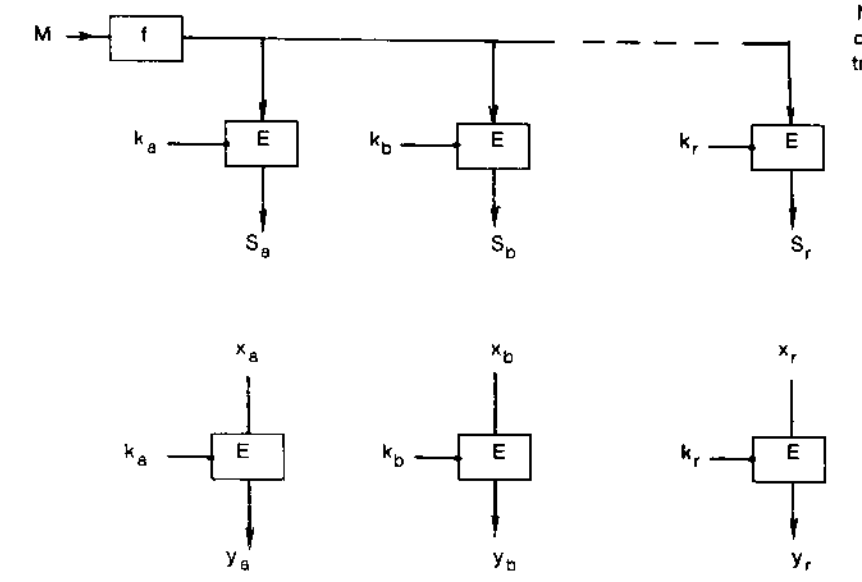
Trong trường hợp xảy ra bất đồng, người phân xử yêu cầu 36 khóa từ người gửi và kiểm tra chúng dựa vào 36 cặp khóa được công bố (x_1, y_1, ..., x_{36}, y_{36}), nghĩa là $y_i = ek_i(x_i)$ với i = 1..36. Sau đó, người phân xử kiểm tra 36 chữ ký ($S_i = k_i(f(M))$), nếu 19 chữ ký này hoặc nhiều hơn đúng thì người phân xử tuyên bố thông báo hợp lệ, nếu 18 chữ ký hoặc nhỏ hơn đúng thì người phân xử tuyên bố thông báo bị giả mạo.

Những người nhận đã cố gắng giả mạo một thông báo có thể làm được như vậy và khai triển 18 chữ ký hợp lệ từ các khóa do người gửi cung cấp, tuy nhiên, họ sẽ không thể đưa ra 18 chữ ký còn lại vốn phù hợp với các cặp khóa được công bố (x_i, y_i). Người gửi



Người gửi

Người nhận



Rabin signature: *chữ ký Rabin.*

có thể cung cấp 18 chữ ký thật và 18 chữ ký giả. Nếu tình cờ người nhận chọn đúng 18 khóa tương ứng với chữ ký thật thì người gửi có thể từ chối thông báo. Tuy nhiên, xác suất chọn lựa 18 số cho trước, một cách ngẫu nhiên, từ 36 số là 10^{10}. Trong thực tế, người nhận sẽ chọn ít nhất một trong các chữ ký giả, thủ tục kiểm tra sẽ bị lỗi trong trường hợp này, và người nhận sẽ từ chối chấp nhận thông báo. Về thực chất việc sử dụng ít hơn 36 khóa sẽ làm tăng khả năng một người gửi sẽ liều đưa ra một thông báo giả.

Kỹ thuật này đòi hỏi một tập hợp lớn các khóa công khai (36 khối 64 bit) và việc truyền với 18 khóa DES, thêm vào đó là 36 khối S 64 bit. Ngoài ra, bộ khóa công khai chỉ có thể được sử dụng dành cho một thông báo. Điều này đưa ra tổng phí truyền thông đối với chữ ký 64 bit là rất lớn. *So sánh với* ElGamal digital signature, Lamport-Diffie signature. *Xem* digital signature.

RACF ***sản phẩm RACF, phương tiện kiểm soát truy nhập tài nguyên***

Trong kiểm soát truy nhập, viết tắt của Resource Access Control Facility, một sản phẩm phần mềm an toàn của IBM, hỗ trợ trong việc kiểm soát sự truy nhập của người sử dụng vào các tập hợp dữ liệu, các khối dữ liệu của ứng dụng, các giao tác và các thiết bị đầu cuối.

RACF là một sản phẩm chương trình chạy trên hệ điều hành MVS và VM của IBM để cung cấp kiểm soát truy nhập được nâng cao. Nó đáp ứng các yêu cầu an toàn hệ thống và người dùng thông qua việc cung cấp các khả năng trong:

- nhận dạng và xác thực những người sử dụng;
- cho phép những người sử dụng truy nhập vào các nguồn tài nguyên được bảo vệ;
- kiểm soát các cách truy nhập vào các nguồn tài nguyên;
- ghi nhật ký và báo cáo hàng loạt các cố gắng truy nhập không được phép vào các nguồn tài nguyên được bảo vệ;
- an toàn quản trị để đáp ứng các mục đích an toàn của một cài đặt.

Truy nhập của người sử dụng có thể được cấp theo một nguyên tắc "cái gì đó người sử dụng biết" hoặc "cái gì đó người dùng có". Những người sử dụng được nhận dạng với một tên duy nhất, nghĩa là số hiệu nhận diện người dùng, và được cấp phát một mật khẩu. Một thẻ định danh của người thao tác cũng có thể được sử dụng thay cho hoặc thêm vào, việc xác minh mật khẩu cho quá trình xử lý tại thiết bị đầu cuối.

Những người sử dụng có thể được cấp truy nhập vào các tài nguyên của hệ thống tùy thuộc vào các đặc quyền truy nhập của họ, các đặc quyền này cũng chỉ rõ kiểu truy nhập được phép, ví dụ như đọc, cập nhật. Hơn nữa, những đặc quyền này có thể bị giới hạn một thời gian và ngày nào đó, như vậy sẽ chống lại được kẻ tấn công, kẻ cố gắng đạt được truy nhập vào một thiết bị đầu cuối ngoài giờ làm việc thông thường.

Việc ghi nhật ký và báo cáo các truy nhập, được RACF cung cấp, có thể cảnh báo quản lý, cả các cố gắng truy nhập không cho phép, một dấu hiệu chung về sự thử tấn công của một kẻ tấn công, lẫn sự sai khác mẫu truy nhập thông

thường của người sử dụng. Những sự khác nhau này có thể là một dấu chỉ báo về việc một kẻ tấn công thực hiện giả mạo thành công như một người sử dụng, hoặc có thể đoán nhận được một người sử dụng thực hiện truy nhập không cho phép.

RACF cung cấp một kiểm soát truy nhập linh hoạt, nó có thể đáp ứng các đòi hỏi an toàn của một cài đặt. Việc quản trị an toàn được làm cho thuận tiện trong RACF thông qua việc sử dụng các hồ sơ, dành cho cả những người sử dụng và các nguồn tài nguyên. Một người sử dụng có thể được nhận dạng như một cá nhân hoặc như một thành viên của một nhóm. Những hồ sơ này cung cấp thông tin an toàn liên quan về người sử dụng, ví dụ như số hiệu nhận diện người dùng, mật khẩu được mã hóa, các phân loại an toàn, thuộc tính của người sử dụng (ví dụ, các đặc quyền của người kiểm tra), chủ sở hữu của hồ sơ ... Thuộc tính của người sử dụng - thu hồi - ngăn chặn người sử dụng không được vào hệ thống, và vì vậy cung cấp một cơ chế cực kỳ đơn giản để rút lại tất cả các đặc quyền truy nhập vào lúc thử truy nhập.

Sự phân loại an toàn cho người sử dụng giống với kiểu phân loại trong quân đội, bao gồm một hệ thống phân cấp và một tập hợp các loại (category). Hệ thống phân cấp được mô tả như mức an toàn, mỗi cài đặt có thể kết hợp với các tên dành cho các mức an toàn, ví dụ như mật, với một số; số cao hơn, thì mức an toàn cao hơn. Một người sử dụng cũng có thể được cấp cho một tập hợp các loại, những loại như vậy có thể liên quan đến các chức năng công việc của chúng. Ví dụ, một nhân viên kế toán quan tâm đến quỹ xây dựng các dự án có thể được gán vào một tập hợp các loại {BUILDING, FINANCE}. Các nguồn tài nguyên được bảo vệ được cấp phát tương tự các phân loại an toàn.

Các quy tắc truy nhập của RACF phù hợp với các phân loại an toàn đều ít phức tạp hơn các phân loại của mô hình Bell-La Padula. Một người sử dụng được phép truy nhập vào một nguồn tài nguyên nếu mức an toàn của người sử dụng là ngang bằng hoặc lớn hơn mức an toàn của nguồn tài nguyên, và nếu tập hợp các loại nguồn tài nguyên là một tập hợp con của tập được người sử dụng nắm giữ. Vì vậy, nhân viên kế toán nêu trên sẽ được phép truy nhập vào một nguồn tài nguyên có phân loại mật và tập các loại {BUILDING}, nhưng không truy nhập vào một dữ liệu cùng mức an toàn nhưng lại thuộc tập loại khác {BUILDING, CONSTRUCTION}.

Việc quản trị kiểm soát truy nhập được đơn giản hóa rất nhiều nếu những người sử dụng đó có mức tương đồng cao theo quan điểm truy nhập, được đối xử như một nhóm. Ví dụ, một nhóm dự án có khả năng sẵn sàng cộng tác sử dụng các tệp đi theo dự án. Trong RACF, tất cả những người sử dụng thuộc về ít nhất một nhóm. Các nhóm lập nên một cấu trúc hệ thống phân cấp với các nhóm cấp trên sở hữu các nhóm khác thấp hơn theo dạng cây. Thông tin về các nhóm được lưu giữ trong các hồ sơ của nhóm trong cơ sở dữ liệu RACF. Các đặc tính an toàn thích hợp của các

nguồn tài nguyên được bảo vệ cũng được mô tả trong các hồ sơ tài nguyên. Trong trường hợp này, thông tin chứa trong hồ sơ bao gồm tên tài nguyên, chủ sở hữu hồ sơ, toàn bộ quyền truy nhập, danh sách truy nhập, phân loại an toàn, các tùy chọn kiểm toán, các tùy chọn cảnh báo và các tùy chọn thông báo.

Sự truy nhập vào nguồn tài nguyên được kiểm soát trước hết thông qua phân loại an toàn; sự phân loại an toàn này gồm một mức an toàn và một tập các loại. Nếu phân loại an toàn của người sử dụng thấp hơn so với phân loại an toàn của tài nguyên thì truy nhập bị từ chối.

Nếu phân loại an toàn của người sử dụng ngang bằng, hoặc hơn, phân loại tài nguyên thì kiểm tra thứ hai được thực hiện để quyết định liệu người sử dụng có đặc quyền truy nhập tùy ý cần thiết đối với tài nguyên không. Danh sách truy nhập vào hồ sơ của tài nguyên sẽ chỉ rõ kiểu truy nhập, ví dụ, cập nhật, đọc, thi hành được phép đối với một người sử dụng hoặc nhóm xác định; đặc quyền "none" ngăn chặn một người sử dụng hoặc nhóm không được truy nhập. Quyền truy nhập vạn năng đại diện cho quyền truy nhập ngầm định; những người sử dụng hoặc các nhóm không định rõ tên trong một danh sách truy nhập có thể được cấp truy nhập thông qua quyền truy nhập vạn năng.

Các thiết bị đầu cuối được tính đến trong tập hợp các tài nguyên được bảo vệ; như vậy, một người sử dụng hợp pháp có thể được cho trước các đặc quyền truy nhập vào một thiết bị đầu cuối xác định. Điều này làm tăng khả năng an toàn; thậm chí nếu một kẻ tấn công có được thông tin về số hiệu nhận dạng người dùng và mật khẩu, thì thông tin này chỉ có giá trị khi kẻ tấn công có thể truy nhập vào hệ thống từ thiết bị đầu cuối được cấp cho người sử dụng hợp pháp, trong các giai đoạn giờ/ngày được xác định cho người sử dụng.

Các hồ sơ của người sử dụng/nhóm và nguồn tài nguyên cung cấp một cơ chế không phức tạp cho RACF để quyết định xem có bảo đảm yêu cầu truy nhập của một người sử dụng hay không.

Truy nhập như vậy chỉ được cấp cho nếu hồ sơ của người sử dụng/nhóm cung cấp với hồ sơ của nguồn tài nguyên được yêu cầu, được bảo vệ.

RACF làm cho việc ghi nhật ký và báo cáo các sự cố an toàn liên quan được thuận tiện. Một nhật ký an toàn được ghi khi có các cố gắng truy nhập trái phép vào hệ thống bị phát hiện và không bắt buộc ghi đối với các cố gắng được phép hoặc không được phép, bị phát hiện truy nhập vào các nguồn tài nguyên được bảo vệ, hoặc để đưa ra các lệnh RACF.

Với các vi phạm an toàn bị phát hiện, hệ thống ghi nhật ký cũng gửi các thông báo tới bảng điều khiển (console) an toàn. Có thể, song không bắt buộc báo cáo trực tiếp về các nỗ lực truy nhập không cho phép phát hiện được vào các tài nguyên được bảo vệ, hoặc sửa đổi nội dung của cơ sở dữ liệu RACF. Thêm vào đó, người sử dụng có thể yêu cầu thông báo một cố gắng truy

nhập không cho phép vào một nguồn tài nguyên. Thông tin mang tính chất thống kê như giờ/ngày hoặc số lần mà người sử dụng nhập vào một hệ thống, hoặc truy nhập một nguồn tài nguyên xác định cũng có thể được cung cấp. Hiện nay RACF cho phép một cài đặt MVS/XA để đáp ứng mức an toàn lớp C2 của Bộ Quốc phòng Mỹ. *Xem* access list, Bell-La Padula model, C2, discretionary access control, intrusion detection, Orange Book, password, security level, something the user has, something the user knows, user id.

radar sensor ***bộ cảm biến rađa*** Trong an toàn vật lý, một bộ phát hiện xâm nhập do các thay đổi trong tần số của một tín hiệu rađa nhận được do sự chuyển động của một vật đi qua tia gây ra. *Xem* Instrusion detection.

radio frequency emissions ***(các) phát xạ tần số vô tuyến*** *Đồng nghĩa với* compromising emanations.

radio frequency interference ***nhiễu tần số vô tuyến*** *Xem* jamming. *Đồng nghĩa với* electromagnetic interference.

radio frequency motion detector ***bộ phát hiện chuyển động bằng tần số vô tuyến*** Trong an toàn vật lý, một hệ thống phát hiện xâm nhập trong đó, các vùng được bảo vệ bị bão hòa các sóng tần số vô tuyến và một tín hiệu cảnh báo được bắt đầu nếu mẫu bị nhiễu. *Xem* radar sensor.

radix ***cơ số*** Trong toán học, trong một hệ thống đếm cơ số, giá trị tổng cộng của một số được biểu diễn bởi một chuỗi các ký tự là tổng của mỗi ký tự nhân với trọng số của nó. Tỷ số trọng số của một chữ số trên trọng số một số đứng trước là cơ số đối với hệ thống số được sử dụng và nó luôn là một số nguyên dương. Vì vậy, trong một hệ thống thập lục phân thì cơ số là 16 và số 123 có giá trị ở hệ 10 là 291 = ((1 x 16 x 16) + (2 x 16) + 3). *Xem* base.

Rainbow series ***xeri chuẩn Rainbow*** Trong an toàn máy tính, một tập hợp các chuẩn có liên quan tới an toàn máy tính do bộ quốc phòng Hoa Kỳ đưa ra. Sách Da Cam xem xét việc đánh giá an toàn máy tính, Sách Vàng giải quyết các cách xác định mức an toàn thích hợp nhất cần thiết đối với một cài đặt riêng biệt. Sách Đỏ xem xét vấn đề an toàn mạng còn Sách Xanh xử lý các cơ sở dữ liệu an toàn. *Xem* Blue Book, Orange Book, Red Book, Yellow Book.

RAM *Xem* random access memory.

RAMP *Xem* Rating Maintenance Program.

random ***ngẫu nhiên*** Trong toán học, một tên các đặc tính có khả năng được lựa chọn như nhau từ tổng số các khả năng, vì thế không thể đoán trước.

random access ***truy nhập ngẫu nhiên*** Trong tính toán, một truy nhập vào dữ liệu mà từ vị trí kế tiếp tính từ nó, một từ hoặc một byte được tìm thấy mà không phụ thuộc vào vị trí của một từ hoặc một byte được truy nhập trước đây. *So sánh với* direct access, sequential access.

random access memory ***bộ nhớ truy nhập ngẫu nhiên*** (1) Trong tính toán, một chip nhớ được sử dụng với các bộ vi xử lý, thông tin có thể được đọc và được ghi vào bộ nhớ nhưng các

nội dung bị mất khi nguồn cung cấp bị ngắt. (2) Trong tính toán, một dạng lưu giữ bất kỳ trong đó thời gian truy nhập đối với mục dữ liệu bất kỳ không phụ thuộc vào vị trí của dữ liệu thu được gần nhất.

random cipher *mã pháp ngẫu nhiên* Trong mật mã, một mã pháp trong đó, với một bản mã cho trước và một khóa cho trước, quá trình giải mã giống như quá trình bất kỳ để đưa ra một bản rõ. Kết quả của quá trình giải mã với một khóa cho trước và một bản mã cho trước được phân phối đồng đều trên dãy đầy đủ các thông báo có nghĩa và vô nghĩa, với độ dài cho trước, về mặt ngôn ngữ. *Xem* cryptographic key, information theory.

random data perturbation *(sự) gây nhiễu bằng dữ liệu ngẫu nhiên* Trong an toàn dữ liệu, một kỹ thuật gây nhiễu dựa vào bản ghi trong đó một số ngẫu nhiên được thêm vào mỗi mục dữ liệu, khi nó được trích ra, và trước khi nó được sử dụng để tính toán một thống kê cần thiết. *So sánh với* random sample queries. *Xem* inference control, perturbation, record based perturbation.

random line switching *chuyển mạch đường ngẫu nhiên* Trong an toàn máy tính, một kỹ thuật giảm ảnh hưởng của các phát xạ gây hại từ một VDU, bằng cách sử dụng thường xuyên chuyển mạch ngẫu nhiên các mẫu tín hiệu. Tuy nhiên, kỹ thuật này có thể tạo ra sự nhấp nháy màn hình và một kẻ nghe trộm có thể giải mã các tín hiệu dựa vào khả năng hoán vị chậm. *So sánh với* white noise emitter. *Xem* compromising emanations, van Eck phenomenon.

random numbers *(các) số ngẫu nhiên* Trong các ứng dụng, các số được sinh ra bởi một quá trình ngẫu nhiên có các thuộc tính là mỗi số không phụ thuộc vào các số được sinh ra trước nó, và phân bố xác suất của các số này tuân theo một luật phân bố xác định, ví dụ phân bố Gauss, Poisson, phân bố đều.

Việc ứng dụng các số ngẫu nhiên này sinh khi một đầu vào được đòi hỏi là không thể đoán trước, nghĩa là độc lập với các đầu vào trước đó. Các số ngẫu nhiên thực sự chỉ có thể được tạo ra bởi một quá trình ngẫu nhiên xác thực, ví dụ: số điện tử phát ra bởi một điện cực được đốt nóng trong một khoảng thời gian ngắn.

Tuy nhiên, phép xấp xỉ các dãy số ngẫu nhiên được hiểu như các số giả ngẫu nhiên có thể được sinh ra bằng các kỹ thuật toán học; các bộ tạo số giả ngẫu nhiên có thể được cung cấp qua các thủ tục phần mềm hoặc được kết hợp vào các phần mềm ngôn ngữ bậc cao. Các số giả ngẫu nhiên này do một thủ tục tất định tạo ra và vì vậy, không phù hợp với định nghĩa chặt chẽ về một số ngẫu nhiên, nhưng trong các giới hạn của mình, chúng vẫn thích hợp với nhiều ứng dụng.

Các chuỗi số giả ngẫu nhiên được sinh ra bởi một đầu vào xác định hoặc mầm khởi tạo. Một kỹ thuật lấy bình phương số trước đó và rút ra các chữ số ở giữa để tạo hành số tiếp theo trong chuỗi; tuy nhiên các thủ tục hiện tại thường dựa trên các bộ tạo số đồng dư tuyến

tính (LCG). Các số được tạo theo công thức sau:

$x2 = \text{mod}(a * x1 + c, m)$.

Trong đó: $x1$ = số ngẫu nhiên trước đó, $x2$ = số ngẫu nhiên hiện tại, a, c, m là các số nguyên được chọn cho bộ tạo số, $\text{mod}(x, m) = x - \{x/m\} * m$ và $\{x/m\}$ = phần nguyên của phép chia. Các tham số a, c và m phải được chọn cẩn thận để đưa ra các chuỗi số giả ngẫu nhiên có đặc tính ngẫu nhiên mong muốn.

Nói riêng, c và m phải không có thừa số chung, a phải lớn hơn căn bậc hai của m, còn m phải là số nguyên tố bằng hoặc nhỏ hơn số nguyên lớn nhất mà ngôn ngữ lập trình có thể xử lý được. Số do LCG tạo ra phụ thuộc vào số trước đó trong chuỗi. Vì vậy, nếu chuỗi luôn luôn khởi đầu với mầm khởi tạo giống nhau thì nó sẽ sinh ra kết quả giống nhau đối với mỗi lần chạy máy tính. Ngoài ra nếu một số cho trước xuất hiện tại vị trí m, và tại vị trí n trong chuỗi thì chuỗi sau vị trí n sẽ đồng nhất với chuỗi sau vị trí m.

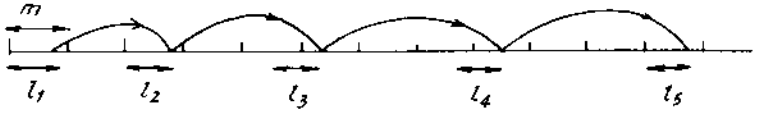
Vì tập tổng các số nguyên giả ngẫu nhiên có thể bị giới hạn trong khoảng $0..m - 1$, nên cuối cùng LCG sẽ đưa ra một số có phân bố sẵn, và vì vậy khi chạy lâu, chắc chắn sẽ bộc lộ các tính chất lặp lại. Chu kỳ của các vòng lặp này thậm chí sẽ nhỏ hơn m nếu c và m có các thừa số chung. Có thể mở rộng chu kỳ với một giá trị m cho trước bằng cách sử dụng hai LCG liên kết với nhau, với các giá trị khác nhau của m.

Phân bố xác suất của các chuỗi LCG trên danh nghĩa là đều, nhưng cũng phải kiểm tra các đặc tính của chúng nếu sử dụng các chuỗi dài. Nếu các số ngẫu nhiên có yêu cầu có phân bố Gauss hoặc Poisson, thì các số phải qua các phép biến đổi cần thiết.

Các thuật toán mã hóa miêu tả các bộ tạo giả ngẫu nhiên hoàn thiện khi một thay đổi nhỏ trong bản rõ sẽ tạo ra một sự thay đổi nghiêm trọng trong văn bản mã sau đó. Các chế độ phản hồi mã và phản hồi đầu ra của DES sử dụng hiệu quả thuật toán để đưa ra một chuỗi giả ngẫu nhiên cho các chuỗi bit mật mã được sử dụng trong phép mã dòng.

Một vùng ứng dụng đối với các số ngẫu nhiên xuất hiện trong lĩnh vực an toàn dữ liệu.

Trong một số trường hợp, việc xác thực giữa hai thực thể truyền thông được thiết lập bằng cách tạo ra một số ngẫu nhiên. Số này sau đó được nối vào một



random numbers: *các số ngẫu nhiên*. Lược đồ một LCG cho thấy cách chia một đường thẳng thành các khoảng bằng nhau m, nó có thể tạo ra các số ngẫu nhiên. Vị trí mỗi số bên trong các khoảng tương ứng bị đặt lung tung. Nó rút ra từ việc dùng hàm modulo và dẫn tới một chuỗi giả ngẫu nhiên.

thông báo, được mã hóa bằng một khóa bí mật và được một bên liên lạc truyền đi. Đáp ứng lại thông báo này, cũng gồm có số ngẫu nhiên tương tự, hoặc một hàm nào đó của nó, cho người gửi ban đầu một đảm bảo rằng, nó là một câu trả lời xác thực cho một thông báo riêng biệt.

Trong trường hợp này, điều chủ yếu là không có kẻ tấn công nào có thể suy luận ra chuỗi các số ngẫu nhiên nếu kẻ tấn công nhận được một trong chúng. Điều này có thể đạt được bằng cách phản hồi lại số ngẫu nhiên được sinh ra sau cùng vào một thiết bị mã, (ví dụ, một vi mạch DES), với khóa bí mật khác, mã hóa nó và thực hiện thêm các thao tác toán học để đưa ra một số ngẫu nhiên kế tiếp.

Một khía cạnh quan trọng của việc tạo ra các số ngẫu nhiên nảy sinh trong quá trình phát triển các chuỗi bit mật mã dành cho các mã pháp dòng. *Xem* cryptographic bit stream, cryptography, high-level language, LCG, replay, seed, stream cipher.

random process ***quá trình ngẫu nhiên*** Trong toán học, một quá trình không thể quyết định hoàn toàn trước đầu ra từ sự hiểu biết về các biến hệ thống. Một quá trình trong đó kết quả phụ thuộc vào một hay nhiều biến cố ngẫu nhiên. *Xem* random numbers.

random rounding ***làm tròn ngẫu nhiên*** Trong an toàn cơ sở dữ liệu, một dạng gây nhiễu dựa trên kết quả trong đó, thống kê được làm tròn ngẫu nhiên hoặc tới một bội số cao hơn, hoặc thấp hơn tiếp đó của cơ số làm tròn. *So sánh với* controlled rounding, systematic rounding. *Xem* inference control, result-based perturbation.

random sample queries ***(các) câu truy vấn mẫu ngẫu nhiên*** Trong an toàn cơ sở dữ liệu, một kỹ thuật gây nhiễu dựa trên bản ghi trong đó, một thống kê được tính toán từ một mẫu các bản ghi, thỏa mãn tiêu chuẩn hỏi đáp, chứ không phải tập toàn bộ. *So sánh với* random data perturbation. *Xem* inference control, perturbation, record based perturbation.

range ***phạm vi, khoảng*** Trong toán học, một tập hợp các giá trị đầu ra của một hàm. *So sánh với* domain.

rank ***xếp hạng // hạng*** (1) Trong toán học, xếp hạng là sắp xếp theo chiều tăng hay giảm theo một tiêu chuẩn nào đó. (2) Trong tính toán, hạng là một số đo vị trí tương đối trong một mảng, nhóm, chuỗi hoặc trong phân loại. *Xem* array.

rate ***suất tin*** Trong lý thuyết thông tin, một độ đo số lượng trung bình các bit thông tin trong mỗi ký tự của một thông báo. Xét tập các thông báo có độ dài N, với một ngôn ngữ cho trước, nếu entropy của các thông báo là H thì suất tin đối với mọi dãy của ngôn ngữ có độ dài N được cho bởi H/N. *Xem* absolute rate, entropy.

rating maintenance program ***chương trình duy trì đánh giá*** Trong an toàn máy tính, một chương trình NCSC cho phép cập nhật việc đánh giá an toàn các hệ thống máy tính, phù hợp với Sách Da Cam vì các hệ thống như vậy trải qua các sửa đổi không tránh được trong vòng đời của chúng. Các thủ

tục đánh giá trong Sách Da Cam dài dòng và nó sẽ không thực tế để đảm trách các đánh giá lại như vậy mỗi lần hệ thống được sửa đổi. *Xem* Orange Book.

rational number ***số hữu tỷ*** Trong toán học, một số bất kỳ có thể được biểu thị bằng tỷ số của hai số nguyên với số chia khác không.

raw data ***dữ liệu thô*** Trong tính toán, dữ liệu chưa được xử lý và rút gọn.

RBAC *Xem* rule-based access control.

RD ***dữ liệu bị hạn chế*** Viết tắt của Restricted data.

RDC *Xem* remote diagnostic center.

read ***đọc*** (1) Trong an toàn máy tính, một thao tác cơ bản mà chỉ dẫn tới luồng thông tin từ một đối tượng tới một chủ thể. *So sánh với* write. *Xem* object, subject. (2) Trong tính toán, một quá trình nhận hoặc diễn dịch dữ liệu từ một thiết bị đầu vào, phương tiện lưu giữ hoặc phương tiện khác.

read access ***truy nhập đọc*** Trong an toàn máy tính, sự cho phép đọc thông tin. *So sánh với* write access. *Xem* read.

read-only memory ***bộ nhớ chỉ đọc*** Trong tính toán, một thiết bị lưu giữ, nội dung của chúng chỉ có thể được thay đổi bởi một người sử dụng riêng biệt, thông qua các điều kiện hoạt động riêng biệt, hoặc bởi một xử lý bên ngoài riêng biệt. Lưu giữ chỉ đọc có thể bao gồm phương tiện lưu giữ tại nơi thao tác ghi bị hệ điều hành hoặc thiết bị máy móc nào đó ngăn chặn, ví dụ, một nhãn trên một đĩa. Thuật ngữ ROM quy ước bao hàm một thiết bị lưu giữ không được thiết kế để các thủ tục ghi thông thường sửa đổi được và được sử dụng để lưu giữ thông tin cố định trên các máy tính và các máy vi tính.

ready state ***trạng thái sẵn sàng*** Trong truyền dữ liệu, một điều kiện tại mạch ghép nối DTE/DCE mà chỉ ra DTE được chuẩn bị để chấp thuận một cuộc gọi đang tới và DCE đã sẵn sàng chấp thuận một yêu cầu gọi. *Xem* DCE, DTE, call request.

real number ***số thực*** Trong toán học, một số có thể được biểu diễn theo một số lượng có hạn hoặc vô hạn các số trong hệ đếm cơ số cố định. *Xem* radix.

realtime ***thời gian thực*** Trong tính toán, nói tới các thao tác được thực hiện kết hợp với quá trình xử lý bên ngoài hoặc người sử dụng nào đó và chúng được yêu cầu để đáp ứng sự ràng buộc về thời gian được đặt ra bởi xử lý hoặc người sử dụng này, ví dụ, kiểm soát một hệ thống hướng dẫn bay, một dịch vụ thông tin trực tuyến. *Xem* realtime input, realtime output, realtime reaction.

realtime input ***đầu vào thời gian thực*** Trong tính toán, dữ liệu đầu vào được nhận vào trong hệ thống theo một thang thời gian, hoặc trong khoảng thời gian ngắn do hệ thống khác nào đó quyết định. *So sánh với* realtime output. *Xem* realtime.

realtime operation ***hoạt động thời gian thực*** *Xem* realtime.

realtime output ***đầu ra thời gian***

thực Trong tính toán, một dữ liệu đầu ra được phân phối trong một thang thời gian, hoặc trong khoảng thời gian ngắn, do hệ thống khác nào đó quyết định . *So sánh với* realtime input. *Xem* realtime.

realtime reaction ***phản ứng thời gian thực*** Trong an toàn máy tính, một phản ứng trước một cố gắng xâm nhập được phát hiện và được chuẩn đoán trong thời gian ngăn chặn xâm nhập thực sự. *Xem* penetration, realtime.

reasonableness check ***kiểm tra tính hợp lý*** Trong tính toán, một kiểm tra sự tồn tại của một lỗi hiển nhiên, ví dụ, bằng cách kiểm tra một giá trị dữ liệu nằm trong một dải giá trị xác định trước.

received data ***dữ liệu được tiếp nhận*** Trong truyền dữ liệu, tuyến dữ liệu dành cho dữ liệu được tiếp nhận. *So sánh với* transmitted data. *Xem* RS-232C.

received line signal detector ***bộ phát hiện tín hiệu qua đường dây thu*** Trong truyền thông dữ liệu, một tín hiệu từ một modem tới một máy tính để báo cho nó biết có thiết bị nào đó đang cố gắng nối tới. Nó có thể được sử dụng để khởi động một máy tính để phát ra một lời mời đăng nhập. *Xem* log on, MODEM, RS-232C. *Đồng nghĩa với* carrier detect.

receive only ***chỉ thu, chỉ nhận*** Trong truyền thông dữ liệu, các thiết bị đầu cuối hoặc thiết bị khác có khả năng nhận dữ liệu hoặc thông báo nhưng thiếu bàn phím hoặc thiết bị nhập khác.

receiver ***máy thu, bên nhận*** (1) Trong truyền thông dữ liệu, một chủ thể đọc từ một kênh truyền thông. *So sánh với* SENDER. *Xem* channel, subject. (2) Người, tổ chức hoặc thực thể khác có trách nhiệm nhận một thông báo. *So sánh với* sender.

receiver's correspondent bank ***ngân hàng tương ứng của người nhận*** Trong hoạt động ngân hàng, một nhà băng nhận các quỹ nhân danh người nhận từ người gửi hoặc nhà băng thích hợp của người gửi. *So sánh với* sender's correspondent bank.

receiver signal element timing ***định thời phần tử tín hiệu nhận*** Trong truyền thông dữ liệu, một tín hiệu được sử dụng trong các modem đồng bộ. Trong trường hợp dữ liệu được tiếp nhận, modem cung cấp tín hiệu này hoặc nhịp đồng hồ. *So sánh với* transmitter signal element timing. *Xem* RS-232C, synchronous modem.

receiving bank ***ngân hàng nhận*** Trong hoạt động ngân hàng, một ngân hàng được phân phối thông báo.

recipient ***nơi nhận, người nhận*** (1) Trong hoạt động ngân hàng, thành viên (logic hoặc không) có trách nhiệm nhận một thông báo dịch vụ mật mã. *So sánh với* originator, sender. *Xem* cryptographic service message. (2) Trong truyền thông dữ liệu, người, tổ chức hoặc thực thể khác mà có trách nhiệm và được phép nhận một thông báo. *So sánh với* originator. *Xem* message.

reciprocal ***tương hoán, tương hỗ*** Trong quản lý rủi ro, một chiến lược khôi phục tai họa, được thông qua trong phạm vi hoặc giữa các tổ chức,

bằng cách sử dụng các bố trí dự phòng tương hỗ giữa các cài đặt trong các tổ chức. *So sánh với* internal reciprocal.

reconciliation ***(sự) làm cho khớp, (sự) điều hòa*** Trong kiểm toán, điều này gắn liền với sự nhận dạng hoặc phân tích các điểm khác nhau được phát hiện ra giữa các giá trị chứa đựng trong hai tệp về căn bản giống nhau hoặc giữa một tệp chi tiết và một tổng kiểm soát.

record ***bản ghi // ghi lại*** (1) Trong tính toán, bản ghi là một tập hợp các dữ liệu có quan hệ với nhau được coi như một đơn vị thống nhất, ví dụ, các chi tiết về tên, địa chỉ, tuổi, nghề nghiệp của một người làm công trong một hồ sơ cá nhân. *So sánh với* field. *Xem* logical record, physical record. (2) Trong tính toán, ghi lại là lưu giữ các tín hiệu trên một phương tiện ghi nhớ để sử dụng sau này.

record based perturbation ***(phép) gây nhiễu dựa trên bản ghi*** Trong an toàn cơ sở dữ liệu, một hình thức gây nhiễu áp dụng cho các bản ghi khi chúng được trích ra trước khi sử dụng chúng trong tính toán thống kê cần thiết. Gây nhiễu có thể ở dạng cộng thêm các số ngẫu nhiên và các mục dữ liệu tìm được hoặc chọn lựa/loại ra các mục dữ liệu, vì vậy toàn bộ thống kê chỉ được tính toán trên cơ sở mẫu dữ liệu tìm được. *So sánh với* result-based perturbation. *Xem* inference, perturbation, statistical database.

record layout ***mẫu bản ghi, sơ đồ bản ghi*** Trong tính toán, một cách thức dữ liệu được tổ chức trong một bản ghi, nghĩa là mô tả và kích thước của các trường. *Xem* field.

record length ***độ dài bản ghi*** Trong tính toán, số lượng các từ hoặc ký tự trong một bản ghi. *Xem* word, record.

record lock ***khóa bản ghi*** Trong tính toán, một phương tiện từ chối truy nhập vào một bản ghi trên một tệp. Nó được sử dụng trong các hệ thống đa người sử dụng để ngăn chặn hai người sử dụng đồng thời cập nhật lên cùng một bản ghi. *So sánh với* file lock. *Xem* record.

record separator character ***ký tự tách bản ghi*** Trong tính toán, thành phần chỉ báo định rõ ranh giới logic giữa hai bản ghi. *Xem* record.

recovery ***(sự) phục hồi, (sự) khôi phục*** Trong lĩnh vực độ tin cậy, hoạt động đặt một hệ thống trở về trạng thái không có lỗi để thao tác thông thường có thể hồi phục lại từ đó.

recovery procedures ***(các) thủ tục khôi phục*** (1) Trong an toàn máy tính, các thao tác cần thiết để phục hồi lại khả năng tính toán của một hệ thống và các tệp dữ liệu sau khi hệ thống bị lỗi hoặc thâm nhập. *Xem* penetration. (2) Trong truyền thông dữ liệu, các quá trình nhờ nó các trạm chỉ ra cố gắng giải quyết các sai sót hoặc các tình trạng xung đột nảy sinh do một trục trặc nào đó, hoặc do hoàn cảnh bên ngoài, trong truyền dữ liệu.

recursion analysis ***phân tích đệ quy*** Trong mã thám, một kỹ thuật quyết định mối quan hệ đệ quy tuyến tính của một thanh ghi dịch chuyển tuyến

tính, tạo ra một dòng bit mật mã cho mã dòng. *Xem* cryptographic bit stream, linear recurrence relation, linear feedback shift register, stream cipher.

recursion length ***độ dài đệ quy*** *Đồng nghĩa với* linear complexity.

recursive routine ***thường trình đệ quy, thủ tục đệ quy*** Trong tính toán, một thường trình có thể được sử dụng như một thường trình của chính nó, tự gọi trực tiếp hoặc được gọi bởi một thường trình khác, một thường trình mà tự gọi đến chính mình. *So sánh với* iteration. *Xem* recursive subroutine.

recursive subroutine ***chương trình con đệ quy*** Trong tính toán, một chương trình con tự gọi nó. Trạng thái của chương trình con này phải được lưu giữ trong mỗi lần gọi kế tiếp, còn dữ liệu biểu diễn trạng thái thường được lưu giữ trên một ngăn xếp. *Xem* recursive routine, stack, subroutine.

red ***đỏ*** Trong an toàn truyền thông, ám chỉ thiết bị và các đường dây điều khiển thông tin không được mã hóa, được phân loại. *So sánh với* black.

red/black concept ***khái niệm đỏ/đen*** Trong an toàn truyền thông, kiểm soát sự tách bạch và lộ trình đối với các hệ thống dây đỏ và đen.

Red Book ***Sách Đỏ*** *So sánh với* Blue Book, Orange Book, Yellow Book. *Xem* Rainbow Series. *Đồng nghĩa với* TNI.

red tape operation ***thao tác nội dịch*** Trong tính toán, một thao tác trên dữ liệu cần thiết cho các mục đích bên trong nhưng không góp phần vào câu trả lời cuối cùng.

reduced set of residues ***tập rút gọn các phần dư*** Trong toán học, một tập hợp con các phần dư đối với số nguyên n cho trước, nơi mà mỗi phần tử của tập hợp này là nguyên tố cùng nhau với n. Ví dụ, nếu n là 12, tập rút gọn của các số phần dư sẽ là {1,5,7,11}. *Xem* relatively prime, residue.

redundancy ***dư thừa, phần dư, phần dự phòng*** (1) Trong lý thuyết thông tin, mức độ khác nhau giữa suất tin tuyệt đối và suất tin của ngôn ngữ. *Xem* absolute rate, rate. (2) Trong lĩnh vực độ tin cậy, việc sử dụng thêm các thành phần của hệ thống để giảm bớt các ảnh hưởng của sự cố thành phần. *Xem* hardware redundancy, information redundancy, software redundancy, time redundancy. (3) Trong truyền thông, một phần nội dung thông tin thô của một thông báo có thể được loại ra mà không làm mất bất kỳ thông tin chính nào. Trong máy tính và truyền thông dữ liệu, các ký tự dư, ví dụ, các bit chẵn lẻ, được thêm vào dữ liệu để cung cấp một phương pháp phát hiện lỗi khi truyền hoặc xử lý. *Xem* parity checking, redundancy checking.

redundancy checking ***(phép) kiểm tra dư thừa*** Trong các mã, việc thực hiện một phép tính trên dữ liệu nhận được và so sánh các kết quả với các mã dư để kiểm tra các lỗi xử lý và lỗi truyền nào đó *Xem* error correction code, error detection code, redundant code.

redundant code ***mã dư*** Trong các mã, các bit phụ được thêm vào các ký tự với các mục đích kiểm tra lỗi, ví dụ, các bit cờ và mã điều chỉnh tự động.

Xem redundancy checking, Hamming code, parity checking.

redundant processing ***xử lý dư*** Trong kiểm toán, sự lặp lại quá trình xử lý và đi kèm theo so sánh các kết quả riêng lẻ sao cho bằng nhau.

RedX ***virut RedX*** Trong an toàn máy tính, đó là một loại virut lây nhiễm các tệp COMMAND.COM, và các tệp COM, ảnh hưởng đến thao tác khi chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

re-encipher from master key ***mã lại từ khóa chính*** Trong quản lý khóa, một phương tiện được cung cấp trong các hệ thống quản lý khóa sử dụng các khóa phiên. Các khóa phiên này được mã hóa bằng khóa mã khóa của thiết bị đầu cuối hoặc truyền thông đan chéo trong suốt quá trình truyền, và được lưu giữ dưới các khóa chính trong khi nằm trên các máy tính chủ hoặc nút. Các phương tiện an toàn phải được cung cấp để chuyển lại các khóa phiên được mã hóa như trên từ phép mã bằng khoá mã khóa thành một khóa khác. Phép mã hóa lại từ khóa chính là một phương tiện tạo ra khóa phiên nhờ giải mã bằng khóa chính, sau đó mã hóa lại nó bằng các khóa thiết bị đầu cuối hoặc truyền thông đan chéo. Các chức năng này được thực hiện trong các modun chống giả mạo với các khóa chính; vì vậy không có các khóa nào trong quá trình, mà luôn có sẵn ở dạng rõ ở bên ngoài modun. *So sánh với* re-encipher to master key. *Xem* key-encrypting key, session key.

re-encipher to master key ***mã lại thành khóa chính*** Trong quản lý khóa, một phương tiện giống với phương tiện giải mã lại từ khóa chính. Trong trường hợp này, các khóa phiên đã mã được giải mã bằng các khóa mã khóa của thiết bị đầu cuối hoặc truyền thông đan chéo, và được mã hóa lại bằng khóa chính. *So sánh với* re-cipher from master key. *Xem* key-encrypting key, session key.

reference ***chuẩn, tham chiếu*** Trong hoạt động ngân hàng, một ký tự nhận diện hoạt động giao dịch thường được tính đến như phần thông tin do chính giao dịch cung cấp, sau đó có thể được sử dụng để phân biệt giao dịch được nhận diện với các giao dịch khác, chẳng hạn sự điều hòa tài khoản nostro. *Xem* nostro account.

reference monitor ***bộ giám sát tham chiếu*** Trong kiểm soát truy nhập, một khái niệm kiểm soát an toàn trong đó một máy trừu tượng dàn xếp các truy nhập tới các đối tượng thông qua các chủ thể. Theo nguyên tắc, một giám sát tham chiếu phải được tách rời (trong đó nó dàn xếp mọi truy nhập) hoàn toàn khỏi việc sửa đổi thông qua các thực thể của hệ thống, và có thể kiểm tra được. Một nhân an toàn là sự thực hiện đầy đủ của một giám sát tham chiếu với một cơ sở phần cứng cho trước. *Xem* component reference monitor, object, reference monitor concept, security kernel, subject.

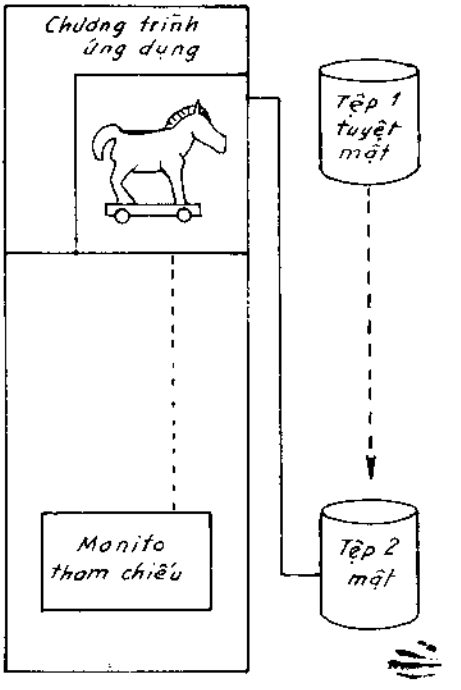
reference monitor concept ***khái niệm giám sát tham chiếu*** (1) Trong kiểm soát truy nhập, một khái niệm kiểm soát truy nhập ám chỉ đến một máy trừu tượng vốn dàn xếp tất cả các

truy nhập tới các đối tượng thông qua các chủ thể. *Xem* access, object, reference monitor, reference validation mechanism, subject. (2) Trong kiểm soát truy nhập, một khái niệm kiểm soát truy nhập trong đó một máy trừu tượng dàn xếp tất cả các truy nhập tới các đối tượng thông qua các chủ thể.

Hệ thống máy tính buộc những người sử dụng, các tiến trình đưa tất cả các yêu cầu truy nhập tới bộ giám sát tham chiếu; các đặc quyền của người sử dụng hoặc tiến trình, những gì liên quan đến đối tượng này đều được kiểm tra với mỗi truy nhập. Theo cách này, có thể không cần thiết phê chuẩn (tính hợp lệ) mỗi đoạn mã của chương trình ứng dụng đối với các vi phạm an toàn tiềm ẩn.

Nếu tiến trình mà chương trình đang hoạt động dưới nó, không có các đặc quyền cần thiết thì sẽ không được bộ giám sát tham chiếu cấp quyền truy nhập vào dữ liệu được phân loại. Nếu tiến trình có các đặc quyền yêu cầu, và chương trình chứa con ngựa thành Toroa nào đó làm rò rỉ dữ liệu đã phân loại vào các tệp chưa được phân loại, thì bộ giám sát tham chiếu có thể phát hiện và chặn đứng sự truy nhập ghi vào tệp. Tuy nhiên, bộ giám sát tham chiếu có thể không phát hiện rò rỉ dữ liệu thông qua một kênh thông tin gián tiếp hơn, nghĩa là qua một kênh ngầm. Nếu bộ giám sát tham chiếu dùng để thực hiện vai trò an toàn của mình thì nó phải đáp ứng 3 yêu cầu thiết kế:

- cơ chế của bộ giám sát tham chiếu phải chống được giả mạo;
- cơ chế phê chuẩn tham chiếu phải thường xuyên được gọi tới;
- cơ chế phê chuẩn tham chiếu phải đủ nhỏ để phân tích và kiểm tra, tính đầy đủ của nó có thể được đảm bảo. *Xem* Orange Book.



reference monitor concept: *khái niệm giám sát tham chiếu.* Con ngựa thành Toroa cố chuyển dữ liệu từ tệp tuyệt mật sang tệp mật song yêu cầu tệp truy nhập phải được chuyển qua Bộ giám sát tham chiếu vốn sẽ chặn nó lại (dữ liệu tuyệt mật chắc sẽ không bị ghi vào tệp mật nữa).

reference PIN ***PIN chuẩn*** Trong hoạt động ngân hàng, một phiên bản PIN chính của người nắm giữ thẻ; được sử dụng để so sánh với PIN được nhập vào, trong thiết bị nhập PIN. *Xem* PIN management and security.

R

reference validation mechanism *cơ chế phê chuẩn tham chiếu* Trong an toàn máy tính, việc thực hiện khái niệm giám sát tham chiếu phê chuẩn mỗi lần tham chiếu tới dữ liệu hoặc các chương trình của một người sử dụng (chương trình) bất kỳ dựa vào một danh sách các loại tham chiếu được phép đối với người sử dụng đó. Nó phải chống được giả mạo, phải thường xuyên được gọi tới và phải đủ nhỏ để phân tích và kiểm tra, tính toàn vẹn của nó có thể được đảm bảo. *Xem* reference monitor concept.

regeneration *tái tạo, tạo lại* Trong truyền thông, một quá trình đưa ra một bản sao của một thông báo hoặc dữ liệu từ tín hiệu rõ ràng song bị méo, ví dụ một tập hợp các xung đóng-ngắt tắt dần trong khi truyền.

register *thanh ghi* Trong tính toán, một thiết bị bộ nhớ, thường có tốc độ cao, và độ dài chỉ ra bị hạn chế, ví dụ, một byte, một từ; được sử dụng dành cho các mục đích đặc biệt, ví dụ, tính toán số học.

register insertion *chèn thanh ghi* Trong truyền dữ liệu, nói tới một kỹ thuật trong đó, một thông báo cần được truyền đi trên một mạng cục bộ trước hết sẽ được nạp vào một thanh ghi dịch. Vòng lặp của mạng bị phá vỡ và thanh ghi dịch được chèn vào khi nó nhàn rỗi hoặc được chèn vào điểm giữa hai thông báo kề nhau. Sau đó, thông báo cần gửi đi được dịch chuyển tới mạng, trong lúc đó, thông báo đến bất kỳ được dịch vào trong thanh ghi dịch, phía sau thông báo được truyền. *So sánh với* control token, daisy chain, message slot. *Xem* local area network.

regrade *nâng cấp lại* Trong an toàn dữ liệu, một quyết định để thông tin được phân loại yêu cầu một mức bảo vệ chống lại việc làm lộ bí mật trái phép khác với mức cung cấp hiện thời, cùng với sự thay đổi định rõ mức phân loại tương ứng với mức độ bảo vệ khác đó. Một sự "nâng cấp" sẽ dẫn tới phân loại cao hơn; một "giáng cấp" sẽ dẫn tới một phân loại thấp hơn.

regulatory agency *cơ quan điều chỉnh cước* Trong truyền thông dữ liệu, đây là một cơ quan kiểm soát cước phí của hãng truyền thông đặc biệt và hãng truyền thông công cộng. *Xem* common carrier, specialized common carrier, tariff.

reimbursement bank *ngân hàng bồi hoàn* Trong hoạt động ngân hàng, một nhà băng cung cấp tiền bảo chứng cho một phiếu trả tiền. *Xem* receiver's correspondent bank, sender's correspondent bank.

reimbursement party *bên trả, bên bồi hoàn* Trong hoạt động ngân hàng, một bên là nguồn quỹ cho bên nhận.

re-key *làm lại khóa* Trong an toàn vật lý, nói tới công việc sửa đổi các ổ khóa hoặc thiết bị đọc thẻ nhằm thực hiện chức năng với một bộ khóa hoặc mã truy nhập mới. *Xem* card reader.

REL *REL* Viết tắt của từ Releasable. Chỉ xóa những thứ được nhắc đến.

relation *quan hệ* Trong cơ sở dữ liệu, một tệp tin hai chiều. Trong một cơ sở dữ liệu quan hệ, dữ liệu được

lưu giữ khi các thực thể, và các thuộc tính của các thực thể này ở trong các mảng 2 chiều, ví dụ, một quan hệ có thể bao gồm tên, số hiệu, phòng và lương của người làm công. *Xem* relational database, flat file.

relational algebra ***đại số quan hệ*** Trong các cơ sở dữ liệu, một ngôn ngữ mà cung cấp một tập các toán tử để xử lý các quan hệ trong một cơ sở dữ liệu quan hệ, ví dụ, nếu có 2 quan hệ *R*1 (số hiệu của người làm công, phòng) và *R*2 (số hiệu của người làm công, dự án) và người sử dụng được đòi hỏi phải biết về các phòng được tính đến trong một dự án cho trước, thì một tập các toán tử sẽ được xác định và quan hệ nhận được sẽ gồm có một bảng các phòng có liên quan đến dự án. *So sánh với* relational calculus. *Xem* join, projection, relational database.

relational calculus ***phép tính quan hệ*** Trong các cơ sở dữ liệu, một ngôn ngữ trong đó, một người sử dụng định rõ một tập các kết quả được đòi hỏi từ việc xử lý dữ liệu trên một cơ sở dữ liệu có quan hệ. Phép tính quan hệ đưa ra một ký hiệu toán học ngắn gọn, rõ ràng cho các câu lệnh, chẳng hạn lấy hai quan hệ (số hiệu nhân viên, dự án) và (số hiệu nhân viên, phòng) và đưa ra quan hệ (phòng) đối với dự án = DYNAMO. Kết quả sẽ là một danh sách các phòng mà có các nhân viên đang làm việc với dự án DYNAMO. Điểm khác biệt giữa đại số quan hệ và phép tính quan hệ là đại số quan hệ xác định các hoạt động cần thực hiện, còn phép tính quan hệ xác định bản chất của kết quả mong muốn. *So sánh với* relational algebra. *Xem* database security, relational database.

relational database ***cơ sở dữ liệu quan hệ*** Trong các cơ sở dữ liệu, một cơ sở dữ liệu trong đó, các tệp riêng biệt được gọi là các quan hệ sẽ giữ dữ liệu dưới dạng các tệp phẳng (tệp hai chiều) hay các bảng. Hạn chế đi kèm dạng các bảng này được cho dưới đây:

- Trong phạm vi hệ thống quan hệ, bảng chỉ phải chứa một kiểu bản ghi. Mỗi bản ghi có số lượng các trường cố định, tất cả chúng được đặt tên một cách tường minh.
- Các trường trong một bảng là phân biệt và không cho phép lặp lại các nhóm.
- Không có các bản ghi đúp.
- Không có sự tuần tự xác định trước của các bản ghi.

Việc xử lý dữ liệu sẽ bao gồm các thao tác trên toàn bộ các bảng, hoặc các quan hệ, hơn là theo từng bản ghi riêng lẻ trong bảng. Kết quả của việc xử lý như vậy là các bảng mới.

Bảng có hình dạng chữ nhật, vì vậy tất cả các mục vào phải chứa dữ liệu và không có các nhóm lặp. Nếu một bản ghi chứa tiểu sử của một nhân viên và số lượng khóa đào tạo (có thể thay đổi) mà anh ta đã tham dự cũng được ghi lại thì sẽ tạo ra một bảng độc lập. Bảng này giả sử có chứa 4 trường, số hiệu của nhân viên, tên của khóa học, ngày bắt đầu và kết quả học tập. Số lượng các khóa học được thay đổi khớp với số các mục vào thay đổi trong quan hệ "khóa đào tạo".

Tất cả các giá trị trên một cột cho trước được xếp vào cùng lớp thuộc tính của các mục vào. Các giá trị này phải được rút ra từ một phạm vi các giá trị có thể nào đó, ví dụ, ngày.

Các phép toán cơ bản trên một cơ sở dữ liệu quan hệ là chọn, chiếu, kết nối, và chia. Tuy nhiên, phép cuối cùng ít được sử dụng thường xuyên. Phép chọn tạo ra một bảng mới có cùng số cột như quan hệ ban đầu, nhưng số hàng sẽ gồm các hàng nào của quan hệ ban đầu mà thỏa mãn tiêu chuẩn xác định nào đó. Ví dụ, nếu bảng được cung cấp các chi tiết về số lượng hàng bán được và người bán hàng thì phép chọn có thể dựa trên cơ sở số lượng hàng bán được lớn hơn 2000.

Phép chiếu trên một bảng định rõ các cột cần chọn. Như vậy, bảng kết quả chỉ chứa một tập con các cột của bảng ban đầu, ngoài ra, nó chỉ có thể chứa một tập nhỏ các hàng. Đó là vì trong các cơ sở dữ liệu quan hệ không cho phép có các bản ghi đúp, và nếu hai hàng chỉ khác nhau trên các cột bị xóa do phép chiếu thì chỉ có một bản ghi được mang quan hệ mới.

Phép kết nối kết hợp thông tin từ hai bảng hoặc nhiều hơn. Một trường chung trong hai bảng được sử dụng làm cơ sở cho việc kết hợp, và các bản ghi với các giá trị bằng nhau trong trường chung được nối ghép vào nhau trong quan hệ kết quả.

Cần phải xem xét cẩn thận đến nội dung của các quan hệ và các mối quan hệ vốn có giữa các thuộc tính của một bản ghi, bao gồm cả các thông tin dư thừa trong một bản ghi có thể nảy sinh các vấn đề, và một quá trình chuẩn hóa là điều cốt yếu trong việc xây dựng một cơ sở dữ liệu quan hệ. *Xem* attribute, division, domain, field, flat file, join, nornal forms, projection, record, relation, relational algebra, relational calculus, repeating group, selection.

relation operator ***toán tử quan hệ*** Trong toán học, một ký hiệu được sử dụng để so sánh 2 giá trị, ví dụ: > (lớn hơn), = (bằng), < (nhỏ hơn).

relationship ***(mệnh đề) liên hệ*** Trong các cơ sở dữ liệu, một mệnh đề liên kết hai thực thể; chẳng hạn, nếu một cơ sở dữ liệu cá nhân có các thực thể: người làm công và phòng, thì "làm việc trong" sẽ là một mệnh đề liên hệ liên kết các thực thể này. *So sánh với* attribute, entity. *Xem* relational database.

relative error ***sai số tương đối*** Trong toán học, tỷ số của sai số tuyệt đối của lượng trên giá trị đúng về mặt lý thuyết, hoặc trên giá trị chỉ ra của nó.

relatively prime ***nguyên tố cùng nhau*** Trong toán học, nói tới hai số nguyên có một ước số chung lớn nhất là 1, ví dụ là 8 và 21. *Xem* greatest common divisor, prime number. *Đồng nghĩa với* coprime.

relative table size control ***kiểm soát tương đối giới hạn bảng*** Trong an toàn cơ sở dữ liệu, một hình thức kiểm soát hạn chế bảng được biết đến như s_m/N - tiêu chuẩn, được sử dụng trong kiểm soát suy luận. Giá trị của s_m là số lượng các ô trong một bảng mô hình giản kích cỡ m, và N là tổng số các bản ghi trong cơ sở dữ liệu. Nếu tỷ số

giữa số các ô trên tổng số các bản ghi vượt quá ngưỡng xác định nào đó thì có khả năng rằng, một số ô tương ứng với số ít các bản ghi và bảng này không được tạo sẵn cho các yêu cầu của người sử dụng. *So sánh với* order control. *Xem* inference control, lattice model, record, table restriction.

relay ***phát lại, chuyển tiếp, tiếp âm*** Trong truyền thông, một hệ thống thu và phát lại theo cấu hình điểm tới điểm.

relay center ***trung tâm chuyển tiếp*** *Đồng nghĩa với* message switching center.

release time and date ***ngày và thời gian phát hành*** Trong hoạt động ngân hàng, thời gian và ngày mà người gửi ủy quyền một dịch vụ chuyển thông báo tới cho người nhận.

reliability ***độ tin cậy*** (1) Phạm vi mà một hệ thống có thể được kỳ vọng thực hiện các chức năng được nhắm tới của nó với độ chính xác cần thiết. (2) Khả năng của một hệ thống để thực hiện chức năng của nó dưới những điều kiện xác định trong một khoảng thời gian định trước. Độ tin cậy tổng thể của một hệ thống là một hàm của thời gian trung bình giữa những lần hỏng hóc, thời gian sửa chữa trung bình, và thời gian khôi phục trung bình. *Xem* mean time between failure, mean time to repair, mean time to recover, redundancy.

reliability of service ***độ tin cậy của dịch vụ*** Trong an toàn thông tin, các chức năng để đảm bảo tính nhất quán và tính sẵn sàng của dịch vụ. *Xem* information technology security evaluation criteria.

remanence ***cảm ứng từ dư*** (1) Trong an toàn máy tính, số đo độ cảm ứng từ, còn lại sau khi khử một lực từ được áp lên trước đó. Cũng có thể chỉ dữ liệu bất kỳ còn lại trên phương tiện lưu giữ ADP sau khi khử nguồn. *Xem* residue. (2) Trong an toàn máy tính, phần từ tính còn dư lại trên phương tiện lưu giữ từ sau khi khử từ. *Xem* degauss.

remitter ***bộ phận trả tiền*** Trong hoạt động ngân hàng, một thuật ngữ chung chỉ nguồn quỹ trong lệnh trả tiền.

remote ***ở xa, từ xa*** (1) Trong truyền thông dữ liệu, nói tới một hệ thống được kết nối với một hệ thống máy chủ thông qua một liên kết truyền thông. (2) Trong truyền thông dữ liệu, nói tới một đơn vị điều khiển nhóm mà được kết nối với một máy tính trung tâm qua một modem, khi được so sánh với một bộ kiểm soát nội bộ được nối dây trực tiếp. *Xem* cluster control unit.

remote access ***truy nhập từ xa*** *Xem* remote.

remote batch processing ***xử lý theo lô từ xa*** *Xem* remote job entry.

remote detector panel ***thiết bị phát hiện từ xa*** Trong an toàn vật lý, một thiết bị được đặt tại một trạm giám sát hơn là được đặt trong một vùng được bảo vệ để giám sát các tuyến "nội bộ vùng". *Xem* monitoring station, protected area.

remote diagnostic center ***trung tâm chẩn đoán từ xa, RDC*** Trong tính toán, một trung tâm được hoạt động thông qua một cơ sở cung cấp thiết bị

để giảm số lần các kỹ sư bảo trì kiểm tra tại chỗ, Những trung tâm này có thể đưa đến các rủi ro về an toàn cho các hệ thống máy tính. Các tệp nhạy cảm phải được giữ ngoại tuyến trước khi bắt đầu một điều tra nghiên cứu RDC, còn các kết nối RDC không được tiến hành trừ khi được phép rõ ràng của một nhân viên điều hành của các hệ thống máy tính.

remote job entry ***nhập công việc từ xa*** Trong các hoạt động, sự trình một công việc vào một thiết bị ngoại vi được kết nối với bộ xử lý thông qua một liên kết truyền thông.

remotely accessed resource-sharing computer system ***hệ thống máy tính dùng chung tài nguyên truy nhập được từ xa*** Một hệ thống máy tính bao gồm một hoặc nhiều khối xử lý trung tâm, các thiết bị ngoại vi, các thiết bị đầu cuối từ xa, thiết bị truyền thông hoặc các liên kết để cấp phát các tài nguyên cho một hoặc nhiều người sử dụng, và nó có thể được đưa vào từ các thiết bị đầu cuối được đặt bên ngoài phương tiện máy tính trung tâm. *Xem* resource sharing computer system.

remote station ***trạm ở xa*** (1) Trong truyền dữ liệu, một trạm mà có thể gọi, hoặc được gọi bởi một trạm trung tâm trên một mạng chuyển mạch điểm tới điểm. (2) Trong một mạng đa điểm, một trạm nhánh. *Xem* tributary station, point-to-point.

remote station fire alarm system ***hệ thống báo hỏa từ xa*** Trong an toàn vật lý, một hệ thống các thiết bị được giám sát bằng điện có mạch bảo vệ trực tiếp giữa các thiết bị kiểm soát, hoặc các thiết bị khởi báo tín hiệu báo động, trong các tòa nhà được bảo vệ và các thiết bị chỉ báo tín hiệu trên một trạm từ xa. *Xem* remote station system.

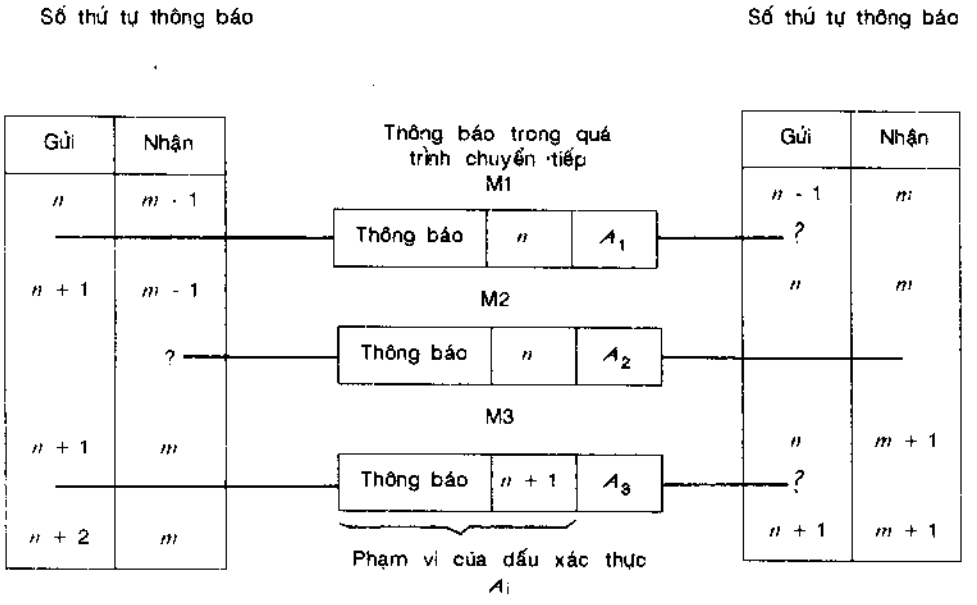
remote station system ***hệ thống trạm xa*** Trong an toàn vật lý, một hệ thống trong đó một trạm từ xa được bố trí nhân viên và được hoạt động thông qua một bộ phận độc lập, ví dụ trạm cảnh sát, được sử dụng để nhận các tín hiệu báo động. *Xem* alarm signal.

removable cartridge disk ***hệ thống đĩa tháo gỡ được*** Trong tính toán, một hệ thống đĩa cứng trong đó các đĩa cứng, trên một hộp đĩa, có thể tháo gỡ hay thay thế được.

repeatability ***tính lặp lại, khả năng lặp lại*** Trong an toàn thông tin, nói tới một trạng thái trong đó, việc đánh giá lặp về cùng đích đánh giá theo cùng đích an toàn bởi cùng ITSEF sẽ cho cùng nhận định như đánh giá đầu tiên. *Xem* information technology security evaluation criteria, information technology security evaluation manual, security target, target of evaluation.

repeater ***thiết bị chuyển tiếp*** Trong truyền thông dữ liệu, một thiết bị kết nối các mạng. Thiết bị chuyển tiếp đơn giản gửi các bit từ mạng này sang mạng khác, và như vậy là thành phần có hiệu quả của tầng vật lý của mô hình tham chiếu kết nối các hệ thống mở. *So sánh với* bridge, gateway, router. *Xem* open systems interconnection, physical layer.

repeating group ***nhóm lặp*** Trong tính toán, một nhóm trong một bản ghi



replay: *tấn công trào đổi.* Hình 1. Trình tự các thông báo.

mà có thể xuất hiện số lần bất kỳ, ví dụ các tên của những người ăn theo trên tệp của một nhân viên. Nó không có khả năng quyết định trước số lượng các trường được cấp phát cho một nhóm như vậy và các bản ghi có các nhóm lặp có thể không phù hợp với các tệp phẳng (hai chiều). *Xem* record, field, flat file.

reperformance test ***phép tra thực hiện lại*** Trong kiểm toán, một kỹ thuật trong đó một người kiểm toán xử lý dữ liệu độc lập và so sánh các kết quả với các kết quả do hệ thống đang xét tới đưa ra.

replay ***tấn công trào đổi, tấn công chuyển tiếp*** Trong xác thực, một hình thức tấn công trong đó trình tự thông báo bị thay đổi hoặc một mục dữ liệu lưu giữ bị thay thế bằng một giá trị được lưu giữ trước đó.

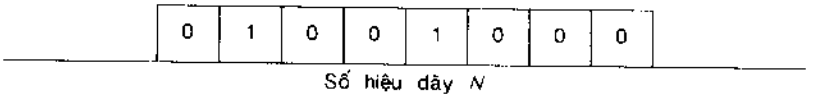
Hình thức tấn công này có thể thành công ngay cả khi thông báo hoặc mục dữ liệu lưu giữ đã được xác thực hoặc được mã hóa. Ở dạng đơn giản nhất, một kẻ tấn công có thể chỉ đơn giản ghi lại một thông báo, bao gồm cả ký hiệu xác thực của nó, và gài lại nó vào trong liên kết truyền thông. Một thông báo như vậy có thể làm cho một giao dịch tài chính được thực hiện 2 lần. Một cách khác, một mục trong một cơ sở dữ liệu có thể được cập nhật bởi một người sử dụng hợp pháp và sau đó một kẻ tấn công đặt lại giá trị ban đầu của nó.

Về nguyên tắc, tấn công chuyển tiếp các thông báo đã truyền đi có thể phát hiện được bằng cách yêu cầu một thông báo khác với tất cả các thông báo trước đó có sử dụng chung khóa. Các kỹ thuật

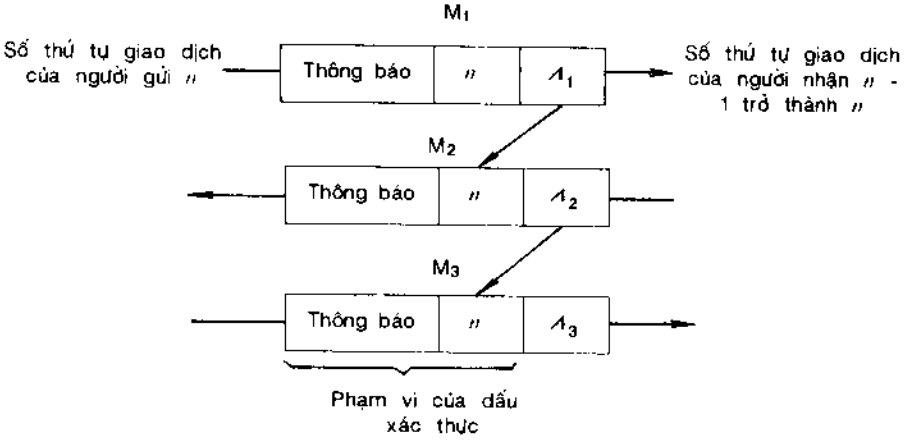
ngăn chặn các tấn công chuyển tiếp là:

- các số thứ tự;
- liên kết thông báo;
- các trao đổi số ngẫu nhiên;
- các trường ngày tháng/thời gian.

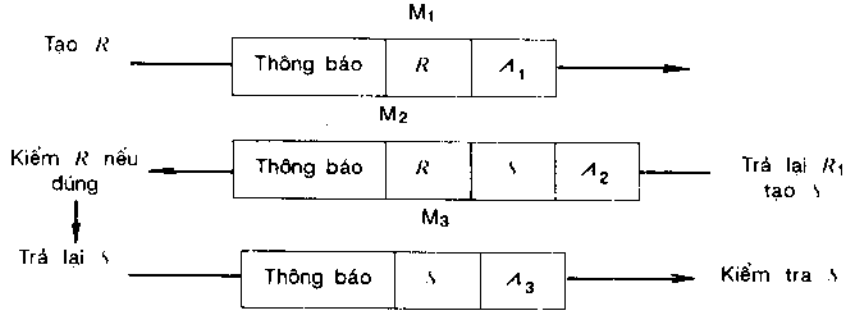
Nếu hai bên truyền thông gài các số thứ tự vào trong các thông báo của họ và tính đến các số này trong các tính toán xác thực thì kẻ tấn công không thể chuyển tiếp một thông báo ban đầu



replay: *tấn công trào đổi*. Hình 2 sơ đồ dãy bit (ảnh nhị phân).



replay: *tấn công trào đổi*. Hình 3. Liên kết thông báo.



replay: *tấn công trào đổi*. Hình 4. Xác thực với các số ngẫu nhiên.

mà không phát hiện, và cũng không thể sửa đổi số thứ tự của thông báo. Hai bên truyền thông phải giữ một bản ghi về số thứ tự cuối cùng của thông báo đã gửi đi hoặc đã nhận.

Việc sử dụng các số thứ tự của thông báo trở nên phức tạp nếu các thông báo được truyền đi trên một mạng mà chúng có thể đến không theo thứ tự, hoặc một số thông báo nào đó có thể bị mất. Người nhận có thể quyết định chỉ chấp nhận các thông báo có các số thứ tự lớn hơn số cuối cùng nhận được, điều này có thể dẫn đến việc loại bỏ các thông báo hợp pháp song đến trễ. Vì vậy, nếu số thứ tự cuối cùng nhận được là 24, và thông báo nhận được có số thứ tự là 31 thì người nhận sẽ loại bỏ các thông báo có số thứ tự từ 25-30.

Một cách khác, người nhận có thể ghi lại tất cả các số thứ tự đã nhận được và kiểm tra một cách đơn giản mỗi số vừa nhận được dựa vào bản ghi này, như vậy hệ thống sẽ có tổng phí lớn trong một môi trường xử lý giao tác.

Một giải pháp thỏa hiệp là sử dụng một dãy bit dịch chuyển (xem hình 2)

Đầu vào 1 trên ảnh bit chỉ ra rằng, một thông báo nhận được có số thứ tự tương ứng. Nếu một thông báo tới đích có số thứ tự nhỏ hơn số thứ tự tương ứng với đầu vào đầu tiên (nghĩa là N trong hình 2) thì nó bị loại bỏ vì không thể phân biệt giữa một thông báo bị trễ lớn và một thông báo chuyển tiếp.

Nếu như số thứ tự tương ứng với một trong các số của dãy bit (ví dụ, N + 2), thì đầu vào tương ứng được kiểm tra. Một đầu vào của dãy bit có giá trị là 0, cho phép thông báo được chấp nhận và đầu vào được cập nhật thành 1. Nếu đầu vào là 1 thì thông báo là một thông báo chuyển tiếp và bị loại bỏ.

Có hàng loạt chiến lược để dịch chuyển cửa sổ và giải quyết tình huống, trong đó số thứ tự nhận được nằm ở xa đỉnh của cửa sổ. Ví dụ, nếu số thứ tự của thông báo nhận được cuối cùng tương ứng với đầu vào đầu tiên trong dãy bit, thì cửa sổ được chuyển sao cho số cơ sở N tương ứng với đầu vào 0 đầu tiên.

Nếu số thứ tự của thông báo nhận được nằm phía ngoài đỉnh của cửa sổ, thì cửa sổ được dịch chuyển đi, cho phép đầu vào được ghi lại và số N tương ứng với đầu vào 0.

Liên kết thông báo giữa hai nhóm A và B có thể đạt được bằng cách gài một trường, lấy từ thông báo cuối cùng nhận được vào thông báo kế tiếp được gửi đi. Ví dụ, ký hiệu xác thực A_1 của thông báo cuối cùng được Alice gửi đi nằm trong thông báo tiếp theo mà Bob gửi cho Alice (xem hình 3). Ký hiệu xác thực A_2 của thông báo này được tính toán theo số cơ sở của văn bản thông báo, cộng với trường chuỗi (A_1).

Một phương pháp liên kết khác có thể thực hiện được bằng liên kết khối mã, hoặc hồi tiếp mã, bằng cách dùng 64 bit cuối cùng của bản mã nhận được như một vectơ khởi đầu của thông báo kế tiếp được gửi đi.

Các số ngẫu nhiên cũng có thể góp trong các thông báo để giúp bảo vệ chống lại sự tấn công chuyển tiếp (replay). Alice góp một số ngẫu nhiên

(R_1) trong thông báo của cô gửi cho Bob, số ngẫu nhiên này được tính đến trong thông báo (M_1) để tính toán ký hiệu xác thực (A_1). Trong thông báo đáp lại, Bob gộp số ngẫu nhiên nhận được (R_1) và một số ngẫu nhiên thứ hai (R_2) do Bob tạo ra; ký hiệu xác thực thứ hai (A_2) được tính toán trên thông báo thứ hai (M_2) và các số ngẫu nhiên (R_1 và R_2). Alice kiểm tra số ngẫu nhiên nhận được R_1 và gửi số ngẫu nhiên nhận được R_2 vào thư trả lời gửi cho Bob.

Trong sử dụng kỹ thuật này, kích thước của các số ngẫu nhiên phải đủ lớn so với số các thông báo, để giảm tối thiểu các nguy hiểm do việc tạo tình cờ các số ngẫu nhiên đúp. Không có thao tác nào được thực hiện như một kết quả của các thông báo trực tiếp cho đến khi thông báo thứ ba được Bob nhận và kiểm tra.

Các số thứ tự, việc liên kết chuỗi ngẫu nhiên và kỹ thuật số ngẫu nhiên để bảo vệ chống lại tấn công chuyển tiếp yêu cầu các bên truyền thông phải đưa vào tổng phí duy trì các bản ghi các số ngẫu nhiên.... Nếu các trễ thời gian trong truyền thông được giữ ở mức thấp hợp lý thì các trường thông báo, chứa thời gian và ngày xuất phát của thông báo nguyên thủy, có thể đưa một thông báo đơn lẻ chống lại tấn công chuyển tiếp, miễn là trường ngày tháng/thời gian được tính đến trong ký hiệu xác thực thông báo.

Một tệp được lưu giữ trong một cơ sở dữ liệu có thể có ký hiệu xác thực riêng của mình nhưng các mục riêng lẻ trong các tệp như vậy có khả năng được cập nhật thường xuyên; mỗi cập nhật yêu cầu tính toán lại ký hiệu xác thức cho toàn bộ tệp. Nếu tệp bị chia ra, với mỗi phần chia được xác thức riêng, thì tồn tại khả năng tấn công thông qua việc sắp xếp lại thứ tự các phần, hoặc khôi phục lại một phần, và ký hiệu xác thực riêng của nó, thành một giá trị trước đó. Nếu các đoạn được truy nhập thông qua địa chỉ của chúng thì việc sắp xếp lại các phần có thể làm cho những người sử dụng bị cung cấp dữ liệu không chính xác.

Hình thức tấn công này có thể ngăn ngừa được bằng cách gộp cả địa chỉ của các phần vào việc tính toán ký hiệu xác thực. Sự nguy hiểm của việc khôi phục lại các phần trước đó có thể chống lại được bằng cách đặt một số hiệu, trên mỗi phần, và duy trì một bản ghi chứa tất cả số hiệu trên bản ghi cập nhật của một tệp được xác thực tách bạch. Bản ghi cập nhật phải tự bảo vệ chống lại việc khôi phục lại bằng cách tạo ra một trường ngày tháng/thời gian. *Xem* authenticator, cipher block chaining, cipher feedback, cryptographic key, date/time stamp, initialization vector, message authentication.

replenishment deposit *(tiền) đặt cọc bổ sung* Trong hoạt động ngân hàng, một khoản tiền trả làm tăng sự cân đối trong tài khoản của người khởi đầu được người nhận phục vụ, ví dụ, kết quả của việc chuyển nhượng của một ngân hàng đối với tài khoản sở hữu của nó. *Xem* originator.

reporting line *đường dây báo động* *Đồng nghĩa với* alarm line.

reproducibility *khả năng tái tạo*

Trong an toàn thông tin, nói tới một trạng thái trong đó một đánh giá được lặp lại, đối với cùng một mục đích an toàn thông qua các ITSEF khác nhau sẽ đưa lại toàn bộ nhận định giống nhau đối với ITSEF đầu tiên. *Xem* information technology security evaluation criteria, information technology security evaluation manual, security target, target of evaluation.

repudiation ***(sự) từ chối*** Trong an toàn truyền thông, sự từ chối của một trong các thực thể trong một cuộc liên lạc có sự tham gia của tất cả hoặc một bộ phận của các bên tham gia truyền thông. *So sánh với* nonrepudiation. *Xem* digital signature.

request for service message ***thông báo yêu cầu dịch vụ*** Trong quản lý khóa, một thông báo gửi các khóa (nhằm tới người nhận cuối cùng) tới trung tâm dịch khóa để dịch. *Xem* ANSI X9.17 - 1985, key translation center.

request reply service ***dịch vụ đáp lại yêu cầu*** Trong truyền dữ liệu, một dịch vụ không kết nối trong đó, người gửi gửi một gói dữ liệu đơn lẻ chứa một yêu cầu và sự hồi âm có chứa câu trả lời. *Xem* connectionless service, datagram.

request response ***đáp ứng yêu cầu*** Trong an toàn truyền thông, một kỹ thuật để cảnh báo những người sử dụng rằng một tấn công trì hoãn/từ chối dịch vụ đang xảy ra. Nếu các tấn công như vậy được bắt đầu trong một tình trạng giao thông không hoạt động thì những người nhận các thông báo sẽ không biết rằng, các thông báo đã bị chặn. Các thông báo yêu cầu hồi âm có thể được gửi đi một cách định kỳ giữa hai thực thể truyền thông để đảm bảo rằng tồn tại các tuyến truyền thông mở. *Xem* delay/denial of service, hot mode, traffic analysis.

request service initiation ***yêu cầu bắt đầu dịch vụ*** Trong quản lý khóa, một thông báo tùy chọn yêu cầu bắt đầu một liên lạc sử dụng khóa mới. *Xem* ANSI X9.17 - 1985.

request to send ***tín hiệu yêu cầu gửi*** Trong truyền dữ liệu, một tín hiệu được sử dụng kết hợp với một tín hiệu khác - tín hiệu thông - như một thủ tục bắt tay trong hoạt động bán song công. Máy tính đưa ra yêu cầu để gửi tín hiệu tới modem và chờ tín hiệu thông trước khi truyền dữ liệu. *So sánh với* clear to send. *Xem* half duplex, handshaking, MODEM, RS-232C.

requirement ***yêu cầu*** Đây là một lệnh của hệ thống, cần thiết để tuân theo một chính sách cho trước. Các yêu cầu được sử dụng để nhận bản đặc tả kỹ thuật của hệ thống. *Xem* policy, specification.

rescue dump ***kết xuất phòng sự cố, xổ để cứu*** Trong tính toán, sự kết xuất hoàn toàn kho lưu trữ dữ liệu máy tính và các trạng thái sang một thiết bị ngoại vi để trong trường hợp hệ thống chính bị hỏng, chẳng hạn mất nguồn thì chương trình có thể được bắt đầu từ trạng thái kết xuất dự phòng cuối cùng. *Xem* dump.

Research in Secured Operating Systems ***nghiên cứu về các hệ điều hành an toàn*** Trong an toàn máy

tính, một công cụ phân tích trực tiếp mẫu. *Xem* pattern directed analysis.

reset ***xác lập lại, khởi động lại*** (1) Trong hoạt động chương trình, sự chấm dứt bằng tay một chương trình trên một máy vi tính. (2) Trong hoạt động chương trình, thiết lập lại một thanh ghi, vị trí lưu giữ hoặc thiết bị lưu giữ, về trạng thái ban đầu của nó.

resident software ***phần mềm thường trú*** Trong tính toán, một chương trình bất kỳ chiếm cố định trong bộ nhớ để cung cấp một dịch vụ cho các chương trình khác, ví dụ, một trình biên dịch thường trú. *Xem* software, compiler.

residual error rate ***tỷ lệ lỗi sót*** Trong truyền thông dữ liệu, một tỷ số của tổng số các bit, các byte hoặc các khối nhận được không chính xác nhưng không được sửa chữa hoặc không phát hiện được qua một thiết bị kiểm soát lỗi, trên tổng số các đơn vị tương ứng được truyền đi.

residual intelligibility ***độ rõ còn lại*** Trong an toàn truyền thông, phần thông báo tiếng nói bị xáo trộn mà vẫn có thể hiểu được trực tiếp. *Xem* voice scrambling.

residual risk ***rủi ro còn lại*** Trong quản lý rủi ro, phần rủi ro còn lại sau khi áp dụng các biện pháp an toàn.

residue ***phần dư, thặng dư*** (1) Trong toán học, nếu b là đồng dư với c modulo n thì b là phần dư của c modulo n. *Xem* congruent. (2) Trong an toàn máy tính, dữ liệu bị bỏ sót trong phương tiện lưu giữ sau khi thực hiện các thao tác xử lý, và trước khi việc khử từ hoặc ghi đè xảy ra. *Xem* degauss. (3) Trong xác thực, *xem* MAC residue.

residue problems ***(các) vấn đề để sót*** Trong an toàn máy tính, một lớp các vấn đề an toàn mà có thể nảy sinh từ việc bỏ sót thông tin trong phương tiện lưu giữ sau khi xử lý. Thông tin như vậy có thể không có giá trị đối với người sử dụng hợp pháp nhưng có thể được phát hiện nhờ những lập trình viên tài giỏi, ví dụ, một tệp bị xóa có thể còn lại trên đĩa và một cờ xóa sẽ ngăn chặn sự truy nhập thông thường qua hệ điều hành, tuy nhiên, tệp vẫn có thể được khôi phục lại qua lập trình cần thiết. *Xem* object, reuse, personal computer security, residue.

resource ***tài nguyên*** (1) Trong an toàn máy tính, bất cứ thứ gì được sử dụng hoặc tiêu thụ trong khi thực hiện một chức năng. Các loại các tài nguyên là thời gian, thông tin, các đối tượng (chứa thông tin), hoặc bộ xử lý (có khả năng sử dụng thông tin). Ví dụ như thời gian CPU, thời gian kết nối thiết bị đầu cuối, tổng số bộ nhớ lập được địa chỉ trực tiếp, không gian đĩa, số lượng các yêu cầu I/O trên 1 phút... *Xem* object. (2) Trong an toàn máy tính, một hệ thống ADP, chức năng bất kỳ, thiết bị bất kỳ, hoặc tập hợp dữ liệu mà có thể được cấp phát cho những người sử dụng hoặc các chương trình.

resource sharing ***chia sẻ tài nguyên, dùng chung tài nguyên*** (1) Trong các hoạt động của máy tính, trong một hệ thống ADP, hơn một người sử dụng, một công việc, một chương trình sử dụng cùng lúc một nguồn tài nguyên

Xem resource. (2) Trong các mạng máy tính, việc sử dụng chung các nguồn tài nguyên có sẵn trên một hệ thống, hoặc mạng, bởi những người sử dụng hoặc các thiết bị ngoại vi, ví dụ, những người sử dụng máy vi tính trên một mạng cục bộ có thể dùng chung một ổ đĩa cứng hoặc máy in. *Xem* hard disk, local area network, server.

resource sharing computer system ***hệ thống máy tính dùng chung tài nguyên*** Một hệ thống mà sử dụng các nguồn tài nguyên của nó, bao gồm các thiết bị I/O, phương tiện lưu giữ, bộ xử lý trung tâm (các khối số học và logic), các đơn vị điều khiển, và các khả năng xử lý phần mềm, cho phép một hay nhiều người sử dụng thao tác dữ liệu và thực hiện các chương trình cùng thường trú theo một cách đồng thời dễ thấy. Giới hạn bao gồm các hệ thống có một hoặc nhiều khả năng liên quan phổ biến như: phân thời, đa lập trình, đa truy nhập, đa xử lý hoặc xử lý đồng thời.

responder ***thiết bị đáp*** Trong truyền thông, một thiết bị truyền tự động một tín hiệu xác định trước, khi được kích hoạt bởi một tín hiệu nhận được. *So sánh với* transponder.

response service message ***thông báo dịch vụ đáp*** Trong quản lý khóa, một thông báo cung cấp một lời đáp được xác thực là đúng cho một thông báo dịch vụ khóa. *Xem* ANSI 9.17 - 1985, key service message.

response time ***thời gian đáp ứng*** (1) Thời gian mà một hệ thống lấy để đạt được một trạng thái xác định hoặc đưa ra một đầu ra xác định, sau khi nhận được một đầu vào. (2) Trong tính toán, thời gian từ lúc tạo ra ký tự cuối cùng tại thiết bị đầu cuối đến lúc nhận được ký tự đầu tiên của tín hiệu đáp.

response to request service message ***thông báo đáp lại dịch vụ yêu cầu*** Trong quản lý khóa, một thông báo được sử dụng để đáp lại một RFS, ERS hoặc RSI. *Xem* ANSI 9.17 - 1985, ERS, RFS, RSI.

restricted area ***vùng bị hạn chế*** Trong an toàn vật lý, một vùng bất kỳ mà việc truy nhập vào nó bị phụ thuộc vào các giới hạn hoặc kiểm soát xác định vì các lý do an toàn hoặc vì bảo vệ tài sản hoặc tài liệu.

result-based perturbation ***gây nhiễu dựa trên kết quả*** Trong an toàn cơ sở dữ liệu, một hình thức gây nhiễu trong đó thống kê chính xác được tính toán và kết quả bị gây nhiễu, thường là dưới hình thức làm tròn nào đó. *So sánh với* record based perturbation. *Xem* inference, perturbation, statistical database.

retailer ***người bán lẻ, người dùng thẻ*** Trong hoạt động ngân hàng, một người nhận thanh toán hóa đơn bằng thẻ trong một hệ thống EFTPOS. *Xem* card acceptor.

retention period ***thời gian lưu (dữ liệu), chu kỳ lưu giữ*** Trong an toàn dữ liệu, khoảng thời gian dành cho một tệp cần được duy trì trước khi nó bị ghi đè. Thời gian lưu giữ và ngày mà tệp được ghi, được sử dụng để tính toán ngày sớm nhất khi tệp hết hiệu lực. Ngày mà tệp được ghi và thời gian

lưu giữ hoặc ngày hết hạn sẽ được ghi như một phần trong nhãn tệp và sẽ được sử dụng như một biện pháp an toàn chống lại sự hủy bỏ ngẫu nhiên một tệp.

retro target ***đích phản xạ*** Trong an toàn vật lý, một cảm biến của máy thu phát mà sử dụng một bộ phản xạ để trả chùm tia ngược trở lại với bộ phận thu của máy thu phát. *Xem* transceiver.

reusability ***khả năng dùng lại*** Trong tính toán, phạm vi trong đó một chương trình có thể được sử dụng trong các ứng dụng khác và có liên quan với việc đóng gói và các chức năng mà chương trình thực hiện.

reverse engineering ***thiết kế đối chiếu, kỹ thuật phân tích ngược*** Đây là một quá trình nhờ nó mà việc thiết kế một sản phẩm được quyết định bởi một sự nghiên cứu chi tiết chính sản phẩm đó, ví dụ, phần mềm trên một ROM có thể được xác định bởi sự nghiên cứu chi tiết của một vi mạch ROM. Các kỹ thuật này có các ứng dụng giúp cho các nhà sản xuất bảo vệ thiết kế sản phẩm. *Xem* ROM.

reverse funds transfer ***chuyển quỹ ngược*** Trong hoạt động ngân hàng, việc chuyển nợ trong đó bên có là người gửi. *Xem* debit party.

reverse interrupt ***ngắt đảo ngược*** Trong truyền dữ liệu, dãy ký tự điều khiển được trạm thu gửi đi, trong một hệ thống thông tin đồng bộ nhị phân, để yêu cầu chấm dứt sớm quá trình truyền đang xảy ra. *Xem* binary synchronous communications.

reversible encryption ***phép mã có thể đảo được*** Trong mật mã, một phép biến đổi DEA của bản rõ, theo cách mà bản mã có thể được giải mã ngược trở lại thành bản rõ ban đầu. *So sánh với* irreversible encryption. *Xem* DEA.

review anh approval ***duyệt và phê chuẩn*** Trong an toàn máy tính, một quá trình nhờ đó thông tin liên quan với tính an toàn và tính toàn vẹn của một hoạt động ADP hoặc mạng sẽ được thu thập, được phân tích và đệ trình trước DAA thích hợp để được công nhận về phạm vi hoạt động hoặc mạng. *Xem* DAA.

RF ***RF*** Viết tắt của Radio Frequency (tần số vô tuyến).

RFE *Xem* radio frequency emissions.

RFI *Xem* radio frequency interference.

rfm *Xem* re-encipher from master key.

rfmk *Xem* re-encipher from master key.

RFS *Xem* request for service message.

ring ***vành, vòng*** (1) Trong tính toán, một cấu trúc trong đó con trỏ cuối cùng của một danh sách móc nối tham chiếu vào phần tử đầu tiên ở cùng danh sách. (2) Trong truyền dữ liệu, cấu trúc hình học của một mạng có dạng vòng, vì vậy mỗi nút chỉ được kết nối với 2 nút khác liền kề. Một ngắt trên mạng ảnh hưởng đến toàn bộ các thành viên. *So sánh với* bus, star. *Xem* local area network.

ring back ***gọi chuông trở lại, tín hiệu chờ*** Trong truyền thông dữ liệu, một thủ tục mà cho phép một điện thoại được sử dụng trong cả các kết nối máy

tính lẫn các cuộc gọi điện thoại thông thường. Các kết nối máy tính yêu cầu 2 cuộc gọi: gọi đầu tiên thường chỉ là một hồi chuông, báo hiệu cho modem là sẽ không có trả lời, tuy nhiên, trừ khi việc đổ chuông dừng lại trong khoảng thời gian nào đó, thông thường là 30 giây. *So sánh với* call back, ring indicator.

ring indicator ***tín hiệu báo chuông*** Trong truyền dữ liệu, một tín hiệu báo hiệu rằng một modem đã nhận cuộc gọi mới. Tín hiệu chỉ báo chuông kêu hoặc ngắt giống như các hồi chuông điện thoại nhờ vậy máy tính có thể trả lời sau một số hồi chuông xác định. *So sánh với* ring back. *Xem* MODEM, RS-232C.

risk ***độ rủi ro*** (1) Trong an toàn máy tính, mất mát tiềm ẩn mà tồn tại giống như kết quả của cặp hiểm họa - điểm yếu. Việc giảm hoặc hiểm họa hoặc điểm yếu làm giảm độ rủi ro. *Xem* threat, vulnerability. (2) Độ bất định của mất mát được biểu thị theo xác suất của mất mát như vậy. *Xem* ALE. (3) Trong an toàn máy tính, khả năng có thể xảy ra hoặc xác suất để một tác nhân gây hiểm họa sẽ cài thành công một tấn công xác định dựa vào điểm yếu của một hệ thống cụ thể. *So sánh với* safeguard. *Xem* matrix methodology, risk analysis, risk analysis methodologies, threat, vulnerability.

risk analysis ***phân tích rủi ro*** (1) Trong quản lý rủi ro, một phần của công việc quản lý rủi ro được sử dụng để giảm tối thiểu rủi ro qua việc áp dụng có hiệu quả các biện pháp an toàn tương xứng với các hiểm họa, điểm yếu liên quan, và các giá trị của các nguồn tài nguyên được bảo vệ. Giá trị của các nguồn tài nguyên gồm cả tác động của các hỗ trợ của hệ thống tự động lên tổ chức, và tác động của sự mất mát hoặc sửa đổi không cho phép đối với dữ liệu. Phân tích rủi ro bao gồm 4 modun sau: đánh giá tính nhạy cảm, đánh giá rủi ro, đánh giá tính kinh tế, và đánh giá và thử nghiệm tính an toàn. *Xem* economic accessment, risk accessment, security test and eveluation, sensitivity accessment. (2) Trong an toàn máy tính, sự phân tích các tài sản hệ thống và các điểm yếu dễ bị tấn công để chứng minh một sự mất mát dự tính từ những sự cố nhất định dựa trên xác suất ước lượng về sự xuất hiện của các biến cố đó.

risk analysis methodology ***phương pháp luận phân tích rủi ro*** Trong quản lý rủi ro, sự phân tích rủi ro về lý thuyết có thể cung cấp cho việc quản lý các dữ liệu cần thiết để thực hiện các thủ tục và các hệ thống an toàn thông tin theo cách sinh lợi và phù hợp. Tuy nhiên, trong thực tiễn, có các cách nhìn nhận khác nhau về tính hiệu quả của cách tiếp cận này và phương pháp được lựa chọn.

Trong nghĩa khái quát nhất, các phương pháp có thể được phân loại như sau:

- định tính hay định lượng;
- bằng tay hay tự động hóa.

Các cách tiếp cận theo định lượng, theo định nghĩa trong suốt nhất, nhằm ngăn chặn sự cân đối chi phí cho biện pháp an toàn dựa trên chi phí khi không thực hiện biện pháp. Ước tính thiệt hại hàng năm (ALE) được dựa vào khái niệm rằng, trong một năm, tồn tại một

xác suất để một mất mát i sẽ xảy ra là f. Vì vậy, chi phí mặc nhiên trong việc thực hiện không phòng ngừa là ALE = $f.i$. Trong các trường hợp này, các biện pháp đối phó với chi phí hàng năm c sẽ có lãi nếu chúng dẫn tới làm giảm ALE, sao cho mức giảm bớt ALE lớn hơn c. Trong thực tế, những tính toán như vậy thường chỉ có thể được thực hiện sau các khảo sát rộng và tốn kém, dựa vào dữ liệu không đầy đủ và dữ liệu có tính chủ quan cao.

Các phương pháp định lượng khác không cố gắng thực hiện các tính toán liên quan trực tiếp đến chi phí như vậy, mà tập trung vào các mục tiêu phát triển để có thể ưu tiên một cách đúng đắn vào việc thực hiện các biện pháp đối phó. Việc đảm bảo rằng có thể cân một cách chặt chẽ chi phí an toàn theo mất mát thương mại ước tính có thể là không thực tế. Tuy nhiên, các tổ chức lớn cần có các cách đảm bảo rằng, các biện pháp đối phó an toàn nhắm trực tiếp tới các vùng cần thiết nhất.

Hàng loạt các phương pháp luận chẳng hạn như CRAMM, thử làm giảm ảnh hưởng của các tính chủ quan, bằng cách gán điểm số theo giá trị (value scores) hơn là các giá trị tiền tệ cho các tài sản. Như vậy, người ta có thể yêu cầu những nhà quản lý ước lượng tác động có thể về mất tính sẵn sàng, tính toàn vẹn hoặc bí mật của một dữ liệu cho trước trong các giới hạn hoạt động, và yêu cầu họ gán một điểm số vào câu trả lời.

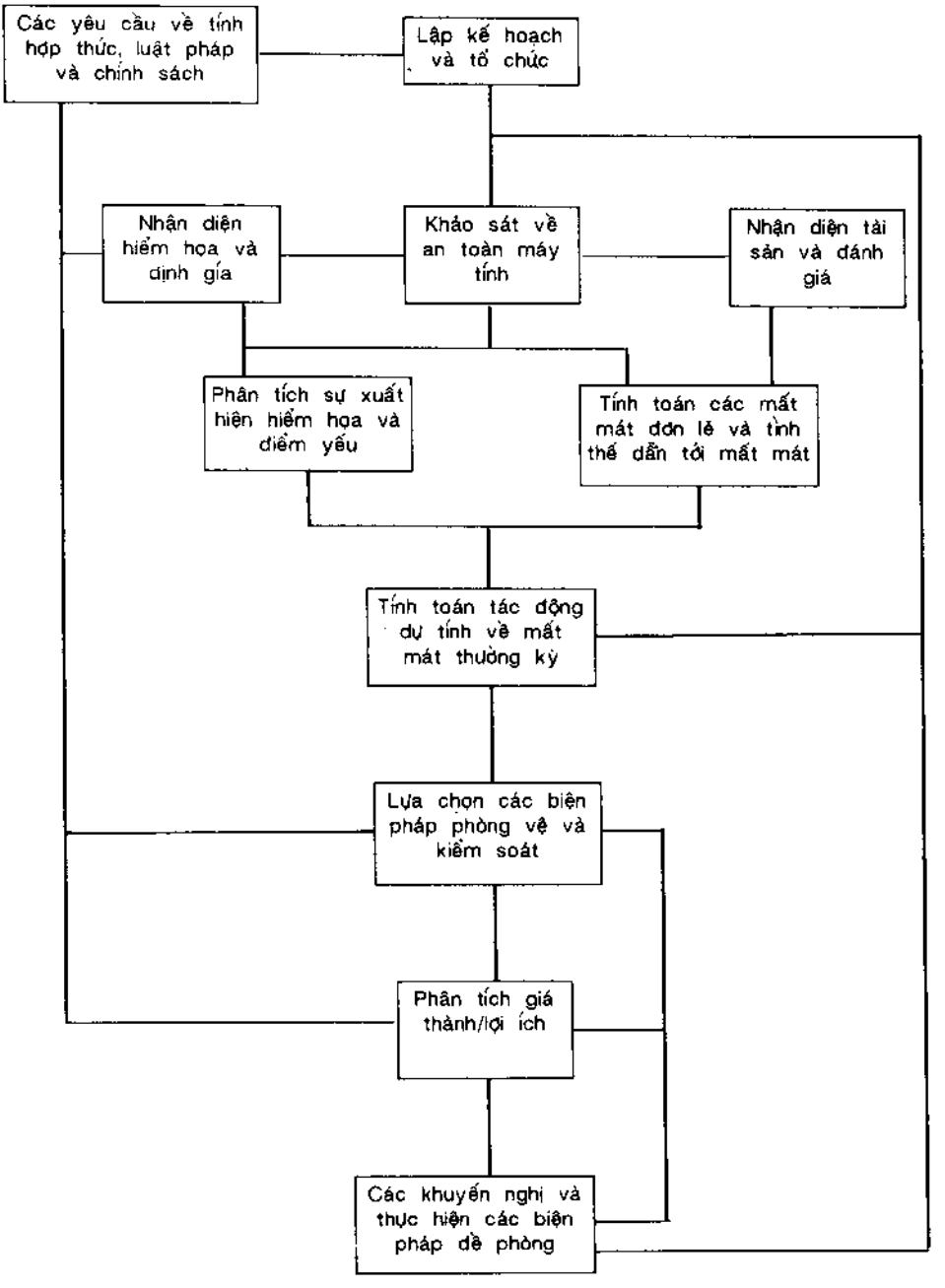
Việc đạt được một ước lượng xác suất của một sự cố an toàn tác động lên một tổ chức, thậm chí còn khó giải quyết hơn là đánh giá vào giá trị tài sản. Các ước lượng như vậy đòi hỏi có chuyên môn và kinh nghiệm cần thiết trong việc đánh giá rủi ro. Chi phí để có được sự ước lượng như vậy có thể không cân xứng với ALE. Một số phương pháp, ví dụ, SCRAMM và MARION cung cấp các cơ sở kiến thức có sẵn để có thể đạt được một số đánh giá hợp lý với chi phí có thể chấp nhận được.

Các hướng định lượng, chẳng hạn như phương pháp luận ma trận sẽ giúp cung cấp sự quản lý với một bức tranh xúc tích về tình trạng rủi ro mà không cố gắng để quyết định các quan hệ tài chính của nó.

Các phân tích rủi ro bao gồm sự thu thập dữ liệu chính, đối chiếu, tính toán, và báo cáo. Nhiều phương pháp được hỗ trợ bởi các bộ phần mềm để làm giảm cố gắng thủ công và công việc giấy tờ. Tuy nhiên, các hướng dựa trên giấy tờ có một số thuận lợi, đặc biệt đối với các nghiên cứu rủi ro ban đầu, chúng tác động như một sự dẫn hướng cho sau này và các dự án chi tiết hơn. Như vậy, các hướng tiếp cận sẽ:

- yêu cầu đào tạo ban đầu ít hơn;
- cung cấp tính mềm dẻo đáng kể trong việc mô tả dữ liệu khảo sát;
- cho phép khảo sát để đáp ứng tình huống bị phát hiện ra trong các phỏng vấn v.v. như vậy cho phép những người phỏng vấn bỏ qua các câu hỏi mà rõ ràng không liên quan đến một phần cụ thể, để thu thập dữ liệu bổ sung có liên quan rõ ràng v.v..

Các phương pháp luận dựa trên máy tính nào đó đòi hỏi việc điều hành phức tạp thông qua các menu, có thể yêu cầu



risk analysis: *phân tích rủi ro.* Quá trình phân tích rủi ro.

đào tạo chuyên sâu, và làm phức tạp nhiệm vụ ghi và tìm kiếm thông tin dành cho các hệ thống khá đơn giản.

Một số hệ thống kết hợp các hướng dựa vào giấy tờ và máy tính, ví dụ, sử dụng máy tính để in ra các hình thức khảo sát chứa thông tin cục bộ có liên quan v.v.. Khối lượng lớn dữ liệu được thu thập cho một khảo sát rộng sẽ đưa ra các vấn đề về đối chiếu, chuẩn bị báo cáo v.v. mà nó chỉ có thể được thay đổi hợp lý thông qua các hệ thống máy tính. Hơn nữa, các phân tích rủi ro thường cần cố gắng gấp đôi, ví dụ, các hệ thống xử lý thông tin giống nhau được sử dụng trên toàn bộ một tổ chức. Các phương pháp dựa trên máy tính có thể làm cho việc tái sử dụng các dữ liệu khảo sát trở nên thuận tiện hơn đối với các hệ thống tương tự.

Có một nhược điểm tiềm ẩn với các phương pháp dựa trên máy tính bởi vì một số trong chúng có thể khuyến khích cách tiếp cận theo kiểu "hộp đen", chấp nhận dữ liệu đầu vào và cung cấp một đáp ứng được tính toán bên trong. Thực trạng của bộ môn phân tích rủi ro là sao cho nhà quản lý có được vị thế buộc toàn bộ quá trình đi theo sự nghiên cứu tới hạn, để đảm bảo rằng không có giả thiết bị che dấu nào lại không thích hợp với tổ chức của họ. Các vết kiểm toán mà cho phép các kết quả theo dõi ngược về dữ liệu khảo sát rất quan trọng. Thêm vào đó, một số hệ thống cung cấp các phương tiện "cái gì xảy ra nếu" ít nhất cũng có thể cho phép nhà quản lý khai thác tính nhạy cảm của các kết quả đối với các nhân tố cục bộ.

Vấn đề hộp đen là vốn có trong các hệ thống chứa đựng cơ sở kiến thức có sẵn vì tài sản chất xám của nền tảng đó tồn tại cùng những người cung cấp. Nền tảng kiến thức có thể được cập nhật bởi những người cung cấp nhưng không có cơ hội cho tổ chức kể cả việc rút ra kinh nghiệm và chuyên môn của chính nó. *Xem* LAVA, CRAMM, Marion, matrix methodology, quantitative risk analysis, risk analysis, RISKCALC, The Buddy System.

risk assessment ***đánh giá rủi ro*** (1) Trong quản lý rủi ro, việc nghiên cứu các điểm yếu, các hiểm họa và các sự cố có thể xảy ra, mất mát hoặc ảnh hưởng, và hiệu quả về mặt lý thuyết của các biện pháp an toàn. Những nhà quản lý sử dụng các kết quả của việc đánh giá rủi ro để phát triển các yêu cầu và đặc tả an toàn. *Xem* risk analysis, threat, vulnerability. (2) Trong an toàn máy tính, sự nhận dạng tài sản của phương tiện ADP xác định, các đe dọa tới các tài sản đó, và tính dễ bị tấn công của thiết bị ADP do các đe dọa này. *Xem* risk analysis, threat, vulnerability. (3) Trong quản lý rủi ro, việc phân tích các tài sản thuộc quyền sở hữu và tính dễ bị tấn công của hệ thống để đạt được mất mát dự tính từ các biến cố nhất định dựa vào các xác suất ước lượng xảy ra các biến cố. Mục đích của việc đánh giá một rủi ro là để xác định liệu các biện pháp đối phó thích hợp có làm giảm xác suất mất mát hoặc ảnh hưởng của mất mát đến mức có thể chấp nhận được không. *Xem* risk analysis, vulnerability. (4) Trong quản lý rủi ro, việc định lượng xác suất của một

tác động không có lợi khi không có sự can thiệp có tính toán bất kỳ. *Xem* matrix methodology, risk analysis.

RISKCALC *hệ phương pháp RISKCALC* Trong quản lý rủi ro, một phương pháp luận phân tích rủi ro. *Xem* risk analysis methodologies.

risk index *chỉ số so sánh rủi ro* Trong an toàn dữ liệu, sự khác biệt giữa mức truy nhập hay quyền tối thiểu của những người sử dụng hệ thống và tính nhạy cảm tối đa (ví dụ, mức phân loại và các loại) của dữ liệu được hệ thống xử lý. *Xem* Orange Book, sensitivity.

risk management *quản lý rủi ro* (1) Toàn bộ quá trình để nhận dạng, kiểm soát, và tối thiểu hóa tác động của các biến cố dễ thay đổi. Mục tiêu của quản lý rủi ro là làm giảm rủi ro, thu được và duy trì sự phê chuẩn DAA. Quá trình làm cho việc quản lý các rủi ro an toàn trở nên thuận tiện hơn thông qua mỗi mức quản lý trong suốt chu kỳ sống của hệ thống. Quá trình phê chuẩn bao gồm 3 yếu tố: phân tích rủi ro, cấp giấy chứng nhận, và phê chuẩn. *Xem* DAA, risk analysis, risk assessment. (2) Một yếu tố của kỹ thuật quản lý liên quan đến việc nhận dạng, đo lường, điều khiển, và tối thiểu hóa các biến cố dễ thay đổi. Một chương trình quản lý rủi ro có hiệu quả bao gồm 4 giai đoạn sau: (*a*) Đánh giá rủi ro, khi nhận được sự đánh giá các hiểm họa và điểm yếu dễ bị tấn công. (*b*) Quyết định quản lý. (*c*) Thực hiện kiểm soát. (*d*) Cân nhắc tính hiệu quả. *Xem* risk analysis, risk assessment. (3) Một hướng có quy tắc được chấp nhận để nhận dạng, đo lường và kiểm soát các biến cố dễ thay đổi để giảm tối thiểu sự mất mát và tiền đầu tư cho các mục đích an toàn. Mục tiêu của quản lý rủi ro là đạt được sự phòng ngừa hiệu quả nhất chống lại việc phá hủy các tài sản thuộc sở hữu, sửa đổi bất hợp pháp hoặc xử lý dữ liệu của công ty, làm lộ trái phép dữ liệu của công ty và chối bỏ các các tài sản thuộc sở hữu và các dịch vụ xử lý dữ liệu cho các cá nhân không được phép. Trong lĩnh vực an toàn máy tính, việc quản lý rủi ro bao gồm phân tích rủi ro, đưa ra quyết định quản lý và thực hiện các biện pháp và các cân nhắc về an toàn. *Xem* matrix methodology, risk analysis.

RISOS *Xem* Research in Secured Operating Systems.

RJE *Xem* remote job entry.

rogue fiber *sợi tinh quái* Trong an toàn truyền thông, một hoạt động nghe trộm chủ động trên một cáp quang, mà có thể được thực hiện thông qua việc nối một sợi vào cáp bằng tác dụng nhiệt. *Xem* active wiretapping, fiber optics.

rollback *khôi phục, phục hồi* (1) Trong lĩnh vực độ tin cậy, một kỹ thuật khôi phục lại từ các sự cố của hệ thống. Các điểm khôi phục được chèn vào tại các khoảng thời gian trong chương trình và khi đạt được một điểm như vậy trong hoạt động chương trình, toàn bộ trạng thái của hệ thống được lưu trong bộ nhớ dự phòng được bảo vệ. Khi một sự cố được phát hiện, đơn vị điều khiển được chuyển mạch sang bộ nhớ dự phòng, các trạng thái của máy được khôi phục lại và chương

trình được thực hiện lại từ điểm khôi phục, bộ nhớ ban đầu được sử dụng thành bộ nhớ dự phòng. *Xem* time redundancy. (2) Trong các cơ sở dữ liệu, một kỹ thuật được sử dụng để bảo vệ cơ sở dữ liệu chống lại các thao tác không chính xác của người sử dụng. Trạng thái của cơ sở dữ liệu được duy trì và các giao tác sau đó được cất giữ, nếu người sử dụng quyết định thực hiện toàn bộ các giao tác thì một lệnh ủy nhiệm được phát ra, nếu lệnh phục hồi được sử dụng thì các giao tác bị bỏ qua và không ảnh hưởng đến cơ sở dữ liệu. *So sánh với* commit.

roll call polling ***hỏi gọi xoay vòng*** Trong truyền dữ liệu, một phương pháp hỏi vòng trong hệ thống đa điểm trong đó, bộ điều khiển gửi các thông báo được đánh địa chỉ tới mỗi một thiết bị đầu cuối với hình thức hỏi lần lượt xem chúng có dữ liệu nào để gửi đi không. *So sánh với* hub polling. *Xem* polling.

rolling up ***cuộn nhóm*** *Đồng nghĩa với* groupping.

ROM *Xem* read only memory.

ROS ***tín hiệu ROS*** Trong an toàn truyền thông, viết tắt bằng tiếng Thụy Điển để chỉ các tín hiệu điện từ. *Xem* van Eck phenomenon.

rotation ***quay vòng*** Trong an toàn máy tính, một chính sách dịch chuyển đều đặn các tệp hoặc các bản sao dự phòng của chúng từ trung tâm dữ liệu hoặc thư viện băng từ tới các vị trí nằm ngoài trung tâm dữ liệu.

rotation of duties ***quay vòng nhiệm vụ*** Trong an toàn thủ tục, một chính sách cá nhân trong đó các nhân viên bị thay đổi nhiệm vụ thường xuyên sau các khoảng thời gian xác định.

Chính sách này ngăn chặn một cá nhân khỏi có sự độc quyền về hiểu biết và hạn chế các hành động gian lận. Nếu một người vẫn giữ nguyên trên một vị trí công tác trong một khoảng thời gian không hạn định thì có thể xảy ra tình trạng trong đó cá nhân trở nên khó thay thế khi anh ta/chị ta đạt được sự độc quyền về sự hiểu biết cần thiết để thực hiện nhiệm vụ đó. Tình trạng này gây trở ngại đáng kể nếu người đó vắng mặt không tránh được hoặc bị bệnh.

Một hoạt động gian lận thường có thể đòi hỏi thủ phạm phải đảm bảo sự giám sát một nhiệm vụ riêng biệt trong các khoảng thời gian kéo dài, gian lận như vậy bị phát hiện một cách bình thường khi thủ phạm không tránh khỏi vắng mặt khỏi nơi làm việc. Như vậy quay vòng các nhiệm vụ làm giảm các cơ hội đối với các hoạt động gian lận như thế.

Các nhược điểm của quay vòng các nhiệm vụ gồm phá vỡ các nhóm làm việc hiệu quả và chi phí đào tạo lại. Sự luân phiên như vậy cũng có thể cho phép nhân viên thu được một kiến thức toàn diện về sự sắp xếp an toàn trong một tổ chức. *So sánh với* separation of duties. *Xem* personnel security.

router ***bộ định tuyến, bộ chọn đường, cầu dẫn*** Trong truyền dữ liệu, một thiết bị kết nối các mạng mà sử dụng cùng tầng vận tải của mô hình tham chiếu kết nối các hệ thống mở nhưng có các tầng mạng khác nhau. *So sánh với* gateway, repeater. *Xem*

network layer, open systems interconnection, transport layer.

routing *(sự) định tuyến, (sự) chọn đường* Trong truyền dữ liệu, việc phân một tuyến đường cho một thông báo hoặc gói để tới đích cuối cùng của nó. *Xem* adaptive routing, data communications, directory routing, hot potato routing.

routing control *kiểm soát định tuyến* (1) Trong an toàn truyền thông, một dịch vụ an toàn trong an toàn kết nối các hệ thống mở để ngăn dữ liệu khỏi bị truyền qua các liên kết, hoặc qua các chuyển tiếp, mà không được xem xét tới việc cung cấp một mức an toàn thích hợp cho dữ liệu đang nói tới. *Xem* OSI security, routing. (2) Trong an toàn truyền thông, việc ứng dụng các quy tắc trong suốt quá trình định tuyến để chọn hoặc tránh các mạng, các liên kết hoặc chuyển tiếp xác định.

routing table *bảng định tuyến* Trong truyền dữ liệu, một bảng tại một nút của một mạng chuyển mạch thông báo, chỉ ra tuyến đường ưu tiên và đôi khi là ưu tiên thứ nhì cho mỗi đích. *Xem* fixed routing, directory routing, routing.

RS *tiền tố RS* Trong truyền dữ liệu, một tiền tố được sử dụng bởi Hội công nghiệp Điện tử (Electronic Industries Association) cho các chuẩn được sử dụng rộng rãi ở Bắc Mỹ. *So sánh với* V, X. *Xem* Electronic Industries Association, RS-232C, RS-366, RS-423A, RS-449.

RS-232C *chuẩn RS-232C* Trong truyền thông dữ liệu, một chuẩn phổ biến nhất được sử dụng trong các kết nối nối tiếp cho máy tính. Tên chính thức là ghép nối giữa thiết bị đầu cuối dữ liệu và thiết bị chấm dứt mạch dữ liệu sử dụng giao diện nhị phân nối tiếp. Chữ cái C trong tiền tố chỉ ra rằng nó đã được duyệt lại.

Chuẩn có 4 phần:

- các đặc trưng của tín hiệu điện;
- các đặc tính cơ của mạch ghép nối;
- mô tả chức năng về các tín hiệu;
- danh sách các loại mạch ghép nối chuẩn.

Các đặc tính của tín hiệu điện xác định các điện áp tương ứng với các giá trị tín hiệu nhị phân. Các đặc tính cơ mô tả cách bố trí kích thước của các chân cắm. Mô tả chức năng các tín hiệu định nghĩa 21 tín hiệu, còn danh sách các tập con chuẩn của các tín hiệu này được sử dụng trong các loại modem khác nhau.

Các khuyến nghị tương ứng của CCITT là V.24 và V.28. RS-232C được thiết kế để kết nối giữa một máy tính và modem tại một đầu của mạch nối điện thoại, và một thiết bị đầu cuối và modem tại đầu kia. Nó cũng thường được sử dụng trong kết nối giữa hai DTE nhưng mối quan hệ này có nhược điểm là việc truyền bị giới hạn trong khoảng cách tối đa là 50 fut và tốc độ truyền tối đa là 19.200 bit/giây. Chuẩn RS-232C không bao gồm thủ tục cho các cuộc gọi trả lời và kiểm soát modem đối với việc đảo ngược trong liên kết bán song công. *So sánh với* RS-366, RS-423A, RS-449. *Xem* CCITT, MODEM, null modem, V.24, V.28.

RS-232 *chuẩn RS-232* *Xem* RS-232C.

RS-366 ***chuẩn RS-366*** Trong truyền thông dữ liệu, một chuẩn EIA xác định cách máy tính đưa ra các chữ số cần gọi vào máy quay số tự động như thế nào, cách máy tính báo kết thúc số và các hoạt động thực hiện khi máy quay số tự động không thể thực hiện cuộc gọi. *Xem* autodialer, EIA, RS-232C, V.25.

RS-422A ***chuẩn RS-422A*** Trong truyền thông dữ liệu, một chuẩn ghép nối EIA dành cho tốc độ dữ liệu cao, 100 kilobit/giây ở khoảng cách 40 fut hoặc 1 kilobit/giây ở khoảng cách 4000 fut. Nó sử dụng 2 dây cho mỗi tín hiệu. Không giống với chuẩn RS-232C, nó chỉ gồm các tính năng kỹ thuật điện. *So sánh với* RS-423A. *Xem* data rate, EIA, RS-232C, V.11, X.27.

RS-423A ***chuẩn RS-423A*** Trong truyền thông dữ liệu, một chuẩn ghép nối sử dụng các truyền không cân bằng với các tốc độ truyền thấp hơn so với chuẩn RS-422A, 100.000 bit/giây ở khoảng cách 40 fut và 1000 bit/giây ở khoảng cách 4000 fut. Giống như chuẩn RS-422A nó chỉ gồm các tính năng kỹ thuật điện. *So sánh với* RS-422A. *Xem* data rate, EIA, RS-232C.

RS-449 ***chuẩn RS-449*** Trong truyền dữ liệu, một chuẩn được thiết kế để thay thế RS-232C. *Xem* RS-232C.

RSA ***thuật toán RSA*** Trong mật mã, viết tắt của Rivest-Shamir-Adleman, là một thuật toán được đặt tên theo tên của những người thiết kế, nó thực sự quan trọng trong mã hóa khóa công khai. Thuật toán sử dụng một hàm một chiều cửa sập dựa vào sự khó khăn trong việc phân tích ra thừa số tích các số nguyên tố lớn (ví dụ, các số nguyên với hàng trăm chữ số thập phân). Như vậy, phép tính toán được gộp trong phép nhân hai số nguyên tố lớn q và p là tối thiểu nhưng không thể tính toán được để nhận được các thừa số p và q từ tích n lên tới vài trăm chữ số thập phân. Tuy nhiên, đã có các báo cáo về việc thử phân tích nhân tử thành công các tích lớn các số nguyên tố bằng cách sử dụng các trạm được nối mạng. Một số lớn các trạm làm việc như vậy được sử dụng với các phép phân tích thuật toán phân tích nhân tử trong chế độ cơ sở, như vậy, chi phí cho hoạt động tương đối thấp, và quá trình thường thực hiện trong vài tuần.

Quá trình phát triển các khóa và việc mã/giải mã các thông báo được miêu tả dưới đây:

- Hai số nguyên tố lớn (p và q) được chọn ngẫu nhiên và tích của chúng là n được xác định. Giá trị n này được để công khai.
- Hàm Euler (Euler totient function) của n, tức là một số gồm các số nguyên trong dải 1... n - 1 là nguyên tố cùng nhau với n, được xác định. Vì p và q là số nguyên tố, nên hàm Euler được cho bởi:
  $\phi(n) = (p - 1)(q - 1)$, với p khác q.
  Giá trị này được giữ bí mật.
- Chọn một số nguyên E trong dải từ 2... $\phi(n)$ - 1 sao cho E là nguyên tố cùng nhau với p - 1 và q - 1. Đây là một khóa mã hóa công khai.
- Tính toán khóa giải mã riêng D qua: $ED \equiv 1 \bmod(\phi(n))$.
- D là khóa giải mã và được giữ bí mật, các giá trị của E và n được để

công khai, nhưng việc tính toán D đòi hỏi phải biết $\phi(n)$ và một kẻ tấn công tính toán hàm này sẽ kéo theo việc phân tích nhân tử n không thực hiện được về mặt tính toán để suy ra p và q.

- Khóa mã công khai E, và n, được để sẵn công khai, ví dụ trong một thư mục.
- Để mã hóa, dữ liệu được chia nhỏ thành nhiều khối M_1, M_2,... với độ dài của các khối được chọn lựa sao cho các khối thông báo riêng lẻ có một giá trị bằng số nhỏ hơn n. Sau đó các khối được nâng lên lũy thừa E theo modulo n, tức là các khối bản mã C_1 ... được tính toán:

  $C_1 \equiv (M_1)^E \bmod n$

  $C_2 \equiv (M_2)^E \bmod n$
- Giải mã thông báo bản mã được thực hiện với thao tác tương tự, được mô tả ở trên, trừ khi các khối bản mã được nâng lên luỹ thừa D theo modulo n, nghĩa là:

  $M_i \equiv (C_i)^D \bmod n \equiv (M_i)^{ED} \bmod n$
- Thông báo ban đầu được khôi phục lại bằng quá trình giải mã vì theo định lý Euler

  $M \equiv M^x \bmod n$ nếu

  $x \equiv 1 \bmod \phi(n)$.

Quá trình này có thể được minh họa qua một ví dụ đơn giản.

- Chọn $p = 101$, $q = 103$, vì thế $n = 101 \times 103 = 10403$.
- $\phi(n) = (p - 1)(q - 1) = 10200$.
- Chọn E nguyên tố cùng nhau với 10200 và trong dải từ 2-10119, giả sử $E = 97$.
- Tính toán D bằng phép suy rộng Euler:

  $97D = 1 \pmod{10200}$.

Tính toán $\phi(\phi(n))$, tức là số các số nguyên trong dải từ 1-10199 là nguyên tố cùng nhau với 10200, $\phi(\phi(10403)) = 2560$.

$D \equiv E^{(\phi(\phi(n))-1)} \bmod (\phi(n))$

$\equiv 97^{(2559)} \bmod (10200)$

$\equiv 8833$

Lưu ý $97 \times 8833 = 856801 \pmod{10200} = 1 \pmod{10200}$.

- E và n được để công khai trên một thư mục công khai với các giá trị tương ứng 97 và 10403.
- Người gửi muốn gửi thông báo $M = 33$. Nó được mã hóa như $C = 33^{97} \pmod{10403} = 4933$.
- Người nhận giải mã thông báo này bằng cách sử dụng khóa bí mật D: $D = 4933^{8833} \pmod{10403} = 33$.

Dường như một kẻ tấn công có thể giải mã thông báo bằng cách mã lặp, như vậy nâng bản mã lên các lũy thừa liên tiếp theo modulo n, cho đến khi khôi phục được bản rõ. Tuy nhiên, trong thực tế, với các khóa mã và giải mã dùng 100 chữ số thập phân hoặc nhiều hơn, số lần lặp lại sẽ quá mức và hình thức tấn công này sẽ không thể thực hiện được về mặt tính toán.

Có một số nghiên cứu về các tấn công tiềm ẩn lên RSA, chúng chỉ ra rằng cần lựa chọn các số nguyên p và q cẩn thận và cả $p - 1$ và $q - 1$ cũng cần có một thừa số lớn cho mỗi số.

RSA là một bước tiến lớn trong mật mã khóa công khai và nó đưa ra một giải pháp rất hay về chữ ký số. Các quá trình mã và giải mã đều đòi hỏi tính

toán nhiều hơn so với DES, và các mã pháp ba lô và vì vậy, có thể ảnh hưởng tới tốc độ dữ liệu tối đa đối với các hệ thống mã của mạng. Độ lớn của các khóa đối với RSA cũng cần được quan tâm hơn so với DES nhưng ít hơn so với mức độ cần thiết dành cho các mã pháp ba lô.

Trong việc quản lý khóa, RSA có thể được sử dụng để mã hóa các khóa DES trên mạng, vì vậy loại bỏ được sự cần thiết dùng các kỹ thuật phức tạp để truyền các khóa mã khóa; lưu lượng các khóa mã hóa khóa là thấp hơn nhiều so với lưu lượng của dữ liệu mạng và lượng tải cần tính toán thêm đối với mã hóa/giải mã RSA sẽ không ảnh hưởng nhiều đến lưu lượng. *So sánh với* knapsack cipher. *Xem* coprime, DES, Euler's Generalization, Euler totient function, key-encrypting key, modulo arithmetic, prime number, public key cryptography, trapdoor one-way function.

RSI *Xem* ANSI X9.17 - 1985, request service initiation.

RSM *Xem* ANSI X9.17 - 1985, response service message.

RTM *Xem* re-encipher to master key.

Rtmk *Xem* re-encipher to master key.

RTR *Xem* ANSI X9.17 - 1985, response to request service message.

rule ***quy tắc*** Trong tính toán, một phát biểu trong một hệ chuyên gia mà cho phép thiết lập khả năng xảy ra một xác nhận hoặc giá trị của một đối tượng. Một quy tắc kết hợp với các xác nhận hoặc các đối tượng ở mức thấp hơn để tạo ra một giá trị cho một xác nhận hoặc các đối tượng ở mức cao hơn. *Xem* expert systems, object, rule-based system.

rule-based access control ***kiểm soát truy nhập dựa trên quy tắc*** Trong kiểm soát truy nhập, một kiểm soát truy nhập dựa vào các quy tắc xác định liên quan đến bản chất của chủ thể và đối tượng, hơn là chỉ nhận dạng chúng, chẳng hạn các nhãn an toàn. *So sánh với* identity based access control. *Xem* mandatory access control.

rule-based security policy ***chính sách an toàn dựa trên quy tắc*** Trong an toàn dữ liệu, các chính sách an toàn dựa vào các quy tắc tổng thể áp đặt cho tất cả những người sử dụng. Các quy tắc này thường dựa vào việc so sánh sự nhạy cảm của các nguồn tài nguyên được truy nhập và quyền sở hữu các thuộc tính tương ứng của những người sử dụng, một nhóm những người sử dụng hoặc các thực thể hoạt động nhân danh họ. *So sánh với* identity-based security policy. *Xem* rule-based access control.

rule-based system ***hệ thống dựa trên quy tắc*** Trong tính toán, một hệ chuyên gia gồm một tập các quy tắc tiền kiểm - hậu thức. Các quy tắc là các phát biểu có điều kiện mà mô tả việc sửa đổi cơ sở dữ liệu như thế nào khi các mẫu nào đó được nhận ra trong dữ liệu. Việc thi hành sẽ tính đến sau khi so khớp mẫu, giám sát các thay đổi của cơ sở dữ liệu, quyết định quy tắc nào nên được thi hành tiếp theo và hiệu năng của sự thi hành. *Xem* database, expert system.

running key ***khóa chạy*** *Đồng nghĩa với* key stream.

run to run totals ***tổng chạy - chạy*** Trong tính toán, việc sử dụng các tổng kiểm soát đầu ra từ một tiến trình như các tổng kiểm soát đầu vào trên khắp quá trình xử lý sau đó. Các tổng kiểm soát được sử dụng làm các liên kết trong một chuỗi liên kết để ràng buộc một tiến trình với tiến trình khác theo một dãy các tiến trình hoặc một chu trình với một chu trình khác trên một khoảng thời gian.

R/W ***đọc/ghi*** Viết tắt của Read/Write.



S-847 ***virut S-847*** Trong an toàn máy tính, một loại virut kết thúc và thường trú, lây nhiễm các tệp COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL. *Xem* virus names.

sabotage ***(sự) phá hoại*** Theo luật pháp, sự phá hủy dự tính trước của con người đối với tài sản hay thiết bị vật lý trong một cố gắng nhằm ngừng hoặc chấm dứt việc sản xuất hoặc các hoạt động khác của một chính phủ hoặc của một tổ chức kinh doanh cá nhân.

Saddam ***virut Saddam*** Trong an toàn máy tính, một loại virut kết thúc và thường trú, lây nhiễm các tệp COMMAND.COM và COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu và liên kết tệp. *Xem* virus names.

safeguard ***phòng vệ*** Trong an toàn máy tính, một biện pháp bảo vệ để làm giảm bớt tác động của các điểm yếu dễ bị tấn công của hệ thống. *Xem* matrix methodology, vulnerability.

safeguarding statement ***lệnh bảo vệ*** Trong an toàn dữ liệu, một câu lệnh được thêm vào đầu ra của máy tính, nó nói lên phân loại cao nhất đang được xử lý trên một hệ thống tự động tại thời điểm kết quả được đưa ra và yêu cầu sự kiểm soát của nó ở mức đó cho đến khi một người có trách nhiệm có thể quyết định mức phân loại thực của nó.

safe prime ***số nguyên tố an toàn*** Trong toán học, một số nguyên tố có dạng $2p + 1$, trong đó p là một số nguyên tố lẻ. Các số nguyên tố an toàn quan trọng trong RSA bởi vì chúng cung cấp bảo vệ tốt nhất chống các thuật toán phân tích nhân tử tinh vi. *Xem* factoring, odd prime, RSA.

safety ***tính chắc chắn, tính an toàn*** Trong an toàn vật lý, một thuộc tính để một hệ thống sẽ thỏa mãn tiêu chuẩn

nhất định liên quan tới việc duy trì tính an toàn cá nhân và tập thể.

SAGITTAIRE *hệ SAGITTAIRE* Trong hoạt động ngân hàng, viết tắt của Systéme Automatique de Gestion Intégré par Télétransmission de Transaction Avec Imputation de Règlements Etrangers (hệ thống tự động quản lý kết hợp viễn truyền giao dịch với việc khấu trừ các thanh toán ngoại hối), một dịch vụ chi trả liên ngân hàng điện tử do Ngân hàng Pháp điều hành trong phạm vi nước Pháp dành cho các thành viên SWIFT và các chi nhánh nhỏ đặt tại nước Pháp và nó chỉ xử lý các việc chi trả dùng đồng frăng Pháp. *Xem* banking networks, SWIFT.

SAISS *hệ SAISS* Viết tắt của Subcommittee on Automated Information System Security (tiểu ban an toàn hệ thống thông tin tự động).

salami technique *kỹ thuật salami* Trong an toàn máy tính, một dạng của con ngựa thành Toroa, nó có tác dụng thêm các lượng nhỏ tiền vào một tài khoản của kẻ gian lận trong các khoảng thời gian dài. Các phần của đơn vị tiền tệ thấp nhất được tạo ra bằng phép xử lý số học, được làm tròn và sau đó được gửi vào tài khoản của thủ phạm. *So sánh với* checking kiting. *Xem* malicious code. *Đồng nghĩa với* french roundoff.

same day funds *quỹ cùng ngày* Trong hoạt động ngân hàng, dùng để chỉ ra hiệu lực của các quỹ trong một ngày giao dịch, chịu sự thanh toán giao dịch thông qua phương pháp chi trả được sử dụng.

sampling *lấy mẫu* Trong an toàn cơ sở dữ liệu, *xem* random sample queries.

sandwich tape *băng lớp kẹp* Trong kiểm soát truy nhập, một chất liệu được sử dụng trong các vạch từ, nó được thiết kế để làm tăng mức độ khó khăn của việc sản xuất các thẻ vạch từ giả mạo. Chất liệu làm vạch từ gồm một chất có độ kháng từ thấp bao quanh chất độ kháng từ cao. Một trường cường độ cao được sử dụng để mã hóa vạch để sao cho cả hai chất liệu đều được từ hóa. Trong thiết bị đọc, vạch đầu tiên bị buộc đi qua một trường xóa có cường độ thấp, nó khử từ đối với nguyên liệu độ kháng từ thấp. Nếu một kẻ làm giả sử dụng chất liệu từ truyền thống thì dữ liệu giả mạo sẽ bị hủy bỏ bằng trường xóa. Nói cách khác, một kẻ làm giả sử dụng chất liệu lớp kẹp phải tiếp cận vào các thiết bị mã hóa từ đắt tiền, có khả năng phát triển các trường từ cao, cần thiết để từ hóa lớp kháng từ cao. *So sánh với* watermark tape. *Xem* coercivity, magnetic stripe card.

sanitization *(sự) giảm mức (phân loại), (sự) thanh lọc* (1) Trong an toàn dữ liệu, một kỹ thuật được chấp nhận để ấn định một phân loại an toàn cho một mục dữ liệu với mức thấp hơn mức phân loại của dữ liệu mà nó nhận được từ đó. Ví dụ tổng số lương chi trả của một tổ chức có thể được có một phân loại thấp hơn so với mức phân loại cấp cho lương của người quản lý, mặc dù các lương của người quản lý sẽ được sử dụng trong việc tính tổng. *Xem* multilevel database security. (2) Trong an toàn dữ liệu, việc loại bỏ thông tin đã

phân loại mật khỏi phương tiện từ tính, cho phép tái sử dụng phương tiện ở mức phân loại thấp hơn, hoặc cho phép phát cho cá nhân chưa được cấp mức truy nhập, hoặc cá nhân không có các quyền truy nhập tới toàn bộ thông tin. *Xem* sanitizing.

sanitizing ***làm giảm mức*** (1) Trong an toàn dữ liệu, xóa bỏ hoặc biến đổi dữ liệu nhạy cảm để làm giảm tính nhạy cảm của nó. *Xem* sensitive information. (2) Trong an toàn dữ liệu, quá trình khử từ hoặc ghi đè lên thông tin nhạy cảm trên phương tiện từ hoặc phương tiện lưu giữ khác. *Đồng nghĩa với* scrubing. *Xem* sanitization.

saturation testing ***thử mức bão hòa*** Trong truyền dữ liệu, một kỹ thuật kiểm tra hiệu năng của một mạng truyền thông bằng một lượng lớn các thông báo. Nó được tiến hành để kiểm tra đối với các lỗi hệ thống chỉ phát sinh trong các trường hợp ngoại lệ, ví dụ việc tới đích đồng thời của hai thông báo. *So sánh với* flood testing.

Saturday 14th ***virut thứ bảy ngày 14, virut Saturday 14*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm vào các tệp COM, EXE, và OVL, định dạng hoặc ghi đè lên toàn bộ hoặc một phần của đĩa, ảnh hưởng thao tác trong thời điểm chạy, làm hỏng các tệp chương trình, và tệp OVL và liên kết tệp. *Xem* virus names.

S box ***hộp S*** Trong mật mã, một hộp thay thế, một thành phần của một thuật toán mã hóa mà thực hiện một mã pháp thay thế trên tín hiệu đầu vào. *So sánh với* P box. *Xem* cryptography, data encryption standard, substitution cipher. *Đồng nghĩa với* substitution box.

scalar ***vô hướng*** Trong toán học, một đại lượng mang một giá trị số đơn lẻ, ví dụ chiều cao. *So sánh với* vector.

scalar product ***tích vô hướng*** Trong toán học, một phương pháp nhân hai vectơ để tạo ra một giá trị vô hướng. Tích vô hướng của các vectơ $(a_1, a_2, ..., a_n)$ và $(b_1, b_2, ..., b_n)$ được cho bởi $S = \sum_n a_i b_i$. *Đồng nghĩa với* dot product.

scan ***quét, duyệt qua*** Trong tính toán, một thủ tục để duyệt mọi nút trong cấu trúc. *Xem* node.

scanner ***thiết bị quét*** Trong an toàn truyền thông, một thiết bị được sử dụng để chặn các cuộc liên lạc vô tuyến, thường là trong vùng dải thông dân dụng, vô tuyến di động, cảnh sát, cứu hỏa, cấp cứu...

scanning ***(sự) quét*** Trong an toàn máy tính, sự tìm kiếm các số điện thoại và các mật khẩu bằng việc thử hàng loạt các tổ hợp của các số và các chữ cái. *Xem* exhaustive attack, hacker. *Đồng nghĩa với* hack hack.

scavenging ***lục rác, bới rác*** Trong an toàn máy tính, việc tìm kiếm dữ liệu không được phép trên bã dữ liệu (residue). *So sánh với* browsing. *Xem* residue.

scenario analysis ***phân tích viễn cảnh*** *Đồng nghĩa với* flaw hypothesis methodology.

scheduled circuits ***(các) mạng lập sẵn, mạng theo lịch biểu*** Trong truyền dữ liệu, các mạng thuê bao do

British Telecom cung cấp được quy định dành riêng cho việc sử dụng dữ liệu. *Xem* conditioning.

schema ***sơ đồ*** Trong các cơ sở dữ liệu, sơ đồ về toàn bộ cấu trúc logic của một cơ sở dữ liệu.

schematic ***lược đồ*** Một sơ đồ về các thành phần và các liên kết hoặc các mối quan hệ của một hệ thống.

Schnorr cipher ***mã pháp Schnorr*** Trong mật mã, một phép biến đổi dựa trên RSA, có các chữ ký ngắn hơn và sinh ra chữ ký nhanh hơn. *Xem* digital signature, RSA.

SCI *Xem* sensitive compartmented information.

scientific and technical information ***thông tin khoa học và kỹ thuật*** Kiến thức và thông tin có thể truyền đạt, rút ra hoặc nói tới sự hướng dẫn và quản lý các nỗ lực nghiên cứu và phát triển. STI được những nhà quản trị, quản lý, các nhà khoa học và các kỹ sư sử dụng trong các nỗ lực khoa học và công nghệ và là nguồn tài nguyên chất xám chủ yếu cho và cũng là kết quả của nỗ lực đó.

SCOMP ***bộ SCOMP, bộ xử lý liên lạc an toàn*** Trong an toàn máy tính, viết tắt của Secure COMmunications Processor. Tên này được gắn liền với máy tính mini Honeywell Level 6 được sửa đổi để làm tăng khả năng bảo vệ của nó. Có 4 vòng bảo vệ được thêm kèm theo đầu vào/đầu ra được khởi tạo bởi người sử dụng vào các thiết bị truy nhập bộ nhớ trực tiếp. *Xem* protection ring, security kernel.

Scott's Valley ***virut Scott's Valley*** Trong an toàn máy tính, một virut máy tính mà mã hóa chính bản thân nó, kết thúc và thường trú, lây nhiễm các tệp COM, EXE, và OVL, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu và liên kết tệp. *Xem* virus names.

scrambler ***bộ xáo trộn*** (1) Trong truyền thông, một thiết bị mã được áp dụng cho các liên kết truyền thông nhằm giữ an toàn hoặc để tránh các mẫu dữ liệu số có hại lặp lại. Những mẫu lặp lại có thể xuất hiện trong các hệ thống điều pha và tạo ra sự dịch pha 0 trong một chu kỳ tương đối dài, gây hậu quả mất đồng bộ giữa các bộ giải mã thu và phát. *Xem* phase modulation. (2) Trong an toàn truyền thông, *xem* voice scrambling.

scrolling ***cuộn*** Trong tính toán, việc dịch chuyển liên tục theo phương thẳng đứng hoặc nằm ngang của màn hình sao cho dữ liệu mới xuất hiện ở mép này thì dữ liệu cũ biến mất khỏi mép kia.

scroll mode terminal ***thiết bị đầu cuối chế độ cuộn*** Trong truyền dữ liệu, một thiết bị đầu cuối không có xử lý cục bộ, các nhấn bàn phím được hiển thị hoặc truyền đi riêng lẻ và các ký tự nhận lại được hiển thị y nguyên. Các dòng được hiển thị cuộn lên trên như chúng được lấp đầy bởi các ký tự được hiển thị. *So sánh với* form mode terminal, page mode terminal.

scrubbing ***(sự) lọc xóa*** *Đồng nghĩa với* sanitizing.

SDLC *Xem* software development life cycle, synchronous data link control.

SDU *Xem* service data unit.

search key ***khóa tìm kiếm*** Trong cơ sở dữ liệu, dữ liệu được so sánh với một phần chỉ ra của mỗi mục trong tìm kiếm. *Xem* key.

SECDEC ***mã SECDEC, mã phát hiện lỗi kép hiệu chỉnh lỗi đơn*** Trong các mã, viết tắt của Single Error Correction Double Error Detection, một mã phát hiện và hiệu chỉnh lỗi có thể phát hiện và sửa các lỗi một bit và phát hiện nhưng không sửa các lỗi hai bit. Các kiểm tra tính chẵn lẻ đơn chỉ có thể phát hiện ra song không hiệu chỉnh được các lỗi một bit, trong khi đó không thể phát hiện ra các lỗi hai bit. *Xem* bit, error correction code, error detection code, Hamming code, parity checking.

secondary channel ***kênh phụ, kênh thứ cấp*** Trong truyền thông dữ liệu, một kênh dữ liệu nhận từ cùng một tuyến vật lý như kênh dữ liệu chính song độc lập hoàn toàn với nó. Nó chuyển tải thông tin bổ trợ, xử lý các kiểm soát tín hiệu thiết bị, chẩn đoán ... ở tốc độ dữ liệu thấp. *Xem* channel.

secondary destination ***nơi đến thứ cấp*** Trong truyền thông dữ liệu, bất kỳ nơi đến nào xác định trong thông báo từ nơi đến đầu tiên.

secondary key ***khóa phụ, khóa thứ cấp*** (1) Trong quản lý khóa, *so sánh với* primary key. *Đồng nghĩa với* key-encrypting key. (2) Trong các cơ sở dữ liệu, khóa không xác định đơn nhất một bản ghi. Khóa chứa giá trị của một thuộc tính khác với danh tính duy nhất. *So sánh với* primary key. *Xem* attribute.

secondary station ***trạm phụ, trạm thứ cấp*** Trong truyền thông dữ liệu, một trạm được chọn để nhận thông tin từ một trạm chính. Sự chỉ định trạng thái thứ cấp chỉ là tạm thời, nó do trạm chính tạo ra trong khoảng thời gian truyền thông báo. *Xem* primary station.

second normal form ***dạng chuẩn thứ hai*** Trong các cơ sở dữ liệu, một thuộc tính của một quan hệ trong cơ sở dữ liệu quan hệ. Một quan hệ ở dạng chuẩn thứ hai nếu nó ở dạng chuẩn thứ nhất và mỗi thuộc tính không cơ bản của quan hệ phụ thuộc có tính chức năng đầy đủ vào mỗi khóa dự bị (khóa có thể) của quan hệ. Một ví dụ về quan hệ không ở dạng chuẩn thứ hai là Số nhân viên, Số dự án, Tên dự án, Ngày hoàn thành dự án. Cặp Số nhân viên, Tên dự án là khóa dự phòng (khóa có thể) cho quan hệ, song Ngày hoàn thành dự án lại phụ thuộc chức năng và một tập con của khóa này, tức là Số dự án và như vậy, phụ thuộc chức năng không đầy đủ vào khóa dự phòng. Nhược điểm của quan hệ này nảy sinh nếu chỉ có một nhân viên gắn với một dự án và nhân viên đó xin thôi việc. Tất cả các bản ghi liên quan tới nhân viên đều bị xóa và các chi tiết về Ngày hoàn thành dự án đều bị mất, thậm chí mặc dù dự án vẫn còn. *So sánh với* first normal form, third normal form. *Xem* candidate key, fully functional dependent, nonprime attribute, normal forms, relational database.

second sourcing ***tạo nguồn thứ cấp, tạo nguồn phụ*** (1) Sự cấp quyền cho việc sản xuất các linh kiện điện tử, thường là các bộ vi xử lý. (2) Sự đảm

bảo cung cấp linh kiện lấy từ hai hoặc nhiều nguồn tách riêng.

secrecy ***(sự) bí mật*** *Đồng nghĩa với* confidentiality.

secrecy classification ***phân loại mật*** Trong an toàn dữ liệu, một thuộc tính của dữ liệu hay các đối tượng biểu thị mối nguy hiểm tiềm ẩn liên quan nảy sinh nếu như dữ liệu hay các đối tượng bị tổn thương trước đối phương. *Xem* compromise.

secrecy order ***chỉ thị về giữ bí mật*** Trong luật pháp, chỉ thị của chính phủ Mỹ, thường liên quan tới các ứng dụng sáng chế mà ngăn cấm sự tiết lộ thông tin hay sáng chế khi nó được chỉ dẫn rằng, sự tiết lộ như vậy có thể sẽ làm hại tới an ninh quốc gia.

secrecy policy ***chính sách giữ bí mật*** Trong an toàn dữ liệu, một chính sách an toàn nhằm nhăn chặn những người sử dụng trái phép đọc thông tin nhạy cảm. *So sánh với* integrity policy. *Xem* security policy.

Secret ***tuyệt mật*** *Xem* classification.

secret clearance ***mức thông tuyệt mật, mức truy nhập tuyệt mật*** Trong kiểm soát truy nhập, một mức truy nhập do Bộ Quốc phòng Mỹ đưa ra, nó thường đòi hỏi sự kiểm tra của cơ quan quốc gia gồm có rà soát các hồ sơ về vân tay và điều tra của FBI Hoa Kỳ và Danh lục điều tra phòng vệ trung ương. Trong một số trường hợp, cũng cần có sự điều tra hơn nữa. *So sánh với* confidential clearance, uncleared, unclassified information, top security clearance, one category, multiple categories. *Xem* clearance.

secret key ***khóa mật*** Trong mật mã, khóa (trong hệ mật mã khóa không đối xứng hay hệ mật mã khóa công khai) trong tập khóa của người sử dụng mà chỉ riêng người sử dụng đó biết. *So sánh với* public key. *Xem* asymmetric algorithm, public key cryptography.

secret key algorithm ***thuật toán khóa mật*** *Đồng nghĩa với* symmetric cryptosystem.

secret key encryption ***mã hóa khóa mật*** Trong mật mã, một thuật toán mã chỉ dùng các khóa mật. *So sánh với* public key cryptography. *Xem* encryption algorithm. *Đồng nghĩa với* private key encryption.

secret sharing scheme ***lược đồ chia sẻ khóa mật*** Trong mật mã, một kỹ thuật cho phép một nhóm n người chia sẻ sự hiểu biết về một khóa mật và chia sẻ với các khóa nhận được sau này từ hiểu biết chung của họ nếu như sau đó, một số trong các thành viên không sử dụng được. Với kỹ thuật chia sẻ khóa mật thích hợp, với giá trị t cho trước nào đó ($t < n$), nhóm con bất kỳ gồm t thành viên có đủ thông tin để nhận được khóa mật, song nhóm con nhỏ hơn bất kỳ trong nhóm con đó sẽ không làm như vậy được. Những kỹ thuật như vậy có thể được dùng để phân phối một khóa chính trong một nhóm gồm các nhà quản lý tin cậy. *Xem* threshold.

sector ***cung (từ), secto*** Trong tính toán, một phần trong thiết bị lưu trữ từ tính quay được mà đầu từ có thể tiếp cận trong quá trình quay cụ thể. Các đĩa từ được chia thành các rãnh tròn và mỗi rãnh sau đó lại được chia

nhỏ ra thành các cung từ giữ một khối dữ liệu. Một cung từ là đơn vị nhỏ nhất của đĩa mà máy tính có thể đánh địa chỉ.

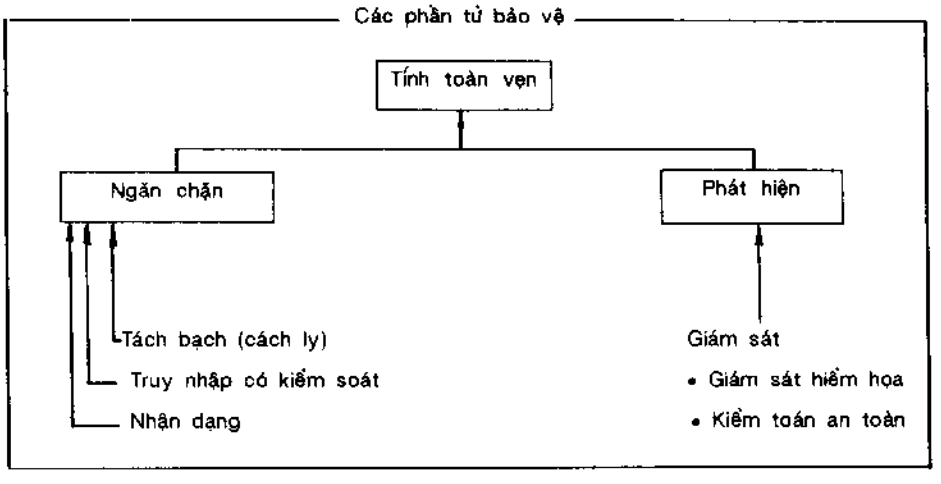
secure channel ***kênh an toàn, kênh bí mật*** Trong an toàn truyền thông, một tuyến thông tin trong đó những người nhận có thể biết tất cả những người gửi có thể, hoặc những người gửi biết tất cả những người nhận. *Xem* receiver, sender.

secure configuration management ***quản lý cấu hình an toàn*** Trong an toàn máy tính, việc sử dụng các thủ tục thích hợp để kiểm soát những thay đổi các cấu trúc phần cứng và phần mềm của hệ thống nhằm bảo đảm rằng, những thay đổi như vậy sẽ không dẫn tới làm giảm tính an toàn của dữ liệu. *Xem* data security.

secure management information base ***cơ sở thông tin quản lý an toàn*** Trong an toàn truyền thông, một cơ sở dữ liệu khái niệm được đề xuất cho các hệ thống kết nối an toàn mở. Cơ sở dữ liệu này giữ thông tin liên quan tới tính an toàn mà những người sử dụng cuối trong các hệ thống mở yêu cầu. *Xem* OSI security.

secure module ***mođun an toàn*** *Đồng nghĩa với* tamper resistant module.

secure operating system ***hệ điều hành an toàn*** Trong an toàn máy tính, một hệ điều hành kiểm soát hiệu quả các chức năng phần cứng và phần mềm nhằm bảo đảm mức bảo vệ thích hợp đối với giá trị dữ liệu và các tài nguyên do hệ điều hành quản lý. *Xem* Bell-La Padula model, operating system, resource.



secure operating system: *hệ điều hành an toàn*. Cấu trúc để phát triển các yêu cầu về hệ điều hành an toàn. Việc phòng ngừa biểu thị tuyến bảo vệ thụ động trong khi sự phat hiện hàm ý không chỉ việc khám phá ra các ý định mà còn cả sự bắt đầu sự phản ứng tích cực. Tính toàn vẹn là sự bảo đảm rằng, hệ thống làm việc như dự định mà mọi nỗ lực truy nhập đều được dàn xếp rằng, sự kiểm soát an toàn được duy trì mọi lúc và không có chế độ hoạt động nào không được biết.

secure path ***tuyến an toàn*** *Đồng nghĩa với* trusted path.

secure state ***trạng thái an toàn*** Trong an toàn máy tính, một điều kiện đã biết, được dự tính trước thông qua việc sử dụng phần mềm tin cậy và được bảo vệ. Trong thời gian xử lý, có thể đạt tới trạng thái an toàn bằng cách khởi động bản sao được điều khiển của hệ điều hành vào lúc bắt đầu mỗi phiên làm việc. *Xem* periods processing, trusted software.

secure telephone system ***hệ thống điện thoại an toàn*** Trong an toàn máy tính, một hệ thống điện thoại trong đó tính an toàn của các cuộc liên lạc được tuân thủ nhờ phép xáo trộn tiếng nói và/hoặc mạch giám sát trực tuyến. *Xem* voice scrambling.

secure working area ***vùng làm việc an toàn*** Trong an toàn dữ liệu, một phương tiện được chính thức công nhận được sử dụng để quản lý, thảo luận hoặc xử lý thông tin bảo vệ nhạy cảm. *Xem* sensitive defence information.

security ***tính an toàn*** Phẩm chất hoặc trạng thái cần được bảo vệ một cách có hiệu quả khỏi những mất mát quá mức (chẳng hạn, mất khách hàng, mất tiền, mất khả năng tiếp tục hoạt động...) *Xem* add-on security, administrative security, communications security, computer security, data security, emanation security, personal security, physiscal security, procedural security, teleprocessing security, traffic flow security.

security architecture ***kiến trúc an toàn*** Trong an toàn máy tính và truyền thông, một tập con kiến trúc máy tính nhằm xử lý tính an toàn của máy tính hoặc hệ thống mạng. *Xem* network architecture.

security area ***vùng an toàn*** Trong an toàn vật lý, một không gian xác định một cách vật lý chứa những thứ đã phân loại mật (tài liệu hoặc chất liệu) chịu sự bảo vệ vật lý và các kiểm soát truy nhập cá nhân. *Xem* restricted area.

security audit ***kiểm toán an toàn*** (1) Trong an toàn dữ liệu, sự xem xét (xem có đạt không) các thủ tục và các biện pháp an toàn nhằm mục đích đánh giá xem chúng có tuân thủ và phù hợp với chính sách đã thiết lập không. (2) Trong an toàn dữ liệu, sự xem xét độc lập và cân nhắc các bản ghi hệ thống và các hành động để kiểm tra sự phù hợp đầy đủ của các kiểm soát hệ thống, nhằm đảm bảo sự tuân thủ theo chính sách đã thiết lập và các thủ tục hoạt động và để khuyến nghị những thay đổi chỉ ra bất kỳ trong các kiểm soát, các chính sách và các thủ tục.

security audit trail ***vệt kiểm toán an toàn*** Trong an toàn dữ liệu, dữ liệu thu thập được và được sử dụng tiềm tàng để tạo thuận lợi cho kiểm toán an toàn. *Xem* security audit.

security breach ***kẽ hở an toàn, vi phạm an toàn*** Trong an toàn dữ liệu, sự vi phạm các kiểm soát an toàn, tạo ra mối nguy hiểm của việc mất mát các thành phần của hệ thống hoặc làm tổn thương thông tin.

security compliant channel ***kênh tuân thủ an toàn*** Trong an toàn truyền thông, một kênh mà sự tuân thủ

chính sách mạng chỉ phụ thuộc vào các đặc trưng của kênh mà hoặc (*a*) được tính đến trong đánh giá, hoặc (*b*) được giả thiết như một điều kiện ràng buộc thực hiện và được lập tài liệu rõ ràng trong Sổ hướng dẫn phương tiện tin cậy.

security critical mechanisms ***(các) cơ chế tới hạn an toàn*** Trong an toàn máy tính, các cơ chế an toàn mà sự hoạt động đúng đắn của nó là cần thiết để đảm bảo tuân thủ chính sách an toàn. Các cơ chế có thể hoặc không phải là một phần của TCB. *Xem* security policy, TBC.

security feasibility study ***nghiên cứu tính khả thi về an toàn*** Trong an toàn máy tính, một nghiên cứu để xác định xem liệu các kiểm soát có sẵn sàng đáp ứng các mục tiêu an toàn hay không, sự mở rộng phạm vi theo đó chúng sẽ thỏa mãn các mục tiêu, hoặc là xem các kiểm soát có phục hồi, ngăn ngừa, phát hiện và có pha trộn tối ưu các kiểm soát về kỹ thuật, vật lý và hành chính hay không. *Xem* risk analysis.

security filter ***bộ lọc an toàn*** (1) Trong an toàn máy tính, một bộ các thủ tục và kỹ thuật phần mềm được dùng trong các hệ thống ADP để ngăn chặn sự chuyển tiếp tự động dữ liệu chỉ ra trên các kết nối không được bảo vệ hoặc cho những cá nhân trái phép. *Xem* security kernel. (2) Trong an toàn cơ sở dữ liệu, *xem* filter.

security flow analysis ***phân tích lưu lượng an toàn*** Trong an toàn máy tính, một kiểu phân tích an toàn được thực hiện dựa trên bản đặc tả hệ thống hình thức phi thủ tục mà định vị các dòng thông tin tiềm ẩn giữa các biến hệ thống. Nhờ gán các mức an toàn cho các biến hệ thống, có thể nhận dạng nhiều kênh thông tin gián tiếp.

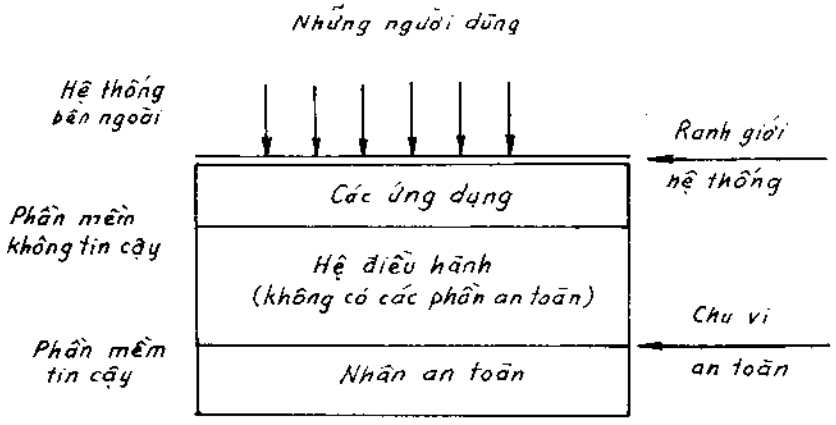
Việc phân tích lưu lượng an toàn sẽ xác định một mô hình an toàn tương tự với mô hình kiểm soát truy nhập (Bell-La Padula) song có mức bảo vệ mịn hơn (chi tiết hơn). *Xem* Bell-La Padula model, granularity.

security function ***chức năng an toàn*** Trong an toàn thông tin, một phát biểu về kiểu an toàn được thực hiện để đáp ứng một mục tiêu an toàn. *So sánh với* security mechanism, security objective. *Xem* information technology security evaluation criteria.

security incident ***sự cố an toàn*** Trong an toàn dữ liệu, hành động hay tình huống bất kỳ liên quan đến thông tin đã phân loại vốn sai lệch với các yêu cầu chỉ phối các công bố an toàn, ví dụ, sự thất thoát, sự có thể thất thoát, sự tiết lộ vô ý và sự sai lệch.

security inspection ***thanh tra an toàn*** Trong an toàn thông tin, một xem xét của một hệ thống ADP để xác định sự tuân thủ theo chính sách an toàn ADP, các thủ tục và thực hành thực tế.

security kernel ***nhân an toàn*** (1) Trong an toàn máy tính, một cơ chế khoanh vùng gồm có phần cứng và mềm mà kiểm soát sự truy nhập của những người sử dụng (và các quá trình thi hành nhân danh họ) để lấy thông tin thường trú trong hệ thống hoặc nối



với hệ thống. Hoạt động chính xác của nhân cùng với các quá trình được tin cậy phù hợp cần đầy đủ để bảo đảm sự tuân thủ các ràng buộc đối với sự truy nhập. Các TCB được thiết lập bằng cách sử dụng các nhân an toàn đi kèm theo các quá trình xử lý tin cậy. *Xem* TCB. (2) Trong an toàn máy tính, các yếu tố phần cứng, chương trình cơ sở, và phần mềm của một TCB mà thực hiện khái niệm giám sát tham chiếu. Nó phải dàn xếp toàn bộ các truy nhập, được bảo vệ khỏi việc sửa đổi, và có thể xác nhận là đúng. *Xem* reference monitor concept, TCB. (3) Trong an toàn máy tính, phần trung tâm của hệ thống máy tính (phần mềm, phần cứng) và thực hiện các thủ tục an toàn cơ bản để kiểm soát truy nhập tới các tài nguyên của hệ thống. *Xem* access control, filter, resource.

security label ***nhãn an toàn*** (1) Trong kiểm soát truy nhập, việc đánh dấu gắn liền với một nguồn tài nguyên (nó có thể là một khối dữ liệu) vốn đặt tên hoặc ấn định các thuộc tính an toàn của tài nguyên đó. (2) Trong an toàn dữ liệu, một bộ chỉ báo nhạy cảm, nó liên kết thường xuyên với dữ liệu được bảo vệ, các quá trình xử lý và hoặc các nguồn tài nguyên khác và nó có thể được sử dụng trong áp đặt chính sách an toàn. *Xem* spray paint. (3) *Đồng nghĩa với* sensitivity label.

security level ***cấp an toàn, mức an toàn*** Trong an toàn máy tính, sự tổ hợp của phân loại theo hệ thống cấp bậc và một tập của các loại (category) không thứ bậc mà đặc trưng cho sự nhạy cảm của thông tin. *Xem* sensitivity.

security life ***tuổi thọ an toàn, thời gian hiệu lực an toàn*** Trong mật mã, khoảng thời gian mà dữ liệu được bảo vệ bằng mật mã còn giá trị.

security line ***đường dây an toàn***

Đồng nghĩa với alarm line.

security log ***bản ghi (nhật ký) an toàn*** Trong an toàn máy tính, một bản ghi ghi toàn bộ các biến cố của máy tính được xem là liên quan đến an toàn, và được duy trì để phát hiện xâm nhập hoặc các điều tra nghiên cứu về lỗi logic của hoạt động lạm dụng máy tính bị nghi ngờ. *Xem* intrusion detection.

security loop ***vòng lặp an toàn*** *Đồng nghĩa với* alarm line.

security management ***quản lý an toàn*** *Xem* OSI security.

security measures ***(các) biện pháp an toàn*** Trong an toàn máy tính, các yếu tố phần mềm, phần sụn, phần cứng, hoặc các thủ tục trong hệ thống để thỏa mãn các đặc tính an toàn. *Xem* firmware.

security mechanism ***cơ chế an toàn*** Trong an toàn thông tin, các cách được sử dụng để thực hiện một chức năng an toàn. *So sánh với* security function, security objective. *Xem* information technology security evaluation criteria.

security model ***mô hình an toàn*** Trong an toàn máy tính, một mô hình xác định các quy tắc an toàn bắt buộc của hệ thống. Nó chỉ rõ các kiểm soát truy nhập trong việc sử dụng thông tin và cách thông tin được cho phép lưu thông trong hệ thống như thế nào. Nó cũng cung cấp cơ chế định rõ cách thay đổi động các kiểm soát truy nhập và các giao diện mà không làm ảnh hưởng đến an toàn của hệ thống.

security modem ***modem an toàn*** Trong an toàn máy tính, một modem được cài đặt trong một thiết bị đầu cuối của người sử dụng với các chức năng an toàn tích hợp. Các modem như vậy kết hợp chặt chẽ yêu cầu ngoài giới hạn an toàn để kiểm soát truy nhập máy chủ từ một đầu cuối của người sử dụng. Người sử dụng nhập vào một mật khẩu dành cho một máy chủ cho trước, modem an toàn kiểm tra mật khẩu dựa vào số điện thoại của máy tính chủ và nếu phù hợp thì modem quay số máy tính và bắt đầu các thủ tục đăng nhập. *So sánh với* port protection device. *Xem* modem, telephone intrusion.

security module ***mođun an toàn*** Một mođun được dùng trong quá trình mã hóa bí mật. *Đồng nghĩa với* tamper resistant module.

security monitor ***bộ giám sát an toàn*** Trong an toàn vật lý, một thiết bị giám sát của một tuyến báo động và thiết bị liên quan. *Xem* alarm line.

security objective ***mục tiêu an toàn*** Trong an toàn thông tin, một phát biểu trên cơ sở hợp lý về các yêu cầu an toàn, các mục tiêu như vậy được đòi hỏi để xác định các chức năng an toàn và cơ chế an toàn cần thiết. *So sánh với* security function, security mechanism. *Xem* information technology security evaluation criteria.

security parameter ***tham số an toàn*** *Xem* cryptographic key, initialization vector, password.

security perimeter ***chu vi an toàn*** *Đồng nghĩa với* control zone.

security peripheral ***thiết bị ngoại vi an toàn*** *Đồng nghĩa với*

cryptographic facility.

security policy ***chính sách an toàn*** (1) Trong an toàn dữ liệu, một tập tiêu chuẩn cung cấp các dịch vụ an toàn. *Xem* identity based security policy, rule based security policy, security service. (2) Trong an toàn máy tính, một tập hợp các luật, các quy tắc, và các thủ tục mà quy định cách thức một tổ chức quản lý, bảo vệ và phân bố các thông tin nhạy cảm. *Xem* sensitive information. (3) Trong an toàn truyền thông, phát biểu về các quy tắc cung cấp các dịch vụ an toàn cho một hoặc nhiều kiểu truyền thông. Một chính sách an toàn dựa trên các dịch vụ an toàn vốn được yêu cầu và bị buộc tuân theo sự quản trị hệ thống thích hợp và các dịch vụ an toàn khác được thực thể mong muốn liên lạc với hệ thống yêu cầu. *Xem* discretionary security, mandatory security. (4) Trong an toàn thông tin, một chính sách an toàn là một cách giải quyết hoặc một kế hoạch hoạt động chung được một tổ chức thông qua để đảm bảo rằng, các tài sản thông tin đều được bảo vệ về tính bí mật, tính xác thực và sẵn sàng.

Khái quát

Chính sách của một tổ chức xác định các yêu cầu, trách nhiệm, và kiểm soát an toàn đối với tổ chức. Chính sách an toàn sẽ xác định các mục tiêu an toàn chính cần đạt được và chứa đựng sự nhìn nhận của tổ chức về rủi ro và khuôn khổ an toàn để đạt được các mục tiêu thương mại. Điều quan trọng là các yêu cầu về chính sách an toàn liên quan đến sự tác động có tính thương mại của các sự cố an toàn, cung cấp một ưu tiên hợp lý đối với các biện pháp an toàn. Chính sách sẽ gắn các trách nhiệm đối với các hoạt động an toàn và chỉ ra mức độ phân định trách nhiệm và được phép của các thành viên chính, một thành viên quản lý cao cấp phải chịu toàn bộ trách nhiệm đối với việc an toàn. Chính sách cũng sẽ chứa chỉ dẫn và các kiểm soát được tính đến trong việc duy trì an toàn.

Các nội dung của chính sách an toàn

Nội dung đặc trưng của một chính sách an toàn gồm có:

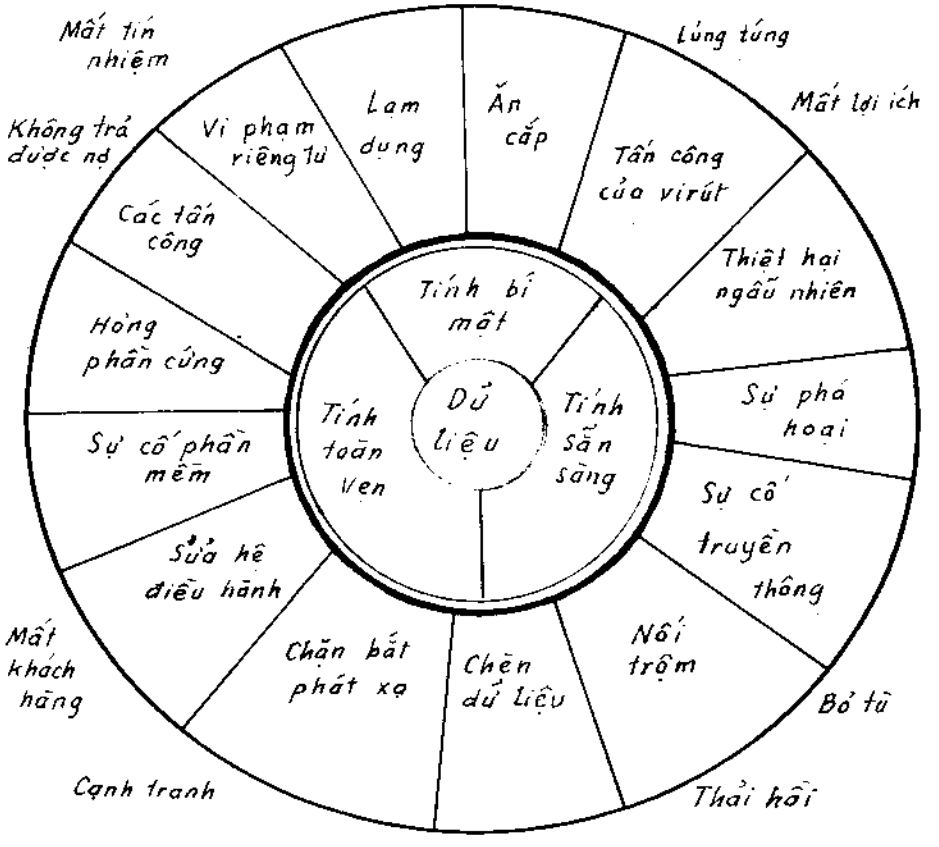
- trách nhiệm của người chủ sở hữu, người sử dụng, người trông coi và các bộ phận đặc biệt, chẳng hạn như an toàn dữ liệu;
- quản lý rủi ro, đánh giá rủi ro và phân loại/đánh giá dữ liệu;
- lên kế hoạch ngẫu nhiên và mềm dẻo;
- an toàn trong quá trình phát triển và thiết lập các hệ thống;
- truy nhập vào dữ liệu và các hệ thống và kiểm soát lưu giữ;
- an toàn truyền thông;
- an toàn máy tính cá nhân;
- an toàn vật lý;
- kiểm soát môi trường và truy nhập;
- các yêu cầu hợp pháp;
- các chính sách nhân sự.

Việc tạo một chính sách an toàn

Sự phát triển một chính sách an toàn có thể do một tổ hợp hoặc một bộ phận an toàn thông tin, hoặc các chuyên viên bên ngoài đảm nhận. Tuy nhiên, quyền sở hữu và sự phê chuẩn đối với chính sách là trách nhiệm của người quản lý cao cấp, sự an toàn phụ thuộc vào quyền hạn và sự công bố chính thức.

Chính sách phải được ủng hộ thông qua quyền hạn của người quản lý cao nhất và các trách nhiệm rõ ràng được thiết lập để duy trì nó. Ở tất cả các mức, các nhân viên phải nhận thức đầy đủ được các hậu quả, bao gồm các hậu quả do vi phạm kỷ luật, vi phạm chính sách. Việc ban bố chính sách đòi hỏi giải quyết theo một số mức. Các hợp đồng với nhân viên cần chỉ ra một cách rõ ràng các trách nhiệm cá nhân và các hoạt động vi phạm kỷ luật tiềm ẩn. Tương tự, khi một nhân viên chấm dứt một hợp đồng, mọi trách nhiệm gắn liền phải được tuyên bố một cách rõ ràng. Các chương trình đạo tạo, quảng cáo, các mẫu đăng nhập, các phát hành có tổ chức, ví dụ, các bản tin không chính thức, cũng nên được sử dụng để duy trì một mức nhận thức thích hợp.

security policy model ***mô hình chính sách an toàn*** Trong an toàn máy tính, sự trình bày phi hình thức một mô hình chính sách an toàn hình



security policy: *chính sách an toàn.* Các ảnh hưởng do vi phạm an toàn. Chính sách an toàn sẽ xác định sự cân bằng các kiểm soát.

thức. *Xem* formal security policy model.

security relevant event ***sự kiện liên quan tới an toàn*** Trong an toàn máy tính, sự kiện bất kỳ nhằm nỗ lực thay đổi tình trạng an toàn của hệ thống, (chẳng hạn thay đổi các kiểm soát truy nhập tùy ý, thay đổi mức an toàn của chủ thể, thay đổi mật khẩu người sử dụng...). Cũng như vậy, sự kiện bất kỳ về những nỗ lực vi phạm chính sách an toàn hệ thống, (chẳng hạn quá nhiều nỗ lực để đăng nhập, các nỗ lực vi phạm các hạn chế của kiểm soát truy nhập bắt buộc của một thiết bị, các nỗ lực giảm cấp một tệp...). *Xem* discretionary access control, log in, mandatory access control, password.

security requirements ***(các) yêu cầu an toàn*** Trong an toàn máy tính, các kiểu và các mức bảo vệ cần thiết đối với thiết bị, dữ liệu, thông tin, các ứng dụng, và các phương tiện.

security safeguards ***(các) phòng vệ an toàn*** Trong an toàn máy tính, các biện pháp và kiểm soát bảo vệ buộc tuân theo để đáp ứng các yêu cầu an toàn được chỉ ra cho AIS. Những phòng vệ an toàn này có thể bao gồm (nhưng không cần thiết phải giới hạn) các đặc tính an toàn phần cứng, phần mềm, các thủ tục hoạt động, các thủ tục phân định trách nhiệm, các kiểm soát truy nhập và phân phối, các ràng buộc trong quản lý, an toàn cá nhân, các cấu trúc, các vùng và các thiết bị vật lý.

security service ***dịch vụ an toàn*** (1) Trong an toàn truyền thông, một dịch vụ do một tầng của các hệ thống truyền thông mở cung cấp, nó đảm bảo an toàn đầy đủ cho các hệ thống hoặc các cuộc truyền dữ liệu. *Xem* OSI security. (2) Trong an toàn truyền thông, một dịch vụ do một tầng của các hệ truyền thông mở cung cấp, nó đảm bảo mức an toàn thích hợp của hệ thống hoặc của những sự chuyển dữ liệu. *Xem* OSI security.

security specifications ***(các) đặc tả an toàn*** (1) Trong an toàn dữ liệu, một mô tả chi tiết các biện pháp phòng vệ an toàn cần thiết để bảo vệ một ứng dụng nhạy cảm. (2) Trong an toàn máy tính, một mô tả chi tiết các biện pháp đối phó cần thiết để bảo vệ một hoạt động hoặc mạng ADP khỏi bị lộ, sửa đổi, hoặc hủy bỏ dữ liệu trái phép (ngẫu nhiên hoặc không định trước), hoặc sự từ chối của dịch vụ. *Xem* denial of service.

security target ***đích an toàn*** Trong an toàn thông tin, việc định rõ các đối tượng an toàn của mục tiêu đánh giá. *Xem* information technology security, evaluation criteria, security objective, target of evaluation.

security test and evaluation ***kiểm tra và đánh giá tính an toàn, ST&E*** (1) Trong an toàn dữ liệu, một quá trình quyết định rằng, các biện pháp an toàn vật lý, kỹ thuật, quản trị của hệ thống là đầy đủ đối với hệ thống; để cung cấp tài liệu và báo cáo các kết quả kiểm tra cho các cấp có thẩm quyền thích hợp, và để lập các khuyến nghị dựa vào các kết quả kiểm tra. Những nhà quản lý có thể chọn để xử lý ST&E như một phần tích hợp của công việc kiểm tra và đánh giá khác. Họ phải đảm bảo rằng, các thay đổi được thực hiện để

khắc phục một vấn đề không ảnh hưởng bất lợi đến các biện pháp an toàn khác được kiểm tra trước đó. (2) Trong an toàn máy tính, một cuộc kiểm tra và phân tích các biện pháp phòng vệ an toàn của một AIS khi chúng đã được áp dụng trong môi trường hoạt động để quyết định tình thế an toàn của AIS. *Xem* AIS, security test.

security testing ***kiểm định tính an toàn*** Trong an toàn máy tính, một quá trình được sử dụng để quyết định rằng, các thuộc tính an toàn của một hệ thống đều được thực hiện như thiết kế và rằng, chúng thích hợp cho môi trường của ứng dụng được đề xuất. Quá trình này bao gồm kiểm tra chức năng thực hành, kiểm tra sự thâm nhập và xác minh. *Xem* functional testing, penetration testing, security test and evaluation, tiger team, verification.

security threats ***(các) hiểm họa an toàn*** Trong quản lý rủi ro, nguồn của các hiểm họa an toàn có thể được liệt kê:

- các lỗi và sự bỏ sót do những người làm công trung thực gây ra;
- những người làm công không trung thực nắm lợi thế trong việc kiểm soát không đầy đủ nào đó hoặc lạm dụng quyền của họ và tìm cách che đậy hoạt động của họ;
- lửa và các thảm họa tự nhiên;
- những người làm công bất bình hoặc những người thôi không làm việc - người muốn gây ra thiệt hại đối với việc quản lý; không giống với những người làm công không trung thực, họ không tìm cách che đậy các kết quả hoạt động của mình;
- nguy hiểm của nước;
- các đe dọa từ bên ngoài, ví dụ, nạn khủng bố, bọn tin tặc, bạo loạn.

Xem hacker.

security violation ***(sự) vi phạm tính an toàn*** Trong an toàn máy tính, một sự cố xảy ra trong đó một người làm hỏng hoặc bỏ qua các kiểm soát an toàn để truy nhập không cho phép được tới thông tin, để sử dụng bất hợp pháp các nguồn tài nguyên của hệ thống hoặc hủy bỏ bất hợp pháp các thành phần của hệ thống.

seed ***hạt giống, mầm*** Trong toán học, một số được cung cấp vào một bộ tạo số ngẫu nhiên để khởi đầu quá trình tạo chuỗi. *Xem* random numbers.

seepage ***(sự) rò rỉ*** Trong an toàn máy tính, dòng ngẫu nhiên của dữ liệu hoặc thông tin bị các cá nhân không có quyền truy nhập vào, nó được giả định là được các biện pháp phòng vệ an toàn của máy tính kiểm soát. *Xem* data leakage.

segment ***đoạn*** (1) Trong tính toán, đây là một phần độc lập của một chương trình máy tính mà có thể chạy được mà không cần toàn bộ chương trình nhất thiết phải nằm trên một bộ nhớ bên trong tại bất kỳ thời điểm nào. (2) Trong truyền thông, một phần của một thông báo mà có thể được cất giữ trong một bộ đệm. *Xem* buffer.

seismic sensor ***bộ cảm biến (phát hiện) động đất*** Trong an toàn vật lý, một bộ cảm biến được thiết kế để phát hiện động đất hoặc phát hiện các chấn

động dưới lòng đất. Chúng bao gồm các cảm biến áp điện, các điện thoại địa vật lý được chôn dưới đất hoặc các cảm biến áp suất cân bằng. *Xem* piezoelectric sensor.

seize ***đoạt, chiếm đường truyền*** Trong truyền dữ liệu, giành được sự kiểm soát của một kênh để truyền một thông báo.

selection ***chọn*** Trong các cơ sở dữ liệu, một thao tác trên một cơ sở dữ liệu quan hệ trong đó, một quan hệ mới được tạo ra bằng cách lựa chọn các bản ghi, từ quan hệ ban đầu, theo tiêu chuẩn được xác định trên các trường. *So sánh với* division, join, projection. *Xem* field, record, relation database.

selective calling ***gọi có lựa chọn*** (1) Trong truyền dữ liệu, một hệ thống mà ở đó các trạm từ xa có thể được gọi tới để truyền các thông báo khi cần loại ra tất cả các trạm khác trên mạng. (2) Trong truyền dữ liệu, phương tiện của một máy phát để chọn lựa các trạm, trên cùng một đường truyền, mà cần nhận thông báo.

selective coded system ***hệ thống mã lựa chọn*** Trong an toàn vật lý, một hệ thống trong đó mỗi trạm báo hỏa thủ công và mỗi nhóm các bộ phát hiện tự động được kết hợp với mã có một, hai, ba hoặc bốn chữ số riêng lẻ. Nó phát ra âm thanh trên tất cả các thiết bị chỉ báo báo động khi trạm thủ công hoặc bộ phát hiện tự động được kích hoạt. *Xem* alarm station.

selective dump ***kết xuất chọn lọc*** Trong tính toán, một sự kết xuất của một hoặc nhiều vùng lưu giữ được chọn lựa. *Xem* dump.

selective field protection ***bảo vệ trường lựa chọn*** Trong an toàn truyền thông, sự bảo vệ các trường xác định trong một thông báo cần truyền đi. *Xem* field.

selective repeat ***(phát) lặp lựa chọn*** Trong truyền thông dữ liệu, một giao thức được sử dụng trong một hệ thống ống dẫn. Sau khi một khung (frame) dữ liệu bị hỏng tới đích, hoặc một khung không tới được đích, máy thu lưu giữ tất cả các khung đến sau vào bộ đệm cho đến khi khung bị hỏng hoặc bị mất được truyền lại và được nhận chính xác. Sau đó máy thu chuyển sang khung đã được truyền lại, sau đó là các khung trong bộ đệm và báo nhận khung được đánh số cao nhất. *Xem* frame.

selector channel ***kênh bộ chọn*** Trong truyền thông dữ liệu, một kênh được thiết kế để hoạt động chỉ với một thiết bị vào/ra tại một thời điểm bất kỳ. Sau khi lựa chọn thiết bị vào/ra, toàn bộ thông báo được truyền đi theo dạng byte tiếp byte. *Xem* byte.

self-banking ***ngân hàng tự hoạt động*** Trong hoạt động ngân hàng, việc sử dụng các máy trả tiền tự động, các máy phát tiền mặt và thiết bị đầu cuối truyền thông thông qua các khách riêng lẻ để thực hiện giao dịch ngân hàng. Thiết bị có thể được đặt tại một nhà băng, nơi làm việc... *So sánh với* home bank. *Xem* automatic teller machine, cash dispenser.

self-checking circuit ***mạch tự kiểm tra*** Trong độ tin cậy, một dạng dự phòng thừa phần cứng và thông tin

trong đó, các mạng có khả năng tự phát hiện các lỗi của chúng và phát hiện việc thiếu sự bảo vệ dự tính trước. *Xem* fail safe, hardware redundancy, information redundancy.

self-correcting code ***mã tự hiệu chỉnh*** *Đồng nghĩa với* error correction code.

self-synchronizing ***tự đồng bộ*** Trong mật mã, một thuộc tính của một mã pháp để khôi phục tự động sau khi một lỗi xuất hiện. Giả sử, một chuỗi bản rõ là đầu vào của hai thiết bị mật mã, chúng sẽ tạo ra đầu ra giống nhau khi các đầu vào giống nhau. Nếu một lỗi xảy ra trong quá trình mã hóa của một trong các thiết bị thì các đầu ra sẽ khác nhau, tuy nhiên, nếu quá trình là tự đồng bộ thì các đầu ra sẽ trở nên bằng nhau sau giai đoạn khôi phục nào đó. *Xem* block cipher chaining, stream cipher chaining. *Đồng nghĩa với* self-synchronous.

self-synchronous ***tự đồng bộ*** *Đồng nghĩa với* self-synchronizing.

semantics ***ngữ nghĩa học*** Sự nghiên cứu hoặc khoa học về mối quan hệ giữa các ký hiệu và ý nghĩa của chúng.

semiweak key ***khóa bán yếu*** Trong mật mã, một cặp khóa DES có thuộc tính là phép giải mã bằng một khóa của cặp tương ứng với phép mã hóa bằng khóa khác và ngược lại. Nói cách khác, nếu bản rõ được mã hóa với một khóa và bản mã kết quả được mã hóa bằng khóa thứ hai thì sẽ nhận được bản mã ban đầu. Các cặp khóa bán yếu đối với DES là:

01FE01FE01FE01FE and FE01FE01FE01FE01
1FE01FE00FE01FE1 and E01FE01FF10EF10E
01E001E001F101F1 and E001E001F101F101
1FFE1FFE0EFE0EFE and FE1FFE1FFE0EFE0E
011F011F010E010E and 1F011F010E010E01
E0FEE0FEF1FEF1FE and FEE0FEE0FEF1FEF1

So sánh với weak key. *Xem* DES.

sender ***thiết bị gửi; người gửi*** (1) Trong truyền dữ liệu, thiết bị gửi là một cài đặt thiết bị mã hóa một giá trị dữ liệu để truyền đi. *So sánh với* recipient. (2) Trong truyền dữ liệu, người gửi là một chủ thể ghi lên một kênh. *So sánh với* receiver. *Xem* channel, subject. (2) Trong truyền dữ liệu, người gửi là một người, tổ chức hoặc thực thể khác có trách nhiệm và có quyền khởi đầu một thông báo. Ở đây, khái niệm trách nhiệm, chẳng hạn, trách nhiệm tài chính, là quan trọng hơn hết. *So sánh với* receiver.

sender's correspondent bank ***ngân hàng đại lý của người gửi*** Trong hoạt động ngân hàng, một nhà băng cung cấp các quỹ nhân danh người gửi tới cho người nhận trực tiếp hoặc thông qua ngân hàng của người nhận. *Xem* receiver's correspondent bank.

sending bank ***ngân hàng gửi*** Trong hoạt động ngân hàng, một nhà băng mà đưa các thông báo vào trong một dịch vụ.

sensitive application ***ứng dụng nhạy cảm*** Trong an toàn dữ liệu, một ứng dụng của công nghệ thông tin đòi hỏi bảo vệ vì nó xử lý dữ liệu nhạy cảm, hoặc vì sự rủi ro và mức độ mất mát hoặc thiệt hại lớn (có thể do thao tác không đúng hoặc việc xử lý ứng dụng

có chủ ý).

sensitive business data ***dữ liệu kinh doanh nhạy cảm*** Trong an toàn dữ liệu, dữ liệu yêu cầu bảo vệ theo Tile 18, USC 1905, và dữ liệu khác mà theo bản chất, đòi hỏi việc phân phối hoặc truy nhập có kiểm soát vì các lý do không gì khác hơn là dữ liệu đã phân loại mật hoặc dữ liệu cá nhân. Nó được công nhận trong các loại sau đây:

(*a*) Chỉ dành cho các cơ quan chính thức - yêu cầu tính bảo mật của thông tin lấy từ một Tổng thanh tra, người có thẩm quyền hoặc từ hoạt động điều tra khác.

(*b*) Dữ liệu tài chính - yêu cầu bảo vệ để đảm bảo tính toàn vẹn của các quỹ hoặc các tài sản tài chính khác.

(*c*) Quản lý nhạy cảm - yêu cầu bảo vệ chống lại sự mất mát tài sản, tài liệu, hoặc kho dự trữ hoặc để bảo vệ chống lại việc làm gián đoạn các hoạt động hoặc thủ tục quản lý thông thường v.v.

(*d*) Tính độc quyền - yêu cầu bảo vệ dữ liệu hoặc thông tin tương hợp với các thỏa thuận về các quyền nhất định, hoặc chúng (dữ liệu và thông tin) là tài sản của doanh nghiệp hoặc cá nhân và được chính phủ mượn để đánh giá và sử dụng hợp lý trong phân xử các hợp đồng.

(*e*) Đặc quyền - yêu cầu bảo vệ thích ứng với các chuẩn thương mại hoặc theo yêu cầu của pháp luật. (Ví dụ, chính phủ mở rộng thông tin bao gồm quyết định của quan tòa đối với một hợp đồng).

So sánh với sensitive defense information, sensitive compartmented information. *Xem* sensitive data, sensitive information.

sensitive compartmented information ***thông tin chia ngăn nhạy cảm*** (1) Thông tin tình báo đòi hỏi các kiểm soát đặc biệt có chỉ rõ việc xử lý có giới hạn. (2) Tất cả thông tin và các tài liệu yêu cầu kiểm soát xã hội đặc biệt chỉ ra việc xử lý có giới hạn trong các chương trình thu thập tình báo và các sản phẩm cuối cùng của chúng trong hiện tại và tương lai. Những kiểm soát xã hội đặc biệt này là các hệ thống hình thức của truy nhập có giới hạn được thiết lập để bảo vệ các khía cạnh nhạy cảm của các nguồn tình báo cũng như các giải pháp và các thủ tục phân tích tình báo của các chương trình tình báo nước ngoài. Thuật ngữ này không bao gồm Dữ liệu được hạn chế như đã được định nghĩa trong mục II, Luật Công cộng số 585, Đạo luật về năng lượng nguyên tử năm 1954, được sửa đổi. *So sánh với* sensitive defense information, sensitive business data. *Xem* sensitive data, sensitive information.

sensitive data ***dữ liệu nhạy cảm*** (1) Trong an toàn dữ liệu, dữ liệu yêu cầu sự bảo vệ tránh rủi ro và mức độ nghiêm trọng của sự mất mát hoặc thiệt hại mà có thể là do sơ suất hoặc cố ý làm lộ, sửa đổi, hủy bỏ dữ liệu. Thuật ngữ bao gồm dữ liệu mà nếu sử dụng không đúng hoặc bị lộ có thể ảnh hưởng bất lợi tới khả năng hoàn thành một nhiệm vụ, nó gồm cả dữ liệu độc quyền, các bản ghi về các cá nhân đòi hỏi bảo vệ theo Đạo luật về tính riêng tư, và dữ liệu không được tiết lộ theo Luật Tự do Thông tin. (2) Trong an toàn dữ liệu, dữ liệu mà theo các cơ quan

có đủ thẩm quyền thì phải được bảo vệ bởi vì sự tiết lộ, sửa đổi, mất mát hoặc hủy bỏ trái phép sẽ gây ra thiệt hại cho cá nhân hoặc cái gì đó có thể nhận thấy được. *Xem* sensitive business data, sensitive defense information, sensitive compartmented information, sensitive information, sensitivity.

sensitive defense information ***thông tin quốc phòng nhạy cảm*** Trong an toàn dữ liệu, thông tin bất kỳ nào mà đòi hỏi một mức độ bảo vệ và nó không nên có hiệu lực thông thường. Kiểu thông tin này bao gồm (nhưng không giới hạn), thông tin được bảo vệ an toàn để:

(*a*) Ngăn chặn thiệt hại cho phòng thủ quốc gia và thường bắt buộc có sự phân loại an toàn.

(*b*) Đảm bảo sự riêng tư cá nhân của các công dân Mỹ theo đạo luật về tính riêng tư năm 1974.

(*c*) Duy trì sự bí mật cho thông tin FOUO có nguồn gốc từ Tổng thanh tra, một tài liệu kiểm toán, hoặc các hoạt động điều tra khác như thông tin về y học hoặc luật pháp, hoặc các thông tin mang tính nguyên tắc có nguồn gốc từ các hồ sơ của bác sỹ/bệnh nhân hoặc từ các mối quan hệ luật sư/khách hàng.

(*d*) Bảo vệ các quỹ, nguồn cung cấp, hoặc tài liệu khỏi bị đánh cắp, gian lận, biển thủ, hoặc lạm dụng. Điều này bao gồm tài sản hoặc nguồn tài nguyên hoặc các hệ thống hoặc các hoạt động được tính đến trong kiểm soát và phân phối các quỹ hoặc quá trình xử lý thông tin, tạo ra cơ hội làm trệch hướng các nguồn tài nguyên có giá trị kinh tế.

(*e*) Bảo vệ thông tin thuộc quyền sở hữu, nó là các tài sản riêng biệt của cá nhân hoặc doanh nghiệp. Thông tin thuộc quyền sở hữu này có thể cho Chính phủ mượn, thuê, hoặc mua hoặc cung cấp cho Chính phủ để sử dụng thích hợp chúng, bao gồm các đánh giá hoặc phân xử hợp đồng.

(*f*) Bảo vệ thông tin đặc quyền do Chính phủ phát triển, gồm cả việc phạt các hợp đồng.

(*g*) Bảo vệ thông tin mà các nhà lãnh đạo coi là yếu tố cần thiết để hoàn thành nhiệm vụ.

So sánh với sensitive business data, sensitive compartmented information. *Xem* FOUO, proprietary data, sensitive data, sensitive information.

sensitive information ***thông tin nhạy cảm*** (1) Trong an toàn dữ liệu, thông tin được chứa đựng trong Danh sách các Công nghệ Quân sự quan trọng, là những thông tin mà có thể hữu ích cho kẻ địch trong việc mở rộng các biện pháp đối phó, là những thông tin mà bao gồm các công nghệ mới và công nghệ cao, là những thông tin mà có thể liên quan tới các chỉ báo chính về các khả năng hoạt động, nó có thể bị kẻ địch sử dụng để xác định các khả năng hoạt động, các điểm yếu, các nhiệm vụ trong thời chiến. *Xem* military critical technology. (2) Trong an toàn dữ liệu, là những thông tin mà theo các cơ quan có thẩm quyền, phải được bảo vệ vì việc làm lộ, sửa đổi, mất mát hoặc hủy bỏ trái phép ít nhất sẽ gây ra thiệt hại cho cá nhân hoặc sự việc nào đó có thể nhận thấy được. (3) Trong an toàn dữ liệu, thông tin bất kỳ, nó yêu cầu một mức độ bảo vệ nào đó và nó không nên

có hiệu lực chung. *Xem* sensitive defense information, sensitive business data, sensitive compartmented information, sensitive data. (4) Trong luật pháp, thông tin mà nếu bị mất, bị lạm dụng, bị truy nhập hoặc sửa đổi không được phép có thể gây ảnh hưởng bất lợi tới sự riêng tư của cá nhân và vi phạm Đạo luật về tính riêng tư của Mỹ. *Xem* data protection, data protection - USA, privacy protection.

sensitive software ***phần mềm nhạy cảm*** Trong an toàn máy tính, phần mềm xử lý dữ liệu bất kỳ mà có thể bỏ qua, thâm nhập, hoặc làm hỏng các kiểm soát an toàn xử lý dữ liệu.

sensitive statistic ***thống kê nhạy cảm*** Trong an toàn cơ sở dữ liệu, một thống kê từ một cơ sở dữ liệu thống kê có thể được sử dụng để khám phá thông tin về một cá nhân. *Xem* inference control, n-respondent, k%-dominance, statistical database.

sensitive systems ***(các) hệ thống nhạy cảm*** Trong an toàn máy tính, một hệ thống xử lý dữ liệu nhạy cảm hoặc thực hiện một chức năng nhạy cảm. Các loại hệ thống nhạy cảm, theo độ nhạy cảm tăng dần được liệt kê dưới đây:

- Các ứng dụng hỗ trợ xử lý chung, ví dụ, các tính toán kỹ thuật được sử dụng trong thiết kế máy bay.
- Việc chi trả, tính toán các quỹ, các hệ thống quản lý tài sản có thể dùng để chi trả, ví dụ, bảng lương.
- Các hệ thống thông tin mục đích chung, ví dụ, các hệ thống quản lý dữ liệu chung.
- Các hệ thống ra quyết định tự động, ví dụ các hệ thống giải ngân và kế toán hoàn toàn tự động.
- Các hệ thống kiểm soát thời gian thực, ví dụ, kiểm soát không lưu.
- Các hệ thống ảnh hưởng đến an toàn quốc gia hoặc xã hội, ví dụ, chuyển nhượng các quỹ điện tử tích hợp.

sensitivity ***tính nhạy cảm; độ nhạy*** (1) Trong an toàn dữ liệu, đặc tính của một tài nguyên, bao hàm các giá trị hoặc tầm quan trọng của nó, và có thể cả tính dễ bị tấn công của nó. *Xem* vulnerability. (2) Trong an toàn máy tính, đặc tính của một tài nguyên mà chứa các giá trị hoặc tầm quan trọng của nó, và cả tính dễ bị tấn công của nó trước các đe doạ mang tính ngẫu nhiên hoặc chủ tâm. *Xem* accidental threat, deliberate threat, sensitive systems.

sensitivity and criticality ***tính nhạy cảm và mức nguy cấp*** Trong an toàn máy tính, một phương pháp được phát triển để định rõ giá trị của hệ thống thông tin bằng cách tính đến chi phí, khả năng, và nguy cơ đối với các hoàn thành nhiệm vụ hoặc sinh mạng gắn kết với hệ thống.

sensitivity assessment ***đánh giá mức nhạy cảm*** Trong an toàn máy tính, sự nghiên cứu dữ liệu để quyết định mức bảo vệ cần thiết.

sensitivity label ***nhãn nhạy cảm*** (1) Trong an toàn dữ liệu, một mức an toàn liên quan tới một đối tượng. *Xem* object, security level. (2) Trong an toàn máy tính, một thông tin đại diện cho một mức an toàn của một đối tượng và

nó mô tả tính nhạy cảm (ví dụ, mức phân loại) của dữ liệu trên đối tượng. Các nhãn nhạy cảm được sử dụng bởi TCB làm cơ sở cho các quyết định kiểm soát truy nhập bắt buộc. *Xem* mandatory access control, object, TCB. *Đồng nghĩa với* security label.

Sentinel ***virut Sentinel*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COMMAND.COM, COM, EXE, và các tệp OVL, làm hỏng liên kết tệp, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu. *Xem* virus names.

separate and mediate ***(nguyên tắc) tách bạch và dàn xếp*** · Trong an toàn máy tính, một nguyên tắc để xây dựng các hệ thống an toàn trong đó, các thực thể của các mức phân loại an toàn khác nhau được tách rời nhau, trừ khi thực hiện các hoạt động điều hành mà yêu cầu truy nhập vào các thực thể từ hai mức trở lên. Các truy nhập như vậy phải được thực hiện thông qua các bộ giám sát tham chiếu tin cậy, đảm bảo tuân theo chính sách an toàn bắt buộc bên ngoài nào đó. *Xem* reference monitor concept.

separation of duties or functions ***tách bạch nhiệm vụ hoặc chức năng*** Trong an toàn thủ tục, việc xây dựng các công việc liên quan đến hệ thống sao cho mỗi công việc mà khả năng bị lộ bí mật an toàn phải ở mức đủ nhỏ để có thể hoạt động có hiệu quả. Đối với việc thực hiện các nhiệm vụ có tính nguy cấp, cần có sự can thiệp của nhiều hơn một người. Nói chung, phải giảm thiểu cơ hội của một người bất kỳ đối với việc phá hoại hoặc gây thiệt hại cho hệ thống. *Xem* computer fraud control, dual control, split knowledge.

separation of privilege ***tách bạch đặc quyền*** Trong an toàn máy tính, nguyên tắc của việc phân chia đặc quyền, là một trong số các nguyên tắc của các hệ thống an toàn. *Xem* principle of secure systems, separation of duties and functions.

sequential card reader ***bộ đọc thẻ tuần tự*** Trong an toàn vật lý, một thiết bị đọc thẻ để kiểm soát truy nhập, có bàn phím nhỏ đi kèm, vốn đòi hỏi cả thẻ truy nhập được phép lẫn việc đưa vào một chuỗi vùng phím được mã hóa trước khi được quyền nhập vào hoặc thoát ra. *Xem* card reader.

sequential switcher ***thiết bị chuyển hướng tuần tự*** Trong an toàn vật lý, một thiết bị chuyển hướng video để lựa chọn các cảnh của máy quay phim và những lần dừng lại theo một trình tự được lập trình trước. *Xem* dwell time, homing sequential switcher, video switcher.

serial communication ***truyền thông tuần tự*** *Xem* serial transmission.

serial computer ***máy tính nối tiếp, máy tính tuần tự*** Trong tính toán, một máy tính trong đó các biến cố xảy ra một cách tuần tự mà có ít hoặc không có sự cung cấp đồng thời hoặc chồng chéo. *So sánh với* parallel computer.

serial interface ***mạch ghép nối nối tiếp, giao diện nối tiếp*** Trong truyền dữ liệu, một mạch ghép nối, ví dụ giữa một DTE và một modem, chỉ có

thể chuyển dữ liệu theo dạng nối tiếp. *Xem* DTE, MODEM, RS-232C. *Xem* serial transmission.

serial transmission ***(sự) truyền tuần tự*** Trong truyền dữ liệu, một giải pháp truyền thông tin trong đó mỗi bit của một ký tự được gửi đi tuần tự. *So sánh với* parallel transmission.

server ***secvơ, trạm dịch vụ, máy (tính) chủ*** Trong tính toán, một khối tại một nút của mạng cung cấp một dịch vụ cụ thể cho người sử dụng mạng, ví dụ, một trạm dịch vụ máy in cung cấp các thiết bị in, một trạm dịch vụ tệp lưu giữ các tệp của người sử dụng. *Xem* communication server, disk server, file server.

service bureau ***văn phòng dịch vụ*** Trong tính toán, một tổ chức cung cấp các dịch vụ tính toán hoặc xử lý dữ liệu cho các cá nhân hoặc các tổ chức khác.

service data unit ***đơn vị dữ liệu dịch vụ*** Trong truyền dữ liệu, thông tin được chuyển từ một tầng sang tầng tương ứng của nó trong mô hình tham chiếu để kết nối các hệ thống mở. Thông tin điều khiển được thêm vào đơn vị dữ liệu dịch vụ, tạo thành một đơn vị dữ liệu giao tiếp, khi nó được chuyển từ tầng *N* sang tầng *N* - 1. *So sánh với* protocol data unit, interface data unit. *Xem* open systems interconnection.

service machine ***máy dịch vụ*** *Đồng nghĩa với* internal subject.

service message ***thông báo dịch vụ*** Trong truyền dữ liệu, một thông báo, chuyển giữa 2 điểm thiết bị đầu cuối, chứa hoặc tìm kiếm thông tin liên quan đến các thông báo khác. *Xem* cryptographic service message.

service provider ***nơi cung cấp dịch vụ*** Trong truyền dữ liệu, một thuật ngữ được sử dụng trong mô hình tham chiếu kết nối các hệ thống mở. Tầng *N* là nơi cung cấp dịch vụ cho tầng *N* + 1. *So sánh với* service user. *Xem* open systems interconnection.

service type ***kiểu dịch vụ*** *Đồng nghĩa với* facility type.

service user ***người dùng dịch vụ*** Trong truyền dữ liệu, một thuật ngữ được sử dụng trong mô hình tham chiếu kết nối các hệ thống mở. Tầng *N* + 1 là người sử dụng dịch vụ của dịch vụ do tầng *N* cung cấp. *So sánh với* service provider. *Xem* open systems interconnection.

session ***phiên (làm việc)*** Trong tính toán, một hoạt động trọng một khoảng thời gian; hoạt động là sự truy nhập của người sử dụng tới tài nguyên của máy tính/mạng; một khoảng thời gian được giới hạn từ lúc bắt đầu phiên làm việc (một dạng đăng nhập) và kết thúc phiên làm việc (dạng ra khỏi mạng).

session key ***khóa phiên*** Trong quản lý khóa, một khóa mật mã chỉ được sử dụng trong một khoảng thời gian nhất định, ví dụ, một phiên làm việc của người sử dụng tại một thiết bị đầu cuối, và sau đó bị loại bỏ. Các khóa phiên là các khóa ở mức thấp nhất trong hệ thống phân cấp khóa và không được sử dụng làm khóa mã hóa các khóa. *So sánh với* transaction key. *Xem*

S

key-encrypting key.

session layer ***tầng phiên*** Trong truyền dữ liệu, một tầng trong mô hình tham chiếu cho kết nối các hệ thống mở ISO. Tầng này cho phép hai nhóm liên lạc thiết lập các phiên. Nó có thể cung cấp một loạt các dịch vụ, điều chỉnh các luồng giữa các quá trình truyền thông mà tại một thời điểm, chỉ có thể truyền dữ liệu theo một hướng, cung cấp sự quản lý thẻ cho các hoạt động tới hạn mà không thể được đảm trách cùng lúc bằng cách chèn các điểm kiểm tra vào các dòng dữ liệu sao cho các hoạt động có thể được bắt đầu lại từ các điểm trung gian trong trường hợp không liên lạc được v.v.. *So sánh với* application layer, data link layer, network layer, physical layer, presentation layer, token management, transport layer. *Xem* host, open systems interconnection.

session security level ***mức an toàn phiên*** Trong an toàn máy tính, một mốc an toàn thấp trong các mức an toàn của người sử dụng, của thiết bị đầu cuối và là một mức được người sử dụng và hệ thống mà phiên được bắt đầu từ đó xác định. *Xem* low water mark, security level.

set ***phép gán; tập hợp*** (1) Trong toán học, phép gán là phép tính trên một bit theo số học nhị phân, để chỉnh giá trị của nó đến 1. *Xem* bit. (2) Trong toán học, tập hợp là tập các phần tử có một thuộc tính chung.

settlement ***thanh toán*** Trong hoạt động ngân hàng, việc chuyển nhượng các quỹ để hoàn thành một hoặc nhiều các giao dịch ưu tiên mà phải tuân theo thanh toán cuối cùng.

shadow ***đoạn khóa*** Trong quản lý khóa, một đoạn của một khóa được sử dụng trong kỹ thuật ngưỡng. *Xem* threshold.

Shake ***virut Shake*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL. *Xem* virus names.

Shannon ***shanon, sanon*** *Xem* information content.

Shannon's five criteria ***năm tiêu chí Shannon, năm chuẩn cứ Shannon*** Trong mật mã, các gợi ý về các tiêu chuẩn của các hệ thống an toàn do Shannon đưa ra năm vào 1940:

- mức độ bí mật được đưa ra;
- kích cỡ của khóa;
- các thao tác mã hóa và giải mã đơn giản;
- sự lan truyền các lỗi;
- sự mở rộng của thông báo.

Xem error propagation, information theory.

Shannon's Law ***định luật Shannon*** Trong truyền thông, một luật quy định một thước đo dung lượng của một đường truyền xét về mặt độ rộng dải thông và tỷ số tín trên tạp của nó. Theo định luật này, mức độ truyền tối đa tính theo bit/giây được cho như sau: $W\log_2(1 + SN)$ sao cho W = độ rộng dải thông, còn SN = tỷ số tín trên tạp. *Xem* bandwidth, signal to noise ratio.

shareware ***phần mềm cổ đông, phần***

mềm tự nguyện Trong phần mềm, các chương trình đã được đăng ký quyền tác giả và được phát hành với một yêu cầu rằng, nhà cung cấp sẽ được hưởng một phần nếu các chương trình này tỏ ra có giá trị đối với người sử dụng. Nhà cung cấp cũng có thể cung cấp một phiên bản hoặc một hướng dẫn tốt hơn khi nhận được phí giấy phép hoạt động. *Xem* bulletin broad.

sharp eyed cashier ***thủ quỹ ranh ma, thủ quỹ không trung thực*** Trong hoạt động ngân hàng, nói tới các thủ quỹ không trung thực, người sử dụng kiến thức của mình và/hoặc các chức vụ để lấy được thông tin để gian lận. Ví dụ, quan sát và ghi nhớ nhập các PIN của khách hàng. *Xem* PIN.

shell site ***vị trí có phòng máy, điểm có phòng máy*** *Đồng nghĩa với* cold site.

shielded cable ***cáp bọc, cáp chắn*** Trong truyền thông, một dây dẫn điện bên trong được bao bọc bởi các dây tết kim loại tiếp đất bên ngoài để bảo vệ các tín hiệu khỏi bị nhiễu. *Xem* coaxial, interference, cable.

shielding effectiveness ***hiệu quả che chắn*** Trong điện tử học, số đo theo dexiben về mức hấp thụ của vỏ chắn dẫn điện. Các thiết bị tính toán của Mỹ phải tuân theo các quy định phát xạ của FCC, và các chất dẻo dẫn điện đặc biệt được sử dụng cho mục đích này. *Xem* coductive shielding, decibel, Tempest proofing.

shift ***(phép) dịch*** Trong mật mã, chênh lệch về vị trí thứ tự abc giữa ký tự của bản rõ, trong mã pháp tịnh tiến, và ký tự tương ứng của bản mã. *Xem* translation cipher.

shift code ***mã dịch*** Trong các mã, một giải pháp làm tăng số lượng ký tự mà có thể được đi kèm với một số bit cho trước. Nếu dùng một mã 6 bit thì có thể phân 64 ký tự. Tuy nhiên, nếu 2 trong các ký tự này được quy định là "dịch" và "không dịch' thì chúng có thể tạo ra tác động dịch đến hoặc từ một bộ ký tự thay thế gồm tới 124 ký tự.

shift factor ***hệ số dịch chuyển*** Trong an toàn truyền thông, khoảng dịch trung bình của các đoạn trong một hoán vị cho trước khi dùng các bộ xáo trộn các phần từ thời gian để xáo trộn tiếng nói. *Xem* time element scrambler, voice scrambling.

shift register ***thanh ghi dịch*** Trong phần cứng, một thanh ghi được thiết kế để dịch chuyển dữ liệu sang phải hoặc trái. *Xem* register.

shouldering ***nhìn lén qua vai, liếc trộm qua vai*** *Đồng nghĩa với* shouder surfing.

shoulder surfing ***liếc trộm qua vai*** Trong an toàn máy tính, một giải pháp để thu được thông tin từ các mật khẩu, các thủ tục đăng nhập v.v. của người sử dụng. Ví dụ, bằng cách liếc trộm qua vai của người sử dụng thiết bị đầu cuối.

shrink-wrapped license ***giấy phép bọc ni lông, hợp đồng gói gọn*** Trong tính toán, một hợp đồng được cung cấp bởi công ty phần mềm, có thể nhìn xuyên qua một vỏ bọc trong suốt bao quanh hộp các đĩa và tài liệu. Hợp đồng

này sẽ quy định các điều kiện mà phần mềm có thể được sử dụng và được coi là có hiệu lực một khi vỏ bọc bị xé ra. Giá trị của kỹ thuật này không rõ ràng ở hầu hết các quốc gia. *Xem* software house. *Đồng nghĩa với* hat box, tear-me-open.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

sieve of Eratosthenes: *sàng Eratosthenes*. Sàng này được xắp xếp thành 6 cột (modulo 6), thì chỉ cột đầu tiên và cột thứ 5 chứa các số nguyên tố bởi vì các số trong cột thứ 3 có thể chia được cho 3 và các số trong các cột khác thì có thể chia được cho 2.

SIC ***bộ mã SIC, bộ mã chuẩn công nghiệp*** Trong hoạt động ngân hàng, tên viết tắt của Standard Industry Codes, do Ngân hàng nước Anh phát triển.

sieve of Eratosthenes ***sàng Eratosthenes*** Trong toán học, một phương pháp tìm kiếm các số nguyên tố với một giá trị thấp hơn một số nguyên xác định. Bộ các số nguyên đầy đủ lên tới giá trị xác định được ghi. Cứ đến phần tử thứ 2 sau 2 bị xóa đi, sau đó mỗi số thứ ba sau 3 cũng bị xóa tương tự (nếu nó chưa bị xóa đi). Quá trình như vậy được lặp lại cho mỗi số thứ 5 sau 5... Các số còn lại tại cuối quá trình là các số nguyên tố. *Xem* prime number.

signal ***tín hiệu*** (1) Một hiện tượng vật lý biến đổi theo thời gian có chủ ý để truyền đạt thông tin. (2) Sự thể hiện vật lý của một thông báo. (3) Một thông báo ngắn, như trong một tín hiệu điều khiển.

signal element ***phần tử tín hiệu*** Trong truyền dữ liệu, một đơn vị cơ bản mà nhờ nó dữ liệu được truyền đi theo một kênh. Mỗi đơn vị là một trạng thái hoặc điều kiện của một kênh biểu diễn cho một hoặc nhiều bit của thông tin số. Một đơn vị có thể là một xung DC, hoặc một tín hiệu AC của một biên độ, pha, hoặc tần số nhất định, nó được nhận dạng và được dịch lại nhờ thiết bị thu.

signalling ***báo hiệu*** Trong truyền thông, việc chuyển các chữ số và các lệnh thiết lập/xóa cuộc gọi giữa máy

điện thoại và đài trung tâm, hoặc tổng đài, hoặc giữa đài trung tâm này và đài trung tâm khác. *Xem* central office.

signal quality detector ***dò chất lượng tín hiệu*** Trong truyền dữ liệu, một tín hiệu do các modem đồng bộ cung cấp, chỉ ra có hoặc không có khả năng xảy ra lỗi cao trong dữ liệu nhận được. *Xem* synchronous modem, RS-232C.

signal to noise ratio ***tỷ số tín trên tạp, tỷ số s/n*** Trong truyền dữ liệu, tỷ số giữa nguồn tín hiệu được yêu cầu và nguồn tín hiệu không mong muốn. *Xem* noise.

signature ***chữ ký (số)*** *Xem* digital signature.

signature analysis ***phân tích chữ ký*** Trong kiểm soát truy nhập, một kỹ thuật sinh trắc dựa vào các phân tích đối với một chữ ký hoặc cách mà nó được ghi. Nhận biết các chữ ký bằng máy là một lĩnh vực nghiên cứu tích cực từ những năm 1970. Các chữ ký mẫu có thể được lưu giữ lên tới 100 byte, các tỷ lệ chấp nhận/loại bỏ sai bằng 1% được báo lại.

Khi cho trước tính chất có thể thay đổi được của các chữ ký được ghi, một số hệ thống cập nhật mẫu được lưu giữ mà tương ứng với mẫu nhập thành công cuối cùng. Việc sử dụng các mẫu được lưu giữ của các mẫu được ghi của một chữ ký, và các vấn đề liên quan trong việc phát triển các mức chấp nhận được của các lỗi loại 1 và lỗi loại 2, khi chữ ký thật có thể thay đổi đáng kể, sẽ làm cho các hệ thống như vậy dễ bị tổn thương trước kẻ giả mạo có trình độ vừa phải.

Một hình thức kiểm tra chữ ký an toàn hơn được dựa vào việc tạo ra chữ ký động. Các hệ thống động này có thể đo thời gian hoàn tất các phần của chữ ký, những sự khác nhau trong khi ấn bút trong suốt quá trình tạo ra chữ ký, tốc độ của bút v.v.. Nếu lấy được các đặc tính của người sử dụng trong việc tạo ra chữ ký, thì một kẻ làm giả sẽ yêu cầu nhiều thông tin hơn nhiều so với việc sao đơn thuần chữ ký đã ghi.

Nhiều công nghệ khác nhau để đo đặc trưng động chữ ký đã được thử nghiệm và đưa ra. Một hệ thống của Phòng thí nghiệm Vật lý Quốc gia của Anh đã lấy mẫu vị trí sử dụng bút, khi sử dụng một bộ số hóa dựa vào các màng áp lực. Viện nghiên cứu Stanford (SRI) đã sử dụng một bút bi với một máy đo sức căng để đo lực kéo lê theo hướng X và Y và áp lực theo hướng Z. SRI cũng phát triển một trục cuốn giấy để đo dữ liệu như vậy với bút bất kỳ. IBM đã tạo ra một thiết bị có các dụng cụ đo gia tốc được gắn vào bút. Viện Battelle Memorial đã đo vận tốc của bút bằng cách sử dụng một đầu từ và một loạt các cuộn dây thứ cấp được cấp điện. Mới đây nhất, Ngân hàng Midland đã thử nghiệm một hệ thống do Công ty Thương mại trách nhiệm hữu hạn Roll-Royce phát triển, nó giám sát âm thanh phát ra từ một bút như khi nó được viết.

Việc loại bỏ sai của các thiết bị như vậy có thể được những người sử dụng riêng lẻ dự liệu khi nhập vào chữ ký của họ và nhận được các lỗi loại 1 cỡ 1%. Tuy nhiên, việc đo các lỗi loại 2 lại

đưa ra vấn đề có độ phức tạp nào đó. Rõ ràng là khó khăn nằm trong sự phát triển một số lớn các thử nghiệm thống kê, phủ khắp những kẻ giả mạo có trình độ khác nhau. Những yếu tố ảnh hưởng tới tỷ lệ chấp nhận sai sẽ gồm: độ dài của chữ ký, trình độ của kẻ giả mạo, phương tiện nghiên cứu việc tạo ra tính động của chữ ký, sự huấn luyện người dùng hợp thức, phương tiện thực nghiệm.

Dạng thử nghiệm lỗi loại 2 cơ bản nhất đơn giản chỉ là cho mỗi chữ ký vào tệp được lưu dựa vào tất cả các chữ ký khác và thử nghiệm số lần chấp nhận sai. Các cuộc thử nghiệm tinh vi hơn đã được giúp đỡ, ít nhất là cho những người không chuyên, bởi những người giả mạo tiến hành những nỗ lực tốt nhất của họ để đánh lừa hệ thống. Ví dụ, IBM đã ghi lại vào năm 1983 những cuộc thử với gồm 2133 lần giả mạo và một tỷ lệ chấp nhận sai thấp cỡ 0,28 %. Sự nhận dạng tự động các chữ ký được gửi gắm nhiều vào khả năng chấp nhận của người dùng, có một số ít người sẽ nhận thấy một phương pháp như vậy có những vấn đề về vật lý hoặc không chấp nhận về mặt xã hội. Với những biện pháp dự phòng hợp lý, kẻ tấn công gặp những vấn đề nghiêm trọng và người dùng có thể thay đổi chữ ký đã lưu của mình nếu họ có lý do tin rằng, dạng số hóa đã bị tổn thương. *Xem* biometrics, Type 1 error, Type 2 error.

signature construction ***xây dựng chữ ký*** Trong mật mã, một phép biến đổi mật mã dữ liệu để đảm bảo xác thực dữ liệu ban đầu. *So sánh với* signature decontruction. *Xem* data origin authentication, digital signature.

signature deconstruction ***phá chữ ký*** Trong mật mã, quá trình đảo ngược quá trình xây dựng chữ ký để đưa ra dữ liệu, từ đó có khả năng quyết định chữ ký nào hợp lệ hoặc không hợp lệ. *So sánh với* signature contruction. *Xem* digital signature.

signature service ***dịch vụ chữ ký*** Trong an toàn dữ liệu, một dịch vụ bảo vệ chống từ chối và giả mạo. *Xem* digital signature, forgery, repudiation.

significant modification ***thay đổi quan trọng*** Trong an toàn máy tính, sự thay đổi thiết bị hoặc hệ thống mà tác động tới sự hoạt động hoặc ảnh hưởng đến các biện pháp an toàn của hệ thống. Việc định rõ ảnh hưởng là sự đánh giá một cách chủ quan và phụ thuộc vào môi trường mà hệ thống hoạt động.

sign in ***khởi nhập*** *Đồng nghĩa với* log in.

sign on ***khởi nhập*** *Đồng nghĩa với* log on.

simple mail transfer protocol ***giao thức chuyển thư đơn giản*** Trong truyền dữ liệu, giao thức thư tín điện tử được phát triển đầu tiên cho mạng ARPANET. *Xem* ARPANET, electronic mail, X.400.

simple security property ***tính an toàn đơn*** Trong an toàn máy tính, một nguyên tắc của mô hình an toàn Bell-La Padula cho phép một chủ thể truy nhập đọc vào đối tượng chỉ khi mức an toàn của chủ thể trội hơn mức an toàn của đối tượng. *Xem* Bell-la

Padula model, dominate, object, read access, security level, subject.

simplex ***đơn công*** Trong truyền thông, nói tới quá trình liên lạc chỉ theo một chiều. *So sánh với* duplex, half duplex.

simplicity ***tính đơn giản*** Trong an toàn máy tính, nguyên tắc tính đơn giản, một trong các nguyên tắc của các hệ thống bí mật, phát biểu rằng, sự đúng đắn của các biện pháp an toàn, được kết hợp với phần cứng và phần mềm, có thể được kiểm tra dễ dàng hơn nếu các biện pháp an toàn này đơn giản và gọn nhỏ. *Xem* principles of secure system.

simulation ***(sự) mô phỏng, (sự) bắt chước*** Trong an toàn máy tính, việc sao chép một quá trình máy tính để quen thuộc với nó để sửa đổi được nó.

simultaneous transmission ***truyền đồng thời*** Trong truyền dữ liệu, một kỹ thuật để truyền các ký tự điều khiển, hoặc dữ liệu, theo một hướng trong khi các thông báo lại được nhận theo hướng khác. *Xem* duplex.

single address message ***thông báo đến địa chỉ duy nhất*** Trong truyền dữ liệu, một thông báo chỉ được phân phối cho một đích.

single-level device ***thiết bị một mức*** Trong an toàn máy tính, thiết bị được sử dụng để xử lý dữ liệu có mức độ an toàn đơn tại bất cứ thời điểm nào. Vì thiết bị này không cần tin cậy để tách dữ liệu ở các mức an toàn khác nhau, nên không phải lưu các nhãn nhạy cảm với các dữ liệu đang được xử lý. *So sánh với* multilevel device. *Xem* security level, sensitivity label.

single point of failure ***điểm sự cố quan trọng*** Trong tính toán, phần bất kỳ của một hệ thống có tính sống còn với hoạt động của nó và là phần mà một hỏng hóc sẽ dẫn tới hỏng hóc trong toàn bộ hệ thống vì không thể bỏ qua nó được. Các hệ thống phải được thiết kế với độ dư thừa (dự phòng) thích hợp để tránh tình trạng này.

single stroke bell ***chuông một tiếng*** Trong an toàn vật lý, một thiết bị cảnh báo mà chỉ rung một tiếng chuông mỗi khi năng lượng hoạt động được cung cấp. *So sánh với* vibrating bell.

single supervised system ***hệ thống giám sát đơn*** Trong an toàn vật lý, một hệ thống trong đó nguồn năng lượng cho tín hiệu báo hỏng hóc không được giám sát. *Xem* trouble signal.

single voiding card reader ***bộ đọc thẻ có khả năng loại bỏ*** Trong kiểm soát truy nhập, một thiết bị đọc thẻ được dùng để kiểm soát truy nhập trong đó có thể khử bỏ một hoặc nhiều mã kiểm soát truy nhập khỏi hệ thống. *Xem* card reader.

sink ***nơi gom (dữ liệu)*** *Đồng nghĩa với* data sink.

sink tree ***cây gom, cây góp*** Trong truyền dữ liệu, tập hợp của tất cả các nhánh đi tới một đích trong mạng truyền thông, khi sử dụng bảng định tuyến cố định. *Xem* routing table.

SIOP-ESI ***chương trình SIOP-ESI*** Viết tắt của Single Integrated Operational Plan-Extremely Sensitive Information (Kế hoạch hoạt động kết

hợp đơn lẻ - Thông tin rất nhạy cảm); một chương trình của Bộ quốc phòng Hoa Kỳ. *Xem* special access program.

SITA high level network ***mạng SITA mức cao*** Trong truyền dữ liệu, cụm từ viết tắt của Société Internationale de Télécommunications Aéronautique (Hiệp hội viễn thông hàng không quốc tế), một mạng phục vụ cho hàng không với tổ hợp của các thiết bị chuyển mạch gói và thông báo. *Xem* packet switching, message switching.

site polling ***hỏi vòng vị trí*** Trong truyền dữ liệu, một kỹ thuật trong đó tất cả các thiết bị đầu cuối đặt tại một vị trí cho trước được hỏi vòng như một nhóm, với một bộ điều khiển cục bộ hoạt động như một bộ giám sát dành cho mục đích này. *Xem* polling.

Skism ***virut Skism*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COM, EXE, và OVL, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng các tệp chương trình, OVL. *Xem* virus names.

slave ***hệ thụ động*** Trong các mạng máy tính, một hệ thống hoặc thiết bị đầu cuối từ xa trong đó các chức năng được điều khiển bởi một hệ thống trung tâm chính.

slice network ***mạng cắt lát, mạng phiến*** Trong truyền dữ liệu, một mođun độc lập, có khả năng được đặt ở nhiều vị trí nếu cần hoặc khi thuận tiện mà trong trường hợp bị tách khỏi phần còn lại của hệ thống, sẽ tiếp tục hoạt động độc lập. Các mođun như vậy sẽ tiếp tục xử lý các chức năng một cách bình thường, được điều khiển bởi các trung tâm điều hành tập trung.

sliding window protocol ***giao thức cửa sổ trượt*** Trong truyền dữ liệu, một dạng sửa đổi của giao thức dừng và đợi. Máy chủ gửi được phép có nhiều khung không được báo nhận tồn tại cùng lúc. Các khung liên tiếp được cho các số hiệu dãy (số thứ tự) thuộc một phạm vi cho trước với các số được tái sử dụng để ngăn chặn chúng mở rộng không có giới hạn. Máy chủ gửi duy trì một bản ghi chứa các khung không được báo nhận và truyền lại chúng sau một khoảng thời gian chờ (tạm ngừng) xác định, hoặc nhận các khung tín hiệu báo phủ nhận từ máy thu, một giới hạn trên số cho phép tối đa các khung không được báo nhận sẽ đảm bảo kiểm soát lưu lượng. *So sánh với* stop and wait protocol. *Xem* frame, negative acknowledgement.

sliding window system ***hệ thống cửa sổ trượt*** Trong an toàn truyền thông, một giải pháp làm giảm trễ thời gian đi kèm với các bộ xáo trộn (tiếng nói) theo các phần tử thời gian. Các hoán vị được lựa chọn sao cho việc dịch chuyển tối đa các đoạn bị giới hạn, vì vậy không cần thiết phải lưu giữ toàn bộ khung trước khi hoán vị tại máy thu và máy phát. *Xem* shift factor, time element scrambler, voice scrambling.

slotted ring ***vòng có khe*** *Xem* message slot.

Slow ***virut Slow*** Trong an toàn máy tính, một một loại virut mã hóa chính bản thân nó, kết thúc và thường trú, lây nhiễm các tệp COM, EXE và OVL, làm ảnh hưởng đến thao tác tại thời

điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu và liên kết tệp. *Xem* virus names.

smart card ***thẻ thông minh*** Trong kiểm soát truy nhập, một thẻ làm bằng chất dẻo có kích thước tương tự với một thẻ sọc từ mà có mạch logic điện tử trong trường hợp của thẻ có dữ liệu được lưu giữ, hoặc có một bộ vi xử lý cho các thẻ có các khả năng xử lý.

Các thẻ có dữ liệu được lưu giữ dự phòng để lưu giữ bí mật dữ liệu vì vậy không giống với thẻ vạch từ, nội dung của nó không thể sao chép được và cũng không sửa đổi được một cách trái phép. Thẻ có khả năng xử lý có một bộ vi xử lý được cài bổ sung thêm các khả năng lưu giữ dữ liệu. Bộ vi xử lý được điều khiển bởi một chương trình được lưu thường xuyên trong một ROM. Một số thẻ có khả năng tải mã xuống một EPROM. Bộ vi xử lý cho khả năng xử lý thông minh, nó cho phép thẻ nhập vào một hội thoại cố định với một máy chủ. Năng lực xử lý như vậy không thể chỉ nhận dạng người sử dụng với máy chủ, mà nó còn có thể cung cấp một bộ lưu giữ thẻ có cơ chế đòi hỏi/đáp ứng để xác thực máy chủ và như vậy ngăn chặn được các tấn công giả dạng.

Phát triển thẻ thông minh

Vào năm 1974, một sáng chế về thẻ làm bằng chất dẻo chứa các vi điện tử do nhà phát minh người Pháp, Roland Moreno đưa ra. Việc phát triển thẻ thông minh được tiếp tục và các giấy phép được cấp cho các công ty khác. Vào năm 1982, các cuộc thử nghiệm được tổ chức tại các thành phố của nước Pháp như Blois, Caen và Lyons để kiểm tra việc sử dụng các thẻ chi trả điện tử trong ba môi trường đặc trưng. Năm 1984, mạng Carte Bleue, một chi nhánh của hệ thống thẻ thị thực tại Pháp, và mạng Credit Agricole, với tổng số người lưu giữ thẻ là 10 triệu, thiết lập một hệ thống trên toàn quốc để thực hiện việc chi trả bằng các thẻ lai. Hãng French Telecom cũng thực hiện sử dụng thẻ điện thoại công cộng.

Các thẻ thông minh cũng được sử dụng để kiểm soát truy nhập. Lầu năm góc đã đưa ra một nghiên cứu giới thiệu một hệ thống ID thẻ thông minh cho các kho của các tổ chức Quốc phòng và trạm bán hàng cho Quân đội Mỹ trên toàn thế giới. Thẻ thông minh cũng có thể được sử dụng kết hợp với các hệ thống văn bản videо và các hệ thống ngân hàng trong nước. Dây chuyền bán lẻ tại Mỹ J C Penny đã có được hệ thống videotex của Ngân hàng Nhà nước, cho phép tiến hành các thử nghiệm với các thẻ thông minh trên mạng máy tính, kết hợp với các ngân hàng khác của Mỹ. Gần đây nhất, các thiết bị đọc thẻ thông minh được cài đặt trong các bộ giải mã TV.

Công nghệ thẻ thông minh

Hiện nay người ta sử dụng 2 loại thẻ thông minh chủ yếu:

- thẻ logic nối dây;
- một thẻ chứa một hoặc nhiều bộ vi xử lý.

Thẻ logic nối dây, ví dụ thẻ Flonic do Flonic-Schlumberger phát triển, bề ngoài tương tự như thẻ vạch từ và chứa một mạch điện được gói gọn trong bề dày của thẻ. Sơ đồ mạch cho phép lưu giữ bí mật và các khả năng thực hiện các

tính toán đơn giản. Như vậy, sự truy nhập vào dữ liệu được lưu giữ sẽ được kiểm soát và dữ liệu được lưu giữ có thể được cập nhật thông qua thiết bị đọc thẻ thích hợp.

Thẻ có chứa bộ vi xử lý thông thường, ví dụ CP8 do Cii Honeywell Bull phát triển, có một bộ vi xử lý 8 bit được cài đơn lẻ, bộ nhớ RAM, ROM, EPROM, hoặc EEPROM (bộ nhớ chỉ đọc xóa được bằng điện).

ROM chứa các chỉ lệnh được lưu giữ, và tất cả các truy nhập vào dữ liệu được lưu đều được bộ vi xử lý kiểm soát. Không có các biện pháp chặn dữ liệu bên ngoài, chảy trên bus của bộ vi xử lý, vì vậy đảm bảo an toàn cao. Cả bộ nhớ EPROM và EEPROM đều cung cấp khả năng chứa dữ liệu cố định. Công nghệ EEPROM cho phép ghi dữ liệu nhưng sau đó không xóa được. Tiếp sau đó, EEPROM lại cho phép xóa sau đó và vì vậy cho phép tái sử dụng không gian bộ nhớ bằng cách loại bỏ dữ liệu cũ. Một số thẻ thông minh có nhiều hơn một bộ vi xử lý.

Một loạt các thẻ thông minh có thể được phân loại như sau:

- các thẻ có bộ nhớ;
- các thẻ thông minh đơn giản;
- các thẻ thông minh;
- các thẻ siêu thông minh;
- các thẻ thông minh không tiếp xúc.

Các thẻ có bộ nhớ có thể có các khả năng lưu giữ trong khoảng từ 50KB tới 1Megabit dữ liệu trong RAM, EPROM hoặc EEPROM, có hoặc không có pin, nhưng không chứa bộ xử lý gắn trong. Về kích thước, chúng giống như những thẻ tín dụng nhưng thường dày hơn và cứng, vì vậy chúng dễ bị gãy nếu bị uốn cong.

Các thẻ thông minh đơn giản không có một bộ vi xử lý gắn bên trong nhưng sự truy nhập vào bộ nhớ trong (EPROM hoặc EEPROM) sẽ chịu sự bảo vệ vật lý, các cầu chì, hoặc bảo vệ logic được điều khiển bởi sơ đồ mạch. Những thẻ như vậy có cùng kích thước và độ dày như các thẻ tín dụng thông thường.

Các thẻ thông minh chứa một bộ vi xử lý, bộ nhớ RAM, ROM và EPROM, hoặc EEPROM, tất cả các truy nhập vào bộ nhớ đều được kiểm soát bởi bộ vi xử lý. Chúng cũng có kích thước và độ dày giống như các thẻ tín dụng.

Các thẻ siêu thông minh có cùng chức năng như một thẻ thông minh nhưng chúng còn có một bàn phím, màn hình LCD và bộ pin, vì vậy giống với một máy tính bỏ túi hơn là một thẻ tín dụng. Chúng dày hơn một thẻ tín dụng và cứng.

Các thẻ thông minh không tiếp xúc, không giống như các thẻ mô tả ở trên, chúng không được cắm vào thiết bị đọc thẻ, nhưng liên lạc thông qua các mạch ghép nối cảm ứng RF. Những thẻ này thường được đặt một cách đơn giản trên một vùng xác định trên đầu của thiết bị đọc, sử dụng chúng thuận tiện hơn và ít bị tấn công gây hỏng. Các thẻ không tiếp xúc hiện nay có thể tuân theo các tiêu chuẩn về độ dày của các thẻ thông minh và đủ mềm dẻo để có thể bỏ trong ví.

Các chuẩn

Tổ chức tiêu chuẩn Thế giới (ISO) đưa ra một chuẩn dành cho các thẻ thông minh (ISO 7816) gồm 3 phần sau:

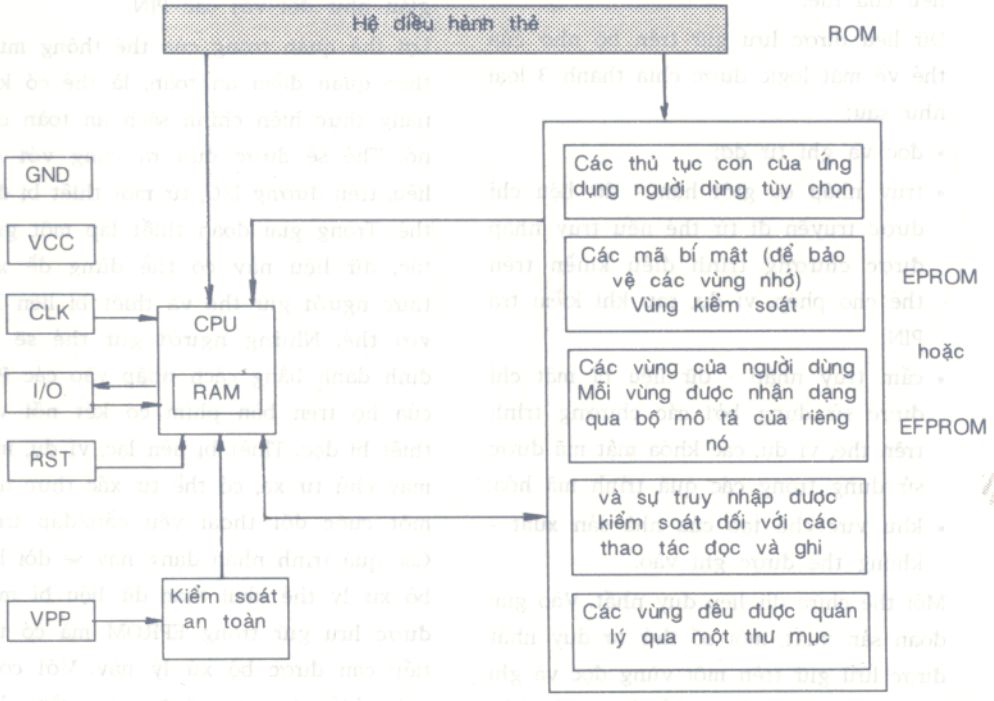
- Phần 1 - Các đặc trưng vật lý;
- Phần 2 - Các kích thước và vị trí của các tiếp điểm;
- Phần 3 - Các tín hiệu điện tử và các giao thức truyền.

Phần 1 xác định các đặc trưng vật lý của thẻ, ví dụ, kích thước (0,68-0,84mm, 53.92-53.03mm, và 85.47-85.72mm). Phần 2 xác định 8 tiếp điểm, 2 trong số chúng được dự trữ cho việc sử dụng sau này, còn lại 6 được quy định như sau:

- VCC - điện áp nguồn của mạch;
- RST - tín hiệu thiết lập lại;
- CLK - tín hiệu đồng hồ;
- GND - điện áp không;
- VPP - điện áp lập trình được;
- I/O - đầu vào/đầu ra dữ liệu.

VCC và GND là các điện áp nguồn, CLK cung cấp một tín hiệu đồng hồ cho các thẻ hoạt động theo chế độ đồng bộ, I/O chỉ cung cấp một kênh để chuyển dữ liệu đi hoặc đến thẻ, RST thiết lập lại chương trình có sẵn trên thẻ và VPP là một tín hiệu điều khiển tùy chọn cho việc sử dụng thông qua thẻ.

Các thẻ thông minh được gài vào trong một thiết bị đọc thẻ, nó cung cấp các điện áp nguồn cần thiết, các tín hiệu đồng hồ...; sau đó thiết bị này chuyển



smart card: *thẻ thông minh.* Hình 1. Bộ nhớ thẻ thông minh.

dữ liệu giữa thẻ thông minh và một đơn vị điều khiển qua một chuẩn ghép nối RS232. Các giao thức truyền được ISO 7816/3 xác định; dữ liệu có thể được truyền đi theo chế độ đồng bộ hoặc không đồng bộ.

Cấu trúc của một thẻ thông minh điển hình được trình bày trong hình 1. Bộ nhớ bao gồm RAM, ROM, EPROM (hoặc EEPROM). Bộ nhớ RAM không ổn định sẽ lưu giữ dữ liệu được phát triển trong quá trình xử lý của một giao tác, ROM lưu giữ các chỉ lệnh chương trình của thẻ mà kiểm soát chức năng của thẻ. EPROM có thể chứa thêm các thủ tục nhỏ của chương trình trên thẻ và dữ liệu của thẻ.

Dữ liệu được lưu giữ trên bộ nhớ của thẻ về mặt logic được chia thành 3 loại như sau:

- đọc và ghi tự do;
- truy nhập có giới hạn - dữ liệu chỉ được truyền đi từ thẻ nếu truy nhập được chương trình điều khiển trên thẻ cho phép, ví dụ, sau khi kiểm tra PIN;
- cấm truy nhập - dữ liệu bí mật chỉ được sử dụng bởi các chương trình trên thẻ, ví dụ, các khóa mật mã được sử dụng trong các quá trình mã hóa;
- khu vực chế tạo của nhà sản xuất - không thể được ghi vào.

Mỗi thẻ chứa dữ liệu duy nhất. Vào giai đoạn sản xuất, một số thứ tự duy nhất được lưu giữ trên một vùng đọc và ghi tự do. Sau đó thẻ có thể được cá nhân hóa thông qua bộ phận phát hành thẻ. Tại giai đoạn này, một hoặc nhiều mã bí mật của bộ phận phát hành thẻ được ghi lại trong vùng cấm truy nhập; sau đó dữ liệu bị khóa lại bằng cách làm nổ các cầu chì bên trong vì vậy sau đó nó không thể bị ghi đè lên.

PIN của người sử dụng được lưu giữ trong vùng cấm truy nhập, và thẻ có thể được bảo vệ chống lại việc thử PIN. Mỗi lần, một PIN không chính xác được nhập vào, bộ đếm được tăng lên 1; khi bộ đếm đạt tới một giá trị xác định trước, việc sử dụng thẻ bị chặn lại. Thông thường, mã của người phát hành thẻ, chỉ có ngân hàng phát hành được biết, phải được nhập vào kết hợp với PIN, để trả thẻ về hoạt động bình thường; việc thử các mã của người phát hành thẻ bị ngăn chặn theo cách đơn giản như đối với các PIN.

Lợi thế quan trọng của thẻ thông minh theo quan điểm an toàn, là thẻ có khả năng thực hiện chính sách an toàn của nó. Thẻ sẽ được đưa ra cùng với dữ liệu, trên đường I/O, từ một thiết bị đọc thẻ. Trong giai đoạn thiết lập một giao tác, dữ liệu này có thể dùng để xác thực người giữ thẻ và thiết bị liên lạc với thẻ. Những người giữ thẻ sẽ tự định danh bằng cách nhập vào các PIN của họ trên bàn phím có kết nối với thiết bị đọc. Thiết bị liên lạc, ví dụ, một máy chủ từ xa, có thể tự xác thực qua một cuộc đối thoại yêu cầu/đáp ứng. Các quá trình nhận dạng này sẽ đòi hỏi bộ xử lý thẻ khai thác dữ liệu bí mật, được lưu giữ trong EPROM mà có thể tiếp cận được bộ xử lý này. Với công nghệ hiện tại, người ta xem rằng bất kỳ cố gắng nào để truy nhập được vào dữ liệu bí mật được lưu thông qua một hình thức tấn công trực tiếp nào đó vào thẻ, là vượt quá khả năng kỹ thuật của

một kẻ tấn công tiềm ẩn.

Sự thuận tiện của các thẻ thông minh trong việc tiến hành quá trình mã hóa sẽ mang lại giá trị của chúng trong các lĩnh vực bao gồm (và vượt quá) các ứng dụng tài chính và kiểm soát truy nhập.

Việc sử dụng các thẻ thông minh trong quá trình mã hóa có những thuận lợi sau đây:

- quá trình được thực hiện trong một môi trường chống giả mạo;
- các khóa mã hóa liên quan đều được lưu giữ bí mật và trong một số trường hợp, các giá trị của chúng không cần có sẵn ở một thiết bị bất kỳ bên ngoài;
- phương tiện mã hóa có sự kiểm soát truy nhập gài sẵn, nghĩa là sử dụng các cơ cấu PIN;
- thẻ được người sử dụng mang theo, như vậy không giống như các thiết bị mật mã trong các máy tính cá nhân, không bao giờ rời khỏi chủ và chịu sự lạm dụng tiềm ẩn;
- phương tiện mã hóa và các khóa mã hóa gài sẵn có thể được người giữ thẻ sử dụng tại bất kỳ thiết bị đầu cuối nào có chứa một bộ phận đọc thẻ thích hợp.

Các thuật toán mã hóa phổ biến hiện nay có giá trị cho các thẻ thông minh là: DES, Feal, RSA, và Fiat-Shamir. Trong trường hợp các mã pháp đối xứng như DES, hoặc FEAL, có thể sử dụng thẻ như một thiết bị kiểm soát truy nhập, để đảm bảo bí mật của các thông báo, để xác thực hoặc ký các thông báo.

Ứng dụng của các thẻ thông minh

Các mảng ứng dụng có thể được phân loại đại thể như các mảng chồng chéo lên nhau:

- ví điện tử;
- các hoạt động giao dịch ngân hàng;
- kiểm soát truy nhập;
- các tệp cá nhân hóa;
- thiết bị mã hóa cá nhân hóa;
- sự trao đổi dữ liệu điện tử.

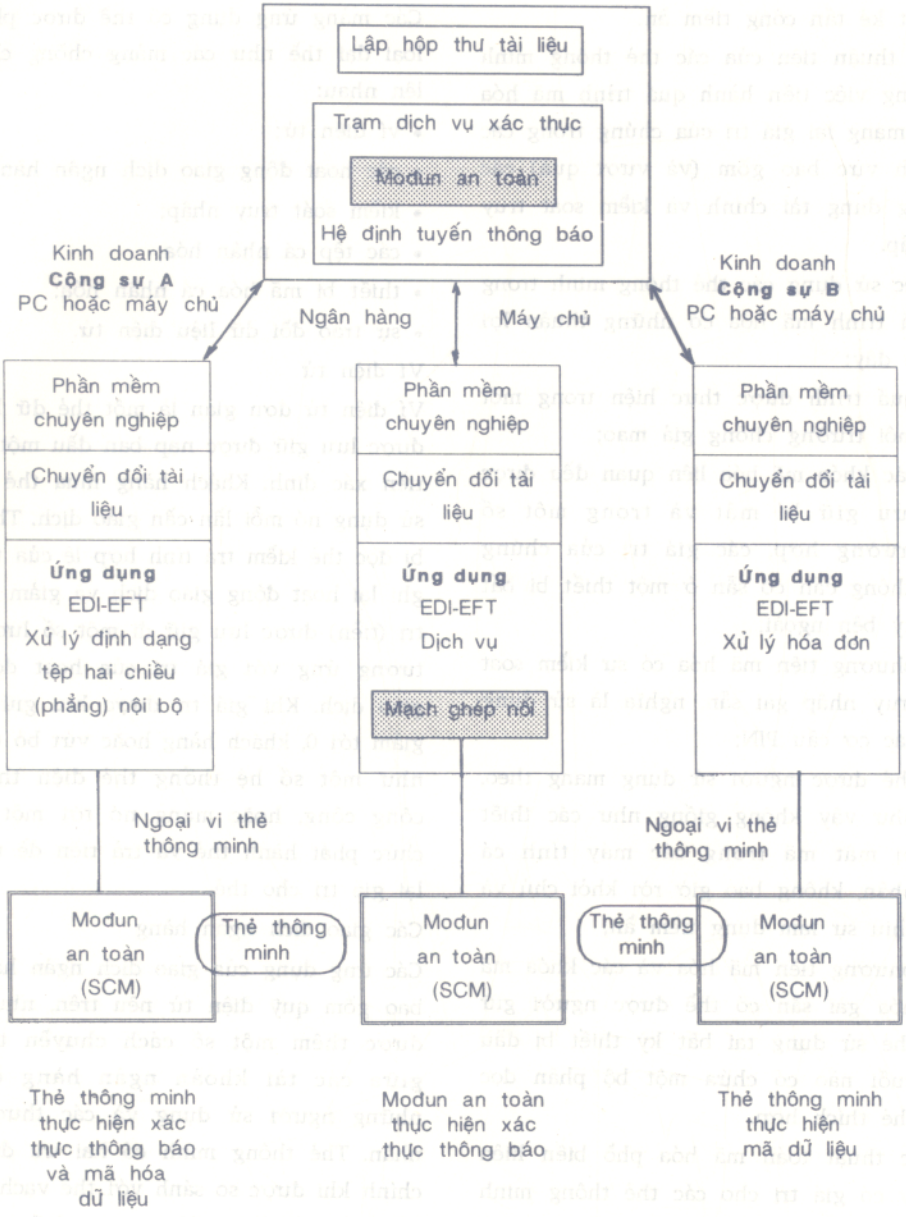
Ví điện tử

Ví điện tử đơn giản là một thẻ dữ liệu được lưu giữ được nạp ban đầu một số tiền xác định. Khách hàng mua thẻ và sử dụng nó mỗi lần cần giao dịch. Thiết bị đọc thẻ kiểm tra tính hợp lệ của thẻ, ghi lại hoạt động giao dịch và giảm giá trị (tiền) được lưu giữ đi một số lượng tương ứng với giá trị của hoạt động giao dịch. Khi giá trị được lưu giữ bị giảm tới 0, khách hàng hoặc vứt bỏ thẻ, như một số hệ thống thẻ điện thoại công cộng, hoặc mang nó tới một tổ chức phát hành thẻ và trả tiền để nạp lại giá trị cho thẻ.

Các giao dịch ngân hàng

Các ứng dụng của giao dịch ngân hàng bao gồm quỹ điện tử nêu trên, nhưng được thêm một số cách chuyển tiền giữa các tài khoản ngân hàng của những người sử dụng và các thương nhân. Thẻ thông minh có hai ưu điểm chính khi được so sánh với thẻ vạch từ đối với các hoạt động giao dịch như vậy, nghĩa là độ an toàn cao và dữ liệu giao dịch đã lưu được cập nhật.

Người sử dụng bất hợp pháp không thể truy nhập tới dữ liệu bí mật được lưu trong các thẻ thông minh. Ngoài ra, thẻ thông minh có thể nhập vào các giao



smart card: *thẻ thông minh.* Hình 2. Thẻ thông minh trong hệ thống trao đổi dữ liệu điện tử.

thức an toàn, như giao thức hỏi/đáp, nó đòi hỏi một khả năng xử lý về phía thẻ.

Ưu điểm thứ hai của thẻ thông minh là thông tin nhạy cảm có thể được bảo vệ lẫn cập nhật, ví dụ, sự cân bằng giá trị hiện tại của khách hàng có thể được cập nhật sau mỗi hoạt động giao dịch. Tính năng này có thể đảm bảo cho thương nhân rằng, không chỉ khách hàng, người lưu giữ thẻ hợp pháp, mà còn cả giới hạn tín dụng của khách hàng đều không bị vượt quá bởi các hoạt động giao dịch trước đó.

An toàn nâng cao do thẻ thông minh mang lại có thể dẫn tới sự quan tâm trở lại đối với các hệ thống ngân hàng tại nhà. Các hệ thống như vậy còn chưa ổn định do chi phí cho các thiết bị đầu cuối an toàn tại nhà cao. Với các phương tiện mã hóa và lưu giữ an toàn dữ liệu bí mật do các thẻ thông minh mang lại, có thể đạt được mức an toàn cần thiết hiện nay bằng các thiết bị đầu cuối tương đối đơn giản tại nhà.

Kiểm soát truy nhập

Thẻ thông minh có thể đáp ứng được các đòi hỏi của nhiều ứng dụng kiểm soát truy nhập. Đặc biệt chúng có những ưu thế theo một quan điểm về kiểm soát truy nhập như sau:

- giá thành của thẻ và thiết bị đọc thẻ giảm;
- bảo vệ chống được việc thử PIN;
- miễn sao chép;
- các giao thức an toàn có hiệu lực;
- bảo vệ chống được các máy chủ giả trang;
- bảo vệ chống được các máy chủ không tin cậy.

Các thẻ có thể được bảo vệ chống được việc thử PIN thông qua các bộ đếm bên trong, nó ghi lại số lần nhập PIN không đúng, và chặn khóa thẻ sau một số lần thử xác định trước. Sau đó, thẻ chỉ có thể được hoạt động lại thông qua nhân viên an ninh được ủy quyền.

Không giống với các thẻ truy nhập, mỗi thẻ thông minh có một số nhận dạng duy nhất không đổi, còn các mã bí mật bên trong không thể hoặc bị sao chép hoặc bị sửa đổi, với mức công nghệ có sẵn đối với một kẻ tấn công tiềm ẩn.

Các giao thức kiểm soát truy nhập phức tạp, chẳng hạn như hỏi/đáp yêu cầu một mức độ xử lý ở phía người sử dụng. Quá trình xử lý như vậy bao gồm việc sử dụng dữ liệu bí mật mà không làm lộ ra ngoài thẻ; thẻ thông minh thích hợp lý tưởng cho dạng giao thức này.

Những giao thức như vậy gồm 2 giai đoạn xác thực. Trước tiên, những người sử dụng chứng minh danh tính của họ trên thẻ, bằng cách gài PIN vào thiết bị đầu cuối đọc thẻ, và sau đó tiến hành hội thoại hỏi đáp giữa thẻ và máy chủ.

Với các hệ thống mã đối xứng, ví dụ như DES, máy chủ phát ra một câu hỏi dưới hình thức một số ngẫu nhiên và số này khi nhận được sẽ được mã hóa bằng một khóa bí mật, và trả lại cho máy chủ. Máy chủ lấy ra khóa bí mật, tương ứng với ID của người sử dụng, và cũng như vậy mã hóa số ngẫu nhiên. Nếu hai khối bản mã giống hệt nhau, người sử dụng được xác thực. Kẻ nghe trộm sẽ không thu được gì từ dữ liệu được trao đổi trên cuộc hội thoại đăng nhập.

Trong một giao thức tương tự sử dụng mật mã khóa mã công khai, thẻ mã hóa số ngẫu nhiên bằng khóa bí mật RSA; máy chủ lấy ra khóa công khai tương ứng với ID của người sử dụng, giải mã bản mã được trả lại bằng khóa công khai mà được lưu giữ cùng với ID của người sử dụng, và kiểm tra kết quả dựa vào số ngẫu nhiên ban đầu. Giao thức hội thoại của Fiat-Shamir tương tự cũng cung cấp một hội thoại khác nhau với mỗi lần đăng nhập, nhưng ít đòi hỏi tính toán hơn so với RSA.

Kỹ thuật hỏi/đáp có thể được sử dụng theo cả hai hướng và như vậy sẽ cho phép người sử dụng xác thực được máy chủ. Với các giao thức khóa công khai, mỗi người sử dụng có thể được cung cấp một bản sao khóa công khai của máy chủ, một quá trình ít mạo hiểm an toàn hơn sự phân phối khối lượng khóa bí mật của máy chủ, mà các hội thoại hỏi/đáp trong DES đòi hỏi.

Hệ thống mật khẩu thông thường của việc xác thực người sử dụng cũng gặp phải bất lợi khi một người sử dụng truy nhập vào một máy chủ không tin cậy, nghĩa là, một hệ thống máy tính không thể tin cậy với dữ liệu bí mật của người sử dụng. Kỹ thuật bất kỳ, được thiết kế để khắc phục vấn đề này, bao gồm một giao thức hội thoại để cung cấp chứng cớ nhận dạng mà không làm lộ thông tin bí mật do người sử dụng nắm giữ. Một kỹ thuật như vậy thường yêu cầu một thiết bị của người sử dụng có thể lưu giữ an toàn thông tin bí mật và đảm trách một mức độ xử lý cục bộ. Kỹ thuật Fiat-Shamir được mô tả ở trên không yêu cầu người sử dụng để lộ thông tin bí mật của họ, hội thoại đăng nhập đơn thuần chỉ cho phép một máy chủ thật tự chứng minh rằng, người sử dụng quả thực không truy nhập tới thông tin bí mật cần thiết.

Các tệp được cá nhân hóa

Các thẻ thông minh có thể có các khả năng lưu giữ cục bộ từ cỡ 10KB lên tới mức megabit. Bởi vậy, chúng có thể được sử dụng để lưu giữ, với phạm vi rộng các dữ liệu nhạy cảm cá nhân như bệnh án hoặc các hồ sơ đánh giá sinh viên. Việc lưu giữ này có thể được cung cấp như một dịch vụ giá trị gia tăng cho thẻ bảo hiểm y tế đã được sử dụng để giải quyết chi trả.

Các thiết bị mã hóa được cá nhân hóa

Thẻ thông minh có thể được sử dụng như một thiết bị mã hóa được cá nhân hóa dành cho các máy tính cá nhân (PC). Người sử dụng gài một thẻ thông minh được cá nhân hóa vào một PC riêng lẻ và sử dụng năng lực xử lý của thẻ thông minh để mã và giải mã các tệp nhạy cảm. Nhược điểm chính của kỹ thuật này, nếu được so với bo mạch có bộ mã hóa của PC, thì sẽ thuộc loại tốc độ dữ liệu tương đối thấp trên đường truyền tới thiết bị đọc thẻ.

Thiết bị mã hóa cũng có thể được sử dụng để xác thực, hoặc kiểm tra tính xác thực của các thông báo. Một thẻ thông minh với một khóa và thuật toán DES có thể được sử dụng để tính toán một MAC cho một thông báo nhận được. Vì vậy, một thẻ thông minh có thể được dùng thông qua tổ chức hành pháp để cung cấp một quyền điện tử cho một hoạt động giao dịch, hoặc kiểm

tra tính xác thực của hoạt động giao dịch nhận được. Tương tự, các thẻ thông minh với các phương tiện khóa công khai có thể cung cấp một chữ ký số thực sự cho một thông báo.

Sự trao đổi dữ liệu điện tử

Một hệ thống EDI sử dụng các thẻ thông minh được minh họa trong hình 2. Sự an toàn sẵn có trong hệ thống EDI đòi hỏi các giao tác chống lại được việc sửa đổi, mất mát, làm lộ trái phép, tiêm tín hiệu, chuyển tiếp và từ chối. Vì vậy, mật mã là đặc trưng chủ yếu của các hệ thống như vậy và việc quản lý khóa sẽ trở nên quan trọng hàng đầu đối với an toàn của hệ thống. Tuy nhiên, nếu các thiết bị mật mã được cài đặt trên thiết bị đầu cuối thì một tổ chức sẽ có trách nhiệm đối với tất cả các giao tác phát ra từ thiết bị đầu cuối này; khi đó, kiểm soát truy nhập của thiết bị đầu cuối sẽ là một yếu tố an toàn chính. Mặt khác, nếu các phương tiện mật mã được chứa trong thẻ thông minh của người quản lý, được gài vào một bộ đọc thẻ liên kết với thiết bị đầu cuối, thì một thiết bị đầu cuối không được quan tâm sẽ là mục tiêu ít hấp dẫn để tấn công.

Các xu hướng trong tương lai

Có hai hướng trong tương lai cho các thẻ thông minh, sự mở rộng thị trường về quy mô và số lượng các lĩnh vực ứng dụng và các phát triển công nghệ trên thẻ.

Thẻ thông minh có khả năng chiếm ưu thế thông qua thị trường khách hàng, và bị chi phối bởi giá cả và khả năng chấp nhận của khách hàng. Có thể đoán trước được là thẻ thông minh sẽ thay thế thẻ vạch từ trong túi của khách hàng. Một ưu thế đặc biệt là bản chất đa ứng dụng của các thẻ thông minh giúp nó có thể thay thế một lượng lớn các thẻ vạch từ hiện đang tồn tại trong các túi và các ví.

Một hướng phát triển quan trọng khác về các thẻ thông minh là việc thay thế các PIN của thẻ, bằng một mẫu sinh trắc học của một người sử dụng. Với mẫu của người sử dụng được cất giữ trên một thẻ thông minh, thì thiết bị đọc sinh trắc có thể đảm bảo rằng người trình thẻ thông minh thực sự là người chủ thẻ hợp pháp mà không phải tìm lại mẫu của người sử dụng từ một cơ sở dữ liệu trung tâm. *Xem* asynchronous transmission, challenge/response, contactless smart card, DES, digital signature, EDI, EEPROM, electronic purse, EPROM, FEAL, Fiat-Shimir algorithm, ISO 7816, LDC, MAC, magnetic stripe card, microprocessor, nonvolatile storage, PIN, public key cryptography, RAM, ROM, RSA, RS232-C, supersmart card, symmetric cipher, synchronous transmission, template, user id, videotex, wired logic card.

smart terminal *(thiết bị) đầu cuối thông minh* Trong tính toán, một thiết bị đầu cuối cung cấp thêm các đặc tính cho một đầu cuối kết xuất nói chung, một thiết bị đầu cuối như vậy có bộ nhớ và khả năng xử lý nào đó có thể cung cấp các phương tiện hiển thị đã định dạng, hiển thị đồ họa, các thiết bị nạp và tải v.v.. *So sánh với* dumb terminal. *Xem* download, upload.

SMF *gói SMF* *Xem* data security package.

SMIB *Xem* secure management information base.

smoke detector ***bộ phát hiện khói*** Trong an toàn vật lý, một thiết bị cảm nhận được sự có mặt các hạt trong của sự đốt cháy. *Xem* combination smoke detector, ionization smoke sensor, photoelectric beam smoke detector.

SMTP *Xem* simple mail transfer protocol.

SNA *Xem* system network architecture.

snapshot ***xem nhanh*** Trong kiểm toán, nói tới việc quan sát các bước xử lý khác nhau trong một chu trình xử lý. *Xem* tagging.

Snefru ***hàm Snefru*** Trong mật mã, một hàm băm một chiều. *Xem* one-way function.

s/n ratio ***tỷ số s/n*** *Xem* signal to noise ratio.

societal vulnerability ***điểm yếu xã hội*** Trong an toàn máy tính, khả năng mất mát, gây tổn hại hoặc sự phủ nhận các quyền bình đẳng đối với một bộ phận dân số quan trọng; cũng như sự yếu kém tiềm ẩn của sự ổn định xã hội hoặc sự nguy hiểm đối với chủ quyền quốc gia do sự phụ thuộc vào công nghệ dựa vào máy tính.

soft error ***lỗi nhẹ, lỗi mềm*** Trong tính toán, một lỗi trong việc đọc dữ liệu từ một đĩa từ, nó có thể được sửa chữa bằng cách đọc lại cung từ hoặc bằng cách dịch chuyển đầu đọc ghi tiến hay lùi. *So sánh với* hard error.

softlifting ***ăn cắp phần mềm*** Trong an toàn máy tính, việc sao chép bất hợp pháp phần mềm được cấp đăng ký để sử dụng riêng. *Xem* software protection.

software ***phần mềm*** Các chương trình, các thủ tục, các chương trình con và các tài liệu có thể tồn tại liên quan đến hoạt động của một hệ thống xử lý dữ liệu. *So sánh với* firmware, hardware.

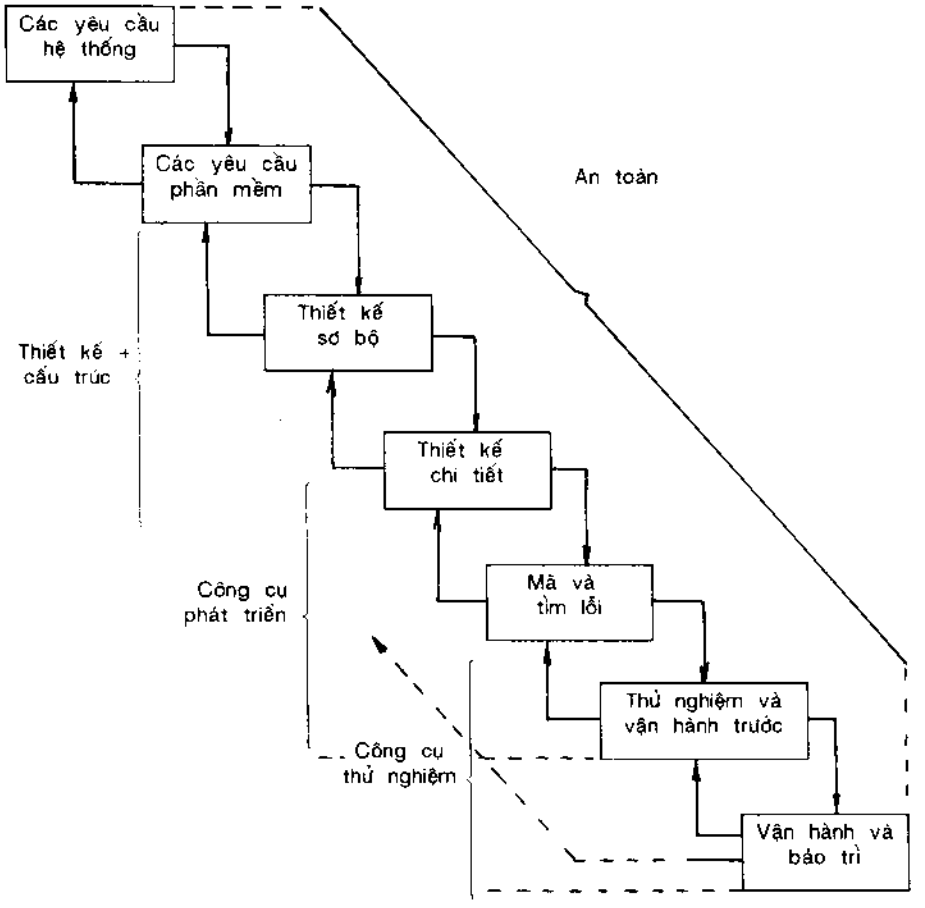
software analysis ***phân tích phần mềm*** Trong an toàn máy tính, các lỗi phần mềm không chỉ là một nguồn các lỗi không có chủ tâm trong một hệ thống, chúng cũng có thể được khai thác như các kẽ hở an toàn. Việc phân tích phần mềm hiện có có thể được các công cụ phần mềm giúp đỡ; nói chung, các công cụ này có thể được phân thành các công cụ phân tích động và phân tích tĩnh. *Xem* dynamic analysis, static analysis, software tool.

software creep ***sao lậu phần mềm*** Trong tính toán, việc sao chép không theo thể thức, bất hợp pháp một chương trình cho một người sử dụng khác nhưng không có động cơ kiếm lời. *Xem* piracy.

software development life cycle ***chu trình phát triển phần mềm*** Trong tính toán, các giai đoạn của chu kỳ đời sống của việc phát triển phần mềm bao gồm: khởi tạo, định nghĩa, thiết kế, lập trình, kiểm tra và hoạt động.

software engineering ***kỹ thuật phần mềm*** Trong tính toán, một môn học được xác định rộng rãi và tích hợp các khía cạnh khác nhau của lập trình, dựa vào việc ghi mã để đảm bảo đáp ứng được các ngân quỹ, cốt để đưa ra phần mềm có hiệu quả và rẻ tiền. *Xem* software.

software house ***hãng phần mềm***



software development life cycle. *chu trình phát triển phần mềm.*

Trong phần mềm, một tổ chức đưa ra phần mềm hỗ trợ các dịch vụ cho những người sử dụng. *Xem* software.

software interface functions ***(các) chức năng giao diện phần mềm*** Trong an toàn máy tính, các hoạt động TCB mà có thể được phần mềm gọi ra. *Xem* TCB.

software interrupt ***ngắt mềm*** Trong tính toán, một ngắt do một chương trình có quyền ưu tiên cao gây ra khi cần các dịch vụ của CPU. *So sánh với* hardware interrupt. *Xem* interrupt, CPU.

software license ***đăng ký phần mềm, bản quyền phần mềm*** Trong tính toán, một thỏa thuận giữa một người sử dụng và một nhà cung cấp phần mềm định rõ các quyền của người sử dụng đối với phần mềm. *Xem* shrink-wrapped license, software.

software maintenence ***bảo dưỡng phần mềm*** Trong tính toán, các cải tiến và các thay đổi cần thiết để giữ

cho các chương trình không bị lỗi thời và đảm bảo hoạt động có hiệu quả. *Xem* software.

software package ***bó phần mềm, gói phần mềm*** Trong tính toán, một tập hợp các chương trình dành cho một mục đích xác định, thường được do một hãng phần mềm viết ra.

software piracy ***vi phạm bản quyền phần mềm*** *Xem* piracy.

software protection ***bảo vệ phần mềm*** Trong an toàn máy tính, việc chấp nhận các biện pháp hợp pháp và có kỹ thuật để ngăn chặn việc sử dụng trái phép hoặc lợi dụng phần mềm. Các phương pháp kỹ thuật thường dùng một số cách để ngăn chặn một chương trình được sao chép hoạt động. Phần mềm có thể được bảo vệ thông qua các luật sở hữu trí tuệ tại một số nước, nhưng điều này thường không chắc chắn và bị hạn chế. Kết quả là, nó đã trở thành truyền thống đối với các nhà cung cấp phần mềm để bổ sung và làm tăng thêm việc bảo vệ này thông qua các điều khoản ký hợp đồng thích hợp chứa trong đăng ký phần mềm.

Cơ sở hợp pháp cho việc bảo vệ bằng hợp đồng

Theo quan điểm tuần túy luật pháp, những nhà cung cấp có 3 mục đích cơ bản nhằm đạt được một hợp đồng với người mua.

- Xác định phạm vi mà người mua có thể sử dụng phần mềm, trên cơ sở là bất cứ việc gì khác sẽ gây ra một sự vi phạm bản quyền. Như vậy, người mua được cấp cho một đăng ký hạn chế theo bản quyền và việc sử dụng bất kỳ ngoài các giới hạn của đăng ký này, về lý thuyết sẽ có thể bị kiện, miễn là việc sử dụng như vậy gây ra một hành động bị cấm, chẳng hạn sao chép lại, dịch và sửa lại theo nghĩa của luật bản quyền thích hợp.
- Duy trì tính bí mật của thông tin bí mật bất kỳ chứa trong phần mềm thông qua việc bắt tuân theo các giới hạn thích hợp. Hầu hết các nước có cách bảo vệ nào đó đối với các thông tin bí mật nhưng điều này sẽ phụ thuộc vào phạm vi thông tin không nằm trong phạm vi công cộng. Việc tuân theo và bắt buộc theo các giới hạn thích hợp có thể giúp duy trì tính bí mật trong phần mềm, đặc biệt phần mềm được phân phối hạn chế.
- Có biện pháp phòng ngừa theo hợp đồng đối với người nhận phần mềm. Người cung cấp phần mềm có thể rất muốn có biện pháp phòng ngừa ghi trong hợp đồng đối với người mua, trong trường hợp không có biện pháp phòng ngừa nào theo luật về bản quyền hoặc bảo mật, và cả ở nơi nào mọi quyền dành riêng đều không liên quan tới vấn đề người cung cấp quan tâm.

Các lợi ích cần được bảo vệ

Các nhà cung cấp muốn bán được số lượng tối đa các bộ phần mềm của họ. Để đạt được như vậy, một nhà cung cấp sẽ muốn:

- mọi người sử dụng đều mua bộ phần mềm của họ;
- trong trường hợp khách hàng có nhiều máy tính, chẳng hạn người sử dụng tập thể, thì bán được mỗi bộ phần mềm cho mỗi máy của khách

hàng;

- hạn chế sử dụng mỗi bộ phần mềm cho sử dụng cá nhân của người mua cụ thể, đặc biệt khi người mua là một trong nhóm của một số lượng lớn các công ty. Ngoài ra, nhà cung cấp phần mềm sẽ muốn ngăn chặn phần mềm khỏi bị lạm dụng hoặc được sử dụng cho các mục đích mà các nhà cung cấp có thể hy vọng tự mình tiêu thụ.

Điều này có nghĩa là một nhà cung cấp muốn ngăn chặn:

- sao chép trái phép, hoặc để sử dụng trong phạm vi tổ chức của khách hàng, hoặc đơn giản là sao chụp phần mềm trái phép để thu lợi;
- sử dụng trái phép trên mạng cục bộ hoặc truy nhập từ xa các hệ thống nhập;
- sử dụng phần mềm để phát triển các sản phẩm cạnh tranh.

Thỏa thuận đăng ký phần mềm truyền thống

Giống như một bài toán thực tế, cách thức có thể áp dụng bảo vệ hợp đồng phụ thuộc rất nhiều vào kiểu phần mềm. Phần mềm máy tính truyền thống luôn được cung cấp theo đăng ký bản quyền, nhà cung cấp nói chung sẽ có hình thức thỏa thuận bản quyền chuẩn mà đòi hỏi khách hàng là người sử dụng phải ký trước khi cho phép sở hữu phần mềm. Loại hợp đồng kiểu này vẫn còn được sử dụng rộng rãi, song chỉ có thể được sử dụng trong môi trường, nơi người dùng và nhà cung cấp hoặc đại diện của nhà cung cấp đều ở vị trí ký thỏa thuận. Điều này cũng đúng với trường hợp khi người dùng mua một hệ phần mềm phức tạp, thường là được thay đổi theo các yêu cầu đặc thù của người dùng, hoặc chuẩn bị mua một hệ phần cứng/phần mềm tích hợp.

Mặt khác, những kiểu thỏa thuận như vậy không còn thích hợp với một lượng lớn phần mềm có trên thị trường dùng với các máy vi tính, và đặc biệt, cho thị trường máy tính tại nhà. Ngày nay, phần mềm như vậy nói chung được bán cho người dùng cuối thông qua các cửa hàng máy tính hoặc các nhà bán lẻ trên phố lớn, những người mà có lẽ ở phía cuối của dây chuyền phân phối sẽ bị loại bỏ khỏi nhà cung cấp phần mềm gốc. Trong tình huống này, đặc biệt, với giá thành phần mềm vào khoảng tương tự một đĩa compac, không thực tế hoặc không thể chấp nhận được với người dùng đang cần ký một hợp đồng.

Để khắc phục vấn đề này, các nhà cung cấp phần mềm đã cố phát triển các kỹ thuật mới đặt các điều kiện hợp đồng lên những người sử dụng cuối. Cụ thể, khắp thế giới, các nhà phân phối phần mềm đã theo kỹ thuật (được phát triển đầu tiên ở Mỹ) về "các hợp đồng bản quyền gói gọn", hay "hợp đồng đăng ký bọc nilông", nhờ đó khách hàng cho rằng đã chấp nhận các giới hạn về việc sử dụng một cách đơn giản nhờ mở gói niêm phong có chứa đĩa.

Tuy nhiên, ở nhiều nước kỹ thuật này không chắc được luật pháp công nhận vì nó bị xem là đã đặt một trách nhiệm phi lý lên người mua không ngờ vực.

Hợp đồng bản quyền gói gọn

Mục tiêu là đặt các giới hạn sử dụng, tương tự như những giới hạn chứa trong các thỏa thuận bản quyền truyền

thống khi khách hàng mua các bộ phần mềm từ những nhà bán lẻ trên phố lớn. Các hợp đồng hay thỏa thuận bản quyền gói gọn được nghĩ ra để cố đáp ứng nhu cầu cho khách hàng mua phần mềm đơn giản tới mức có thể.

Nhà sản suất đóng gói phần mềm theo cách để người dùng theo thứ tự, truy nhập được tới các đĩa, mở gói hay phong bao mà trên đó in các giới hạn của thỏa thuận bản quyền. Bao gói được niêm phong để hướng người dùng cuối tới các giới hạn của đăng ký bản quyền, cùng với yêu cầu rằng, việc mở hộp đĩa sẽ chỉ ra sự thừa nhận của người mua về các giới hạn. Vị thế được tăng cường nhờ thêm cả việc diễn đạt thích hợp về bộ phần mềm, làm nó trở nên rõ ràng với người dùng cuối, rằng nhờ mua nó, anh hay chị đang chấp nhận các giới hạn của hợp đồng.

Ý kiến về mặt luật pháp nằm sau phương pháp này là, người dùng cuối đã mua toàn bộ hộp đĩa, tài liệu hướng dẫn và các thể hiện vật lý khác của bộ phần mềm, song chỉ nhận một bản quyền hạn chế để dùng các chương trình. Thực tế, người ta cần chứng minh những khó khăn theo nhiều quyền hạn pháp lý, ví dụ như ở Anh, với các nhà sản xuất, để làm các giới hạn bất kỳ có hiệu lực, phải dựa trực tiếp vào người dùng vì các vấn đề về tính quan hệ riêng của hợp đồng nếu ta nhớ rằng, chính người bán lẻ là phía bên kia của hợp đồng bán hàng thực sự.

Các điều khoản của thỏa thuận gói gọn

Thỏa thuận bản quyền gói gọn thường chứa các dự phòng liệt kê dưới đây:

- *Các điều kiện về mua*. Bản quyền trước hết đưa ra tuyên bố chung trong suốt các dòng rằng, sản phẩm được bán sẽ chịu các hạn chế về việc sử dụng được phép theo thông lệ bán phần mềm máy tính để sử dụng cá nhân. Nó cũng cốt để thông báo cho người dùng rằng, những điều khoản của thỏa thuận đều ghi trên sản phẩm và việc mở bộ đĩa là sự chấp nhận các hạn chế đó. Điều phổ biến là ở đây cần một công bố rằng, nếu người dùng không chấp nhận các giới hạn thì sản phẩm cần được trả về người bán lẻ và được hoàn lại tiền mua.
- *Các sử dụng được phép*. Thỏa thuận bản quyền thường gồm các dự phòng nhờ đó: bản quyền được cấp là chỉ cho sử dụng cá nhân; phần mềm chỉ được sử dụng trên mục bất kỳ có phần cứng tương thích mà người sử dụng sở hữu hoặc sử dụng được; đôi khi phần mềm chỉ được dùng trên một máy vi tính vào một thời điểm bất kỳ.
- *Các sử dụng không được phép*. Khi đó bản quyền chỉ ra những sử dụng không được phép theo giấy phép. Chúng gồm: sử dụng phần mềm trên bộ đa xử lý hoặc bố trí đa vị trí; sử dụng phần mềm trong kinh doanh dịch vụ máy tính, hoặc để cửa truy nhập ở xa; tạo các đĩa sao chép và tài liệu đi kèm, loại trừ khả năng với các mục đích an toàn; tạo bản thay thế phần mềm; quyền cấp bản quyền con; gài hoặc biên dịch; tạo các bản dịch hoặc sửa đổi phần mềm để sử dụng với phần cứng không tương thích.

Hoàn toàn độc lập với hiệu lực của

những điều khoản này khi xét về luật theo hợp đồng hay luật bản quyền, trong một số quyền hạn pháp lý, có thể cũng có những lý lẽ về chống tơrớt, nhất là ở Mỹ. *Xem* copy protection, copyright, diskette, execute protection, local area network, shrink-wrapped license, software license.

software quality ***chất lượng phần mềm*** *Đồng nghĩa với* computer software quality.

software redundancy ***dự phòng phần mềm, dư thừa phần mềm*** Trong lĩnh vực độ tin cậy, một phần của chương trình mà sẽ không cần thiết nếu hệ thống được đảm bảo không có lỗi.

software security ***an toàn phần mềm*** Trong an toàn máy tính, nói tới phần mềm dành cho mục đích chung, ví dụ, hệ điều hành, tiện ích, công cụ phát triển phần mềm, và các chương trình và các thủ tục của các ứng dụng mà bảo vệ dữ liệu hoặc thông tin được xử lý bởi một hệ thống xử lý dữ liệu và các nguồn tài nguyên của nó.

software security certification ***chứng thực an toàn phần mềm*** Trong an toàn máy tính, việc đánh giá một hệ thống máy tính cho trước và tất cả cá nhân và các phương tiện liên quan xuất phát từ triển vọng của một ứng dụng cụ thể. Mục đích cơ bản của quá trình này là chứng thực mức độ an toàn do môi trường máy tính trong đó ứng dụng hoạt động cung cấp, tương thích với mức an toàn mà ứng dụng yêu cầu. *Xem* certification.

software tool ***công cụ phần mềm*** Trong tính toán, một chương trình được sử dụng để tạo thuận lợi cho việc phát triển, hoặc phân tích các chương trình khác. Hầu hết các hệ điều hành cung cấp các bộ soạn thảo để tạo ra và sửa đổi các tệp chương trình nguồn, các bộ biên dịch để chuyển đổi từ các ngôn ngữ bậc cao hoặc ngôn ngữ bậc thấp sang ngôn ngữ máy, liên kết các chương trình tải để lắp ráp các modun được biên dịch tách biệt thành dạng thích hợp để thực hiện, và các chương trình hiệu chỉnh lỗi để xem xét các chương trình có lỗi.

Solano ***virut Solano*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL, dữ liệu và liên kết tệp. *Xem* virus names.

SOM ***ký tự khởi đầu thông báo*** Trong truyền dữ liệu, viết tắt của start of message, một ký tự trong một đáp ứng hỏi vòng, nó đứng trước địa chỉ, hoặc các địa chỉ, của các trạm dữ liệu bất kỳ chứ không phải trạm chủ nhận thông báo. *Xem* polling.

something the user has ***cái người dùng sở hữu*** Trong kiểm soát truy nhập, một kỹ thuật nhờ đó sự truy nhập được cấp dựa trên cơ sở quyền sở hữu của đối tượng vật lý nào đó hoặc thẻ bài. *So sánh với* something the user is, something the user knows. *Xem* token.

something the user is ***cái là đặc tính người dùng*** Trong kiểm soát truy nhập, một kỹ thuật qua đó, truy nhập được cấp dựa trên cơ sở của một

đặc tính vật lý của người sử dụng, ví dụ, vân tay, hoặc đặc tính hoạt động nào đó, ví dụ, cách ký một chữ ký. *So sánh với* something the user has, something the user knows. *Xem* biometrics, PIN.

something the user knows ***cái người dùng biết*** Trong kiểm soát truy nhập, một kỹ thuật qua đó, truy nhập được cấp dựa trên cơ sở những thông tin mà người sử dụng nắm giữ, ví dụ, mật khẩu hoặc PIN. *So sánh với* something the user has, something the user is. *Xem* password, PIN.

SON ***lệnh SON*** Viết tắt của Statement of Need (câu lệnh nhu cầu).

sonic motion detector ***thiết bị phát hiện chuyển động nhờ âm thanh*** Trong an toàn vật lý, một thiết bị phát hiện sự xuất hiện của một kẻ thâm nhập bởi sự nhiễu loạn trong một mẫu của các tín hiệu âm thanh được tạo ra trong vùng bảo vệ. *So sánh với* ultrasonic motion detector. *Xem* motion detector, protected area.

sonogram ***biểu đồ âm thanh*** Trong an toàn truyền thông, sự biểu diễn đồ thị 3 chiều của một tín hiệu âm thanh. Hai trục biểu diễn thời gian và tần số, trong khi đó biên độ được biểu diễn theo mức xám của đồ thị, ví dụ màu đen chỉ ra biên độ cao và màu trắng chỉ ra biên độ thấp. *Xem* voice scrambling.

sonograph ***âm phổ ký*** Trong an toàn truyền thông, một thiết bị dùng để tạo ra một biểu đồ âm thanh. *Xem* sonogram.

Sorry ***virut Sorry*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COMMAND.COM và COM, làm ảnh hưởng đến thao tác tại thời điểm chạy, làm hỏng chương trình, các tệp OVL. *Xem* virus names.

source ***nguồn (tin)*** Trong truyền dữ liệu, một điểm nhập thông báo vào hệ thống. *So sánh với* sink.

source authorization ***(sự) ủy quyền nguồn, (sự) cấp nguồn*** Trong an toàn dữ liệu, một cấp phép cho trước để người gửi phát đi thông báo nhạy cảm hoặc có ưu tiên cao. Sự cấp phép này là một biện pháp đối phó chống lại sự gửi tràn ngập mạng. *Xem* flooding.

source code ***mã nguồn*** Trong tính toán, mã ban đầu của một chương trình của người sử dụng trước khi được dịch, ví dụ như được biên dịch, dịch hợp ngữ, diễn dịch. *So sánh với* object code. *Xem* source language.

source code analyzer ***bộ phân tích mã nguồn*** Trong an toàn máy tính, một công cụ phần mềm, được sử dụng trong đánh giá tĩnh, nó cung cấp các chi tiết về các đặc tính xác định của chương trình nguồn, ví dụ phép kiểm tra tham chiếu chéo các biến mà có thể thi hành các quyết định kiểm soát. *So sánh với* code review, penetration study. *Xem* software tool, source program, static evaluation.

source code escrow ***(sự) ủy nhiệm lưu giữ mã nguồn*** *Xem* escrow agent.

source language ***ngôn ngữ nguồn*** Trong tính toán, một ngôn ngữ tính toán bậc cao mà chương trình của người sử dụng được viết theo. *So sánh*

với object language.

source program ***chương trình nguồn*** Trong tính toán, một chương trình máy tính được viết bằng ngôn ngữ nguồn. *Xem* source code, source language.

source suppression ***(sự) triệt nguồn (phát xạ)*** Trong an toàn tuyền thông, thiết kế cẩn thận của mạnh điện và sơ đồ bố trí mà không phát ra các tín hiệu gây hại. *So sánh với* encapsulation. *Xem* Tempest proofing.

SOW ***lệnh SOW*** Viết tắt của Statement of Work (câu lệnh làm việc).

space ***dấu cách, ký tự trống; khoảng trống*** (1) Dấu cách là một cột hoặc ký tự trống. (2) Trong truyền thông, khoảng trống là một xung, hoặc thời gian nghỉ của một xung báo hiệu trạng thái nhị phân 0. *So sánh với* mark.

space division multiplexing ***đồn kênh phân khoảng*** Trong truyền thông, sự nhóm hơn một đường truyền vật lý. Trong liên lạc bằng đường dây hữu tuyến, nhiều cặp dây có thể được tổ hợp vào một cáp; trong liên lạc vệ tinh, một anten có thể hội tụ một số lượng các chùm vết tới những vị trí địa lý khác nhau. *So sánh với* time division multiplexing. *Xem* multiplexing.

space division switching ***chuyển mạch phân khoảng*** Trong truyền thông, một phương pháp chuyển mạch trong đó mỗi kết nối qua chuyển mạch chiếm một đường truyền vật lý khác nhau. *So sánh với* time division multiplexing.

space protection ***bảo vệ vùng*** *Đồng nghĩa với* area protection.

span sensor ***bộ cảm biến khoảng cách*** Trong an toàn vật lý, một bộ cảm biến bao quát một vùng hẹp và liên tục giữa hai điểm, ví dụ bộ cảm biến quang điện *Xem* photoelectric sensor.

spatial redundancy ***dự phòng không gian*** *Đồng nghĩa với* protective redundancy.

Special ***ngôn ngữ Special*** *Xem* hierarchical development methodology.

special access programs ***(các) chương trình truy nhập đặc biệt*** Trong an toàn máy tính, các chương trình bất kỳ đặt nhu cầu cần biết hoặc các yêu cầu có liên quan đến an toàn hoặc các ràng buộc về an toàn vượt quá mức bình thường, được cung cấp cho việc bảo vệ các thông tin đã được phân loại thuộc một trong ba mức an toàn, nghĩa là mật, tuyệt mật, tối mật. Một chương trình như vậy sẽ bao gồm (mà không hạn chế) về mức truy nhập đặc biệt, các yêu cầu phân xử, hoặc điều tra nghiên cứu, sự bổ nhiệm đặc biệt các công chức được phép quyết định nhu cầu cần biết, hoặc các danh sách hoặc các chỉ thị đặc biệt về nhân sự được xác định là có nhu cầu cần biết. SIO-PESI là một ví dụ về một chương trình truy nhập đặc biệt của Bộ Quốc phòng Hoa Kỳ (DOD). Các nguồn khác về kiểm soát truy nhập bổ sung hoặc các yêu cầu an toàn thích hợp khác mà nói chung không thể áp dụng chung vào cùng bảng phân loại an toàn trong DOD, bao gồm:

(*a*) Đạo luật về năng lượng nguyên tử năm 1954;

(*b*) các thủ tục dựa trên các yêu cầu

của hiệp ước quốc tế; và

(c) các chương trình để thu thập tin tức tình báo nước ngoài hoặc các chương trình dưới quyền hạn của Ủy ban tình báo Nước ngoài hoặc của Ban an toàn truyền thông của Mỹ.

Xem need to know, SIO-PESI.

specialized common carier ***hãng truyền thông chuyên dụng*** Trong truyền thông, một tổ chức của Mỹ, không phải là một công ty điện thoại, được cấp phép thông qua quyết định 1971 FCC để cung cấp một dịch vụ truyền thông điểm nối điểm trên cơ sở truyền thông công cộng. *Xem* common carrier, FCC, point-to-point.

special marking ***đánh dấu đặc biệt*** Trong an toàn dữ liệu, các đánh dấu không phải là các mức phân loại, chúng được sử dụng trên các tài liệu đã được phân loại nào đó để chỉ ra tài liệu có sự truy nhập đặc biệt hoặc các yêu cầu. *Đồng nghĩa với* handling caveats, handling restrictions.

special purpose ***mục tiêu đặc biệt*** Nói tới các hệ thống và các thiết bị có thiết kế đặc biệt để sử dụng trong một tập giới hạn các ứng dụng.

specification ***đặc tả*** Sự mô tả có tính kỹ thuật về hoạt động mong muốn của một hệ thống, xuất phát từ các yêu cầu của nó. Một đặc tả được sử dụng để phát triển và kiểm tra việc thực hiện của một hệ thống. *Xem* requirement.

speech invertor ***bộ đảo tiếng nói*** Trong an toàn truyền thông, một dạng của xáo trộn tiếng nói mà có sự thay đổi lẫn nhau giữa các tần số cao và tần số thấp của tín hiệu tiếng nói. Sóng âm thanh được điều chế biên độ với tín hiệu sóng mang, và dải biên thấp hơn được phát đi. Nếu một tín hiệu hình sin tần số f_m được điều chế biên độ với sóng mang có tần số f_c thì tần số của dải biên thấp là $f_c - f_m$. Như vậy các thành phần tần số cao của tín hiệu nguyên thủy xuất hiện như các thành phần tần số thấp của tín hiệu được truyền đi. Sự thay đổi do kỹ thuật này tạo ra hầu như không đủ để làm giảm độ nghe rõ còn lại tới mức vừa ý. Hơn nữa, một kẻ chặn bắt có thể đảo ngược quá trình xáo trộn, làm lộ ra thông báo ban đầu. *Xem* amplitude modulation, band shift invertor, carrier, residual intelligibility, voice scrambling.

speech recognizer ***bộ nhận dạng tiếng nói*** Trong tính toán, một hệ thống nhận lời nói được phát ra và nhận dạng thông báo. Đầu ra của hệ thống sau đó có thể được sử dụng để khởi tạo các hành động hoặc các đáp ứng thích hợp. *So sánh với* speech synthesizer.

speech scrambling ***xáo trộn tiếng nói*** *Đồng nghĩa với* voice scrambling.

speech synthesizer ***bộ tổng hợp tiếng nói*** Trong các giao tiếp giữa máy và con người, một hệ thống tạo ra âm thanh của các câu nói theo các lệnh và đoạn văn đã được lưu giữ. Các phương pháp hiện tại được chia thành 2 loại, các dạng sóng âm thanh số hóa được lưu và sự tổng hợp focmăng. *Xem* formant.

SPEED ***hệ SPEED*** Trong hoạt động ngân hàng, một từ cấu tạo bằng chữ đầu của những từ khác nhau theo

ngôn ngữ chính thức của Malaysia để chỉ hệ thống thanh toán liên ngân hàng tự động ở Malaysia. *Xem* banking networks.

split knowledge ***tri thức phân tích*** (1) Trong an toàn thủ tục, một kỹ thuật mà trong đó, hai hoặc nhiều nhóm giữ dữ liệu phải được tổ hợp lại để nhận được tham số an toàn hoặc để đảm trách một hoạt động nhạy cảm. *Xem* separation of duties or functions, threshold. (2) Trong quản lý khóa, một điều kiện mà theo đó, hai hoặc nhiều nhóm riêng biệt có các thành phần khóa không chứa các thông tin về khóa mã tổng hợp. Khóa tổng hợp chỉ tồn tại trong các thiết bị an toàn như kết quả của phép cộng loại trừ-hoặc được tạo ra tự động của các thành phần khóa độ dài đầy đủ, mỗi thành phần này được nhập vào riêng lẻ và bí mật. *Xem* cryptographic key, EXCLUSIVE OR, ANSI X9.17 - 1985.

split site ***trạm tách, địa điểm tách, vị trí tách*** Trong quản lý rủi ro, nói tới việc sử dụng hai trạm để thực hiện các chức năng xử lý dữ liệu của một công ty sao cho các chức năng cơ bản có thể tiếp tục được thực hiện nếu một trong các trạm ngừng hoạt động. Khả năng của trạm nhỏ hơn (trong hai trạm) là phải đủ khả năng để thực hiện tất cả các chức năng cơ bản. Hai trạm phải đủ gần để duy trì liên lạc sau khi sự cố xảy ra, nhưng cũng vừa đủ tách biệt để đảm bảo rằng chúng không bị ảnh hưởng bởi cùng sự cố. *So sánh với* hot site.

spoofing ***(sự) đánh lừa, (sự) nhái; spufinh*** (1) Trong an toàn dữ liệu, đánh lừa là sự khoác các đặc tính của hệ thống máy tính khác hoặc người sử dụng khác nhằm mục đích lừa gạt. (2) Trong quản lý khóa, đánh lừa là việc chặn/sửa đổi các khóa trao đổi bởi một kẻ tấn công. Nếu hai nhóm sử dụng mật mã khóa công khai để trao đổi các khóa DES, thì việc trao đổi bình thường có thể được mô tả như sau:

- Alice yêu cầu khóa mã công khai của Bob.
- Bob đáp ứng lại yêu cầu này và gửi khóa mã E_B cho Alice.
- Sau đó Alice sẽ gửi một dữ liệu DES hoặc mã hóa khóa, khóa K_A được mã bằng E_B, nghĩa là $eK_B(K_A)$ cho Bob.
- Bob nhận $eK_B(K_A)$ và giải mã nó bằng D_B, là khóa giải mã riêng của Bob, anh ta thu được K_A, sau này sẽ được sử dụng để liên lạc với Alice.

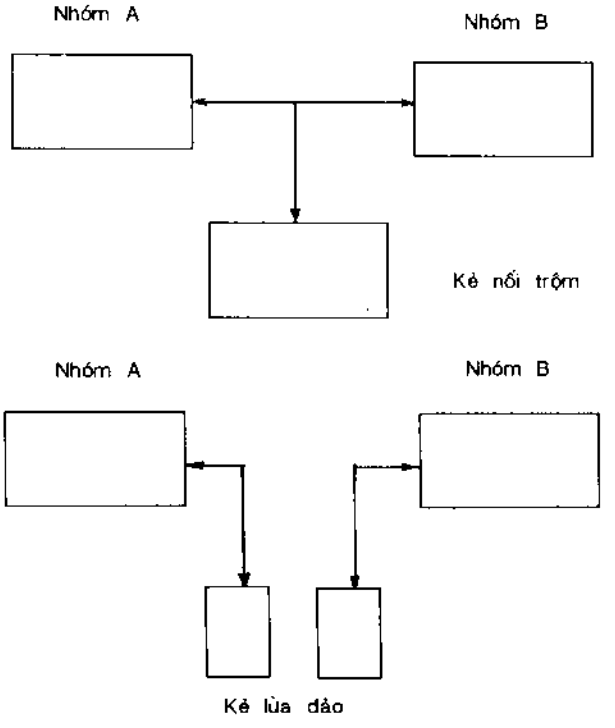
Một đối tượng lừa đảo chặn và sửa đổi sự truyền thông giữa các bên. Trong trường hợp này, xảy ra một chuỗi các sự kiện:

- Alice hỏi khóa mã công khai của Bob.
- Đối tượng lừa đảo chặn thông báo này lại, trả lại khóa mã công khai của anh ta là E_S cho Alice và sau đó gửi tiếp yêu cầu về khóa mã công khai của Bob.
- Alice gửi đi khóa DES K_A, khóa này được mã bằng E_S tới Bob và thông báo này thêm một lần nữa lại bị kẻ lừa đảo kia chặn lấy.
- Trong lúc ấy, Bob đáp lại yêu cầu về khóa mã công khai E_B khóa này lại bị kẻ lừa đảo giành lấy.
- Đối tượng lừa đảo giải mã $eE_S(K_A)$ bằng D_S và mã hóa khóa DES giống

hệt hoặc một khóa DES khác bằng khóa công khai E_B của Bob.

- Thông báo sau khi được mã hóa được gửi tới Bob.
- Alice và Bob bây giờ tiến hành liên lạc bằng một khóa hoặc nhiều khóa do kẻ lừa đảo cung cấp, kẻ đã chặn thông báo này và đọc hoặc sửa đổi chúng theo ý muốn.

Dù đối tượng lừa đảo chỉ hoạt động trong một khoảng thời gian hạn chế thì những nguy hiểm nghiêm trọng cũng có thể đổ lên đầu hai nhóm. Một dạng bảo vệ phòng chống lại những kẻ lừa đảo đòi hỏi hoặc một đường truyền thông riêng biệt trực tiếp hoặc các mật khẩu đã thỏa thuận được trao đổi qua một kênh an toàn. Các nhóm có thể xác thực các thông báo của họ và giữ lại dữ liệu xác thực. Nếu Bob xác thực khóa E_A và giữ khối xác thực thì sau đó Alice có thể thực hiện chức năng xác thực tương tự trên khóa thu được. Một cú điện thoại giữa hai nhóm để kiểm tra lại các khối xác thực sẽ phát hiện ra bất kỳ sự sửa đổi nào liên quan đến các khóa.



spoofing: *sự lừa đảo*. Kẻ nối trộm phải nối trộm vào kênh thông tin và giám sát lưu thông trên mạng trong khi kẻ lừa đảo tự chèn vào một kết nối sao cho các nhóm liên lạc vẫn có cảm giác liên lạc trực tiếp. Kẻ lừa đảo sẽ thử và dùng chung một khóa với nhóm A và khóa khác với nhóm B và như vậy phá vỡ an toàn truyền thông. Quá trình lừa đảo bỏ qua nhiệm vụ giải mã cực kỳ khó khăn lưu lượng qua mã thám, một vấn đề mà kẻ nối trộm phải đối mặt với dữ liệu mã hóa.

Nếu hai thành viên có các mật khẩu được trao đổi trước đó thì có thể phát hiện các hoạt động của đối tượng lừa đảo. Alice mã hóa mật khẩu P_A của cô bằng khóa hiện tại đang sử dụng để liên lạc với Bob, nhưng chỉ một nửa khối đã mã được gửi tới Bob. Cũng như vậy, Bob gửi đi một nửa khối đã mã của mật khẩu P_B. Khi hai nửa này đã được mỗi thành viên nhận thì họ gửi đi nửa thứ hai của khối mã, giải mã toàn bộ thông báo này và kiểm tra lại các mật khẩu đã chỉ định dùng trước đó.

Đối tượng lừa đảo, kẻ giải mã bằng một khóa và mã hóa lại thông báo bằng một khóa thứ hai để truyền tiếp nó đi, bây giờ lại ở tình thế khó khăn. Các nhóm *A* và *B* sẽ không truyền nửa thứ hai của các khối mật khẩu đã mã hóa cho đến khi họ nhận được nửa đầu từ nhóm kia. Tuy nhiên, đối tượng lừa đảo không thể giải mã và mã hóa lại một cách hợp lý các khối nửa thu được để phát nó đi tiếp, bất kỳ thông báo nào do kẻ lừa đảo truyền đi thay cho nửa khối đầu tiên cũng không thể ghép lại sau đó với nửa khối thứ hai để giải mã ra mật khẩu đã biết. *Xem* DES, Diffie-Hellman, technique, key-encryting key, public key cryptography. (3) Trong an toàn máy tính, đánh lừa là sự xui khiến cố tình một người sử dụng hoặc một tài nguyên để thực hiện một hoạt động không đúng. (4) Trong truyền dữ liệu, spufinh là một kỹ thuật cho phép vô số các máy tính trao đổi với hàng loạt các thiết bị đầu cuối. Các bộ mô phỏng phần mềm chạy trên các bộ vi xử lý trong các mạch ghép nối kênh sẽ lập thành mạng mà xuất hiện trước các thiết bị đầu cuối như một kiểu máy tính sở hữu của chính nó, còn các thiết bị đầu cuối xuất hiện trước các máy tính như một kiểu thiết bị đầu cuối sở hữu của chính nó. *Xem* channel, emulator, software.

spoofing program ***chương trình lừa mật khẩu*** Trong an toàn máy tính, một đoạn mã có ác ý mà giả dạng như hệ điều hành, đưa ra màn hình đăng nhập hệ thống và đánh lừa người sử dụng nhập vào các mật khẩu của họ để khám phá ra các mật khẩu đó. *Xem* malicious code.

pray paint ***sơn phun, vẽ hoa*** Trong an toàn dữ liệu, một kỹ thuật sử dụng các tổng kiểm tra mật mã để đảm bảo rằng, sự phân loại an toàn, hoặc dữ liệu, của một bản ghi cơ sở dữ liệu không thể bị sửa đổi bởi một kẻ tấn công mà không bị phát hiện. Một MAC được tính toán cho thông báo gồm bản ghi và phân loại của nó, nhờ sử dụng một khóa bí mật. Kỹ thuật này cũng đã được đặt tên như vậy bởi vì một bản ghi được tô màu không thể tẩy xóa được cùng với phân loại của nó. *Xem* MAC. *Đồng nghĩa với* integrity locking.

spurious association initiation ***(sự) khởi đầu kết hợp sai*** Trong an toàn tuyền thông, sự tấn công trong đó các PDU (đơn vị dữ liệu giao thức) từ một thông báo hợp pháp trước đây sẽ được quay lại (nghe lại), hoặc là từ một sự liên kết được thiết lập dưới một đặc tính nhận dạng sai. *So sánh với* denial of message service, message stream, modification. *Xem* PDU, replay.

spurious key decipherment ***giải mã bằng khóa không xác thực*** Trong mật mã, một thông báo đủ nghĩa, do quá trình giải mã tạo ra trên một bản đã mã cho trước, nó có thể hoặc không khác với một thông báo có đủ nghĩa khác được sinh ra từ sự giải mã một bản mã tương tự bằng một khóa khác. Nếu phép giải mã thông báo đã mã C_1 bằng khóa K_1, sinh ra một thông báo có nghĩa P_1, thì thông báo P_2 được giải mã bằng khóa không xác thực được tạo ra bằng cách giải mã C_1 bằng một khóa khác là K_2: P_2 có thể giống hệt như P_1. *Xem* cryptographic key. *Đồng nghĩa với* false solution.

SPX ***đơn công*** *Xem* simplex.

Spyer ***virut Spyer*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào các tệp COM, EXE, OVL, ảnh hưởng tới hoạt động trong thời gian chạy, làm sai lạc các tệp chương trình và OVL. *Xem* virus names.

SRN ***số tham chiếu hệ thống, SRN*** Trong hoạt động ngân hàng, viết tắt của System Reference Number, một số nhận dạng thông báo bên trong một dịch vụ. *Đồng nghĩa với* SSN.

SSN ***số thứ tự hệ thống, SSN*** Trong hoạt động ngân hàng, cụm từ viết tắt của System Sequence Number. *Đồng nghĩa với* SRN.

SSO *Xem* system security officer.

stack ***ngăn xếp*** Trong tính toán, một cấu trúc mà các mục được thêm vào cuối của một danh sách nối tiếp và chỉ có thể được lấy lại được từ điểm cuối tương ứng. Như vậy chiến lược LIFO được áp dụng. *So sánh với* queue. *Xem* LIFO.

stack pointer ***con trỏ ngăn xếp*** Trong tính toán, một vị trí nhớ lưu giữ địa chỉ của hầu hết các mục được cất giữ gần nhất trong ngăn xếp. *Xem* stack.

Staf ***virut Staf*** Trong an toàn máy tính, một virut kết thúc và nằm thường trú, nó lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng đến hoạt động trong thời gian chạy, ngắt chương trình, các tệp OVL và các liên kết tệp. *Xem* virus names.

stale message ***thông báo nhàm chán, thông báo cũ*** *Đồng nghĩa với* replay.

standards ***(các) chuẩn*** Trong an toàn dữ liệu, các phương pháp và giao thức chung để bảo vệ dữ liệu, cho phép trao đổi dữ liệu an toàn giữa các nhóm có thể không thuộc cùng một tổ chức. Các chuẩn an toàn dữ liệu bao hàm các thuật toán mật mã, chế độ sử dụng các thuật toán như vậy và truyền thông các thông báo bí mật. Các tổ chức có liên quan tới các chuẩn an toàn dữ liệu gồm có Ủy ban tiêu chuẩn viễn thông quốc tế, NIST, NSA, ANSI, BSI, DIN, AFNOR và ISO. Một tiểu ban đặc biệt của ISO là TC97/SC20, đã thiết lập các chuẩn an toàn dữ liệu. DES được thông qua bởi chính phủ Mỹ như một chuẩn cho mã hóa dữ liệu đối xứng và sau đó đã được chấp nhận như chuẩn quốc gia của Mỹ và được gọi là Thuật toán mã dữ liệu (Data Encryption Algorithm). Thêm vào các chuẩn cho các thuật toán mã hóa là các yêu cầu đối các chuẩn dựa trên chế độ sử dụng các thuật toán này, ví dụ ECB, CBC, CFB và OFB. Các chế độ sử

dụng này được đề cập tới trong Chuẩn xử lý thông tin Liên bang (1980) và Chuẩn quốc gia của Mỹ (1983). Kiến trúc OSI cung cấp một chuẩn truyền dữ liệu và vai trò của mật mã bên trong kiến trúc đó cũng là chủ đề đối với một chuẩn. Chuẩn viễn thông Liên bang 1026 đưa ra định nghĩa rõ ràng về việc thực hiện mã hóa ở tầng vật lý, còn ANSI đưa ra một chuẩn định nghĩa sự thực hiện tại tầng vật lý và tầng liên kết dữ liệu. Trong lĩnh vực ngân hàng, chuẩn X9.8 của ANSI mô tả sự quản lý các PIN, chuẩn X9.9 giải quyết việc ứng dụng DES để xác thực các thông báo tài chính, còn chuẩn X9.17 đề cập tới quản lý khóa liên quan đến giao dịch buôn bán qua ngân hàng. Chuẩn viễn thông Liên bang 1027 xác định các yêu cầu về an toàn vật lý đối với các thiết bị sử dụng DES. *Xem* AFNOR, ANSI, ANSI X9.8 - 1982, ANSI X9.9 - 1986, ANSI X9.17 - 1985, BSI, CBC, CFB, data link layer, DIN, ECB, FIPS, NIST, NSA, OFB, OSI security, physical layer.

standby ***(chế độ) dự phòng*** Trong lĩnh vực độ tin cậy, một điều kiện để có thể bắt đầu lại hoàn toàn sự hoạt động ổn định trong một thời gian ngắn. *Xem* cold standby, warm standby, hot standby.

standby equipment ***thiết bị dự phòng*** Trong lĩnh vực độ tin cậy, một hệ thống nhân đôi (bản sao) được sử dụng nếu khối chính không hoạt động được do có sự trục trặc. *Xem* standby.

standby facility ***phương tiện dự phòng*** Trong quản lý rủi ro, một phương tiện không làm gì cho đến khi thiết bị chính bị mất. Có thể có một vài sự thay đổi bao gồm một thiết bị thực hiện một công việc có tính thủ tục sẵn sàng tiếp quản trong tình trạng khẩn cấp.

star ***mạng hình sao*** Trong truyền dữ liệu, một cấu trúc liên kết mạng trong đó, mỗi nút chỉ kết nối với một bộ điều khiển trung tâm. Mạng này thường được áp dụng khi một số các thiết bị đầu cuối được kết nối với máy tính chủ đơn lẻ và phần lớn việc giao lưu thông tin có liên quan đến truyền thông giữa máy chủ với thiết bị đầu cuối hơn là giữa thiết bị đầu cuối với thiết bị đầu cuối. Tuy nhiên, cấu trúc liên kết này có một số nhược điểm sau:

- một ngắt hỏng tại máy chủ sẽ làm phá vỡ hết tất cả giao lưu thông tin;
- thông lượng bị hạn chế bởi khả năng của máy chủ;
- giá thành chi phí cho việc mua cáp nối và nối cáp rất cao;
- không có tuyến thay phiên nhau trong trường hợp đường dây giữa máy chủ và thiết bị đầu cuối bị hỏng.

So sánh với ring. *Xem* local area network.

Star Dot ***virut Star Dot*** Trong an toàn máy tính, một virut kết thúc và nằm thường trú, lây nhiễm sang các tệp COM, ảnh hưởng đến hoạt động trong thời gian chạy, ngắt chương trình, các tệp OVL và các liên kết tệp. *Xem* virus names.

star property ***thuộc tính sao*** Trong an toàn máy tính, một quy tắc của mô hình an toàn Bell-La Padula cho phép một chủ thể truy nhập ghi lên một đối tượng chỉ khi mức an toàn của chủ

thể trội hơn mức an toàn của đối tượng. *Xem* Bell-la Padula model, dominate, object, security level, subject. *Đồng nghĩa với* confinement property, star security property.

star security property ***thuộc tính an toàn sao*** *Đồng nghĩa với* star property.

start bit ***bit khởi đầu*** Trong các mã, một bit được sử dụng để truyền không đồng bộ, nó đứng trước một ký tự nối tiếp và báo hiệu bắt đầu của ký tự đó. *So sánh với* stop bit. *Xem* asynchronous transmission.

start element ***phần tử khởi đầu*** *Xem* start bit.

start of header ***(ký tự) bắt đầu phần tiêu đề*** Trong truyền thông dữ liệu, một ký tự điều khiển được đặt ngay đầu của một dãy các ký tự, tạo thành thông tin về địa chỉ hoặc thông tin về lộ trình cho thông báo. *Xem* header.

start of text ***(ký tự) bắt đầu văn bản*** Trong truyền thông dữ liệu, một ký tự điều khiển truyền báo kết thúc phần tiêu đề của thông báo và chỉ ra rằng, các ký tự kế tiếp liên quan đến phần văn bản của thông báo. *So sánh với* end of text.

start-stop envelope ***nhóm (ký tự) khởi-ngừng*** Trong truyền dữ liệu, một chuỗi các phần tử dữ liệu bao gồm các phần tử bắt đầu, dữ liệu nhị phân, và các phần tử kết thúc sử dụng trong liên lạc không đồng bộ. Nhóm ký tự có thể tới đích bất kỳ lúc nào, bên thu giữ nguyên ở chế độ rỗi cho đến khi phần tử bắt đầu tới đích và trở lại chế độ rỗi sau khi nhận được phần tử kết thúc. *Xem* asynchronous transmission, start bit, stop bit.

state ***trạng thái*** Trong toán học, một khái niệm trừu tượng chỉ ra toàn bộ lịch sử của một hệ thống, thường dưới dạng các biến trạng thái.

statement ***câu lệnh*** Trong tính toán, một biểu thức có đủ ý nghĩa được sử dụng để xác định một thao tác và thường hoàn thành trong ngữ cảnh của ngôn ngữ được sử dụng.

static analysis ***phân tích tĩnh*** Trong an toàn máy tính, một phương pháp phân tích phần mềm mà trong đó mã nguồn được phân tích mà không cần thi hành nó. Các công cụ phần mềm cho phân tích tĩnh được phân loại:

- phân tích mã;
- phân tích cấu trúc;
- phân tích giao diện của mođun;
- phân tích trình tự các sự kiện.

Phân tích mã là sự kiểm tra cú pháp của mã nguồn mà có hiệu lực trong quá trình biên dịch. Việc kiểm tra như vậy có thể phát hiện ra các lỗi lập trình, chẳng hạn, các biến được sử dụng nhưng không được khởi tạo hoặc các biến được khởi tạo nhưng không sử dụng tới. Việc kiểm tra như vậy được thực hiện qua nhiều trình biên dịch mới, nhưng nó có ích đối với phần mềm được phát triển dưới các trình biên dịch kém hơn và cũ hơn.

Việc phân tích cấu trúc có thể được sử dụng để phát triển các lược đồ của chương trình, phát hiện ra các thiếu sót chẳng hạn như những chỗ lồng nhau không chính xác của các vòng lặp, các nhãn không được tham chiếu và các câu

lệnh không thể tìm thấy. Việc phân tích giao diện modun kiểm tra những sai sót về ngữ nghĩa vượt qua ranh giới; việc phân tích này có thể phát hiện các mâu thuẫn trong việc sử dụng các tham số và các cấu trúc dữ liệu toàn cục.

Việc phân tích trình tự các sự kiện xem xét các sự kiện đã xác định để đảm bảo rằng, chúng tuân theo một theo trình tự đúng, ví dụ quá trình mở, ghi và đóng một tệp. *So sánh với* dynamic analysis. *Xem* compiler, complexity analysis, control flow analysis, data flow analysis, pattern directed analysis, global, label, software tool.

static data ***dữ liệu tĩnh*** Trong hoạt động ngân hàng, dữ liệu không bị thay đổi thường xuyên, ví dụ các chi tiết về khách hàng, trái ngược với các chi tiết liên quan đến các cuộc giao dịch.

static dump ***kết xuất tĩnh*** Trong tính toán, một kết xuất được thực hiện tại một điểm đặc biệt tại thời điểm liên quan tới một hoạt động của máy, ví dụ tại điểm kết thúc hoạt động của máy. *Xem* dump.

static evaluation ***đánh giá tĩnh, ước lượng tĩnh*** Trong an toàn máy tính, sự xem xét chi tiết và phân tích tài liệu và mã của hệ thống để phát hiện các "bẫy" cố ý hoặc các sửa đổi trái phép. Các kỹ thuật thường được sử dụng trong đánh giá tĩnh bao gồm: duyệt lại mã, nghiên cứu quá trình thâm nhập và các bộ phân tích mã nguồn. *So sánh với* dynamic testing. *Xem* code review, penetration study, source code analyzer.

station ***trạm*** Trong truyền dữ liệu, một vị trí vào và ra của một hệ thống truyền thông, nó bao gồm các nguồn và các nơi chứa các thông báo và các phần tử điều khiển luồng thông báo trên các liên kết.

statistical database ***cơ sở dữ liệu thống kê*** Trong an toàn cơ sở dữ liệu, một cơ sở dữ liệu chứa thông tin tổng hợp liên quan tới các tập con lớn chứa các thực thể, ví dụ dữ liệu điều tra dân số. Dữ liệu như vậy có thể được một kẻ tấn công sử dụng để phát hiện thông tin liên quan tới các cá nhân trừ khi một trong các kỹ thuật kiểm soát suy luận được áp dụng. *Xem* data protection, inference control.

statistically unique ***duy nhất thống kê*** Trong hoạt động ngân hàng, nói tới một tình huống có xác xuất thống kê thấp chấp nhận được của một mục (ví dụ khóa hoặc mã) bị nhân đôi do ngẫu nhiên hoặc có mục đích.

statistical time division multiplexing ***dồn kênh phân thời thống kê, ghép kênh phân thời thống kê*** Trong truyền dữ liệu, một dạng của dồn kênh phân thời trong đó các khe thời gian chỉ được cấp phát cho các thiết bị đầu cuối hoạt động. Kỹ thuật này làm tăng số các thiết bị đầu cuối có thể kết nối với các kênh có dung lượng cho trước. Một bộ nhớ đệm tập hợp dữ liệu và thường vừa đủ để cất các ký tự kênh nếu lưu lượng trên kênh tạn thời vượt quá tốc độ liên kết dữ liệu của bộ dồn kênh. *Xem* multiplexer, time division multiplexing.

statmux ***dồn kênh phân thời thống kê*** *Xem* statistical time division multiplexing.

status poll ***thăm dò trạng thái*** Trong tính toán, một yêu cầu thông tin do một máy tính đề xuất về trạng thái hiện tại của một thiết bị đầu cuối. *Xem* polling.

STDM *Xem* statistical time division multiplexing.

Stealth virus ***virut Stealth*** Trong an toàn máy tính, một virut tìm kiếm và che dấu sự hiện diện của nó bằng cách chiếm quyền kiểm soát của máy tính. *Xem* virus.

ST&E *Xem* security test and evaluation.

steganography ***nguỵ trang ký*** Trong an toàn dữ liệu, việc che dấu sự tồn tại của các thông báo, thực chất là ghi phủ lên. Trong an toàn máy tính, quá trình này tạo nên một dạng lấp đầy vào các chỗ trống giữa thông báo bằng các ký tự đệm. Như vậy, mặc dù sự tồn tại của liên kết truyền thông không che dấu được, kẻ tấn công vẫn không nhận được thông tin ngay khi các thông báo đang được phát đi. *So sánh với* cryptography.

ST&E tools and equipment ***(các) công cụ và thiết bị ST&E*** Trong an toàn máy tính, các kỹ thuật chuyên dụng, các thủ tục, các tiêu chí, các chuẩn, các chương trình, hoặc thiết bị được các nhân viên ST&E (kiểm tra và đánh giá tính an toàn) có đủ trình độ chuyên môn chấp nhận để dùng cùng cách thức hoặc chuẩn trong kiểm tra và đánh giá các tính năng an toàn của hệ thống hoặc các mạng ADP. *Xem* ST&E.

STI *Xem* scientific and technical information.

Stone-90 ***virut Stone-90*** Trong an toàn máy tính, một virut lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động trong thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

Stoned ***virut Stoned*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm đến cung khởi động của đĩa mềm và bảng phân hoạch đĩa cứng, ảnh hưởng tới hoạt động thời gian chạy, ngắt cung khởi động và các liên kết tệp. *Xem* virus names.

stop-and-wait protocol ***giao thức dừng và đợi*** Trong truyền dữ liệu, một thuật toán kiểm soát luồng trong đó máy chủ phát chờ đợi tín hiệu báo nhận từ máy chủ thu, để thu được các khung không có lỗi trước khi phát tiếp các khung khác. *So sánh với* sliding window protocol. *Xem* frame, host.

stop bit ***bit dừng*** Trong các mã, một bit được sử dụng trong liên lạc không đồng bộ (dị bộ), chỉ vị trí kết thúc một ký tự. *So sánh với* start bit. *Xem* asynchronous transmission. *Đồng nghĩa với* caboose.

stop element ***phần tử dừng*** *Xem* stop bit.

storage object ***đối tượng lưu trữ*** Trong an toàn máy tính, một đối tượng hỗ trợ cả truy nhập đọc lẫn truy nhập ghi. *Xem* object, read access, write access.

storage protection ***bảo vệ bộ nhớ*** *Xem* memory protection.

store and forward ***lưu và chuyển tiếp, nhớ và chuyển tiếp*** Trong

truyền dữ liệu, một hệ thống cất giữ các gói thông báo tại các điểm trung gian trước khi truyền đi tiếp. *Xem* computer network, packet, message switching.

stream cipher ***mã pháp dòng, mã dòng*** Trong mật mã, một phương pháp mã hóa có khả năng cung cấp độ mật hoàn hảo. Các bản gốc (bản rõ) được mã hóa thành các số, thường là số nhị phân, và một dòng khóa các số gần ngẫu nhiên được kết hợp với bản gốc để tạo thành bản mã. Phía thiết bị thu được cung cấp một dòng khóa các số ngẫu nhiên giống hệt và kết hợp đảo ngược bản mã và dòng khóa để tìm ra bản gốc. Nếu dòng khóa là các số nhị phân được cộng modulo 2 với bản gốc thì thao tác mã hóa và giải mã là hoàn toàn giống nhau.

Kỹ thuật này không đòi hỏi bản gốc phải chia thành các khối, với kích thước khối do người thiết kế thuật toán mã hóa xác định, bản gốc có thể được mã hóa theo các đoạn có chiều dài mong muốn bất kỳ theo từng bit một. Vì vậy nó có giá trị trong các hệ thống truyền nơi mà các thông báo cần được mã hóa theo từng ký tự, hoặc thậm chí theo từng bit.

Nhược điểm chủ yếu trên thực tế của kỹ thuật này là việc yêu cầu truyền an toàn các dòng khóa có cùng chiều dài như các thông báo giữa bên phát và bên thu. Trong thực tế, một khóa bí mật ngắn hơn được sử dụng để tạo ra các dòng bit giả ngẫu nhiên ở bên phát và bên thu. Để tránh sự nhầm lẫn có thể về thuật ngữ giữa khóa bí mật và dòng khóa được tạo ra, thuật ngữ dòng bit mật mã thông thường được sử dụng để mô tả dòng các chữ số nhị phân ngẫu nhiên do bộ tạo mã tạo ra.

Nếu một kẻ tấn công có thể giành được quyền truy nhập tới một phần của bản rõ P, và với bản mã C tương ứng, thì dòng bit mật mã KS phải sử dụng để mã hóa bản gốc có thể dễ dàng được xác định. Ví dụ, nếu phép cộng modulo 2 được sử dụng để tạo ra bản mã từ bản gốc và dòng bit mật mã thì:

$C = P +_2 KS$. Do đó $KS = C +_2 P$.

Rõ ràng là, dòng bit mật mã giống nhau không được sử dụng để mã hóa các thông báo khác nhau. Nếu dòng bit mật mã được tạo ra bởi một thuật toán dựa trên một khóa bí mật thì nó phải đảm bảo rằng, việc biết một đoạn dòng bit mật mã không thể sử dụng được để xác định các đoạn khác; hơn nữa, dòng bit mật mã phải được tạo ra từ các điều kiện ban đầu khác nhau để cho dòng bit mật mã không được lặp lại trong lần gọi kế tiếp của thuật toán.

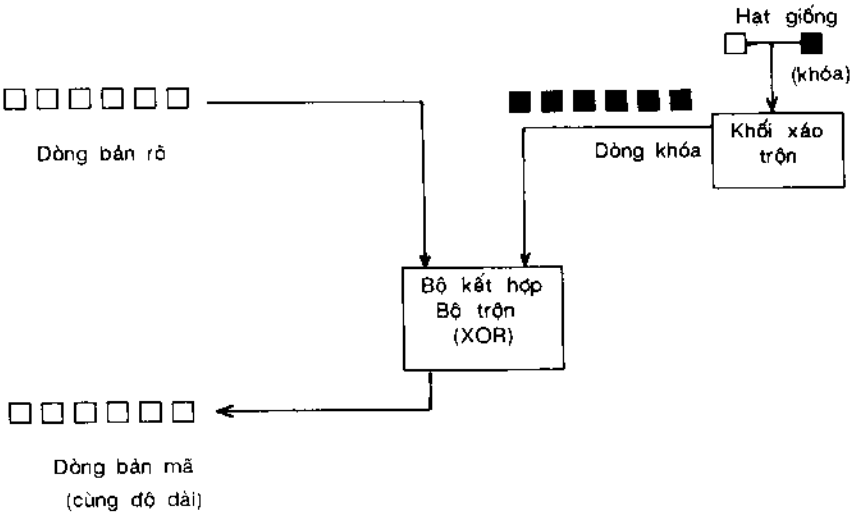
Điều kiện khởi tạo thường được xác định bởi vectơ khởi tạo IV. Vectơ này được phát đi ở dạng rõ như một lời tựa của thông báo. Nói chung IV không được lặp lại trong các thông báo tiếp theo vì bất kỳ sự lặp lại nào sẽ sinh ra các dòng bit mật mã giống hệt nhau. Nếu các bản gốc được tạo dạng ở mức độ cao thì một kẻ tấn công có thể thu thập các đoạn bản gốc/bản mã cho mỗi IV. Giả sử rằng IV chỉ gồm 1 byte, thì kẻ tấn công có thể phát triển 256 sổ mã (từ điển mã) cho cặp bản gốc/bản mã.

IV được sử dụng để tạo ra một khối bản mã, mà một phần hoặc toàn bộ khối

đó được chọn như làm đoạn đầu tiên của dòng bit mật mã. Sự phản hồi từ dòng bit mật mã, bản gốc, bản mã hoặc tổ hợp giữa chúng sau đó được sử dụng để tạo điều kiện khởi tạo cho quá trình tạo ra đoạn thứ hai của dòng bit mật mã.

Các đặc tính mở rộng lỗi của mã pháp phụ thuộc vào số lượng được chọn cho sự phản hồi. Nếu chỉ chọn riêng dòng bit mật mã để phản hồi thì sẽ không có mở rộng lỗi. Trong trường hợp này, mã pháp cung cấp không theo dạng xác thực nào: một kẻ tấn công có thể sửa đổi bản mã và tạo ra những sự thay đổi giống hệt nhau trong bản mã thu được tương ứng. Sự phản hồi từ bản gốc và bản mã sẽ tạo nên mức độ mở rộng lỗi mà ít nhất cũng báo rằng, bản mã thu được là không đồng nhất với bản mã được phát đi. *So sánh với* block cipher, block cipher chaining. *Xem* authentication, cryptographic bit stream, cipher block chaining, cipher feedback, error extension, initialization vector, key stream, modulo arithmetic, perfect secrecy, Vernam cipher.

stream cipher chaining ***liên kết mã dòng, móc xích mã dòng*** Trong mật mã, một mã pháp dòng dùng mạch phản hồi để tạo ra một dòng bit mật mã. Các mã dòng mà sử dụng một dòng bit mật mã độc lập với bản mã sẽ không làm mở rộng lỗi mà cũng không có sự tự đồng bộ. Nếu dòng bit mật mã độc lập với bản mã được phát đi thì một kẻ tấn công có thể tác động trực tiếp lên bản gốc thu được, theo từng bit. Việc sử dụng phản hồi từ bản mã để tạo ra dòng bit mật mã đảm bảo rằng, sự thay đổi của một bit trong bản mã, hoặc ngẫu nhiên hoặc chủ ý gây ra, làm ảnh hưởng đến hơn một bit trong bản gốc thu được, như vậy cung cấp dấu hiệu về sự thay đổi bản mã. Các mã dòng không có phản hồi, bản rõ hoặc bản mã cũng không cung cấp khả năng khôi phục lỗi. Khi có một lỗi trong quá trình



stream cipher: *mã dòng.*

xử lý mã dẫn đến sự khác nhau giữa các dòng bit mật mã tại các bên phát và thu. Sự liên kết trong các mã dòng có thể sinh ra mức độ tự đồng bộ cần thiết. *So sánh với* block cipher chaining, output feedback. *Xem* cipher feedback, cryptographic bit stream, error extension, self-synchronizing, stream cipher.

strength ***độ bền*** Trong quản lý khóa, một đặc tính của một quá trình sinh khóa. Nếu độ bền của một quá trình sinh khóa tối thiểu bằng độ bền của khóa nhận được được dùng thì việc tấn công vào quá trình sinh khóa không có lợi thế gì hơn thuật toán mã hóa tương ứng. *Xem* cryptographic key, key generation.

Stricker ***virut Stricker*** Trong an toàn máy tính, một virut lây nhiễm đến các tệp COM, ngắt cung khởi động, các tệp dữ liệu, các liên kết tệp, ảnh hưởng đến hoạt động trong thời gian chạy. *Xem* virus names.

string ***xâu, chuỗi, dòng (ký tự)*** Trong tính toán, một dãy các ký tự mà có thể tương ứng với thông báo nguyên bản.

stripe reader ***bộ đọc sọc từ, bộ đọc vạch từ*** Trong tính toán, một thiết bị đọc dữ liệu được mã hóa trên vạch từ của các thẻ tín dụng và đưa thông tin vào máy tính. *Xem* magnetic stripe card.

stripping ***bóc, gỡ, mở (thư)*** Trong truyền dữ liệu, việc xử lý trích các phần tử thông tin chủ yếu của một thông báo bằng cách loại bỏ các phần tiêu đề và phần đuôi của phong bì thông báo. *Xem* header, tail.

strong intersymbol dependence ***(sự) phụ thuộc liên ký hiệu mạnh*** Trong mật mã, một thuộc tính của phép mã khối trong đó, mỗi bit của khối đầu ra là một hàm đủ phức tạp của mỗi bit của khối đầu vào và khóa. Một thông báo DES chứa một khối 64 bit đơn sẽ tạo ra sự phụ thuộc liên ký hiệu bền vững. *So sánh với* intersymbol dependence. *Xem* DES.

structural redundancy ***dư thừa cấu trúc*** Trong lĩnh vực độ tin cậy, một dạng dư thừa phần cứng được cung cấp ở vị trí cổng, nơi thiết lập nhiều tuyến song song giữa đầu vào và đầu ra. *So sánh với* modular redundancy.

structure analysis ***phân tích cấu trúc*** *Xem* static analysis.

STU-III ***hệ thống STU-III*** Trong an toàn truyền thông, một hệ thống điện thoại mật sử dụng mật mã khóa điểm tới điểm. *Xem* end-to-end encryption, secret key encryption.

stub ***công cụ mẫu, stub*** Trong tính toán, một công cụ thường là phần mềm, có thể sử dụng để mô phỏng hoạt động của các bộ phận của một hệ thống. Nó thường được sử dụng trong phần mềm kiểm tra dựa trên các bộ phận này của hệ thống được mô phỏng qua công cụ mẫu. Các stub khiến có thể kiểm tra một hệ thống trước khi tất cả các bộ phận của nó được hoàn thành.

STX *Xem* start of text.

subject ***chủ thể*** Trong an toàn máy tính, một thực thể tích cực, nhìn chung dưới dạng một người, một tiến trình, hoặc một thiết bị mà làm cho thông tin chảy giữa các đối tượng hoặc làm thay

đổi trạng thái của hệ thống. *So sánh với* object.

subject security level ***mức an toàn chủ thể*** Trong an toàn máy tính, một mức an toàn chủ thể ngang bằng với mức an toàn của các đối tượng. Nó có cả quyền truy nhập đọc lẫn quyền truy nhập ghi lên đó. Mức an toàn chủ thể phải luôn luôn trội hơn mức truy nhập của người sử dụng mà chủ thể được liên kết tới. *Xem* dominate, security level, subject.

sub-key ***khóa con*** (1) Trong mật mã, một khóa 48 bit, được tạo ra từ khóa mật mã 56 bit, được sử dụng cho một trong 16 vòng của phép mã và giải mã DES. *Xem* cryptographic key, data encryption standard. (2) Trong an toàn cơ sở dữ liệu, một dạng mã hóa hướng bản ghi. Bản ghi được mã là một hàm đơn trị của tất cả các giá trị của các trường của nó; mỗi trường được mã hóa/giải mã bằng một khóa riêng biệt. Mỗi khóa giải mã của mỗi trường chỉ dùng để giải mã trường tương ứng trong bản ghi.

Subliminal ***virut Subliminal*** Trong an toàn máy tính, một virut kết thúc và thường trú, lây nhiễm các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động trong thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

subroutine ***chương trình con, thủ tục con*** Trong tính toán, một dãy liên tiếp các chỉ thị lệnh để thực hiện một hành động thường được đòi hỏi trong một chương trình hoặc một tập hợp các chương trình, chẳng hạn, để sắp xếp một tập các xâu theo thứ tự bảng chữ cái.

subschema ***lược đồ con*** Trong cơ sở dữ liệu, cái nhìn tổng quan về dữ liệu của người lập trình ứng dụng hoặc của người sử dụng. *Xem* schema.

subscriber's unit ***đơn vị thuê bao*** *Đồng nghĩa với* authorized access control switch.

subset ***tập con*** Tập hợp các phần tử, mỗi phần tử là một thành viên của một tệp cho trước khác. *Xem* set.

substantive testing ***phép kiểm tra trọng yếu, phép kiểm tra tổng thể*** Trong an toàn máy tính, công việc kiểm tra một khối lượng lớn các giao dịch, để kiểm toán viên có thể xác minh rằng, các giao dịch đó là đúng. Thường được thực hiện khi phép kiểm tra tính phù hợp sẽ cho thấy các khuyết điểm trong hệ thống. *Xem* compliance testing.

substitute character ***ký tự thay thế*** Trong các mã, một ký tự điều khiển thay cho một ký tự bị xem là sai, hoặc không thể biểu thị được trên một thiết bị có sẵn.

substitution box ***hộp thay thế*** *Đồng nghĩa với* S box.

substitution cipher ***mã pháp thay thế*** Trong mật mã, một mã pháp trong đó mỗi ký tự hoặc một nhóm cố định các ký tự được thay thế bằng ký tự khác hoặc nhóm các ký tự khác. *So sánh với* transposition cipher. *Xem* cipher, cryptography, monoalphabetic cipher, polyalphabetic cipher.

summary processing ***quá trình giản lược*** Trong tính toán, một quá trình

xử lý dư thừa nhờ sử dụng một giá trị tổng kết thực. Quá trình này được so sánh bằng với một tổng kiểm tra xuất phát từ việc xử lý các mục chi tiết. *Xem* redundant processing.

summation check ***kiểm tra tổng số*** Trong các mã, một phép kiểm tra dựa trên việc so sánh tổng các chữ số của một số với giá trị được tính trước đó để chỉ ra bất kỳ sự thay đổi tình cờ nào trong giá trị của một chữ số trong khi truyền hoặc sao chép lại. *Xem* check sum, redundancy checking.

Sunday ***virut Sunday*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào các tệp COM, EXE, OVL, ảnh hưởng tới hoạt động trong thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

supercomputer ***siêu máy tính*** Trong tính toán, một máy tính lớn có năng lực tính toán vô cùng lớn được sử dụng để tính toán các bài toán có độ phức tạp lớn đòi hỏi tốc độ và dung lượng bộ nhớ lớn, ví dụ như dự báo thời tiết.

superencipherment ***siêu mã*** (1) Trong mật mã, một phương pháp mã bội. *Xem* multiple des encipherment. (2) Trong an toàn dữ liệu, một kỹ thuật trong đó, một thông báo gốc trước hết được mã hóa, tức là mỗi câu hoặc một cụm từ được thay đổi thành một mã được lựa chọn trước, sau đó thông báo đã mã hóa này lại được mã hóa. *Xem* cipher, code, cryptography.

superimposed circuit ***mạch chồng chập*** *Đồng nghĩa với* superposed circuit.

superincreasing series ***dãy siêu tăng*** Trong toán học, dãy các số nguyên mà mỗi số hạng lớn hơn tổng của tất cả các số hạng đứng trước đó. Vì vậy, với một tập các số nguyên có thứ tự $(a_1, a_2, ..., a_n)$ đối với mỗi số hạng thì: $a_j > \sum_{i=1,j-1} a_i$. *Xem* knapsack cipher.

superposed circuit ***mạch chồng chập*** Trong truyền thông, một kênh phụ nhận được từ một hoặc nhiều mạch, thông thường được cung cấp cho các kênh khác, theo cách để tất cả các kênh có thể được sử dụng đồng thời mà không gây trở ngại cho nhau. *Đồng nghĩa với* superimposed circuit.

supersmart card ***thẻ siêu thông minh*** Trong kiểm soát truy nhập, một dạng nâng cao của thẻ thông minh có bàn phím thu nhỏ và màn hình hiển thị bên trong. Thẻ siêu thông minh này có độ an toàn cao hơn thẻ thông minh thông thường, là loại thẻ phải dựa vào bàn phím và màn hình hiển thị trên bộ đọc thẻ thông minh. Nếu thiết bị đọc thẻ thông minh bị sửa đổi bất hợp pháp thì người sử dụng không thể chắc chắn rằng các thông báo được hiển thị có phản ánh đúng hoạt động giao dịch hay không, và các phím được ấn xuống có gửi các tín hiệu tương ứng với các phím đó không, hoặc là PIN của thẻ không bị lấy trên đường tới thẻ thông minh. Vì vậy người sử dụng có thể chủ tâm:

- cho phép một giao dịch tài chính khi giá trị thực của giao dịch khác với giao dịch đang được hiển thị;
- hủy bỏ một giao dịch nhưng sự hủy bỏ đó không được ghi nhận lại như một một sự cho phép;
- làm lộ PIN của thẻ.

So sánh với smart card. *Đồng nghĩa với* intelligent terminal.

superuser ***người dùng siêu đặc quyền*** Trong an toàn máy tính, người quản trị hệ thống trong hệ thống Unix, người có đặc quyền truy nhập rộng rãi tới hệ thống, các tệp của người sử dụng và các lệnh. *Xem* UNIX.

supervised line ***kênh được giám sát*** Trong an toàn vật lý, một đường dây phải chịu sự theo dõi giám sát.

supervised system ***hệ thống được giám sát*** Trong an toàn vật lý, một hệ thống sẽ khởi đầu một tín hiệu báo hỏng hóc khi việc truyền một tín hiệu cảnh báo có thể bị ngăn chặn lại bởi sự hỏng hóc, hoặc bị chập đất trên đường dây. *Xem* alarm signal, trouble signal.

supervision ***(sự) giám sát*** Trong an toàn vật lý, việc bảo vệ bằng điện một dây dẫn nối giữa các điểm xác định. Một thay đổi trong mạch chẳng hạn như ngắt, nối chéo, tăng hoặc giảm dòng điện hoặc điện trở sẽ khởi tạo một tín hiệu báo động. *Xem* alarm signal, supervised system.

supervisor state ***trạng thái giám sát*** *Đồng nghĩa với* executive state.

supervisory sequence ***dãy giám sát*** Trong truyền dữ liệu, một dãy các ký tự điều khiển thực hiện một chức năng kiểm soát định trước.

supervisory signal ***tín hiệu giám sát*** (1) Trong truyền thông, một tín hiệu chỉ ra có mạch nào đang được sử dụng hay không. (2) Trong truyền thông, một tín hiệu được sử dụng để chỉ ra các trạng thái hoạt động khác nhau của các tổ hợp mạch.

superzapping ***(quá trình) xóa mức cao, siêu xóa*** (1) Trong an toàn dữ liệu, nói tới các hoạt động lạm dụng chương trình truy nhập chung của máy tính để mà bỏ qua sự sắp đặt an toàn thông thường và cho phép một kẻ tấn công tiến hành các sửa đổi không hợp pháp đối với các chương trình hoặc dữ liệu. (2) Trong tính toán, một quá trình sửa đổi một chương trình bằng cách thay đổi trực tiếp tới đối tượng và mã máy. *Xem* patch. (3) Trong an toàn máy tính, một chương trình tiện ích được thiết kế để các thao tác viên của hệ thống sử dụng trong tình trạng khẩn cấp. Chương trình này bỏ qua các kiểm soát an toàn thông thường và có thể xóa thông tin. (4) Trong an toàn máy tính, nói tới việc sử dụng một chương trình tiện ích ZAP mà có thể sửa đổi các chương trình, bỏ qua các kiểm soát, để thay đổi các chương trình và dữ liệu được cất giữ trong máy tính.

SURIV01 ***virut SURIV01*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào các tệp COM, ảnh hưởng tới hoạt động trong thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

SURIV02 ***virut SURIV02*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào các tệp EXE, ảnh hưởng tới hoạt động trong thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

susceptibility ***tính nhạy cảm*** Trong an toàn máy tính, tình trạng hoặc đặc

trưng bị khai thác nhiều hơn do mức độ nhạy cảm cao hơn của các hoạt động.

suspense account ***trương mục treo, bản kê treo*** Trong tính toán, sự tổng kiểm soát đối với mục dữ liệu đang chờ để được tiếp tục xử lý. *Xem* suspense file.

suspense file ***tệp treo*** Trong tính toán, một tệp chứa các mục chưa được xử lý hoặc được xử lý một phần đang chờ các hoạt động tiếp theo.

SVC *Xem* switched virtual call.

Sverdlov ***virut Sverdlov*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào các tệp COMMAND.COM, COM, EXE và OVL, ảnh hưởng tới hoạt động thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

Swap Boot ***virut Swap Boot*** Trong an toàn máy tính, một virut mà kết thúc và nằm thường trú, lây nhiễm vào cung khởi động của đĩa mềm, ngắt cung khởi động. *Xem* virus names.

sweeping ***quét*** *Xem* electronic countermeasures sweeping.

SWFT ***dịch vụ SWFT*** Trong hoạt động ngân hàng, cụm từ viết tắt của Society for Worldwide Interbank Financial Telecommunications (Hiệp hội viễn thông tài chính liên ngân hàng thế giới), một dịch vụ truyền thông quốc tế tư nhân cho các ngân hàng. *Xem* banking networks.

Swiss 143 ***virut Swiss 143*** Trong an toàn máy tính, một virut mà lây nhiễm vào các tệp COMMAND.COM và COM, ảnh hưởng tới hoạt động thời gian chạy, ngắt chương trình và các tệp OVL. *Xem* virus names.

switched network ***mạng chuyển mạch*** Trong truyền thông, mạng bất kỳ sử dụng chuyển mạch để thiết lập các cuộc nối. *Xem* switching.

switched network backup ***dự phòng mạng chuyển mạch*** Trong truyền thông, một phương tiện tùy chọn cho phép một người sử dụng chỉ rõ một tuyến lựa chọn nếu tuyến ban đầu vì một lý do nào đó không sẵn sàng.

switched virtual call ***gọi ảo có chuyển mạch*** Trong truyền dữ liệu, một kết nối giữa hai thiết bị đầu cuối mà chỉ được tạo ra khi có yêu cầu, tiếp sau một cuộc gọi thiết lập thủ tục. *Xem* packet switching, virtual call service.

switching ***(sự) chuyển mạch*** Trong truyền thông, sự cung cấp cho các kết nối điểm nối điểm giữa các nguồn và các nơi gom thay đổi động. *Xem* source, sink, circuit switching, message switching, packet switching.

switching center ***trung tâm chuyển mạch*** Trong truyền thông, nơi kết thúc nhiều mạch và có khả năng giao lưu truyền thông giữa các mạch hoặc các mạch liên kết nối. *Đồng nghĩa với* switching office.

switching office ***bộ phận chuyển mạch*** *Đồng nghĩa với* switching center.

Sylvia/Holland ***virut Sylvia/Holland*** Trong an toàn máy tính, một virut mà lây nhiễm vào các tệp COM, ngắt chương trình và các tệp OVL. *Xem* virus

names.

symmetric algorithm ***thuật toán đối xứng*** Trong mật mã, một thuật toán mật mã dùng cùng một giá trị khóa cho cả quá trình mã hóa lẫn giải mã hoặc cho cả quá trình xác thực và phê chuẩn hợp lệ. *So sánh với* asymmetric algorithm. *Xem* authentication, validation. *Đồng nghĩa với* one-key cryptosystem, symmetric cipher, symmetric cryptosystem.

symmetric cipher ***mã pháp đối xứng*** *Đồng nghĩa với* one-key cryptosystem, symmetric algorithm, symmetric cryptosystem.

symmetric cryptosystem ***hệ thống mã đối xứng*** Trong mật mã, một hệ thống mật mã trong đó các khóa mã hóa và giải mã là như nhau, hoặc từ cái này có thể dễ dàng suy ra cái kia. *So sánh với* asymmetric cryptosystem, public key cryptography. *Đồng nghĩa với* one-key cryptosystem, symmetric algorithm, symmetric cipher, symmetric key system.

symmetric key system ***hệ thống khóa đối xứng*** Trong mật mã, một hệ mật mã phụ thuộc vào độ mật của một khóa đơn lẻ (hoặc cặp khóa) đã sử dụng cho cả việc mã hóa lẫn giải mã. *So sánh với* asymmetric key system. *Đồng nghĩa với* one key cryptosystem, symmetric cryptosystem.

SYN ***ký tự SYN, ký tự đồng bộ*** Trong truyền dữ liệu, một ký tự điều khiển sự truyền phát được sử dụng trong liên kết truyền thông đồng bộ nhị phân để thiết lập đồng bộ giữa thiết bị phát và thiết bị thu. *Xem* binary synchronous communications.

sync ***đồng bộ*** *Xem* synchronous.

sync bit ***bit đồng bộ*** Trong truyền dữ liệu, một bit được sử dụng cho đồng bộ hóa. *Xem* bit, synchronization.

synchronization pulses ***(các) xung đồng bộ*** Trong điện tử học, các xung được gửi tới thiết bị thu, bằng cách phát các khối đơn vị, giữ cho hai khối đơn vị đúng nhịp. *Đồng nghĩa với* sync pulses.

synchronous ***đồng bộ*** Nói tới hai và nhiều quá trình đòi hỏi các sự kiện theo quy luật chung, ví dụ các xung định thời cho hoạt động của chúng. *So sánh với* asynchronous.

synchronous data link control ***điều khiển liên kết dữ liệu đồng bộ*** Trong truyền dữ liệu, một giao thức điều khiển liên kết dữ liệu của IBM dùng cho SNA. Nó là bắt buộc để quản lý sự chuyển thông tin đồng bộ, trong suốt về mã, nối tiếp từng bit qua một liên kết. Điều khiển liên kết dữ liệu đồng bộ tuân theo các tập con các thủ tục kiểm soát liên kết dữ liệu nâng cao và kiểm soát liên kết dữ liệu mức cao của ISO. *Xem* ADCCP, ANSI, bit, HDLC, protocol, serial transmission, synchronous transmission, transparent.

synchronous data network ***mạng dữ liệu đồng bộ*** Trong truyền dữ liệu, một mạng trong đó, tín hiệu nhịp của tất cả các thành phần của mạng đều được điều khiển bởi một nguồn nhịp thời gian riêng.

synchronous idle character ***ký tự rỗi đồng bộ*** Trong truyền dữ liệu,

một ký tự điều khiển quá trình phát được DTE sử dụng để đồng bộ hoặc điều chỉnh lại đồng bộ, đặc biệt khi không có các ký tự khác được truyền đi. *Xem* synchronous data network, DTE.

synchronous modem ***modem đồng bộ*** Trong truyền dữ liệu, một modem có đồng hồ nhịp bên trong, tạo ra một dòng dữ liệu liên tục ở một tốc độ truyền cố định. Sự đồng bộ được đòi hỏi ở mức bit, byte và mức thông báo. *Xem* bit, byte, MODEM, synchronous transmission.

synchronous stream cipher ***mã dòng đồng bộ*** Trong mật mã, một phương pháp mã dòng mà trạng thái tiếp theo của dòng bit mật mã chỉ phụ thuộc vào trạng thái trước đó mà không phụ thuộc vào đầu vào. *Xem* cryptographic bit stream, output feedback, stream cipher.

synchronous transmission ***truyền đồng bộ*** Trong truyền dữ liệu, một phương thức truyền trong đó mỗi bit được phát đi theo một trình tự thời gian cho trước. Nó có thể cung cấp tốc độ bit cao hơn truyền không đồng bộ (dị bộ) nhưng yêu cầu bên thu và bên phát duy trì sự đồng bộ chính xác trong thời gian dài. *So sánh với* asynchronous transmission. *Xem* bit rate.

sync pulses ***(các) xung đồng bộ*** *Đồng nghĩa với* synchronization pulses.

syntax ***cú pháp*** (1) Mối quan hệ qua lại của các ký tự hoặc của các nhóm ký tự độc lập với ý nghĩa, cách thể hiện hoặc với việc sử dụng chúng. (2) Trong tính toán, các quy tắc ngữ pháp bao trùm lên việc sử dụng một ngôn ngữ.

Syslock ***virut Syslock*** Trong an toàn máy tính, một virut mã hóa chính nó, lây nhiễm vào các tệp COM và EXE, ngắt chương trình và các tệp dữ liệu và OVL. *Xem* virus names.

SYSOP ***người điều hành hệ thống, SYSOP*** Trong tính toán, cụm từ viết tắt của SYStems OPerator, người điều hành một bảng thông báo điện tử, người này phải chịu trách nhiệm về bản chất của thông tin đã được đưa ra. *Xem* bulletin board.

system ***hệ, hệ thống*** (1) Trong tính toán, một tập hợp các thành phần phụ thuộc lẫn nhau mà có thể được xem như một thể thống nhất, ví dụ, một tập hợp được nối thành mạng của các hệ thống máy tính, một hệ thống phân tán, một trình soạn thảo và biên dịch, một hệ thống nhớ. (2) Trong tính toán, cụm máy tính và/hoặc phần cứng, phần mềm, phần sụn truyền thông được cấu hình cho mục đích phân loại, sắp xếp, trù liệu, tính toán, tổng kết, truyền và thu, cất giữ và nhận lại dữ liệu để hỗ trợ người sử dụng.

systematic ranges ***(các) khoảng có hệ thống*** Trong an toàn cơ sở dữ liệu, một dạng gây nhiễu dựa trên kết quả trong đó, các giá trị thống kê được biểu diễn như một khoảng các giá trị hơn là một giá trị được làm tròn riêng lẻ. *So sánh với* systematic rounding.

systematic rounding ***làm tròn có hệ thống*** Trong an toàn cơ sở dữ liệu, một dạng gây nhiễu dựa trên kết quả trong đó, giá trị thống kê được làm tròn thành số nguyên gần nhất với một số

làm tròn cố định. *So sánh với* controlled rounding, random rounding. *Xem* inference control, result based perturbation, perturbation, systematic ranges.

system authentication ***xác thực hệ thống*** Trong xác thực, một quá trình kiểm tra tính hợp lệ của hệ thống để giành được quyền truy nhập vào nó và để thông tin đã được phân loại được truyền đi. *Xem* masquerading.

system card reader ***bộ đọc thẻ hệ thống*** *Đồng nghĩa với* online card reader.

system code ***mã hệ thống*** *Đồng nghĩa với* card identification code.

system high ***mức (an toàn) hệ thống cao*** Trong an toàn dữ liệu, mức an toàn cao nhất được một hệ thống hỗ trợ tại một thời điểm đặc biệt hoặc trong một môi trường đặc biệt. *So sánh với* system low. *Xem* security level, system high security mode.

system high security mode ***chế độ an toàn hệ thống cao*** (1) Trong an toàn máy tính, một chế độ hoạt động tại đó, tất cả các cá nhân truy nhập vào hệ thống tự động đều có mức truy nhập an toàn, nhưng không có nhu cầu cần biết đối với tất cả các tài nguyên chứa trong hệ thống. Một hệ thống hoạt động trong chế độ an toàn cao của hệ thống khi mà phương tiện máy tính trung tâm và tất cả các thiết bị ngoại vi, các thiết bị đầu cuối ở xa được kết nối của nó được bảo vệ theo yêu cầu mức phân loại cao nhất của tài nguyên chứa trong hệ thống. Trong chế độ này, thiết kế và hoạt động của hệ thống phải cung cấp sự kiểm soát bên trong nào đó đối với tài nguyên đã được phân loại có sẵn đồng thời trong hệ thống trên cơ sở nhu cầu cần biết. *So sánh với* multilevel security mode. *Xem* discretionary access control, need to know, mandatory access control. (2) Trong an toàn máy tính, chế độ hoạt động trong đó phần cứng/phần mềm của hệ thống chỉ được tin cậy để cung cấp bảo vệ nhu cầu cần biết giữa những người sử dụng. Trong chế độ này, toàn bộ hệ thống gồm tất cả các bộ phận được nối với nhau về mặt vật lý hoặc điện, phải hoạt động với các biện pháp an toàn tương xứng với mức phân loại cao nhất và sự nhạy cảm của thông tin được xử lý và/hoặc được cất giữ. Tất cả những người sử dụng của hệ thống trong môi trường này phải có mức truy nhập và các quyền đối với tất cả các thông tin chứa trong hệ thống. Tất cả các đầu ra của hệ thống phải được đánh dấu rõ ràng với mức phân loại cao nhất và tất cả các quy định hệ thống, cho tới khi thông tin được cá nhân có ủy quyền xem xét lại để đảm các phân loại phù hợp và các quy định đều phải được đóng dấu. *So sánh với* multilevel security mode. *Xem* discretionary access control, need to know, mandatory access control. (3) Trong an toàn máy tính, một chế độ hoạt động ở đó, tất cả những người sử dụng có quyền truy nhập tới AIS tạo ra đều có mức truy nhập an toàn và sự phê chuẩn truy nhập chính thức, mà không cần thiết có nhu cầu cần biết đối với tất cả dữ liệu do AIS xử lý. *Xem* AIS, need to know.

system integrity ***toàn vẹn hệ thống*** Trong an toàn máy tính, một trạng thái tồn tại khi có sự đảm bảo đầy đủ rằng, dưới mọi điều kiện, một hệ thống ADP được dựa trên sự chính xác logic, độ tin cậy của hệ điều hành, sự đầy đủ về logic của phần cứng và phần mềm mà thực hiện cơ chế bảo vệ, và toàn vẹn dữ liệu. *Xem* data integrity, system integrity procedures.

system integrity procedures ***(các) thủ tục toàn vẹn hệ thống*** Trong an toàn máy tính, các thủ tục được thiết lập để đảm bảo rằng, phần cứng, phần mềm và dữ liệu trong một hệ thống ADP sẽ duy trì trạng thái của chúng về toàn vẹn nguyên thủy và không bị can thiệp bởi những thay đổi chương trình. *Xem* system integrity.

system low ***mức (an toàn) hệ thống thấp*** Trong an toàn dữ liệu, mức an toàn thấp nhất do hệ thống hỗ trợ tại một thời điểm đặc biệt hoặc trong một môi trường đặc biệt. *So sánh với* system high.

system manager ***người quản lý hệ thống*** Trong tính toán, một quan chức của ADP, người chịu trách nhiệm về hoạt động của hệ thống ADP.

system network architecture ***kiến trúc mạng hệ thống*** Trong truyền dữ liệu, một kiến trúc mạng của IBM dùng cho xử lý dữ liệu phân tán. Nó cho phép hệ thống phân tán bất kỳ truy nhập tới bộ xử lý chủ bất kỳ trong mạng qua các phương tiện nối mạng đa hệ thống. Nó cũng cung cấp kiến trúc phân tán giữa các bộ xử lý phức tạp, cũng như giữa một hoặc nhiều bộ xử lý và các hệ thống truyền thông thông minh từ xa. *So sánh với* OSI, processor interconnection. *Xem* multisystem networking.

system penetration ***(sự) thâm nhập hệ thống*** Trong an toàn máy tính, sự vi phạm hoặc sự phá vỡ các biện pháp bảo vệ hệ điều hành. *Xem* operating system, penetration.

system saboteur ***kẻ phá hoại hệ thống*** Trong an toàn máy tính, kẻ cố tình gây sai sót trong hệ điều hành để tạo ra ít nhất là tính không tin cậy của nó. *Xem* operating system.

system analysis ***phân tích hệ thống*** Trong tính toán, sự phân tích về một hành động hay một hệ thống để xác định xem liệu (và cách thức) có thể cải tiến hệ thống nhờ dùng các hệ thống máy tính không. *Xem* structured system analysis.

system security audit ***kiểm toán tính an toàn hệ thống*** Trong an toàn máy tính, quá trình đánh giá an toàn của các hệ thống hoặc trên cơ sở quan niệm, hoặc trên cơ sở một xem xét về một thực hiện cụ thể. Các mục tiêu của kiểm toán là nhận diện các nhược điểm về an toàn và đề xuất kỹ thuật hiệu chỉnh, các biện pháp về thủ tục hoặc tổ chức.

System Security Officer ***quan chức an toàn hệ thống*** Trong an toàn máy tính, cá nhân chịu trách nhiệm đảm bảo rằng, sự an toàn được dự phòng và đã được thực hiện trong suốt chu trình tồn tại của hệ thống ASI, từ lúc bắt đầu giai đoạn phát triển có tính khái niệm tới lúc thiết kế, phát triển, hoạt động,

bảo dưỡng và bố trí an toàn. *Xem* ASI.

system user ***người sử dụng hệ thống*** Trong an toàn máy tính, những người sử dụng có nối trực tiếp tới hệ thống và cả những cá nhân không có các nối trực tiếp, những người nhận đầu ra hoặc tạo đầu vào mà không bị xem xét một cách xác thực về phân loại bởi một cá nhân có trách nhiệm. Mức truy nhập của người sử dụng hệ thống được dùng trong tính toán chỉ số rủi ro. *Xem* risk index.

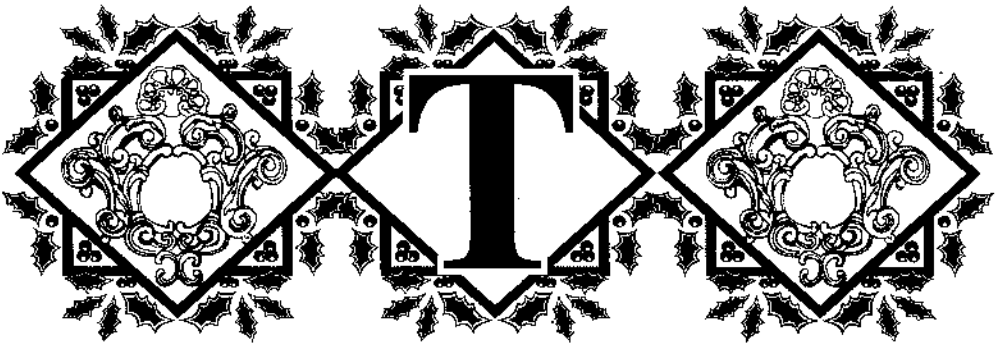


table ***bảng*** Trong tính toán, tập dữ liệu ở dạng phù hợp để có thể tham chiếu nhanh chóng, thường được lưu ở những vị trí nhớ liền nhau hoặc được ghi ở dạng mảng.

table restriction ***giới hạn bảng*** Trong an toàn cơ sở dữ liệu, một dạng kiểm soát không nhớ trong đó các bảng thống kê đầy đủ được giới hạn để tối thiểu hóa khả năng làm lộ của con người. Trong mô hình dàn, sự hạn chế này hàm ý rằng các bảng ở mức thấp hơn, tức là có nhiều chiều hơn sẽ bị giới hạn. *Xem* lattice model, inference control, memoryless control.

TAC *Xem* terminal access controller.

tagged keys ***(các) khóa gắn nhãn*** Trong quản lý khóa, một kỹ thuật chứa các ký tự nhận dạng chức năng trong phạm vi các khóa mã. Các khóa DES có 64 bit song chỉ có thể chọn độc lập 56 bit trong chúng, 8 bit còn lại dùng để kiểm tra tính chẵn lẻ. Các khóa gắn nhãn dùng 8 bit dự trữ để chuyển thông tin về chức năng của một khóa dùng trong hệ thống quản lý khóa, chẳng hạn, khóa dữ liệu để mã hóa, khóa mã khóa v.v... Các khóa gắn nhãn được mã hóa cùng với các khóa mã khóa trong sử dụng thông thường, vì thế không thể bị kẻ tấn công quan sát hoặc thay đổi được. Khi các khóa gắn nhãn bị lộ trong modun chống giả mạo, nhãn bị kiểm tra để đảm bảo nó ứng với một khóa hợp lệ trong thao tác đưa ra. Trong trường hợp khóa hợp lệ, các bit nhãn được thay thế bằng các bit chẵn lẻ thích hợp trước khi dùng khóa trong thao tác mã hoặc giải mã. Kỹ thuật này ngăn được những tấn công trong đó khóa MAC được mã bằng khóa MAC chính bị lộ do dùng sai các phương tiện giải mã dữ liệu trong các modun mật. *So sánh với* control vector. *Xem* crypto- graphic key, data encryption standard, parity bit, re-encipher from master key.

tail ***mục cuối; mã kết thúc*** (1) Trong tính toán, mục dữ liệu chỉ sự kết thúc một danh sách. *Xem* list. (2) Trong liên lạc dữ liệu, mã kết thúc là một chuỗi mã chỉ sự kết thúc một thông báo.

tailgating ***truy nhập nối đuôi*** Trong kiểm soát truy nhập, thủ đoạn sử dụng một thẻ truy nhập để dùng liên tiếp cho hai cá nhân hoặc nhiều hơn truy nhập. *Xem* anti-passback. *Đồng nghĩa với* piggybacking.

Taiwan ***virut Taiwan*** Trong an toàn máy tính, một loại virut lây nhiễm các tệp COM. Phá hoại các tệp chương trình và các tệp OVL. *Xem* virus names.

Taiwan3 ***virut Taiwan3*** Trong an toàn máy tính, một virut chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, phá hoại các tệp dữ liệu, OVL và chương trình. *Xem* virus names.

Taiwan4 ***virut Taiwan4*** Trong an toàn máy tính, một virut chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, phá hoại các tệp dữ liệu, OVL và chương trình. *Xem* virus names.

take-grant access control ***kiểm soát truy nhập kiểu lấy - cấp*** Trong kiểm soát truy nhập, một dạng hệ thống có khả năng trong đó các chủ thể và những người sử dụng có các đặc quyền chuyển sang các thẻ tích kê (nhãn kiểm).

Trong mô hình lấy-cấp, có thể thêm những người sử dụng mới vào hệ thống, các tệp mới được tạo ra hay xóa đi, các quyền truy nhập được chuyển khỏi người chủ sở hữu tệp để cho phép người sử dụng khác đọc hay thay đổi tệp, hoặc người chủ sở hữu có thể cho phép người sử dụng khác lấy tất cả các đặc quyền của anh ta đối với một tệp kể cả tặng các đặc quyền. Những hoạt động này được hình thức hóa trong mô hình lấy-cấp theo các quy tắc Tạo, Hủy, Cấp và Lấy.

- Tạo - hoạt động của quy tắc này để tạo ra một chủ thể hay đối tượng mới. Chủ thể tạo ra nút sẽ chọn một tập các quyền cho chủ thể/đối tượng mới đó và chúng là tệp con của tất cả các quyền có thể.
- Hủy - quy tắc này sẽ giảm bớt tập các đặc quyền mà một chủ thể/đối tượng có đối với chủ thể/đối tượng khác.
- Cấp - các quyền có thể được đặt cùng với quy tắc này.
- Lấy - quy tắc này cho phép một chủ thể quyết định lấy tập con đặc quyền nào mà nó muốn chấp nhận.

Xem capability.

tamper-proof ***đề phòng can thiệp*** Trong an toàn dữ liệu, nói tới một thiết bị được thiết kế để bảo vệ nội dung hay chức năng của nó chống các tấn công vật lý. Những thiết bị như vậy chứa một số bộ phát hiện bên trong, chẳng hạn như các bộ phát hiện độ nghiêng, các bộ phát hiện ánh sáng mà sẽ xóa dữ liệu đã lưu, như các khóa mật mã, trong tình huống có các hành động thực truy nhập bất hợp pháp. Hiện nay người ta ưa dùng thuật ngữ chống can thiệp hơn vì nó mô tả chính xác hơn mức độ bảo vệ mà nó cung

cấp. *Xem* tamper-resistant module.

tamper-resistant module ***môđun chống can thiệp*** Trong an toàn dữ liệu, một thiết bị lưu thông tin nhạy cảm (ví dụ như khóa mã chính) và thực hiện các chức năng mã hóa. Thiết bị có một hoặc nhiều bộ cảm biến để phát hiện các tấn công vật lý do đối phương cố truy nhập tới thông tin được lưu, trong trường hợp đó, thông tin nhạy cảm đã lưu sẽ bị phá tức thì. *Xem* key.

tape ***băng an toàn; băng (từ)*** *Xem* foil.

tape dialer ***thiết bị quay số băng từ*** Trong an toàn vật lý, một thiết bị tự động báo cáo một báo động tới một hoặc nhiều vị trí ở xa nhờ quay số điện thoại xác định và chạy một thông báo được ghi trên băng từ. *Xem* telephone dialer.

tape streamer ***bộ cuộn băng từ chạy suốt*** Trong tính toán, một cơ cấu chuyển tải băng từ được thiết kế để đọc hoặc ghi các dòng dữ liệu liên tục, chẳng hạn như hoạt động sao chép dự phòng. Nó đơn giản hơn về mặt cơ và vì thế rẻ hơn thiết bị khởi/ngừng. *Xem* backing storage.

target of evaluation ***mục tiêu đánh giá*** Trong an toàn thông tin, hệ thống hoặc sản phẩm cần được đánh giá so với tiêu chuẩn an toàn. *Xem* information technology security evaluation criteria.

tariff ***giá cước, cước phí*** Trong truyền thông, tập các mức giá, các quy tắc và các điều luật liên quan tới các dịch vụ và thiết bị do cơ quan viễn thông công cộng cung cấp. *Xem* common carrier.

task ***nhiệm vụ, tác vụ*** Trong lập trình, về cơ bản là một chương trình ứng dụng song không cần là một chương trình đầy đủ; nó có thể là một thủ tục con hay chương trình con do một chương trình ứng dụng gọi tới để dùng riêng.

TBDF *Xem* transborder data flow.

T carrier ***phân cấp T*** Trong truyền thông, một phân cấp của hệ thống truyền thông số điện thoại Bell đặt tên là *T1*, *T2* và *T4*.

TC 11 ***tiểu ban 11*** Tiểu ban kỹ thuật của IFIP đề cập tới an toàn và bảo vệ các hệ thống xử lý thông tin. *Xem* IFIP.

TC 68/SC2 ***tiểu ban 68/SC2*** Trong an toàn dữ liệu, tiểu ban của ISO đối với các chuẩn cho hoạt động ngân hàng an toàn. *Xem* ISO.

TC 97/SC17/WG4 ***nhóm TC 97/SC 17/WG4*** Trong an toàn dữ liệu, nhóm làm việc của Ủy ban thuộc ISO để xem xét các chuẩn đối với các tính chất vật lý và giao diện của các thẻ thông minh. *Xem* ISO, smart card.

TC 97/SC20 ***nhóm TC97/SC20*** Nhóm làm việc của Ủy ban ISO về các chuẩn an toàn. *Xem* ISO.

TCB *Xem* trusted computing base.

TCB Subset ***nhóm con TCB*** Trong an toàn máy tính, một tập con *M* của cơ sở tính toán tin cậy là một tập các phần mềm, phần sụn và phần cứng (có thể không có thành phần nào đó) dàn xếp việc truy nhập của tập *S* các chủ thể vào tập *O* các đối tượng trên cơ sở

chính sách truy nhập đã công bố *P* và thỏa mãn các tính chất:

- *M* dàn xếp truy nhập bất kỳ tới các đối tượng thuộc *O* qua các chủ thể thuộc *S*;
- *M* chống can thiệp;
- *M* đủ nhỏ để có thể phân tích và thử nghiệm, tính đầy đủ của nó có thể được bảo đảm.

Xem Blue Book, reference monitor concept, trusted computing base.

TCP *Xem* transmission control protocol.

TCP/IP ***giao thức TCP/IP*** Trong an toàn dữ liệu, giao thức kiểm soát truyền dẫn (TP)/giao thức Internet (IP). Những giao thức này là một phần của bộ các giao thức truyền thông đã được phát triển như một phần của dự án ARPANET (Advanced Research Project Agency Network, tức mạng cơ quan dự án nghiên cứu tiên tiến) ở Hoa Kỳ. Công trình này được bắt đầu vào cuối những năm 1960 dưới sự bảo trợ của Bộ quốc phòng Hoa Kỳ.

Giao thức kiểm soát truyền dẫn (TCP) về khái niệm tương tự với giao thức tầng vận tải trong mô hình tham chiếu OSI. (TCP/IP tương đương về chức năng với giao thức vận tải lớp 4 của mô hình tham chiếu OSI). TCP/IP cung cấp dịch vụ nối định hướng tin cậy giữa các hệ thống máy tính chủ trên các mạng truyền thông, tức là TCP/IP là một giao thức điểm tới điểm (hay máy chủ tới máy chủ). TCP/IP được thiết kế để hoạt động trên một mạng truyền thông có thể có một hay nhiều mạng con nối với nhau. Những mạng con này có thể không tin cậy, ví dụ các gói truyền có thể mất, bị thay đổi hay bị trễ tùy ý.

Giao thức Internet (IP) là một tập các thủ tục được thiết kế để các thông báo có thể được chuyển tải giữa các hệ máy tính chủ đi qua nhiều mạng con. Nó cung cấp dịch vụ không nối (dịch vụ gói tin) và tương tự về mặt chức năng với giao thức mạng liên kết được phát triển như một phần bổ sung vào giao thức tầng mạng trong mô hình tham chiếu OSI. *Xem* connectionless service; datagram, Internet, open systems interconnection.

TCSEC *Xem* trusted computer security evaluation criteria. *Đồng nghĩa với* Orange Book.

TDF *Xem* Transborder data flow.

TDM *Xem* time division multiplexing.

tear-me-open ***xé để mở, giấy phép học ni lông*** *Đồng nghĩa với* shrink wrapped license.

technical and office protocol ***giao thức kỹ thuật và văn phòng*** Trong bộ các chuẩn, giao thức chỉ ra các tiêu chuẩn và các tùy chọn trong phạm vi các tiêu chuẩn thích hợp với các mạng cục bộ và các đầu cuối, các tài nguyên tính toán... dành cho môi trường văn phòng và kỹ thuật. *So sánh với* manufacturing automation protocol. *Xem* local area network, open systems interconnection.

technical data ***dữ liệu kỹ thuật*** (1) Thông tin đã hoặc chưa xếp vào loại mật loại bất kỳ có thể được dùng, hoặc sửa lại để dùng trong các lĩnh vực thiết kế, chế tạo, sản xuất, sửa chữa, kiểm tra đại tu, xử lý, kỹ thuật, phát triển,

vận hành, bảo dưỡng, hoạt động tái tạo lại, hàng hóa hoặc đạn dược; hay bất kỳ công nghệ nào thúc đẩy trình độ khoa học kỹ thuật, hay thiết lập một kỹ nghệ mới trong lĩnh vực quân sự quan trọng có tính ứng dụng ở Hoa Kỳ. Dữ liệu có thể ở dạng hữu hình như mô hình, nguyên mẫu, bản thiết kế hay sổ tay hướng dẫn hoạt động, hoặc ở dạng vô hình (không sờ mó được) như một dịch vụ kỹ thuật, các tương tác trực quan hay đối thoại. (2) Thông tin được ghi lại liên quan tới các công việc về kỹ thuật, thí nghiệm, phát triển có thể dùng để xác định một quá trình kỹ thuật hay sản xuất, hoặc để thiết kế, tìm kiếm, chế tạo, hỗ trợ, duy trì, phân tích, sửa chữa hay kiểm tra toàn diện. Dữ liệu có thể là ở dạng đồ thị, hình phác họa trong các môi trường như hình vẽ, ảnh chụp, các đặc tả ở dạng văn bản hay các tài liệu kiểu thiết kế hoặc dạng dữ liệu in ra từ máy tính. Các ví dụ về dữ liệu kỹ thuật gồm các số liệu nghiên cứu, số liệu công trình, các bản vẽ kỹ thuật, các danh sách kèm theo, các bản đặc tả các chuẩn, các trang xử lý, sổ tay tra cứu, các báo cáo kỹ thuật, các thông tin liên quan và các tài liệu phần mềm máy tính.

technical policy ***quy tắc kỹ thuật, chính sách kỹ thuật*** Trong an toàn máy tính, một tập các quy tắc điều khiển sự truy nhập của các chủ thể tới các đối tượng được tuân thủ theo tập con TCB. *Xem* Blue Book, TCB, subset.

technical security ***an toàn kỹ thuật*** Các trang thiết bị, các thành phần, các thiết bị và tài liệu hay phương tiện kèm theo có liên quan tới mật mã hoặc tới sự an toàn liên lạc và các hệ thống thông tin tự động.

technical vulnerability ***tính dễ tổn hại về mặt kỹ thuật, điểm yếu về kỹ thuật*** Trong an toàn máy tính, điểm yếu của phần cứng, phần mềm hay phần sụn hoặc thiếu sót thiết kế dẫn tới sự lợi dụng tiềm ẩn từ bên trong, hoặc bên ngoài đối với hệ thống thông tin tự động, từ đó dẫn tới rủi ro hay tổn hại thông tin, sự biến đổi thông tin hoặc sự từ chối phục vụ. Thông tin dễ bị tổn hại về kỹ thuật, nếu nó luôn có sẵn trước những kẻ trái phép có thể làm AIS bị lợi dụng, dẫn tới sự nguy hiểm nghiêm trọng đối với an ninh quốc gia. *Xem* AIS, denial of service, vulnerability.

technological attack ***tấn công công nghệ*** Trong an toàn máy tính, một kiểu tấn công gây ra bằng cách làm hỏng hoặc vô hiệu hóa các cơ chế kiểm soát truy nhập phần cứng và phần mềm chứ không phải bởi sự phá hoại của riêng hệ thống hay những người sử dụng khác. *Xem* access control, mechanisms.

technology ***công nghệ*** Thông tin kỹ thuật và bí quyết có thể dùng để thiết kế, chế tạo, sản xuất, sử dụng hoặc tái tạo lại các vật dụng bao gồm dữ liệu kỹ thuật, phần mềm máy tính. Bản thân thuật ngữ không chỉ chính các vật dụng. *Xem* know-how.

telebanking ***hoạt động ngân hàng từ xa*** Trong hoạt động ngân hàng, một phương tiện thực tiện các giao dịch ngân hàng phía khách trên mạng truyền thông, chẳng hạn văn bản video, truyền

hình cáp có tương tác. *Xem* home baking security, self banking, videotex.

telecommunications ***viễn thông, liên lạc viễn thông*** (1) Một thuật ngữ chung biểu thị sự truyền dữ liệu giữa một hệ thống tính toán và các thiết bị đặt ở xa qua một khối thực hiện phép biến đổi định dạng cần thiết và các kiểm soát tốc độ truyền. (2) Sự truyền, phát hoặc nhận bất kỳ các tín hiệu, dấu hiệu, chữ viết, hình ảnh, âm thanh hay thông tin khác qua các hệ thống dây, vô tuyến, hiển thị hay hệ thống điện từ bất kỳ. (3) Sự điều chế, sự truyền, liên lạc hoặc quá trình xử lý liên quan tới thông tin bằng các biện pháp cơ điện, điện từ hay quang điện. (4) Sự liên lạc chủ yếu cách nhau một khoảng cách. Công nghệ truyền có thể thuộc một trong ba dạng, tức là các tín hiệu điện đi dọc một dây dẫn, bức xạ điện từ hay các tín hiệu ánh sáng dọc một cáp quang. Các tín hiệu này trong một số trường hợp có thể có dạng như tín hiệu ban đầu, song trong nhiều trường hợp khác, thông tin cần truyền sẽ điều chế tín hiệu sóng mang. *Xem* modulation, fiber optics.

telecommunications and automated information systems security ***an toàn các hệ thống thông tin tự động và viễn thông*** Trong an toàn máy tính và an toàn liên lạc, sự bảo vệ cho các hệ thống thông tin tự động và viễn thông để ngăn chặn sự lợi dụng thông qua chặn tín hiệu, truy nhập điện từ trái phép hoặc các mối đe dọa tình báo kỹ thuật có liên quan và để đảm bảo tính xác thực. Sự bảo vệ như vậy thông qua việc ứng dụng các biện pháp an toàn (gồm mật mã, an toàn truyền dẫn, an toàn phát xạ và an toàn máy tính) đối với các hệ thống tạo, lưu trữ, xử lý, chuyển hoặc truyền thông tin trước đối phương, nó cũng gồm cả sự bảo vệ vật lý các chất liệu (material) an toàn nhạy cảm về kỹ thuật và thông tin an toàn nhạy cảm về kỹ thuật. *Xem* authentication, Tempest proofing, van Eck phenomenon, wiretaping.

teleconferencing ***hội nghị từ xa*** Trong các ứng dụng, việc sử dụng các mạng máy tính và các hệ thống liên lạc cho phép những người cách xa nhau về địa lý có thể tham gia các hội nghị hay các dự án chung liên quan tới sự hợp tác chặt chẽ. Ở một mức độ, những người tham gia được hỗ trợ các đầu cuối máy tính và họ trao đổi với nhau không nhất thiết đồng thời trên các mạng liên lạc dữ liệu. Hoạt động của hệ thống được kiểm soát bởi người hay hệ thống quản trị. Đó là nơi có trách nhiệm phân phối thông tin tới các thành viên tham gia. Các hệ thống tinh vi hơn cung cấp các kết nối video, các hệ thống bỏ phiếu, ghi lại các hoạt động của hội nghị v.v..

teleinformatic services ***(các) dịch vụ viễn tin học*** Trong liên lạc, thuật ngữ của CCITT nhấn mạnh tới tất cả các dịch vụ viễn thông kiểu bàn ghi không ở dạng tiếng nói hay lời nói chẳng hạn như fax, điện báo, văn bản video. *Xem* videotex, facsimile, common carrier.

telemetering ***đo từ xa*** Trong liên lạc dữ liệu, phép đo từ xa lượng tiêu thụ của các thiết bị gia dụng. *Xem* telemetry.

telemetry ***phép viễn trắc, phép đo từ xa*** Trong liên lạc dữ liệu, sự truyền các tín hiệu nhận từ các thiết bị đo ở những khoảng cách lớn.

telemonitoring ***giám sát từ xa*** Trong liên lạc dữ liệu, sự giám sát từ xa các thiết bị đo thường đặt ở gia đình, có dùng một kết nối viễn thông, chẳng hạn đọc các đồng hồ đo điện năng. *Xem* telemetering.

telephone dialer ***bộ quay số điện thoại*** Trong an toàn vật lý, một thiết bị tự động gọi tới một trạm trung tâm và báo cáo một trạng thái báo động. *Xem* digital communicator, tape dialer. *Đồng nghĩa với* dialer.

telephone intrusion ***đột nhập qua điện thoại*** Trong an toàn máy tính, sự đột nhập vào một hệ thống máy tính bằng sự truy nhập qua quay số; một dạng tấn công phổ dụng của bọn tin tặc. Những tấn công như vậy tăng lên trong những năm gần đây do:

- những phương tiện của các mạng quay số;
- sẵn có thiết bị thâm nhập;
- chuyên môn cao của kẻ đột nhập;
- các bảng thông báo điện tử.

Sự tăng các phương tiện mạng điện thoại trong những năm gần đây đã cho phép những kẻ đột nhập quay trực tiếp vào các hệ thống máy tính từ những khu vực khác nhau trên thế giới, cho phép, ví dụ kẻ đột nhập ở Trung Đông và Châu Âu gọi tới các máy tính ở Hoa Kỳ. Sự giảm giá thành và tăng năng lực của các máy tính cá nhân và modem cho phép, thậm chí các thanh thiếu niên có được thiết bị đột nhập tinh vi. Các tin tặc đôi khi thể hiện một trình độ chuyên môn cực kỳ cao và sự sao chép bất hợp pháp các bảng thông báo điện tử cho phép bọn này phổ biến kiến thức, các mật khẩu thu được, các phần mềm đột nhập v.v..

Sự bảo vệ chống các tấn công quay số bao gồm phần mềm đặc biệt, các phần cứng bổ sung và biện pháp quản trị. Các phương tiện an toàn hoạt động cần được sử dụng đầy đủ và cần xóa bỏ các mật khẩu do nhà cung cấp hỗ trợ thường có mức đặc quyền cao. Các trình quản trị gồm ngắt nối các modem trong thời gian người dùng không yêu cầu truy nhập, buộc tuân thủ dùng các mật khẩu tốt, ghi sổ các sự kiện tấn công, hạn chế số lần đăng nhập thử và che giấu thông tin về hệ thống máy tính cho tới khi các kiểm soát mật khẩu được đáp ứng đầy đủ. Gợi ý được đưa ra là, không cho phép nhập vào nào khi một lần thử nhập mạng không thành công, song hệ thống sẽ mời thử lại để thu thập thông tin về kẻ đột nhập. Tuy nhiên phải thực hiện thận trọng để tránh những phí tổn đánh bẫy (charges of entrapment).

Những thiết bị an toàn bổ sung có thể phân loại thành các hệ thống một đầu và hệ thống hai đầu. Các hệ thống một đầu được cài đặt hoặc tại máy tính chủ hoặc ít phổ dụng hơn là tại thiết bị đầu cuối của người dùng hợp pháp. Các thiết bị bảo vệ cổng được nối tại máy tính chủ; các modem an toàn cho các thiết bị đầu cuối của người dùng sẽ kết hợp các tính năng an toàn tích hợp trong modem.

Các thiết bị hai đầu cho độ an toàn

nâng cao nhờ có phần cứng an toàn ở cả hai đầu của kết nối điện thoại hợp pháp, những thiết bị như vậy liên lạc với nhau để thực hiện các chức năng an toàn.

Sự phát triển các dịch vụ điện thoại mới, chẳng hạn ISDN, cung cấp số điện thoại của người gọi cho người được gọi, có ưu thế lớn trong việc chống đột nhập qua điện thoại. Hệ thống máy tính được gọi có thể đơn giản từ chối các cuộc gọi truy nhập không kèm theo số gọi và kiểm tra tất cả các số gọi dựa vào danh sách được ủy nhiệm. *Xem* call back, ISDN, one-end device, password, PPD, security modem, two-end device.

telephone scrambler ***bộ xáo trộn điện thoại*** *Xem* voice scrambling.

telephone tap ***bộ mắc trộm điện thoại*** Trong an toàn liên lạc, một thiết bị nghe trộm điện tử. *Xem* electronic listening device, wiretapping.

teleprocessing ***xử lý từ xa*** (1) Trong liên lạc dữ liệu, nói tới hệ thống truyền thông tin kết hợp liên lạc viễn thông, các hệ thống ADP và thiết bị giao tiếp người - máy nhằm mục đích giao tác và lập chức năng như một hệ thống tích hợp đầy đủ. *Xem* telecommunications. (2) Trong liên lạc dữ liệu, việc xử lý dữ liệu được kết hợp với thông tin từ xa, chẳng hạn, việc sử dụng một mạng điện thoại để nối một đầu cuối ở xa với một máy tính hoặc để nối hai máy tính với nhau. *Xem* teleprocessing security.

teleprocessing security ***an toàn xử lý từ xa*** Trong an toàn dữ liệu, sự bảo vệ rút ra từ tất cả các biện pháp được thiết kế để ngăn chặn sự tiết lộ, nhận, hoặc thay đổi trái phép cố ý hay vô ý thông tin trong hệ thống xử lý từ xa. *Xem* teleprocessing.

telesoftware ***phần mềm từ xa, TSW*** Trong kỹ thuật videotex, phần mềm truyền tới hệ hiển thị dữ liệu thông minh hoặc terminal teletext, hoặc tới máy vi tính lập trình để mô phỏng đầu cuối videotex. *Xem* software, teletext.

teletext ***viễn truyền văn bản, truyền văn bản từ xa*** Trong văn bản video, một phương pháp truyền thông tin được lưu trên một máy tính tới các máy thu hình được điều chỉnh thích hợp ở gia đình. Trong các dịch vụ phát rộng, các tín hiệu số được truyền liên kết với các chương trình vô tuyến thông thường.

teletext decoder ***bộ giải mã văn bản từ xa*** Trong văn bản video, một thiết bị cho phép một máy thu hình trong nhà hiển thị thông tin văn bản từ xa. *Xem* teletext.

TELNET ***giao thức TELNET*** Trong liên lạc dữ liệu, một giao thức đăng nhập từ xa do ARPANET phát triển. *Xem* ARPANET, protocol.

Telpak ***quy định Telpak*** Trong liên lạc, sự quy định giá cả gán mức giá dung lượng lớn đối với các tuyến nhiều kênh trên cơ sở hai hay nhiều điểm.

Tempest ***Tempest*** (1) Trong an toàn máy tính, một tên ngắn chỉ sự điều tra và nghiên cứu về những nguồn phát xạ gây hại. Đôi khi nó được dùng đồng nghĩa với thuật ngữ "các nguồn phát xạ gây hại", ví dụ các thử nghiệm Tempest, sự kiểm tra Tempest. *Xem* compromising

emanations, Tempest control zone, Tempest proofing. (2) Trong an toàn máy tính, sự nghiên cứu và kiểm soát các tín hiệu điện tử tạp phát ra từ thiết bị ADP. *Xem* ADP, Tempest proofing.

Tempest control zone ***vùng kiểm soát Tempest*** Trong an toàn máy tính, vùng không gian liên tục bao quanh thiết bị và các hệ thống phân phối và nằm dưới sự kiểm soát vật lý và kỹ thuật đầy đủ để ngăn ngừa sự chặn bắt các nguồn phát xạ gây hại. Kiểm soát vật lý và kỹ thuật là mức kiểm soát cho phép các lực lượng an ninh có trách nhiệm bảo vệ không gian đã kiểm soát nhằm phát hiện, điều tra và loại bỏ cá nhân hay thiết bị bất kỳ đáng ngờ bị phát hiện ra ở đây. *Xem* compromising emanations, Tempest.

Tempest proofing ***chống Tempest*** Trong an toàn liên lạc, việc ngăn ngừa sự phát bức xạ từ một hệ thống máy tính có thể cho phép kẻ nghe trộm ghi lại được thông tin mật. Sự phát xạ điện tử có thể thoát ra qua nhiều tuyến và để loại trừ mối nguy hiểm này, người ta dùng cách bao bọc và chặn nguồn cùng với việc bọc che tất cả các dây cáp. Các cáp sợi quang không phát ra bức xạ điện tử. *Xem* conductive shielding, encapsulation, fiber optics, source suppression, van Eck phenomenon.

template ***mẫu, khuôn mẫu*** Trong kiểm soát truy nhập; dạng số hóa của một phép đo sinh trắc một đặc trưng của người sử dụng, ví dụ vân tay. Mẫu của người dùng được lưu và được so sánh với mẫu đã đo được khi có yêu cầu truy nhập hay có sự ủy quyền. *Xem* biometrics.

temporal separation ***(sự) phân tách thời gian*** *Xem* isolation enforcement. *Đồng nghĩa với* periods processing.

tera ***tera*** Một triệu triệu, tức 10^{12}.

term ***kỳ hạn; thuật ngữ*** (1) Trong hoạt động ngân hàng, kỳ hạn là một khoảng thời gian để một phương tiện phải tiếp tục cho tới ngày đáo hạn. (2) Thuật ngữ là từ hay biểu thức có một nghĩa chính xác theo một số kiểu dùng nào đó, hoặc đặc biệt về mặt khoa học, nghệ thuật, về nghề nghiệp hay chủ đề.

terminal ***thiết bị đầu cuối, đầu cuối*** (1) Trong các thiết bị ngoại vi, một thiết bị vào/ra để truyền và nhận dữ liệu trên đường dây liên lạc. (2) Trong liên lạc, một vị trí trong hệ thống tại đó thông tin có thể được truyền hay thu.

terminal access controller ***bộ kiểm soát truy nhập đầu cuối*** Trong liên lạc dữ liệu, một kiểu bộ xử lý giao tiếp thông báo mà có thể được gọi trực tiếp qua một thiết bị đầu cuối. *Xem* interface message processor.

terminal authentication device ***thiết bị xác thực đầu cuối*** Trong an toàn máy tính, một thiết bị hai đầu được thiết kế để xác thực thiết bị đầu cuối của người dùng xác định. Các cặp thiết bị phù hợp được gài vào kênh liên lạc. Ví dụ, thiết bị này được cài đặt giữa thiết bị đầu cuối và modem còn thiết bị kia được gắn vào cổng máy tính chủ. Thiết bị phía máy chủ sẽ tạo ra những câu hỏi cho khối thiết bị nối vào thiết bị đầu cuối. *Xem* challenge/response, telephone intrusion, two-end device.

terminal handler *bộ quản thiết bị đầu cuối* Trong liên lạc dữ liệu, một phần mạng dữ liệu phục vụ các thiết bị đầu cuối dòng ký tự đơn giản.

terminal identification *(sự) định danh thiết bị đầu cuối, (sự) nhận dạng thiết bị đầu cuối* Trong an toàn máy tính, các biện pháp được dùng để thiết lập danh tính duy nhất của một thiết bị đầu cuối qua một hệ thống ADP.

terminal key *khóa thiết bị đầu cuối, khóa terminal* (1) Trong quản lý khóa, một khóa mã khóa được cấp cho thiết bị đầu cuối và được dùng để mã các khóa phiên. *So sánh với* session key. *Xem* midnight attack. (2) Trong quản lý khóa, một khóa mã trong hệ thống khóa giao dịch được dùng để nhận được các khóa đã dùng để bảo đảm an toàn giao dịch. *Xem* transaction key system.

terminal thief *kẻ trộm thiết bị đầu cuối* *Đồng nghĩa với* hacker.

Teror *virut Teror* Trong an toàn máy tính, một loại virut làm chấm dứt và nằm thường trú trong bộ nhớ, làm lây nhiễm các tệp COMMAND.COM, COM, EXE, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL, định dạng và ghi đè lên tất cả hay một phần của đĩa. *Xem* virus names.

test *mã thử nghiệm, mã kiểm tra* Trong hoạt động ngân hàng, một mã nằm trong một thông báo giữa người gửi và nhận được dùng để xác nhận nguồn của thông báo mà cũng có thể xác nhận những thành phần nào đó của thông báo như lượng, ngày tháng và trình tự của nó. Mã là kết quả của sự thỏa thuận tay đôi dựa trên phương pháp tính toán. *Xem* authenticator, message authentication, test key.

test amount *tổng thử* Trong hoạt động ngân hàng, tổng các phần nguyên của tất cả các tổng số tiền và các số lượng trong một thông báo.

test data *dữ liệu kiểm tra, dữ liệu thử nghiệm* (1) Trong kiểm toán, các giao dịch mẫu đã được xử lý từ những bản ghi chính được dùng để xét đoán tính hiệu quả của hệ thống và các kiểm soát đã lập trình. (2) Trong tính toán, dữ liệu được chuẩn bị chỉ để kiểm tra độ chính xác của chương trình và logic của một hệ thống. Dữ liệu thử nghiệm được dùng để chứng minh từng nhánh và sự kết hợp các nhánh của một chương trình và bởi vậy, sẽ bao quát tới mức có thể. Các sai sót có tính toán sẽ được đưa vào dữ liệu thử nghiệm, chẳng hạn gài các ký tự chữ cái vào các trường số, để đảm bảo rằng, những sai sót này sẽ bị chương trình phát hiện ra. Tại phần cuối của cuộc chạy thử nghiệm, đầu ra sẽ được kiểm tra so với các kết quả xử lý dữ liệu chờ đợi để xem xem liệu chúng có tương hợp với nhau không. *Xem* dynamic testing.

Tester *virut Tester* Trong an toàn máy tính, một loại virut làm chấm dứt và nằm thường trú trong bộ nhớ, làm lây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

test key *khóa chạy thử* Trong hoạt động ngân hàng, các bộ ký tự và phương pháp tính toán được thiết kế

chỉ các nhóm tương ứng biết. Khi các bộ chữ cái được dùng theo thỏa thuận về phương pháp, kết quả sẽ là bài trắc nghiệm. *Xem* authenticator, message authentication, test.

text ***văn bản*** Trong liên lạc, nội dung thông tin trong thông báo.

text compression ***nén văn bản*** Trong liên lạc dữ liệu, nói tới sự loại bỏ dữ liệu dư, ví dụ các số không đứng trước, các khoảng trống ở phần đuôi, ra khỏi một thông báo. *Xem* data compression, Huffman code.

The Buddy System ***hệ thống Buddy*** Trong quản lý rủi ro, một phương pháp luận phân tích rủi ro. *Xem* risk analysis methodologies.

theoretically secure ***an toàn về mặt lý thuyết*** Trong mã thám, một hệ thống an toàn ngay cả khi nhà mã thám có thời gian, các phương tiện và tiền của không hạn chế.

third normal form ***dạng chuẩn thứ ba*** Trong các cơ sở dữ liệu, một tính chất của một quan hệ trong một cơ sở dữ liệu quan hệ. Một quan hệ ở dạng chuẩn thứ ba nếu nó ở dạng chuẩn thứ hai và mỗi thuộc tính phụ của quan hệ sẽ phụ thuộc một cách không bắc cầu vào mỗi khóa dự bị của quan hệ. Thực vậy, yêu cầu này nêu lên rằng, mỗi trường sẽ chỉ phụ thuộc vào khóa chính và không phụ thuộc vào trường bất kỳ khác trong phạm vi quan hệ. Một ví dụ về quan hệ không ở dạng chuẩn thứ ba là số hiệu bộ, số hiệu dự án, tên dự án, thời hạn hoàn thành dự án với số hiệu bộ là khóa. Thời hạn hoàn thành dự án phụ thuộc có tính chức năng vào số hiệu dự án và nếu chỉ có một dự án mỗi bộ thì số hiệu dự án phụ thuộc có tính chức năng vào khóa số hiệu bộ. Vì số các dự án có thể có thời hạn hoàn thành giống nhau nên sẽ có sự phụ thuộc bắc cầu giữa thời hạn hoàn thành dự án và khóa. Quan hệ không phải ở dạng chuẩn thứ ba đưa ra những vấn đề trong vận hành cơ sở dữ liệu, chẳng hạn, sẽ không thể lưu thời hạn hoàn thành cho một dự án cho tới khi dự án được gán cho một bộ. *So sánh với* first normal form, second normal form, normal form. *Xem* candidate key, functional dependence, nonprime attribute, normal form, relational database, transitive dependence.

third party transfer ***chuyển thanh toán cho bên thứ ba*** Trong hoạt động ngân hàng, một sự chuyển thanh toán có lợi cho bên thứ ba chứ không phải cho người gửi hay nhận.

threaded tree ***cây liên kết*** Trong tính toán, một cây mà các con trỏ bổ sung có tham dự rà soát cây. *Xem* tree, pointer, scan.

threat ***hiểm họa, mối đe dọa*** (1) Trong an toàn máy tính, biện pháp qua đó có thể biểu lộ khả năng hay ý định của một tác nhân đe dọa gây bất lợi tới một hệ thống, phương tiện hay thao tác tự động. Sự phân hạng theo hệ thống và phân lớp các hiểm họa như sau:

Các hạng	*Các lớp*
Con người	Chủ tâm
	Không chủ tâm
Môi trường	Tự nhiên
	Nhân tạo

Xem threat agent, vulnerability. (2) Trong quản lý rủi ro, sự vi phạm tiềm ẩn tính an toàn. (3) Trong an toàn máy tính, hoàn cảnh hay sự cố tiềm ẩn gây nên thiệt hại cho hệ thống ADP hoặc hoạt động ở dạng phá hoại, làm lộ, biến đổi dữ liệu hoặc từ chối phục vụ. Hiểm họa là một khả năng gây hại. Sự tồn tại hiểm họa không có nghĩa là sẽ nhất thiết gây hại thực sự. Nó tồn tại bởi chính sự hiện hữu của hệ thống hay hoạt động chứ không phải vì nhược điểm đặc biệt bất kỳ nào. Ví dụ, hiểm họa hỏa hoạn tồn tại ở tất cả các phương tiện trừ phi lực lượng chống hỏa hoạn luôn sẵn sàng. *Xem* denial of service. (4) Trong quản lý rủi ro, một khía cạnh của môi trường hệ thống mà nếu có cơ hội, có thể gây ra sự cố có hại. *So sánh với* safeguard. *Xem* harmfull event, matrix methodology, vulnerability.

threat agent ***tác nhân gây hiểm họa*** Trong quản lý rủi ro, các phương pháp và những thứ được dùng để lợi dụng một khả năng dễ tổn thương trong một hệ thống, một phương tiện hay hoạt động thông tin, ví dụ, hỏa hoạn, thảm họa thiên nhiên... *Xem* threat.

threat analysis ***phân tích hiểm họa*** Trong mật mã, quá trình tiến hành các thao tác phân tích mật mã, chẳng hạn trong sơ đồ quản lý khóa, theo một loạt các tấn công giả định. *So sánh với* cryptanalysis. *Xem* key management.

threat monitoring ***giám sát hiểm họa*** Trong an toàn máy tính, sự phân tích, đánh giá và nhìn nhận lại các vệt kiểm toán và các dữ liệu khác thu thập được nhằm tìm ra những sự kiện có tính hệ thống có thể tạo ra các vi phạm hay dẫn tới rắc rối liên quan tới các vấn đề về dữ liệu riêng tư. *Xem* audit trail.

threat team ***đội chống hiểm họa*** Trong an toàn máy tính, một đội gồm những nhân viên chủ chốt trong một tổ chức có nhiệm vụ tìm những hiểm họa và những điểm yếu trong một hệ thống và họ tạo ra các bối cảnh có thể xảy ra về sự tấn công lên hệ thống. *Xem* threat monitoring, tiger team.

three-layer architecture ***kiến trúc khóa ba lớp*** Trong quản lý khóa, một hệ thống trong đó khóa mã khóa được phân phối thủ công và khóa này được dùng để mã khóa mã khóa lớp thứ hai. Khóa này là đối tượng phân phối tự động. Các khóa dữ liệu là khóa lớp thứ ba, chúng được mã hóa bằng khóa mã khóa mức hai để phân phối tự động. *So sánh với* two-layer architecture. *Xem* ANSI X9.17 - 1985, cryptographic key, data key, key-encrypting key.

threshold ***ngưỡng*** Trong quản lý khóa, nói tới một kỹ thuật bảo vệ các khóa chính chống tiết lộ và phá hoại. Nhiều sơ đồ quản lý khóa dùng sự phân cấp bằng một khóa chính đơn ở mức cao nhất. Nếu khóa này bị lộ thì toàn hệ thống rất dễ bị tổn thương trước hành động bất hợp pháp; mặt khác, nếu chỉ có bản sao của nó bị phá thì những người sử dụng hợp pháp không thể truy nhập tới thông tin đã mã.

Nếu các bản sao của khóa chính được phân phối tới những nơi giữ đáng tin cậy thì các nguy cơ tiết lộ khóa chắc chắn sẽ tăng lên. Kỹ thuật ngưỡng cố gắng cải thiện vấn đề này qua việc

phân phối những đoạn khóa cho những người đáng tin cậy. Khóa (K) được chia thành n mảnh được gọi là các phần chia (đoạn khóa). Sự phân chia khóa được thực hiện theo cách sau:

- nếu có m phần chia bất kỳ trong số các phần chia thì rất dễ tính được khóa K;
- không thể tính toán được khóa K với $m - 1$ phần chia hoặc ít hơn m phần chia.

Như vậy, nếu không có hơn $m - 1$ người giữ làm mất các đoạn khóa của mình, hoặc hiệp sức cùng nhau để khôi phục lại được khóa K thì khóa sẽ không bị lộ. Mặt khác, nếu một hay hiều hơn phần chia bị mất một cách ngẫu nhiên thì vẫn có thể khôi phục lại được khóa miễn là ít nhất vẫn còn m phần chia. Kỹ thuật phân tách có những tính chất nêu trên có thể được thực hiện bằng các phương pháp toán học xác định. *Xem* cryptographic key, secret sharing.

throughput ***năng suất*** Một đại lượng đo lượng công việc hữu ích do hệ thống thực hiên trong khoảng thời gian cho trước.

ticket ***thẻ, tích kê, nhãn (kiểm)*** Trong kiểm soát truy nhập, một thuật ngữ được dùng trong hệ thống Kerboros. Nó thực hiện nhiệm vụ tương tự như một chứng chỉ trong hệ thống mã không đối xứng. Thẻ chứa tên của máy khách và máy chủ, địa chỉ mạng của máy khách, thời hạn hết hiệu lực, tem thời gian và một khóa phiên DES dùng giữa máy khách và máy chủ. Thẻ sau đó được mã hóa bằng khóa mật mã chỉ máy chủ phát hành thẻ biết được và là máy chủ mà máy khách muốn truy nhập tới. Thẻ được chuyển tiếp tới máy khách. *Xem* certificate, data encryption standard, Kerboros, symmetric cipher.

tie line ***tuyến liên kết, đường dây liên kết*** *Đồng nghĩa với* tie trunk.

tie trunk ***đường trục liên kết*** Trong liên lạc, một kênh liên lạc điểm tới điểm kết nối các hệ hoặc tổng đài điện thoại nhánh lẻ (PBX). *Đồng nghĩa với* tie line.

tiger team ***đội con cọp*** Trong an toàn máy tính, một nhóm người được ủy quyền để kiểm tra tính an toàn tổng thể của một hệ thống bằng lối vào "mọi" (không hợp pháp) hoặc các biện pháp khác. *Xem* threat team.

time and space requirements ***(các) yêu cầu không gian và thời gian*** Trong toán học, bậc độ lớn của các yêu cầu tính toán trong lời giải của một thuật toán. Yêu cầu về không gian hoặc thời gian được nói tới là thời gian đa thức nếu nó là bậc của n^t với t là hằng số còn n đặc trưng cho kích thước của đầu vào. Nếu $t = 0$ thì yêu cầu là hằng số, nếu $t = 1$ thì yêu cầu là tuyến tính, nếu $t = 2$ thì nó là bình phương v.v.. Nếu yêu cầu không gian hoặc thời gian là bậc của $t^{f(n)}$ trong đó $f(n)$ là đa thức thì yêu cầu là hàm mũ.

time bomb ***bom hẹn giờ, bom thời gian*** Trong an toàn máy tính, một dạng con ngựa thành Toroa có hành động ác ý được khởi sự trong những thời điểm và vào ngày tháng nhất định. *Xem* malicious code, Trojan Horse.

time-date stamp ***tem thời gian -***

ngày tháng Trong an toàn dữ liệu, một trường trong thông báo chỉ thời gian và ngày tháng ra thông báo. *Xem* replay.

time-dependent password ***mật khẩu phụ thuộc thời gian*** Trong kiểm soát truy nhập, một mật khẩu chỉ hợp lệ vào thời gian nhất định trong ngày hoặc trong khoảng thời gian nào đó. *Xem* password.

time-derived channel ***kênh dẫn xuất theo thời gian*** Trong liên lạc dữ liệu, một kênh nhận được nhờ phép dồn kênh chia thời gian. *Xem* time division multiplexing.

time division multiple access ***đa truy nhập phân thời*** Trong liên lạc dữ liệu, một kỹ thuật trong hệ thống dồn kênh phân thời trong đó một chuỗi các khe thời gian được cấp cho những người dùng theo yêu cầu của họ. *So sánh với* frequency division multiple access. *Xem* division multiplexing.

time division multiplexing ***dồn kênh phân thời*** Trong liên lạc, một phương pháp cấp phát một kênh dung lượng cao cho một số cặp người gửi/người nhận. Thông tin từ mỗi người gửi được cấp theo các khoảng thời gian trong kênh chính và các phần của các thông báo được chen vào đó cùng với những thông báo của những người sử dụng khác tại đầu vào của kenh. Các đoạn thông báo được tách riêng còn thông báo đầy đủ được khôi phục lại tại bên thu. Sự giảm chi phí của mạch số làm nó trở nên rẻ hơn kỹ thuật dồn kênh phân tần đòi hỏi các mạch lọc tương tự đắt tiền. Tuy nhiên, nó chỉ có thể dùng được cho các tín hiệu số. Các tín hiệu tương tự như tiếng nói phải được chuyển thành dạng số bằng phép điều chế mã xung (PCM) trước khi có thể dùng kỹ thuật này. *So sánh với* frequency division multiplexing. *Xem* analog signal, digital signal, packet switching, PCM.

time division switching ***chuyển mạch phân thời*** Trong liên lạc dữ liệu, một phương pháp chuyển mạch cho các kênh dồn kênh phân thời. Dữ liệu đưa vào tầng chuyển mạch trong một khe thời gian và hợp vào trong những dữ liệu khác. Để chuyển mạch các kênh điều chế mã xung, mỗi khe thời gian chứa một mẫu đã mã, ví dụ mã 8 bit. *So sánh với* space division switching. *Xem* time division, multiplexing, pulse code modulation.

time element scrambler ***bộ xáo trộn phần tử thời gian*** Trong an toàn liên lạc, một dạng xáo trộn tiếng nói dựa trên các kỹ thuật dồn kênh phân thời. Tín hiệu tiếng nói được chia thành các khung dài cỡ vài trăm miligiây, và các khung lại được chia nhỏ hơn thành các đoạn dài từ 20 tới 60 miligiây. Phép xáo trộn được thực hiện bằng cách hoán vị thứ tự của các đoạn trong phạm vi một khung. Các hoán vị được thay đổi theo dãy chỉ máy thu và máy phát biết. *Xem* time division multiplexing, voice scrambling.

time limit cutout ***ngắt hạn chế thời gian*** Trong an toàn vật lý, một hệ thống hạn chế thời khoảng của tín hiệu báo động bằng cách đưa ra khoảng thời gian cố định hay thay đổi. *Xem* alarm signal.

time out ***thời gian ấn định; quá giờ, hết giờ*** (1) Trong tính toán, thời gian ấn định là khoảng thời gian quy định cho một số hoạt động xảy ra. (2) Trong tính toán, hết giờ là tính năng của thiết bị đầu cuối cho một người sử dụng rời hệ thống nếu mục đầu vào không được thực hiện trước khi hết một khoảng thời gian nhất định. *Xem* log off.

time redundancy ***dư thừa thời gian*** Trong lĩnh vực độ tin cậy, một kỹ thuật trong đó một phần của một chương trình được dùng để kiểm tra đúp các tính toán quan trọng. Hoặc cùng chương trình con được lặp lại hoặc dùng thuật toán khác. *So sánh với* special redundancy.

time sharing ***phân thời, chia sẻ thời gian*** Trong tính toán, một kỹ thuật cho phép máy tính quản lý đồng thời những người dùng và các ngoại vi. Mỗi hoạt động của máy tính được thực hiện theo thứ tự song tốc độ cao, cùng với kỹ thuật phân chia nhỏ thời gian tạo ra dáng vẻ của dịch vụ đa người dùng đồng thời.

time slice ***lát thời gian, thời lượng*** Trong tính toán, khoảng thời gian của bộ xử lý không giành quyền ưu tiên trước được cấp cho một nhiệm vụ cụ thể trong hệ thống chia sẻ thời gian. Tất cả các tác vụ đều nhận được các lát thời gian luân phiên cho tới khi chúng hoàn thành, như vậy, không có tác vụ nào có thể độc quyền bộ xử lý. *Xem* time sharing.

time stamp ***tem thời gian, dấu thời gian*** *Xem* time-date stamp.

Tiny ***virut Tiny*** Trong an toàn máy tính, một loại virut lây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian chạy và làm hỏng các tệp chương trình và OVL. *Xem* virus names.

Tiny-133 ***virut Tiny-133*** Trong an toàn máy tính, một loại virut lây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian chạy và làm hỏng các tệp chương trình và OVL. *Xem* virus names.

TLS *Xem* top-level specification.

TMR *Xem* triple modular redundancy.

T network ***mạng chữ T*** Trong điện tử học, một mạng chứa ba phần tử được kết nối chung theo dạng chữ T.

TNF *Xem* third normal form.

TNI ***diễn dịch mạng tín nhiệm*** Trong an toàn liên lạc, viết tắt của Trusted Network Interpretation (diễn dịch mạng tín nhiệm) của tiêu chuẩn đánh giá hệ thống máy tính tin cậy. *Xem* TCSEC.

TOCTTOU problems ***(các) bài toán TOCTTOU*** Trong an toàn máy tính, viết tắt của Time Of Check To Time Of Use (thời điểm kiểm tra tới thời điểm sử dụng), một lớp các bài toán nảy sinh do những thay đổi bất hợp pháp sau khi đã thực hiện kiểm tra. Ví dụ, một yêu cầu về hệ điều hành được kiểm tra và đã thấy là hợp lệ song sau đó, một tham số của yêu cầu bị thay đổi trước khi nó được thực hiện. *Xem* asynchronous attack.

TOE *Xem* target of evaluation.

token ***thẻ bài, thẻ kiểm soát*** (1) Trong kiểm soát truy nhập, một thiết bị vật lý cần thiết để xác thực người

sử dụng. (2) Trong kiểm soát truy nhập, một đối tượng vật lý phải được một cá nhân có yêu cầu truy nhập giữ. *Xem* something the user has. (3) Trong liên lạc dữ liệu, một mẫu các bit mà một máy trạm phải thu được trước khi nó được phép truyền rộng rãi một tín hiệu. *Xem* token bus, token ring.

token authenticator ***bộ xác thực thẻ bài*** Trong kiểm soát truy nhập, một mãy tính cỡ bỏ túi có thể tham gia trong một sơ đồ xác thực theo mô hình hỏi/đáp. *Xem* challenge/response.

token bus ***bus dùng thẻ bài*** Trong truyền thông dữ liệu, một giao thức cho mạng cục bộ dùng một cấp dạng cây hay tuyến tính. Các máy trạm được nối với nhau theo một vòng logic, mỗi máy trạm có địa chỉ của hai trạm nằm hai bên của nó trong vòng logic này; chúng nhận một thẻ bài từ trạm bên cạnh và chuyển tiếp nó tới trạm tiếp sau trong mạng vòng. Các trạm chỉ được phép truyền khi nó giữ thẻ bài. *So sánh với* IEEE 802.3, token ring. *Xem* local area network, token.

token management ***quản lý thẻ bài*** Trong truyền thông dữ liệu, một kỹ thuật được dùng để bảo đảm rằng, hai hệ thống không hành động giống nhau đồng thời. Chỉ một hệ thống giữ thẻ bài mới được phép thực hiện hoạt động chủ chốt. *Xem* token bus, token ring.

token ring ***mạng vòng dùng thẻ bài*** Trong truyền thông dữ liệu, một kiến trúc mạng kiểu vòng trong đó, mỗi nút sẽ đợi một thẻ bài điều khiển tới từ nút theo hướng ngược lại trước khi gửi một thông báo tới nút theo hướng xuôi tiếp sau. Trên mạng, tại một thời điểm chỉ có một thẻ bài; khi một nút có thông báo cần gửi đi nhận được thẻ bài, nó sẽ truyền thông báo tiếp sau thẻ, thẻ chuyển qua các nút cho tới khi nó đến nút có thông báo truyền. *So sánh với* carrier sense multiple access - collision detection, token bus. *Xem* control token, IEEE 802.5, local area network.

TOP *Xem* technical and office protocol.

top down method ***phương pháp từ trên xuống*** Một phương pháp thiết kế hệ thống hay chương trình máy tính bắt đầu từ kiến trúc tổng thể đơn giản, sau đó mới đi vào chi tiết tinh tế để mô tả các thành phần nhỏ tương tự cho tới khi nhận được kiến trúc chi tiết.

top-level specification ***đặc tả mức cao*** Sự mô tả không tuân theo thủ tục về hành vi của hệ thống ở mức trừu tượng nhất. Thông thường, một đặc tả chức năng sẽ bỏ qua tất cả các chi tiết thực hiện. *Xem* descriptive top-level specification, formal top-level specification.

topology ***cấu trúc liên kết, topo*** Trong liên lạc, dạng kết nối các nút trong một mạng. *Xem* bus, ring, node, star.

Top Secret ***tối mật*** *Xem* classification.

top secret clearance ***mức truy nhập tối mật, mức thông tối mật*** Trong kiểm soát truy nhập, các mức truy nhập của Bộ Quốc Phòng (Hoa Kỳ), là mức truy nhập được quy định là tối mật dựa trên sự điều tra cơ bản hiện tại (TS(BI)), hoặc là mức truy nhập tối mật dựa trên sự điều tra cơ bản đặc biệt hiện tại

(TS(SBI)). Mức truy nhập tối mật được dựa trên sự điều tra cơ bản hiện tại đòi hỏi sự điều tra gồm có sự kiểm tra của cơ quan an ninh, các tiếp xúc cá nhân, nghiên cứu hồ sơ và thẩm tra bằng văn bản. Thông thường nó gồm sự điều tra rộng tới 5 năm trước đó, thường là kiểm tra dấu vết 15 năm về trước. Mức truy nhập tối mật dựa trên sự điều tra cơ bản đặc biệt hiện tại, đòi hỏi ngoài sự điều tra giống TS(BI) còn thêm những kiểm tra về họ hàng gần gũi nhất của đối tượng (nếu sinh ở nước ngoài), về vợ (chồng), láng giềng để xác minh mỗi nơi cư trú trước đó của đối tượng ở Hoa Kỳ, nơi mà đối tượng đã cư trú 6 tháng hoặc hơn nữa. Nó gồm cả sự điều tra rộng về 15 năm trở về trước. *So sánh với* confidential clearance, multiple categories, one category, secret clearance, unclassified information, uncleared. *Xem* clearance.

TP *Xem* transformation procedure, transaction processing.

Traceback ***virut Traceback*** Trong an toàn máy tính, một loại virut chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COM và EXE, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

trace packet ***gói vạch vết, gói đò dấu vết*** Trong liên lạc dữ liệu, một gói khiến cho một báo cáo tiến trình trên mỗi giai đoạn của nó qua mạng được truyền tới trạm kiểm soát mạng. *Xem* network control station, packet switching, packet switching network.

tracker ***trình theo dõi, bộ theo dõi*** Trong an toàn cơ sở dữ liệu, một kỹ thuật được kẻ tấn công dùng để phá hoại một hệ thống bằng cách lợi dụng sự kiểm soát kích cỡ tập hợp các câu truy vấn. Một yêu cầu đối với một tập nhỏ các bản ghi được đếm có chủ ý bằng các bản ghi lớn cho tới khi tập câu truy vấn đủ lớn để đáp ứng tiêu chuẩn kiểm soát kích cỡ tập câu truy vấn. Sau đó kẻ tấn công trừ kết quả về các bản ghi đếm khỏi các thống kê đã đưa ra. *Xem* inference control, query set, query set size control, record.

tractable ***có thể giải được, có thể kiểm soát được*** Trong lý thuyết độ phức tạp, nói tới bài toán có thể giải được trong thời gian đa thức. *So sánh với* intractable. *Xem* time and space requirements.

trade cycle ***chu trình thương mại*** *Đồng nghĩa với* banking cycle.

traffic ***lưu lượng tin*** Trong liên lạc, các tín hiệu hay thông báo do một hệ thống thông tin xử lý.

traffic analysis ***phân tích lưu lượng*** (1) Trong an toàn liên lạc, sự suy luận ra thông tin từ việc quan sát các lưu lượng (có, không có, số lượng, hướng và tần số). *Xem* traffic flow confidentiality, traffic padding. (2) Quá trình giám sát các tuyến, không chấn thông tin đang truyền song lại xác định được tốc độ truyền. (3) Trong an toàn liên lạc, một dạng tấn công thụ động trong đó kẻ phá hoại theo dõi địa chỉ đích và địa chỉ nguồn, tần số và độ dài các thông báo. Các biện pháp đối phó với sự phân tích lưu lượng là ngụy trang các mẫu trong thông báo để lộ địa chỉ nguồn/đích, độ dài thông báo

v.v. Phép mã liên kết (link encryption) tự động chống lại sự phân tích lưu lượng vì các phần tiêu đề thông báo cũng như các nội dung của nó đều được mã hóa. Trong trường hợp mã điểm tới điểm, mức bảo vệ chống lại phân tích lưu lượng phụ thuộc vào mức áp dụng mã hóa. Gần như không thể ngụy trang lưu lượng ở mức máy chủ tới máy chủ (host to host), muốn làm như vậy, cần phải nhân đôi các thông báo cho tất cả các máy chủ và như vậy gây nên sự tràn lưu lượng trên mạng. Nếu dùng mã hóa ở mức cao, chẳng hạn, ở mức người dùng riêng thì tất cả các ghi chép tiêu đề thông báo tiếp sau phải được cộng vào bản rõ. Trong trường hợp này, sự phân tích lưu lượng sẽ tạo ra thông tin chính xác ở mức người dùng. Mặt khác, nếu các thông báo được mã hóa ở mức thấp hơn thì các mẫu lưu lượng trong phạm vi máy chủ sẽ được ngụy trang. *Xem* end-to-end encryption, link encryption, network encryption, OSI security, passive attack, traffic flow security, traffic padding. *Đồng nghĩa với* violation of transmission security.

traffic flow confidentiality ***bảo mật dòng lưu lượng*** Trong an toàn liên lạc, một dịch vụ giữ bí mật để bảo vệ chống lại sự phân tích lưu lượng. *Xem* traffic analysis.

traffic flow security ***an toàn luồng thông tin*** Trong an toàn liên lạc, sự bảo vệ nhận được từ những tính năng trong thiết bị mật mã nào đó, cho phép che dấu những thông báo có giá trị trên mạch liên lạc, thường là bằng cách tạo ra mạch bận mọi lúc, hoặc bằng cách mã hóa các địa chỉ nguồn và đích của những thông báo có giá trị. *Xem* cryptographic equipment, encrypt, traffic analysis, traffic padding.

traffic padding ***đệm lưu lượng*** (1) Trong an toàn liên lạc, sự tạo ra những tình huống liên lạc giả, các khối dữ liệu giả và dữ liệu giả trong các khối dữ liệu. *Xem* traffic analysis. (2) Trong an toàn liên lạc, một kỹ thuật được dùng để phân biệt các luồng thông tin; nó bao gồm việc đệm các thông báo ngoài độ dài chuẩn, tạo các thông báo giả và các nối giả. *Xem* traffic analysis, traffic flow security. (3) Trong an toàn liên lạc, sự tạo ra các tình huống liên lạc giả, các khối dữ liệu giả và/hoặc các dữ liệu giả trong các khối dữ liệu.

trailer ***nhãn đuôi; bản ghi kết thúc*** (1) Trong tính toán, nhãn đuôi là nhãn nằm cuối một băng từ, đưa ra các thống kê tóm tắt về dữ liệu được ghi. (2) Trong tính toán, một bản ghi kết thúc là một bản ghi tại phần cuối của một tệp chứa thông tin tóm tắt trên các bản ghi dữ liệu hợp thành. *Xem* file, magnetic tape, record.

tranquility ***quy tắc bình lặng*** Trong an toàn máy tính, một quy tắc của mô hình an toàn phát biểu rằng, mức an toàn của một đối tượng chủ động sẽ không thay đổi. *Xem* object, security level, security model.

transaction ***giao dịch, giao tác, toàn tác*** (1) Trong hoạt động ngân hàng, một đối thoại giữa thiết bị đầu cuối và người nhận (acquirer) được tiến hành theo một tập các khóa mã, tập khóa

giao tác. *Xem* funds transfer transaction, transaction key set. (2) Trong cơ sở dữ liệu, một khối công việc rời rạc. Nó xoay quanh việc cập nhật một số trường trong cơ sở dữ liệu và nó phải được thi hành trong trạng thái toàn vẹn để tránh những mâu thuẫn về dữ liệu. *Xem* field.

transaction code ***mã giao tác, mã toàn tác*** (1) Trong xử lý dữ liệu, một trường trong bản ghi giao tác quy định bản chất của giao dịch. *Xem* field, record.

transaction driven system ***hệ điều vận bằng toàn tác, hệ giao tác dẫn hướng*** Trong tính toán, một chế độ hoạt động trong đó, một giao tác xảy ra sẽ làm gián đoạn các hoạt động xử lý theo lô khi các tài nguyên được chuyển hướng để giải quyết giao tác *Xem* transaction processing.

transaction key ***khóa giao dịch*** (1) Trong hoạt động ngân hàng, một khóa mật mã dùng để mã và giải mã dữ liệu trong một thông báo và để tính (hay xác minh) mã xác thực thông báo đi theo thông báo. Khóa giao dịch là duy nhất về mặt thống kê đối với hai nhóm cụ thể (thiết bị đầu cuối và người nhận) và chỉ hợp lệ trong thời gian một giao dịch đơn lẻ. *Xem* acquirer, key management, message authentication code, statistically unique, transaction. (2) Trong quản lý khóa, khóa được dùng để mã hóa dữ liệu của một giao dịch riêng lẻ. *So sánh với* session key. *Xem* decoupling key.

transaction key set ***bộ khóa giao dịch, tập khóa giao tác*** Trong hoạt động ngân hàng, một bộ chứa một hay nhiều khóa giao dịch hợp lệ nhận được từ một giá trị của thanh ghi khóa riêng lẻ và một nguồn các khóa tách riêng. Trong chế độ dựa trên thẻ, nguồn các khóa tách riêng là thẻ dùng cho cuộc giao dịch hiện tại. Các khóa tách riêng khác nhau được tạo ra để đạt được tính an toàn tương tác giữa các nhóm tham gia giao dịch. *Xem* card based mode, decoupling key, key register, transaction key.

transaction key system ***hệ thống khóa giao dịch*** Trong quản lý khóa, một sơ đồ được mô tả theo Chuẩn Australia 2805.6.2 đã phát triển cho mạng EFTPOS. Nó khác với hệ thống phiên chính thông thường và không đòi hỏi tải xuống và mã khóa phiên bằng khóa mã khóa.

Môi trường cho sơ đồ gồm các thiết bị đầu cuối EFTPOS ở cơ sở của những người bán lẻ, những người nhận (acquirer) và người phát hành thẻ. Thiết bị đầu cuối EFTPOS chuyển các giao dịch tới người nhận (acquirer), những người này xử lý mật mã thông báo và chuyển tiếp nó tới người phát hành thẻ phù hợp để kiểm tra PIN và giấy phép giao dịch.

Sơ đồ được thiết kế để:

- PIN không bị lộ ngay cả khi các khóa phiên giữa thiết bị đầu cuối và người nhận (acquirer) bị tổn thương;
- các giấy phép giao dịch chỉ có thể được người phát hành thẻ phát ra, ngay cả khi các khóa phiên giữa thiết bị đầu cuối và người nhận (acquirer) bị tổn thương.

Thiết bị đầu cuối dùng hai bộ khóa

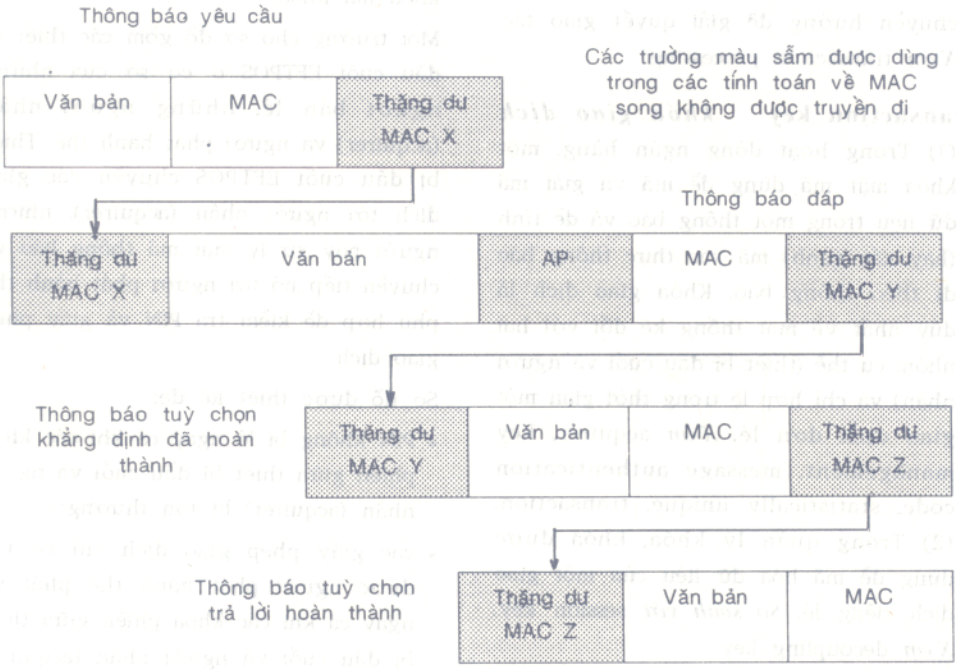
mã/biến hiệu quả. Một bộ được dựa trên khóa terminal hiện tại mà chỉ thiết bị đầu cuối và người nhận (acquirer) biết. Bộ khóa thứ hai nhận được từ "Dữ liệu Thẻ khác" chỉ thiết bị đầu cuối và người phát hành thẻ biết.

Khóa terminal đầu tiên được nạp thủ công vào thiết bị đầu cuối và hệ thống của người nhận (acquirer). Khi giao dịch được thực hiện, các chi tiết về khách hàng được đọc từ thẻ. Những chi tiết này gồm Số tài khoản gốc (PAN) và Dữ liệu Thẻ khác (OCD). Khóa terminal được dùng cùng với các trường của PAN và các hằng số để tạo ra khóa riêng K_{pr}, khóa MAC là KMAC và khoá mã PIN là KPE. Trong mỗi trường hợp đều dùng hàm một chiều.

Thông báo yêu cầu giao dịch được tạo ra gồm Số Tài khoản Gốc; MAC được lập ra cùng với KMAC và thông báo được truyền đi. Người nhận (acquirer) sẽ triển khai một thông báo trả lời gồm thặng dư MAC của thông báo yêu cầu khi thặng dư MAC được tính toán, song nó không được truyền đi cùng với thông báo trả lời. Kỹ thuật này liên kết mật mã các thông báo yêu cầu và trả lời.

Khi giao dịch đã hoàn thành, khóa terminal được cập nhật bằng hàm một chiều, khóa terminal hiện hành và thặng dư MAC của thông báo hỏi/đáp. Như vậy, sự cập nhật khóa terminal là chức năng của giao dịch song lại dùng dữ liệu không thực sự được truyền đi.

Dữ liệu Thẻ khác (OCD) là một trường đặc biệt trên thẻ có sọc từ. Nó được



transaction key system: *hệ thống khóa giao dịch.*

đọc bằng đầu cuối chỉ người phát thành thẻ biết song không được truyền đi tới người nhận (acquirer). OCD được dùng cùng với thông tin khác chẳng hạn như PAN, lượng giao dịch, bộ phận nhận diện thiết bị đầu cuối, số hiệu dãy thông báo v.v. trong sự phát triển của khóa thẻ (KC) và tham số cấp phép AP. PIN được mã hóa đầu tiên bằng KC rồi sau đó bằng KPE. Người nhận giải mã khối PIN bằng KPE và chuyển tiếp *e*KC (khối PIN) (khối này được mã bằng khóa phiên để liên kết với người phát hành thẻ người nhận (acquirer-card)) tới người phát hành thẻ. Người phát hành thẻ tính toán KC từ OCD... , giải mã khối PIN, kiểm tra PIN, tính tham số cấp phép dựa trên Dữ liệu Thẻ khác, lượng giao dịch... cho người nhận (acquirer). AP giống như thặng dư MAC nằm trong thông báo đáp giữa người nhận - thiết bị đầu cuối để mã xác thực thông báo song không được truyền đi.

Như vậy, nhà doanh nghiệp có thể được bảo đảm rằng, thông báo cấp phép đã được triển khai nhờ dùng AP chỉ do người phát hành thẻ khởi đầu. *Xem* aquirer, EFTPOS, key management, one-way function, other card data, PIN, primary account number.

transaction number ***số hiệu giao dịch*** Trong hoạt động ngân hàng, một kỹ thuật an toàn trong hoạt động ngân hàng tại nhà trong đó, khách hàng được cung cấp một lô các số ngẫu nhiên qua bưu điện. Lần lượt, mỗi giao dịch do khách hàng khởi đầu phải chứa số hiệu giao dịch kế tiếp trong lô, ngoài ra còn có số tài khoản và PIN. Kỹ thuật này bảo đảm kẻ nghe trộm không thể nhận được đủ thông tin từ một cuộc giao dịch để tiến hành một giao dịch gian lận sau đó. *Xem* home banking security.

Transaction/Payment Message ***thông báo giao dịch/thanh toán*** Trong hoạt động ngân hàng, một thông báo chứa một chỉ thị cho người nhận để thanh toán hoặc thông báo đã thanh toán xong. Nó gồm các giao dịch của khách hàng và các chuyển khoản của ngân hàng.

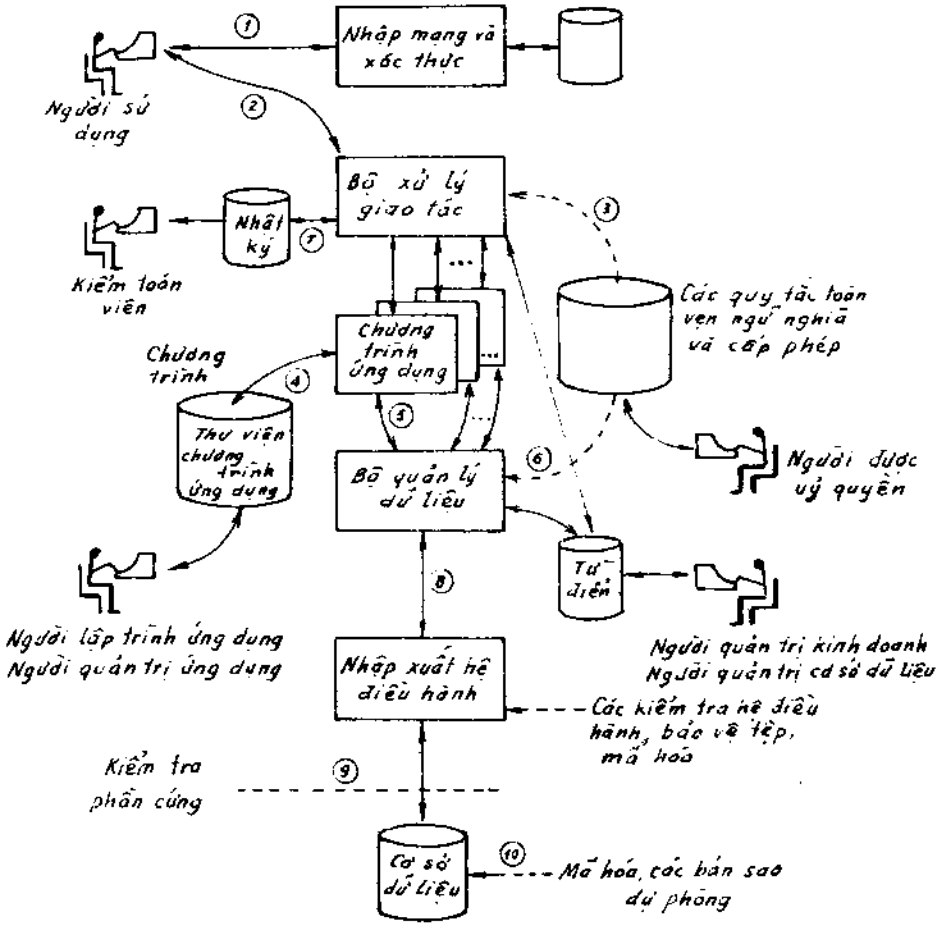
transaction processing ***xử lý giao tác*** Trong tính toán, một chế độ sử dụng máy tính mà người dùng nhập dữ liệu và ra lệnh từ một thiết bị ở xa, thường là qua kết nối truyền thông. Các kết quả được hiển thị trên thiết bị đầu cuối. Một chế độ hoạt động tương tự đối với tính toán nhiều người dùng; thường nó được sử dụng khi người dùng đang làm việc với một gói ứng dụng đặc biệt. *Xem* transaction driven system.

transaction set ***tập giao tác*** *Xem* ANSI - X.12.

transaction trail ***vết giao dịch*** *Đồng nghĩa với* audit trail.

transborder data flow ***dòng dữ liệu vượt đường biên*** Trong liên lạc dữ liệu, dòng dữ liệu giữa các nước hay các quốc gia và bởi vậy được chuyển từ phạm vi quyền hạn này tới phạm vi quyền hạn khác. Điều này thể hiện một lĩnh vực khá phức tạp dưới góc độ pháp luật khác nhau đối với việc bảo vệ dữ liệu, bản quyền... ở những khu vực khác nhau trên thế giới. *Xem* copyright, data protection, software protection, transborder restrictions.

transborder restrictions *(các) hạn chế vượt đường biên* Trong liên lạc dữ liệu, nói tới những hạn chế được đặt lên trên dòng dữ liệu mã chuyển qua đường biên giữa các nước. Ở bên ngoài Hoa Kỳ, vấn đề này thường là trách nhiệm của cơ quan trung ương của Chính phủ mà thường là PTT.



transaction processing: *xử lý giao tác*. Một số biện pháp phòng vệ được xây dựng trong một hệ thống cơ sở dữ liệu. (1) Người dùng đăng nhập và được xác thực; (2) người dùng cố giao dịch, (3) và được phê chuẩn. Quá trình giao tác có thể gồm: truy lục các chương trình từ một thư viện (4) và các yêu cầu dữ liệu (5) tới hệ thống quản trị cơ sở dữ liệu. Sự cấp quyền được kiểm tra một lần nữa (6) và DBMS duy trì một nhật ký về sự truy nhập tới cơ sở dữ liệu (7). Khi các yêu cầu truy nhập tới cơ sở dữ liệu được phê chuẩn, chúng được chuyển thành các cuộc gọi I/O và chuyển tới hệ điều hành (8). Phần cứng có thể bổ sung khả năng bảo vệ (9) và dữ liệu có thể được mã hóa (10).

Những quy định có thể giải quyết là:

- cấm dòng dữ liệu mã chuyển qua đường biên;
- dòng dữ liệu mã chuyển qua đường biên được cho phép khi khóa mã được đăng ký với cơ quan bảo vệ dữ liệu;
- bắt buộc không có các hạn chế.

OECD đã thông qua và chấp nhận một tập tối thiểu các chuẩn bảo vệ mà các nước thành viên phải đáp ứng. Nó được mô tả trong ấn phẩm Các đường lối chủ đạo Quản lý việc Bảo vệ các dòng Dữ liệu và Dữ liệu cá nhân Chuyển qua đường biên. *Xem* data protection, transborder data flow.

transceiver ***máy thu phát, bộ phận thu phát*** Trong phần cứng, một bộ điều khiển bus có thể chuyển dữ liệu theo hai hướng vì thế kết hợp cả nhiệm vụ của máy phát và thu. *Xem* receiver, transmitter. *Xem* bus driver.

transfer ***(sự) chuyển khoản*** *Xem* funds transfer, funds transfer transaction.

transformational coding ***phép mã biến đổi*** Trong các phép mã, sự áp dụng một tập không có ngoại lệ các quy tắc trong phép biến đổi dữ liệu thành dạng đã mã.

transformational procedure ***thủ tục biến đổi*** Trong các mô hình hình thức, một thuật ngữ được dùng trong mô hình Clark-Wilson. Thủ tục biến đổi là một chương trình con được phép cập nhật một mục dữ liệu bị ràng buộc theo các thủ tục chứng thực. *Xem* Clark Wilson model, constrained data item.

transitive dependence ***(sự) phụ thuộc bắc cầu*** Trong các cơ sở dữ liệu quan hệ, sự phụ thuộc gián tiếp giữa các thuộc tính. Giả sử A, B và C là ba thuộc tính hay các tập hợp riêng biệt các thuộc tính của quan hệ R. Nếu C phụ thuộc chức năng vào B và B phụ thuộc chức năng vào A thì C sẽ phụ thuộc chức năng vào A, nếu A không phụ thuộc chức năng vào B hoặc B không phụ thuộc chức năng vào C thì C là phụ thuộc có tính bắc cầu vào A. *Xem* functional depedence.

translation cipher ***mã pháp tịnh tiến*** Trong mật mã, một dạng mã thay thế đơn giản trong đó, mỗi ký tự được mã hóa nằm ở khoảng cách cố định trong bảng chữ cái so với ký tự bản rõ tương ứng. Ví dụ với phép dịch 5, F sẽ thay thế cho A, G thay thế cho B... *Đồng nghĩa với* additive cipher. *Xem* Ceasar cipher.

translator ***bộ dịch*** Trong liên lạc, một thiết bị chuyển thông tin từ hệ thống biểu diễn này sang hệ thống biểu diễn khác, chẳng hạn, chuyển các chữ số quay số thành thông tin định tuyến cuộc gọi.

transmission ***(sự) phát, (sự) truyền*** (1) Trong hoạt động ngân hàng, một dãy dữ liệu, chẳng hạn các thông báo và trả lời, được truyền giữa hai nhóm và hoạt động từ lúc thiết lập nối đến lúc nó chấm dứt. (2) Trong liên lạc, hoạt động gửi thông tin từ vị trí này tới vị trí khác để lại thông tin nguồn không bị thay đổi.

transmission control protocol ***giao thức kiểm soát sự truyền dữ liệu*** Trong liên lạc dữ liệu, một giao thức

vận tải cho mạng định hướng nối. *Xem* TCP/IP, transport layer.

transmission window ***cửa sổ truyền*** Trong liên lạc dữ liệu, bước sóng tại đó một cáp sợi quang trong suốt nhất.

transmitted data ***dữ liệu được phát đi*** Trong liên lạc dữ liệu, một nhánh dữ liệu dành cho dữ liệu được truyền từ một máy tính. *So sánh với* received data. *Xem* RS-232C.

transmitter ***máy phát*** Trong kiểm soát truy nhập, một phương pháp được dựa vào quyền sở hữu của người dùng. Một máy phát vô tuyến công suất thấp do người dùng mang và phát ra một tín hiệu mã cấp quyền truy nhập tới một khu vực vật lý và/hoặc kích hoạt một thiết bị đầu cuối; thiết bị đầu cuối sẽ tự động bị vô hiệu hóa khi máy phát bị chuyển khỏi vùng lân cận. Máy phát đòi hỏi nạp acquy hàng ngày và như vậy nó có giá trị hạn chế đối với kẻ trộm. *Xem* access control, proximity card reader.

transmitter signal element timing ***định thời phần tử tín hiệu phát*** Trong liên lạc dữ liệu, một tín hiệu được dùng với các modem đồng bộ cho dữ liệu được truyền đi. Modem có thể tạo ra sự định thời phần tử tín hiệu của máy phát tín hiệu đồng hồ (nguồn DCE) hoặc thiết bị máy tính có thể tạo tín hiệu định thời khi định thời phần tử tín hiệu của máy phát (nguồn DTE). *So sánh với* receiver signal element timing. *Xem* RS-232C, synchronous modem, transmitted data.

transparent ***trong suốt*** (1) Nói tới quá trình hay thủ tục do người sử dụng gọi tới mà không biết gì về sự tồn tại của nó. *So sánh với* virtual. (2) Trong liên lạc, nói tới một mạng hay phương tiện cho phép một tín hiệu đi qua nó mà không thay đổi.

transparent data communication code ***mã truyền thông dữ liệu trong suốt*** Trong liên lạc dữ liệu, một chế độ dùng một giao thức độc lập với mã. Việc hoạt động đúng độc lập với mã hoặc bộ ký tự. *Xem* transparent.

transponder ***bộ phát đáp, bộ chuyển tiếp*** Trong liên lạc, một thiết bị nhận và phát lại tín hiệu. Trong liên lạc vệ tinh, các tín hiệu nhận được được khuếch đại và truyền lại ở một tần số khác. *So sánh với* responder.

transport layer ***tầng vận tải*** Trong liên lạc dữ liệu, một tầng trong Mô hình kết nối các hệ thống mở OSI. Tầng này nhận các thông báo từ tầng phiên, chặt chúng thành các đoạn nhỏ nếu cần và đảm bảo chúng sẽ được nhận lại chính xác tại tầng vận tải của máy nhận. Tầng vận tải sẽ thực hiện chức năng này theo nghĩa hiệu quả nhất và bảo vệ tầng phiên khỏi những thay đổi bất kỳ về công nghệ phần cứng. *So sánh với* application layer, data link layer, network layer, physical layer, presentation layer, session layer. *Xem* bit stream, open systems interconnection.

transposition cipher ***mã chuyển vị*** Trong mật mã, một mã pháp trong đó các ký tự được sắp lại trật tự song không được ngụy trang riêng lẻ. *Xem* cipher, cryptography.

trapdoor ***bẫy, cửa sập*** (1) Trong an toàn máy tính, một cơ chế phần cứng

hoặc phần mềm được che dấu cho phép lừa các cơ chế bảo vệ hệ thống. Nó hoạt động theo cách hỏi không rõ ràng (ví dụ dãy khóa giả ngẫu nhiên đặc biệt tại thiết bị đầu cuối). (2) Trong an toàn máy tính, sự vi phạm cố tình trên hệ thống ADP nhằm thu thập, thay đổi hoặc phá hủy dữ liệu. (3) Trong an toàn máy tính, một điều kiện tồn tại trong phần mềm hay phần cứng máy tính có thể khởi sự phá hoại các tính năng an toàn phần cứng hay phần mềm của hệ thống. Về cơ bản, điều kiện được đặt ở bên trong (như bộ đếm, giá trị thời gian hoặc ngày tháng hay tập hất kỳ các các tình huống thiết lập sẵn) hay bên ngoài (như thông qua một thiết bị đầu cuối ở xa hay một thông báo nhập vào chương trình ứng dụng). *Xem* time bomb, Trojan Horse.

trapdoor one-way function ***hàm cửa sập một chiều*** Trong toán học, một hàm số có thể tính dễ dàng song không thể tính được ham đảo trừ phi có sẵn thông tin đặc biệt được dùng trong thiết kế hàm. Như vậy, hai số nguyên tố lớn có thể được nhân với nhau, tạo ra một tích số, nhưng có thể không khả thi về mặt tính toán để rút ra các thừa số khi chỉ cho trước giá trị của tích số. Việc biết một thừa số trong trường hợp này sẽ tạo thành thông tin cửa sập. *Xem* public key cryptography.

Treaty of Schengen ***Hiệp ước Schengen*** Trong luật pháp, một thỏa thuận được ký giữa các nước Pháp, Đức, Niu Di Lân, Luexămbua và Bỉ về việc thiết lập một hệ thống tự động hóa để trao đổi tin tức của cảnh sát. *Xem* data protection, data protection EC.

tree ***cây*** *Xem* tree structure.

tree databases ***cơ sở dữ liệu dạng cây*** *Đồng nghĩa với* hierarchical database.

tree structure ***cấu trúc cây*** Trong tính toán, một loạt các nút được nối với nhau không có vòng. Một nút được gọi là gốc và là điểm bắt đầu của tất cả các nhánh, một hoặc nhiều nút khác được gọi là lá tại các vị trí cuối của các nhánh. Một nhánh xuất phát từ nút bất kỳ hướng tới lá sẽ không bao giờ đi qua một nút riêng lẻ quá một lần. Nó có thể được dùng để biểu diễn các cấu trúc phân cấp, ví dụ cây gia hệ.

trellis coding ***mã hóa dạng mắt cáo*** Trong liên lạc dữ liệu, một giao thức dùng phép sửa lỗi tiến, phép sửa lỗi này dùng trong một số modem tốc độ cao. *Xem* forward error correction, MODEM.

tribit ***bộ ba bit, bit bội ba*** Trong liên lạc dữ liệu, ba bit liên tiếp. Trong các hệ thống điều pha, bit bội ba được biểu diễn bằng sự thay đổi pha 0, 45, 90, 135,... 315 độ. *Xem* phase modulation.

tributary station ***trạm phụ*** Trong liên lạc dữ liệu, trạm bất kỳ khác với trạm kiểm soát trên mạch nhiều điểm. Nó chỉ có thể liên lạc với trạm kiểm soát khi được trạm chọn. *Xem* multipoint circuit, polling.

trigram ***bộ ba chữ, bộ ba ký tự*** Trong mã thám, một bộ ba các chữ cái liên tiếp. *Xem* bigram.

triple modular redundancy ***dư thừa mô đun bội ba*** Trong lĩnh vực độ tin cậy, một dạng dư thừa modun dùng ba khối tích cực nối song song. Các đầu

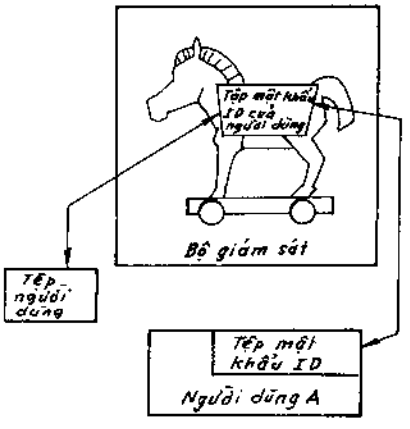
ra của tất cả ba khối được so sánh với nhau và đầu ra của hệ thống thu được bằng sự nhất trí đa số của ba đầu ra của ba khối. So sánh với dual redundancy, hybrid redundancy, NMR. *Xem* modular redundancy.

TRM *Xem* tamper-resistant module.

Trojan Horse ***con ngựa (thành) Tơroa*** (1) Trong an toàn máy tính, một chương trình máy tính dường như hoặc thực sự có chức năng hữu dụng, chứa các chức năng phụ (ẩn) lén lút dùng các ủy quyền hợp pháp gọi tới quá trình có hại tới tính an toàn. Ví dụ, tạo một "bản sao không nhìn thấy" của một tệp nhạy cảm cho trình tạo con ngựa Tơroa. (2) Trong an toàn máy tính, một chương trình máy tính dường như hoặc thực sự hữu ích và chứa một cửa sập. *Xem* trapdoor. (3) Trong an toàn máy tính, một chương trình do kẻ tấn công gài vào một hệ thống máy tính. Nó thực hiện các chức năng không được nêu trong các bản đặc tả chương trình, lợi dụng các quyền thuộc về môi trường gọi để sao chép, lạm dụng hoặc phá hủy dữ liệu. Ví dụ, con ngựa Tơroa trong một trình soạn thảo văn bản có thể sao chép thông tin mật trong một tệp đang soạn thảo vào một tệp mà kẻ tấn công có thể truy nhập tới. *Xem* leakage, Trojan Horse direct release, Trojan Horse leakage.

Trojan Horse direct release ***phát hành trực tiếp con ngựa Tơroa*** Trong an toàn cơ sở dữ liệu, một dạng hiểm họa trong đó, con ngựa thành Tơroa tạo điều kiện để đưa dữ liệu xếp vào loại mật cho người có phân loại an toàn thấp hơn. Dữ liệu không được ủy quyền sẽ được phát ra do nó được con ngựa thành Tơroa dán nhãn an toàn thấp. Điều này thực hiện được nhờ thay đổi nhãn an toàn, đặt dữ liệu vào bản ghi hay trường có phân loại thấp hơn, hoặc làm hỏng quá trình điều chỉnh phân loại an toàn khi mức phân loại của dữ liệu tăng lên. *So sánh với* direct access, indirect access, Trojan Horse leakage. *Xem* field, record, Trojan Horse.

Trojan horse leakage ***rò rỉ thông tin do con ngựa Tơroa*** Trong an toàn cơ sở dữ liệu, một dạng hiểm họa trong đó con ngựa Tơroa làm hệ thống dường như đang trả lời một câu truy vấn hợp pháp song thực tế lại trả lời một câu hỏi khác, tức là câu hỏi đòi hỏi có phân loại an toàn cao hơn. Dữ liệu không được phép được mã hóa thành dữ liệu cho phép được trả lại cho người dùng. *So sánh với* direct access, indirect access,



Trojan Horse: *con ngựa thành Tơroa*. Trong ví dụ này, một thiết bị giám sát thực hiện phần mềm đánh giá một chương trình phần mềm cũng như thu thập dữ liệu nhạy cảm đi kèm chương trình.

Trojan Horse direct release. *Xem* Trojan Horse.

trouble condition ***tình thế gây sự cố*** Trong an toàn vật lý, một tình huống trong một hệ thống báo động bị mất điều khiển do chập mạch, hỏng nguồn...

troubleshoot ***xử lý trục trặc*** (1) Tìm kiếm, định vị và sửa các sự cố. (2) Trong lập trình, gỡ rối. *Xem* debug.

trouble signal ***tín hiệu báo trục trặc*** Trong an toàn vật lý, một tín hiệu xuất hiện khi có vấn đề, chẳng hạn ngắt mạch hoặc tiếp đất trong thiết bị hay dây dẫn trong hệ thống báo hỏa. *So sánh với* trouble condition.

trunk ***đường trung chuyển, đường trục chính*** Trong liên lạc, một mạch hay một kênh nối chung hai tổng đài hoặc thiết bị chuyển mạch, có khả năng chuyển mạch ở cả hai đầu và được cung cấp cùng với thiết bị báo hiệu và kết thúc cần thiết.

trust ***(sự) tin cậy, (sự) tín nhiệm*** Sự tin tưởng rằng hệ thống sẽ đáp ứng các đặc tính kỹ thuật của nó. *Xem* specification.

trusted ***được tín nhiệm, được tin cậy*** Trong an toàn dữ liệu, nói tới các hệ thống phần mềm hay phần cứng được thiết kế và được kiểm tra nhằm tránh khả năng bị tổn thương, bị hỏng hay từ chối cung cấp thông tin nhạy cảm. *Xem* compromise, corrupt data, delay/denial of service, trusted computing base.

trusted channel ***kênh tin cậy*** Trong an toàn liên lạc, một cơ chế nhờ nó, hai phần chia NTCB (cơ sở tính toán tin cậy mạng) có thể liên lạc trực tiếp với nhau. Cơ chế này được kích hoạt nhờ cả hai phần chia NTCB không thể bị phần mềm không tin cậy bắt chước và nhờ duy trì tính toàn vẹn của thông tin gửi qua nó. Sự hoạt động của các cơ chế an toàn khác có thể cần tới kênh tin cậy. *Xem* NTCB partition.

trusted communications path ***tuyến liên lạc tin cậy*** Trong an toàn liên lạc, một cơ chế mà nhờ nó, một chủ thể của mạng có thể liên lạc trực tiếp với cơ sở tính toán tin cậy. Cơ chế này chỉ có thể hoạt động nhờ chủ thể mạng hay TCB và phần mềm không tin cậy không thể bắt chước theo. *Xem* trusted computing base.

trusted computer security evaluation criteria ***tiêu chí đánh giá an toàn máy tính tin cậy*** *Đồng nghĩa với* Orange Book.

trusted computer system ***hệ thống máy tính tin cậy*** Trong an toàn máy tính, một hệ thống dùng các biện pháp toàn vẹn phần mềm và phần cứng đầy đủ, cho phép sử dụng nó để xử lý đồng thời các thông tin mật và nhạy cảm. *Xem* Orange Book, trusted, trusted computing base.

trusted computing base ***cơ sở tính toán tin cậy*** Trong an toàn máy tính, toàn bộ các cơ chế bảo vệ bên trong một hệ thống máy tính, gồm cả phần cứng, phần mềm và phần sụn, sự kết hợp của chúng nhằm tuân thủ chính sách an toàn. Nó tạo ra một môi trường bảo vệ cơ bản và cung cấp các dịch vụ bổ sung cho người dùng mà một hệ

thống máy tính tin cậy đòi hỏi. Khả năng của cơ sở tính toán tin cậy đối với việc tuân thủ đúng chính sách an toàn phụ thuộc vào các cơ chế trong TCB và vào việc người quản trị hệ thống đưa đúng các thông số liên quan tới chính sách an toàn vào (chẳng hạn mức truy nhập của người dùng). *So sánh với* network trusted computing base. *Xem* security policy, trusted, trusted computer system.

trusted functionality ***(tính) chức năng tin cậy*** Trong an toàn máy tính, chức năng nhận biết được là đúng với tiêu chuẩn nào đó, ví dụ khi được thiết lập bởi một chính sách an toàn. Tính chức năng sẽ không được không đạt hoặc không vượt tiêu chuẩn đề ra. *Xem* security policy, trusted.

trusted identification forwarding ***chuyển tiếp định danh tin cậy*** Trong an toàn liên lạc, một phương pháp định danh dùng trên mạng nơi máy chủ bên gửi có thể xác minh xem người dùng được phép trên mạng có đang nối tới máy chủ khác không. Máy chủ bên gửi sẽ truyền thông tin xác thực người dùng cần thiết tới máy chủ bên nhận. Khi đó, máy chủ bên nhận có thể sẽ xác minh xem người dùng truy nhập tới hệ thống của nó có hợp lệ không. Hoạt động này có thể trong suốt đối với người dùng.

trusted path ***tuyến tin cậy*** Trong an toàn máy tính, một cơ chế nhờ nó một cá nhân tại một đầu cuối có thể liên lạc trực tiếp với TCB. Cơ chế này chỉ được người dùng hay TCB thực hiện mà phần mềm không tin cậy không thể bắt chước được. *Xem* trusted software, TCB.

trusted process ***quá trình tin cậy*** Trong an toàn máy tính, một quá trình không làm ảnh hưởng tới tính an toàn của hệ thống. Đôi khi nó được cấp (không thường xuyên) các đặc quyền khắc phục được các quy tắc mà nhân bắt tuân theo. Các khả năng hay các đặc trưng bảo vệ của một quá trình tin cậy phải được chứng minh một cách chắc chắn là tuân theo các yêu cầu đã công bố, thông qua việc xác minh hình thức khi có thể. Các quá trình tin cậy đôi khi được dùng để thi hành phần mềm NKSR. *So sánh với* untrusted process. *Xem* NKSR, security kernel.

trusted products ***(các) sản phẩm tin cậy*** Các sản phẩm được người phụ trách xác nhận NCSC nằm trong danh sách Các sản phẩm đã đánh giá. *Xem* evaluated products list, NCSC.

trusted software ***phần mềm tin cậy*** Trong an toàn máy tính, phần mềm có TCB. *Xem* trusted, trusted computer system, trusted computing base, trusted process.

trusted subject ***chủ thể tin cậy*** (1) Trong an toàn máy tính, một chủ thể là một phần của TCB. Nó có khả năng vi phạm chính sách an toàn song được tin là sẽ không làm điều đó. Ví dụ, trong mô hình Bell-La Padula, một chủ thể tín nhiệm không bị ràng buộc bởi thuộc tính sao (*) và như vậy có khả năng ghi thông tin nhạy cảm lên một đối tượng có mức an toàn không trội hơn mức tối đa của chủ thể song nó được tin chỉ ghi thông tin lên đối tượng có mức thực sự phù hợp với

nhãn của thông tin. *Xem* Bell-La Padula model, object, star property, subject. (2) Trong an toàn máy tính, một chủ thể được phép đồng thời xem và truy nhập luân phiên tới các đối tượng có nhiều hơn một mức nhạy cảm. *Xem* Bell-La Padula model, Orange Book.

trusted system ***hệ thống tin cậy*** Một hệ thống dùng các biện pháp toàn vẹn đầy đủ, cho phép dùng nó để xử lý thông tin tình báo liên quan tới nguồn lẫn phương pháp tình báo nhạy cảm. *Xem* trusted, trusted computer system, trusted computing base, trusted process.

trustworthiness ***tính đáng tin cậy*** Sự bảo đảm để một hệ thống xứng đáng được tin cậy. *Xem* trust.

TSW *Xem* telesoftware.

TTAP ***chương trình TTAP*** Trong an toàn máy tính, viết tắt của Trust Technology Assessment Program (chương trình đánh giá công nghệ tin cậy), một chương trình hướng trực tiếp tới sự định giá sản phẩm về tính an toàn với các yêu cầu bảo đảm tối thiểu. Nó đã được phát triển nhằm giúp cho việc nhận biết có tính quốc tế về các đánh giá sản phẩm, tối thiểu hóa thời gian và chi phí định giá sản phẩm và tối ưu hóa tính sẵn sàng của chúng. *So sánh với* TCSEC. *Xem* FC-FIPS, MFSR.

tuned circuit card ***thẻ mạch được điều hưởng*** *Xem* proximity card reader.

Tunes ***virut Tunes*** Trong an toàn máy tính, một loại virut chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COM, EXE và OVL, tác động trong thời gian chạy và làm hỏng các tệp chương trình và OVL. *Xem* virus names.

tuning ***tinh chỉnh*** Tối ưu hóa khả năng của hệ thống nhờ điều chỉnh tinh.

tunneling attack ***tấn công theo kiểu đào hầm*** Trong an toàn máy tính, một nỗ lực lợi dụng nhược điểm trong hệ thống ở mức rút tin cấp thấp.

tuple ***bộ quan hệ*** Trong toán học, một tập hợp các giá trị có liên quan. *Xem* N-tuple.

turnkey system ***hệ thống chìa khóa trao tay*** Trong tính toán, một hệ thống trọn vẹn được thiết kế cho người dùng đặc biệt. Với các hệ thống lớn, phức tạp, người dùng chỉ cần chuyển mạch tới hệ thống, người cung cấp chủ chốt sẽ nhận hết trách nhiệm đối với việc thiết kế, cài đặt, cung ứng phần cứng, phần mềm và tài liệu của hệ thống. Với các gói phần mềm, người dùng không cần biết về hệ điều hành; quá trình tải lên đĩa tất cả các lệnh hoạt động sẽ được hiển thị cho người dùng thấy. *Xem* operating system.

twisted pair ***cáp xoắn đôi*** Trong liên lạc, một loại cáp được tạo ra nhờ xoắn hai dây dẫn mảnh riêng biệt, cách điện lại với nhau. Cách thức này làm giảm điện dung giữa các dây.

two-dimensional scrambler ***bộ xáo trộn hai chiều*** Trong an toàn liên lạc, một kiểu bộ xáo trộn tiếng nói hoán vị tín hiệu trong cả miền thời gian lẫn miền tần số. Tín hiệu tiếng nói được chia thành các khung, mỗi khung có một số đoạn (segment). Các tín hiệu trong phạm vi mỗi đoạn được chuyển

sang miền tần số và các thành phần tần số này được hoán vị. Bản thân các đoạn trong một khung cũng được hoán vị. *So sánh với* discrete Fourier transform scrambler. *Xem* voice scrambler.

two-end device ***thiết bị hai đầu*** Trong an toàn máy tính, một thiết bị được cài đặt cả ở máy chủ và người dùng hợp pháp tại đầu nối điện thoại để chống sự xâm nhập bằng điện thoại. Các thiết bị hiện tại cung cấp sự xác thực của thiết bị đầu cuối hoặc vị trí của người dùng và dữ liệu được truyền đi và che dấu dữ liệu truyền. Việc xác thực người dùng được cung cấp bình thường qua một số dạng thẻ bài do người dùng chuyển tới; những thẻ bài như vậy cho phép người dùng nhập một mật khẩu đóng. Xác thực đầu cuối yêu cầu một khối trong thiết bị đầu cuối có thể tự động đưa vào một đối thoại hỏi/đáp với máy chủ. Xác thực dữ liệu được thực hiện bằng việc tạo ra một MAC trên nội dung thông báo và che dấu dữ liệu được tạo ra bằng phép mã liên kết. *So sánh với* one-end device. *Xem* challenge/response, dynamic password, link encryption, message authentication code.

two-key cryptosystem ***hệ thống mã hai khóa*** *Đồng nghĩa với* asymmetric cryptosystem. *Xem* public key cryptography.

two-layer architecture ***kiến trúc hai tầng*** Trong quản lý khóa, một hệ thống trong đó, khóa mã khóa được phân phối thủ công và khóa này được dùng để mã các khóa dữ liệu, các khóa dữ liệu này được phân phối tự động. *So sánh với* three-layer architecture. *Xem* ANSI X9.17 - 1985, cryptographic key, data key, key-encrypting key.

two-wire circuit ***mạch hai dây*** Trong liên lạc, một mạch có hai dây dẫn cách điện với nhau, tạo nên kênh đi và đến cho các tín hiệu cùng tần số. *So sánh với* four-wire circuit.

TX *Xem* transmitter.

Tymnet ***mạng Tymnet*** Trong liên lạc, một phương tiện chuyển mạch gói công cộng ở Hoa Kỳ. *Xem* packet switching.

type ***kiểu*** Trong lập trình, nói tới dải các giá trị và thao tác hợp lệ của một biến.

Type I ***Loại I*** Trong mật mã, *xem* NASA COMSEC module.

type accreditation ***(sự) công nhận tác quyền*** Trong an toàn máy tính, sự ủy quyền chính thức bởi DAA cho sử dụng một hệ thống trong môi trường xác định. Sự ủy quyền này bao gồm một công bố về mức rủi ro còn lại, phác họa môi trường hoạt động và việc sử dụng riêng. Nó được thực hiện khi nhiều bản sao của một hệ thống bị lộ. *Xem* DAA.

Type 1 cryptographic product ***sản phẩm mật mã loại 1*** Trong mật mã, một sản phẩm được NSA xác nhận để giữ bí mật thông tin xếp vào loại mật. *So sánh với* Type 2 cryptographic product. *Xem* NSA.

Type 2 cryptographic product ***sản phẩm mật mã loại 2*** Trong mật mã, một sản phẩm được NSA xác nhận chỉ để giữ bí mật thông tin chưa xếp vào loại mật. *So sánh với* Type 1

cryptographic product. *Xem* NSA.

Type 1 error ***lỗi loại 1*** Trong kiểm soát truy nhập, một lỗi trong hệ thống sinh trắc đã bác bỏ yêu cầu truy nhập của người dùng hợp pháp. *So sánh với* Type 2 error. *Xem* biometrics.

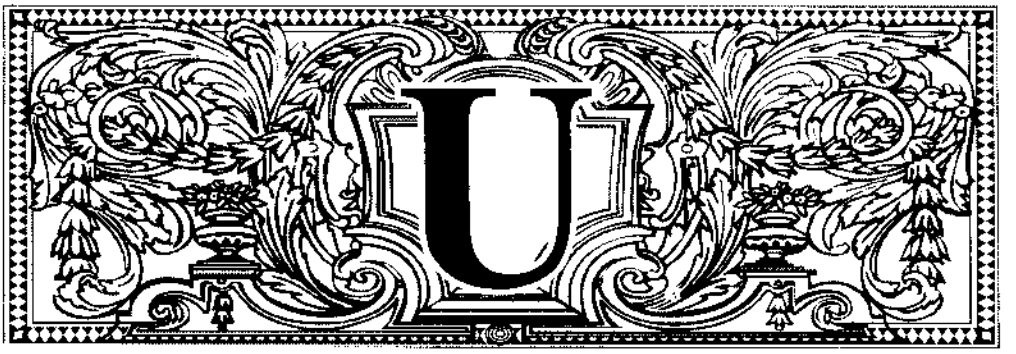
Type 2 error ***lỗi loại 2*** Trong kiểm soát truy nhập, một lỗi trong hệ thống sinh trắc đã chấp nhận yêu cầu truy nhập của người dùng bất hợp pháp vì số đo sinh trắc đã khớp không đúng với số đo của người dùng bất hợp pháp. *So sánh với* Type 1 error. *Xem* biometrics.

Type 1 magnetic media ***môi trường từ tính loại 1*** Trong điện tử học, môi trường từ tính có các hệ số kháng từ không vượt quá 325 ơstet. *Xem* coercive force, oersted.

Type 2 magnetic media ***môi trường từ tính loại 2*** Trong điện tử học, môi trường từ tính có các tham số kháng từ vượt quá 325 ơstet, có thể lên tới 750 ơstet. *Xem* coercive force, oersted.

Typo Boot ***virut Typo Boot*** Trong an toàn máy tính, một loại virut máy tính tác động trong thời gian chạy và làm hỏng các cung khởi động. *Xem* virus names.

Typo/Fumble ***virut Typo/Fumble*** Trong an toàn máy tính, một loại virut máy tính chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm tới các tệp COM, tác động trong thời gian chạy và làm hỏng các tệp chương trình và OVL. *Xem* virus names.



UA *UA* Viết tắt của User Agent (đại diện người dùng). *So sánh với* MTA, MTS. *Xem* user agent.

UCCI *gói UCCI* Trong kiểm soát dữ liệu, một gói chương trình an toàn dữ liệu. *Xem* data security package.

UDAC *kiểm soát truy nhập hướng người sử dụng* *Xem* user-directed access control.

UDI *mục dữ liệu không hi giới hạn* *Xem* unconstrained data item.

UL *Xem* Underwriter's Laboratory.

ultimate beneficiary *người hưởng cuối cùng* *Đồng nghĩa với* beneficiary.

ultrasonic motion detector *bộ phát hiện chuyển động bằng siêu âm* Trong an toàn vật lý, một kiểu thiết bị phát hiện xâm nhập dùng sóng siêu âm. Sự hiện diện của kẻ đột nhập sẽ được phát hiện khi sự chuyển động của cơ thể tác động lên tần số của tín hiệu phản xạ ngược trở lại bộ cảm biến. *So sánh với* sonic motion detector. *Xem* motion detector.

ultraviolet fire detector *bộ phát hiện lửa bằng tia cực tím* Trong an toàn vật lý, bộ phát hiện cháy được kích hoạt bằng độ tăng bức xạ tia cực tím phát ra từ một ngọn lửa. Các bộ phát hiện này đáp ứng với một khoảng hạn chế tần số và bởi vậy ít bị tác động gây các báo động sai, ví dụ sự phóng điện. *Xem* photoelectric beam smoke detector.

unapproved software *phần mềm không được chấp thuận* Trong an toàn máy tính, phần mềm chưa được định danh, đánh giá và kiểm tra bởi người có thẩm quyền để bảo đảm rằng nó thực hiện chính xác các đặc tả đề ra. *So sánh với* trusted software.

unary operation *phép toán một ngôi* Trong toán học, một phép toán chỉ có một toán hạng, chẳng hạn phép phủ định dùng để đảo dấu một số hạng.

Xem operand.

unauthorized disclosure ***(sự) tiết lộ trái phép, (sự) làm lộ không được phép*** Trong an toàn dữ liệu, quá trình làm thông tin trở nên khả dụng cho những cá nhân, các thực thể hay các quá trình không được phép.

unbalanced transmission ***truyền không cân bằng*** Trong liên lạc dữ liệu, một kỹ thuật dùng một dây cho mỗi tín hiệu, còn tuyến trở về chung dành cho mọi tín hiệu. *So sánh với* balanced transmission.

unbreakable cipher ***' mã pháp không thể phá được*** *Xem* perfect secrecy.

unclassified ***không xếp vào loại mật, không mật*** Trong an toàn dữ liệu, mức phân loại thấp nhất của dữ liệu và vì thế không yêu cầu bảo vệ chống làm lộ trái phép. *Xem* classification.

unclassified information ***thông tin chưa xếp vào loại mật*** Trong an toàn dữ liệu, mức truy nhập (clearance) của Bộ Quốc phòng Mỹ cho người được ủy quyền truy nhập tới thông tin nhạy cảm chưa xếp vào loại mật, chẳng hạn chỉ dùng cho văn phòng, thông qua sự cấp phép tường minh của chính quyền hoặc thông qua sự cấp phép ngầm nảy sinh từ công việc của những người có trách nhiệm. *So sánh với* confidential clearance, multiple categories, one category, secret clearance, top secret clearance, uncleared. *Xem* clearance.

uncleared ***không phân mức truy nhập*** Trong an toàn dữ liệu, mức truy nhập (clearance) của Bộ Quốc phòng Mỹ cho người không cần cấp phép truy nhập. Thông tin không bị kiểm soát bất kỳ đều được phép truy nhập, chẳng hạn thông tin công bố công khai. *So sánh với* confidential clearance, multiple categories, one category, secret clearance, top secret clearance, uncleared information. *Xem* clearance.

unconditionally secure ***an toàn không điều kiện*** Trong mã thám, đề cập tới một mã pháp không thể bị phá, ngay cả khi người mã thám có lượng bản mã không hạn chế. Một cách hình thức, điều này đòi hỏi độ bất định của khóa không tiến tới 0 ngay cả khi bức điện cực dài. *Xem* information theory, key equivocation, perfect secrecy.

unconfirmed service ***dịch vụ không được xác nhận*** Trong liên lạc dữ liệu, một dịch vụ trong đó người gửi phát ra một yêu cầu và yêu cầu được chuyển tới người nhận song không có xác nhận nào được gửi trả lại cho người gửi. *So sánh với* confirmed service.

unconstrained data item ***mục dữ liệu không bị ràng buộc*** Trong các mô hình hình thức, thuật ngữ được dùng trong mô hình Clack-Wilson để chỉ mục dữ liệu được nhập vào trước quá trình kiểm tra cần thiết về sự tuân thủ các quy tắc của một mục dữ liệu bị giới hạn. *So sánh với* constrained data item. *Xem* Clack-Wilson model.

undecidable ***không khả quyết*** Trong toán học, đề cập tới bài toán không có thuật toán nào cho lời giải của nó. *So sánh với* intractable.

Underwriter's Laboratory ***Phòng thí nghiệm của tổ chức ký nhận*** Trong an toàn vật lý, một phòng thí nghiệm kiểm định không nhằm mục đích kinh

doanh ở Hoa Kỳ để kiểm định và chứng nhận các loại thiết bị về tính an toàn và tính tin cậy.

unicity distance ***khoảng duy nhất*** Trong mật mã học, độ dài tối thiểu của thông báo mã mà độ bất định của khóa tiến tới không. Khoảng duy nhất của thông báo mã là lượng bản mã cần thiết về mặt lý thuyết để xác định duy nhất được khóa. *Xem* cryptographic key, key equivocation.

unipolar ***đơn cực, một cực*** Trong liên lạc dữ liệu, nói tới tín hiệu lệch tới giá trị dương hay âm so với giá trị 0 song không phải cả hai, chẳng hạn, nó chứa một dãy các xung dương. *So sánh với* bipolar.

unique identification ***nhận diện duy nhất, định danh duy nhất*** *Đồng nghĩa với* fingerprint.

unit buffer terminal ***thiết bị đầu cuối có bộ đệm thiết bị*** Trong truyền thông, một thiết bị đầu cuối không có bộ đệm truyền thông.

universal quantifier ***lượng từ phổ dụng*** Trong toán học, một ký hiệu được dùng trong các phép tính vị ngữ và phép tính quan hệ, được đọc là "với mọi".

universal set ***tập vạn năng, tập phổ biến*** Trong toán học, tập tất cả các phần tử có thuộc tính xác định, chẳng hạn 0, 1, 2... 9, là tập phổ biến các số nguyên một chữ số, không âm. *Xem* set.

universal signature ***chữ ký phổ dụng*** Trong xác thực, một chữ ký số mà người nhận có thể công nhận mà không cần trọng tài. *So sánh với* arbitrated signature. *Xem* digital signature.

Unix ***hệ điều hành Unix*** Trong tính toán, nhãn thương mại của hệ điều hành nhiều người sử dụng, đa năng thích hợp cho một dải rộng các máy tính nhỏ, máy vi tính. Nó xuất xứ từ Phòng thí nghiệm Bell vào năm 1969 cho máy tính mini PDP-7 và trở thành hệ điều hành phổ biến rộng rãi trong các nhà khoa học máy tính. Unix chứa đựng các công cụ lập trình tạo một môi trường phong phú cho các phát triển phần mềm nhờ một nhóm nhà lập trình. Unix có tính cơ động cao và việc sử dụng nó đang mở rộng nhanh chóng trong các khu vực máy tính cá nhân. Nó là hệ thống nhiều người sử dụng, cung cấp các phương tiện để chia sẻ các tài nguyên hệ thống (không gian đĩa, thời gian CPU v.v.) và các cơ chế bảo vệ các tệp của người dùng. Với mỗi tệp, người dùng có thể chỉ ra các đặc quyền đọc, ghi, thi hành riêng cho bản thân họ, các thành viên của nhóm và tất cả những người dùng khác. Hệ thống là hệ điều hành đa nhiệm, cho phép người dùng loại riêng những chương trình đòi hỏi người dùng không tương tác với xử lý nền trong khi lại tương tác với chương trình ưu tiên.

unprotect ***chương trình khắc phục bảo vệ*** Trong an toàn máy tính, một chương trình vượt qua được những tính năng bảo vệ phần mềm và sao chép những phần mềm được bảo vệ đặc biệt. *Xem* software protection.

untrusted ***không tin cậy*** Trong an toàn máy tính, nói tới hệ thống không

được thẩm tra về những tính chất an toàn của nó. *So sánh với* trusted.

untrusted process ***quá trình không tin cậy*** Trong an toàn máy tính, một quá trình mà sự thi hành không đúng hoặc thi hành ác ý của nó không thể tác động tới tính an toàn hệ thống. Việc xác minh thường không áp dụng cho các quá trình không tin cậy. *So sánh với* trusted process.

update inconsistency ***tính không nhất quán khi cập nhật*** Trong cơ sở dữ liệu, một hiện tượng nảy sinh trong cơ sở dữ liệu nhiều người sử dụng. Trình tự các sự kiện như sau:

- Alice truy lục một bản ghi;
- Bob cũng truy lục bản ghi đó;
- Alice cập nhật một trường của bản ghi và ghi ngược nó trở lại cơ sở dữ liệu trong khi Bob cũng đã truy lục được bản ghi đó;
- Bob cập nhật một trường khác của bản ghi đó và ghi ngược trở lại cơ sở dữ liệu, đè lên phần cập nhật của Alice.

Người ta dùng cách khóa lại để tránh tình huống này. *Xem* field, lockout, record.

upload ***tải lên, tải ra*** Trong tính toán, gửi một tệp từ một máy tính nhỏ hơn hay một máy tính cục bộ tới một máy tính ở xa hay một máy tính lớn hơn. *So sánh với* download. *Xem* file transfer.

uptime ***thời gian vận hành, thời gian chạy máy*** Trong tính toán, thời gian mà một máy tính đã sẵn sàng cho hoạt động thông thường. *Đồng nghĩa với* available time.

upward compatibility ***(tính) tương thích hướng lên*** Trong tính toán, khả năng của máy tính này thi hành các chương trình được viết cho máy khác song quá trình ngược lại thì không được.

usability ***tính khả dụng*** Trong tính toán, nỗ lực cần thiết để học, làm việc, chuẩn bị đầu vào và biên dịch đầu ra của một chương trình.

usage ***mức độ sử dụng*** Trong an toàn dữ liệu, nói tới tính toàn vẹn của dữ liệu, đặc biệt là tập các biện pháp đề phòng để đảm bảo và duy trì tính hợp lệ của dữ liệu và tạo ra sự tồn tại liên tục và khả năng phục hồi của nó.

usage sensitive pricing ***định giá theo mức độ sử dụng*** Trong liên lạc, cước phí cho dịch vụ dựa trên mức độ sử dụng.

USASCII ***mã chuẩn của Mỹ để trao đổi thông tin*** Viết tắt của USA standard Code for Information Interchange. *Đồng nghĩa với* ASCII.

USASI ***Viện tiêu chuẩn Hợp chủng Quốc Hoa kỳ*** Viết tắt của United States of America Standards Institute.

user ***người dùng, người sử dụng*** (1) Trong an toàn liên lạc, cá nhân bất kỳ tương tác trực tiếp với hệ thống mạng. Nó gồm cả những người được phép tương tác với hệ thống và những người không được phép (chẳng hạn những người nghe trộm tích cực và thụ động). *So sánh với* subject. *Xem* wiretap. (2) Trong các hoạt động, một tổ chức hay một thực thể chương trình nhận dịch vụ từ một phương tiện công nghệ thông tin. Người dùng có thể hoặc là

người trong hay ngoài tổ chức có trách nhiệm đối với phương tiện song thường không báo cáo cho người quản lý hay, giám đốc của phương tiện hoặc cho chính người giám sát trực tiếp. *So sánh với* customer. *Xem* information technology facility. (3) Trong quá trình hoạt động, cá nhân hay tổ chức bất kỳ truy nhập tới hệ thống tự động hóa theo mạng truyền thông qua một thiết bị từ xa, hoặc người được phép đưa dữ liệu vào hệ thống qua các phương tiện trung gian khác. "Những người sử dụng" không phải là những người hay tổ chức được xác định là khách hàng. *So sánh với* customer. (4) Trong an toàn máy tính, người có thể truy nhập vào AIS hoặc qua nối trực tiếp (tức qua cắt thiết bị đầu cuối) hoặc qua các nối gián tiếp (tức chuẩn bị dữ liệu vào hoặc phần mềm hoặc nhận đầu ra mà không bị người có trách nhiệm xem xét về nội dung và mức phân loại. *Xem* ASI. (5) Trong an toàn máy tính, cá nhân bất kỳ có khả năng thao tác thiết bị bất kỳ có thể truy nhập tới hệ thống xử lý dữ liệu tự động ADP. *Xem* ADP. (6) Trong an toàn máy tính, cá nhân bất kỳ tương tác trực tiếp với hệ thống máy tính. (7) Trong an toàn máy tính, người, chức năng hay tổ chức nhận và dùng sản phẩm ra của một ứng dụng máy tính. Các chức năng của người sử dụng đều nằm ngoài ranh giới vật lý của phương tiện máy tính song người sử dụng có thể tương tác trực tiếp với hệ thống qua một thiết bị đầu cuối. *Xem* end user.

user acceptability ***khả năng chấp nhận của người dùng*** Trong an toàn máy tính, nguyên tắc về khả năng chấp nhận của người dùng - một trong những nguyên tắc của hệ thống an toàn phát biểu rằng, những biện pháp an toàn sẽ không gây trở ngại quá đáng tới công việc của những người sử dụng trong khi vẫn có đầy đủ tất cả các ràng buộc cần thiết về an toàn. *Xem* principles of secure systems.

user agent ***bộ phận người dùng, đại lý người sử dụng*** Trong liên lạc dữ liệu, một quá trình theo chuẩn X.400 của CCITT đối với việc xử lý thông báo. Bộ phận người dùng có vai trò tương tự như người dùng hệ thống bưu điện: người cho thư vào phong bì, ghi địa chỉ và sau đó chuyển nó đi. *So sánh với* message transfer agent. *Xem* X.400.

user alternative plan ***kế hoạch dự phòng người dùng, kế hoạch thay thế cho người dùng*** Trong quản lý rủi ro, một tập các kế hoạch để người sử dụng dùng một chương trình ứng dụng khi việc xử lý ứng dụng đó bị hỏng. *Xem* contingency plans.

user authentication ***xác thực người sử dụng*** *Xem* access control, authentication.

user-directed access control ***kiểm soát truy nhập hướng người dùng*** Trong kiểm soát truy nhập, sự kiểm soát truy nhập trong đó những người dùng (hay nói chung là các chủ thể) có thể thay đổi các quyền truy nhập. Ví dụ những thay đổi như vậy có thể được hạn chế tới các cá nhân nào đó thông qua các kiểm soát truy nhập và như vậy, họ có thể bị hạn chế đối với người chủ của một đối tượng. *So sánh với*

administratively directed access control. *Xem* discretionary access control.

user friendly ***tiện cho người dùng, thuận lợi cho người dùng, thân thiện với người dùng*** Nói tới hệ thống bất kỳ được thiết kế để dùng không cần đào tạo thao tác viên và nhắm tới việc giúp người dùng nhận được lợi ích tối đa từ hệ thống.

user id ***số hiệu nhận dạng người dùng, ID người dùng*** (1) Trong an toàn máy tính, một ký hiệu hay một chuỗi ký tự duy nhất được hệ thống ADP dùng để đinh danh duy nhất một người sử dụng. Tính an toàn được hệ thống mật khẩu cung cấp sẽ không dựa vào độ mật của ID của người dùng. *So sánh với* network user identity. *Xem* ADP, password, PIN. (2) Trong quá trình hoạt động, một mã định danh người dùng cho phép máy tính nhận dạng và phân lệ phí cho người dùng.

user profile ***hồ sơ người sử dụng, lược tả người dùng*** (1) Bản mô tả về các tham số cơ bản của người dùng đối với hệ thống đã cho. (2) Trong các mạng máy tính, việc xác định kiểu tương tác của người dùng với một mạng, được người dùng hỗ trợ như một tập các tham số, hoặc các tùy chọn vào lúc đăng ký.

user programs ***(các) chương trình của người dùng*** Trong tính toán, một nhóm các chương trình được người dùng viết khác với phần mềm mà nhà sản xuất cung cấp. *Xem* application program.

users group ***nhóm người dùng*** Một nhóm người sử dụng thỏa thuận dùng chung các chương trình, trao đổi thông tin, ví dụ về một lớp các hệ thống máy tính. *So sánh với* closed user group.

USSR ***virut USSR*** Trong an toàn máy tính, một loại virut mã lên chính nó, lây nhiễm tới các tệp EXE, tác động trong thời gian hoạt động, làm hỏng các chương trình và các tệp OVL. *Xem* virus names.

UU ***người sử dụng trái phép*** Viết tắt của Unauthorized User.



V *Xem* V-series recommendations of CCITT.

V.1 ***chuẩn V.1*** Trong tập các tiêu chuẩn, khuyến nghị của CCITT về sự tương đương giữa các ký hiệu nhị phân và các trạng thái có nghĩa của mã hai trạng thái.

V.2 ***chuẩn V.2*** Trong tập các chuẩn, khuyến nghị của CCITT về hai mức công suất đối với sự truyền dữ liệu trên các kênh điện thoại.

V.3 ***chuẩn V.3*** Trong tập các chuẩn, khuyến nghị của CCITT về bảng mã chữ cái quốc tế No 5 để truyền dữ liệu và các thông báo. *Xem* International Alphabet Number 5.

V.4 ***chuẩn V.4*** Trong tập các chuẩn, khuyến nghị của CCITT để tạo cấu trúc các tín hiệu của bảng mã chữ cái quốc tế No 5 để truyền dữ liệu và thông báo trên mạng điện thoại công cộng. *Xem* International Alphabet Number 5.

V.5 ***chuẩn V.5*** Trong tập các chuẩn, khuyến nghị của CCITT đối với việc tiêu chuẩn hóa tốc độ tín hiệu dữ liệu để truyền dữ liệu đồng bộ trên mạng điện thoại chuyển mạch công cộng.

V.6 ***chuẩn V.6*** Trong tập các chuẩn, khuyến nghị của CCITT để tiêu chuẩn hóa các tốc độ tín hiệu dữ liệu để truyền dữ liệu đồng bộ dùng trên mạch kiểu điện thoại thuê bao.

V.10 ***chuẩn V.10*** Trong tập các chuẩn, khuyến nghị của CCITT về các đặc trưng điện cho các mạch hoán đổi dòng kép không cân bằng để dùng với thiết bị mạch tích hợp trong lĩnh vực truyền dữ liệu.

V.11 ***chuẩn V.11*** Trong tập các chuẩn, khuyến nghị của CCITT về các đặc trưng điện cho các mạch hoán đổi dòng kép cân bằng để dùng với thiết bị mạch tích hợp trong lĩnh vực truyền dữ liệu.

V.13 ***chuẩn V.13*** Trong tập các

chuẩn, khuyến nghị của CCITT về các bộ mô phỏng khối hỏi đáp.

V.15 ***chuẩn V.15*** Trong tập các chuẩn, khuyến nghị của CCITT để dùng ghép âm thanh cho truyền dữ liệu.

V.16 ***chuẩn V.16*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem truyền tương tự dữ liệu y tế. *Xem* MODEM.

V.19 ***chuẩn V.19*** Trong tập các chuẩn, khuyến nghị của CCITT cho các modem truyền dữ liệu song song ở tần số tín hiệu báo điện thoại. *Xem* MODEM.

V.20 ***chuẩn V.20*** Trong tập các chuẩn, khuyến nghị của CCITT cho các modem truyền dữ liệu song song được chuẩn hóa để dùng phổ cập trong mạng điện thoại chuyển mạch phổ thông. *Xem* MODEM.

V.21 ***chuẩn V.21*** Trong tập các chuẩn, khuyến nghị của CCITT cho các modem tốc độ 300 baud được chuẩn hóa để dùng cho mạng điện thoại chuyển mạch phổ thông. *Xem* MODEM.

V.22 ***chuẩn V.22*** Trong tập các chuẩn, khuyến nghị của CCITT về chỉ tiêu kỹ thuật cho các modem có tốc độ 1200 bit/giây. *So sánh với* Bell 212A. *Xem* bit per second, CCITT, MODEM.

V.22 bis ***chuẩn V.22 lần hai, chuẩn V.22 bis*** Trong tập các chuẩn, khuyến nghị của CCITT về chỉ tiêu kỹ thuật dựa trên tốc độ báo hiệu đường dây 600 baud khi dùng điều chế biên độ vuông góc. Theo chuẩn này, mỗi góc pha của bộ điều chế biên độ vuông góc QAM sẽ biểu diễn bốn bit liên tiếp. Sự kết hợp 600 lần thay đổi tín hiệu trên giây với bốn mẫu bit trên tín hiệu sẽ tạo ra tốc độ 2400 bit/giây. *So sánh với* V.bb, V.22. *Xem* baud, bits per second, quadrature amplide modulation.

V.23 ***chuẩn V.23*** Trong tập các chuẩn, khuyến nghị của CCITT đối với modem tốc độ 600/1200 baud được chuẩn hóa để dùng trên mạng điện thoại chuyển mạch phổ thông. *Xem* MODEM.

V.24 ***chuẩn V.24*** Trong tập các chuẩn, một khuyến nghị của CCITT có thể so với RS-232C. *Xem* RS-232C, V.28.

V.25 ***chuẩn V.25*** Trong tập các chuẩn, một khuyến nghị của CCITT có thể so sách được với RS-366. *Xem* RS-366.

V.26 ***chuẩn V.26*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với modem tốc độ 2400 bit/giây được chuẩn hóa để dùng trên mạng thuê bao bốn dây. *Xem* MODEM.

V.26 bis ***chuẩn V.26 lần hai*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem tốc độ 2400/1200 bit/giây được chuẩn hóa để dùng trên các mạng điện thoại chuyển mạch công cộng. *Xem* MODEM.

V.27 ***chuẩn V.27*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem tốc độ 4800 bit/giây được chuẩn hóa để dùng trên các đường thuê bao. *Xem* MODEM.

V.27 bis ***chuẩn V.27 lần hai*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem tốc độ 4800 bit/giây có bộ hiệu chỉnh tự động được chuẩn hóa để dùng trên các đường thuê bao. *Xem* MODEM.

V.27 ter ***chuẩn V.27 ter*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem tốc độ 4800/2400 bit/giây được chuẩn hóa để dùng trên các các mạng điện thoại chuyển mạch phổ thông. *Xem* MODEM.

V.28 ***chuẩn V.28*** Trong tập các chuẩn, khuyến nghị của CCITT xác định các đặc trưng của tín hiệu điện có thể so sánh với những đặc trưng của RS-232C. *Xem* RS-232C, V.24.

V.29 ***chuẩn V.29*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các modem tốc độ 9600 bit/giây dùng trên các đường thuê bao. *Xem* MODEM.

V.30 ***chuẩn V.30*** Trong tập các chuẩn, khuyến nghị của CCITT đối với các hệ thống truyền dữ liệu song song dùng phổ dụng trên mạng điện thoại chuyển mạch chung. *Xem* MODEM.

V.31 ***chuẩn V.31*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với các đặc trưng điện cho các mạch tráo đổi đơn dòng được kiểm soát bằng tiếp điểm thường đóng. *Xem* MODEM.

V.32 ***chuẩn V.32*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với một chỉ tiêu kỹ thuật dựa trên tốc độ tín hiệu 2400 baud nhờ dùng điều chế biên độ vuông góc. Mỗi góc pha của sao QAM biểu diễn 5 bit liên tiếp. Sự kết hợp 2400 lần thay đổi tín hiệu trên giây với một mẫu 5 bit/ trên một lần thay đổi tín hiệu sẽ tạo ra tốc độ 12000 bit/giây; tuy nhiên, thông lượng bit dữ liệu hiệu quả chỉ là 9600 bit/giây vì một bit ra trong 5 bit chuyển được dùng để sửa lỗi. *So sánh với* V.22 bis. *Xem* baud, bits per second, quadrature amplitude modulation.

V.35 ***chuẩn V.35*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với sự truyền tín hiệu ở tốc độ 48 kilobit/giây khi dùng các mạch ở băng tần nhóm 60 đến 108 kHz.

V.36 ***chuẩn V.36*** Trong tập các chuẩn, một khuyến nghị của CCITT cho các modem để truyền dữ liệu đồng bộ khi dùng các mạch ở băng tần nhóm từ 60 đến 108 kHz. *Xem* MODEM.

V.37 ***chuẩn V.37*** Trong tập các chuẩn, một khuyến nghị của CCITT để truyền dữ liệu đồng bộ ở tốc độ báo dữ liệu cao hơn 72 Kbit/giây khi dùng các mạch ở băng tần nhóm 60 đến 108 kHz.

V.40 ***chuẩn V.40*** Trong tập các chuẩn, một khuyến nghị của CCITT về chỉ thị lỗi bằng thiết bị cơ điện.

V.41 ***chuẩn V.41*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với hệ thống kiểm soát lỗi độc lập mã.

V.50 ***chuẩn V.50*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với các giới hạn chuẩn về chất lượng truyền của truyền dữ liệu.

V.51 ***chuẩn V.51*** Trong tập các chuẩn, một khuyến nghị của CCITT về việc tổ chức bảo dưỡng các mạch điện thoại quốc tế được dùng để truyền dữ liệu.

V.52 ***chuẩn V.52*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với các đặc trưng của các thiết bị đo tỷ lệ lỗi và méo khi truyền dữ liệu.

V.53 ***chuẩn V.53*** Trong tập các chuẩn, một khuyến nghị của CCITT đối

với các giới hạn để bảo dưỡng các mạch kiểu điện thoại được dùng để truyền dữ liệu.

V.54 ***chuẩn V.54*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với thiết bị kiểm tra mạch vòng dùng cho modem. *Xem* MODEM.

V.55 ***chuẩn V.55*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với chỉ tiêu kỹ thuật cho dụng cụ đo tạp âm dạng xung trong các mạch kiểu điện thoại.

V.56 ***chuẩn V.56*** Trong tập các chuẩn, một khuyến nghị của CCITT đối với các phép thử đối chiếu các modem để dùng trên các mạch kiểu điện thoại. *Xem* MODEM.

V-299 ***virut V-299*** Trong an toàn máy tính, một virut lây nhiễm các tệp COM, tác động trong thời gian hoạt động. *Xem* virus names.

V-555 ***virut V-555*** Trong an toàn máy tính, một virut chấm dứt và thường trú trong bộ nhớ, lây nhiễm tệp COMMAND.COM, COM, EXE, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

V800 ***virut V800*** Trong an toàn máy tính, một virut lén lút mã lên chính nó, chấm dứt và thường trú trong bộ nhớ, lây nhiễm các tệp COM, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp *Xem* virus names.

V-801 ***virut V-801*** Trong an toàn máy tính, một virut làm chấm dứt và thường trú trong bộ nhớ, lây nhiễm tệp COMMAND.COM, COM, EXE, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

V-961 ***virut V-961*** Trong an toàn máy tính, một virut làm chấm dứt và thường trú trong bộ nhớ, lây nhiễm tệp COMMAND.COM, COM, EXE, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

V2000 ***virut V2000*** Trong an toàn máy tính, một virut làm chấm dứt và thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

V2100 ***virut V2100*** Trong an toàn máy tính, một virut làm chấm dứt và thường trú trong bộ nhớ, lây nhiễm các tệp COM, EXE, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

vaccine ***vacxin*** Trong an toàn máy tính, một sản phẩm phần mềm được thiết kế để phát hiện một virut. Một số sản phẩm cũng công bố là loại bỏ được virut. *Xem* antiviral measures.

Vacsina ***virut Vacsina*** Trong an toàn máy tính, một virut làm chấm dứt và thường trú trong bộ nhớ, lây nhiễm các tệp COM, EXE và OVL, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

VAD ***bộ VAD*** Viết tắt của Value Added Distributor (bộ phân phối giá trị

gia tăng).

validation *(sự) phê duyệt, (sự) xác nhận tính hợp lệ, (sự) phê chuẩn hợp lệ* (1) Trong mật mã, quá trình kiểm tra tính toàn vẹn dữ liệu của một thông báo, hoặc các phần chọn ra của một thông báo. *Xem* data integrity. (2) Phần phát triển ST&E, các thủ tục, các công cụ và thiết bị chuyên dụng cần thiết để có được sự chấp thuận sử dụng liên kết của một hay nhiều bộ phận của DOD hay những nhà thầu khoán của họ. Hoạt động như vậy bao gồm phát triển cuối cùng, đánh giá, thử nghiệm dẫn tới sự chấp nhận của các chuyên gia trong giới chức ST&E thuộc ba Ban Quân sự hay Sở Bảo vệ và sự phê chuẩn sử dụng liên kết của đại diện thứ trưởng Bộ Quốc phòng trước Policy Review. (3) Trong an toàn máy tính, sự thực hiện kiểm định và đánh giá việc tuân thủ các yêu cầu và chỉ tiêu kỹ thuật về an toàn. (4) Trong lập trình, sự kiểm tra dữ liệu vào về tính đúng đắn so với tiêu chuẩn thiết lập, chẳng hạn định dạng, phạm vi... có thể thực hiện bằng tay hay tự động. *Xem* validity checking.

validity checking *kiểm tra tính hợp lệ* (1) Trong lập trình, một thủ tục kiểm tra xem nhóm mã có đúng là ký tự của mã đang dùng không. (2) Trong lập trình, một thủ tục kiểm tra dữ liệu trong đó các bản ghi vào dữ liệu đều được kiểm tra về phạm vi, biểu diễn hợp lệ... *Xem* resonableness check.

valid password *mật khẩu hợp lệ* Trong kiểm soát truy nhập, một mật khẩu cá nhân sẽ xác thực danh tính của cá nhân trước hệ thống mật khẩu, hay một mật khẩu truy nhập cho phép truy nhập theo yêu cầu trước hệ thống mật khẩu. *Xem* personal password, password.

value added network service *dịch vụ mạng giá trị gia tăng* Trong truyền thông, một dịch vụ thông tin dùng mạng thông tin của công ty truyền thông công cộng để truyền và cung cấp các dịch vụ bổ sung dữ liệu tách biệt với thiết bị bổ sung. Các dịch vụ bổ sung có thể gồm lưu trữ, chuyển tiếp thông báo, giao tiếp thiết bị đầu cuối và máy chủ; những người sử dụng kể cả những người không thuộc tổ chức cung cấp dịch vụ.

value added service provider *nhà cung cấp dịch vụ giá trị gia tăng* Trong truyền thông, một dịch vụ, chẳng hạn hỏi cơ sở dữ liệu trên mạng giá trị gia tăng song được đánh dấu và được hỗ trợ nhờ một tổ chức riêng từ một công ty VANS. *So sánh với* closed user group. *Xem* VANS.

value date *ngày hợp lệ, ngày có giá trị* Trong hoạt động ngân hàng, ngày chuyển mục thực sự vào tài khoản; hoặc ngày nhận được chỉ thị hoặc ngày trong tương lai nào đó được người gửi quy định. *So sánh với* pay date.

value of service pricing *định giá giá trị của dịch vụ* Trong truyền thông, một hệ thống giá trong đó cước phí liên quan tới giá trị của dịch vụ đối với người dùng chứ không phải tới chi phí của nhà cung cấp.

vandalware *phần mềm phá hoại* *Đồng nghĩa với* malware.

van Eck phenomenon *hiện tượng van Eck* Trong an toàn máy tính, nói

tới bức xạ từ một thiết bị hiển thị (VDU). Van Eck đã báo cáo rằng, các tín hiệu được gửi đi từ một VDU có mức điện áp cao và bức xạ điện từ của những tín hiệu như vậy khá mạnh; hơn nữa, tín hiệu nằm trong dải siêu cao tần(UHF). Dưới những điều kiện tối ưu, bức xạ này có thể thu được ở khoảng cách xa từ 0.66 tới 1.25 dăm và có thể hiển thị đọc được. Bức xạ có thể được tách và hiển thị bằng một máy thu hình ở dải UHF sau khi đã thay đổi một số thành phần điện tử chuẩn giá thành thấp. Hiện tượng van Eck bởi vậy có liên quan tới các lĩnh vực an toàn máy tính và tác động của nó đã được chứng tỏ trên một chương trình truyền hình. *Xem* compromissing emanations, Tempest proofing.

VANS *Xem* value added network service.

VANS security ***an toàn VANS*** Trong an toàn dữ liệu, Dịch vụ mạng giá trị gia tăng đặt ra những vấn đề an toàn đặc biệt cho những người thao tác. Nói chung, những vấn đề an toàn này này sinh do:

- người thao tác không thể đảm bảo những người dùng thực hiện các biện pháp và thủ tục an toàn;
- các thiết bị đầu cuối đặt tại các cửa hàng, gia đình... khó kiểm soát truy nhập được;
- khó quy trách nhiệm pháp lý khi một giao dịch người dùng có thiếu sót, chẳng hạn một thông báo bị mất do kết nối liên lạc hỏng.

Những mối nguy hiểm tiềm ẩn đối với người thao tác VANS do hệ thống lỗi hoặc trục trặc các bộ phận là:

- mất thu nhập dịch vụ;
- những yêu sách từ phía người dùng và nhóm thứ ba;
- mất đi sự tin cậy của công chúng.

Mất thu nhập có thể do trục trặc thiết bị, từ đó từ chối sự truy nhập của người dùng, sự gian lận bằng việc phớt lờ các thủ tục lập hóa đơn... Những yêu sách từ phía người dùng hay các nhóm thứ ba có thể này sinh nếu có truy nhập trái phép tới dữ liệu riêng tư, nếu giao dịch hay thông báo bị biến đổi, chẳng hạn như trong giao dịch EFTPOS hoặc nếu các thông báo hay dữ liệu bị mất do bộ phận hay hệ thống thông tin bị hỏng hóc. Mất đi sự tin cậy của công chúng rất đáng lo ngại vì việc cho toàn bộ công chúng biết một lạm dụng của tin tặc có thể gây tổn thất rất lớn so với thiệt hại thực sự trong thực tế hoặc mất đi tiềm năng kinh doanh từ phía người sử dụng.

Có thể dùng các kiểm soát để tối thiểu hóa những nguy hiểm nêu trên và cần xem xét chúng trong tương quan về chi phí với rủi ro mất thu nhập. Chi phí các kiểm soát không chỉ tính theo thiết bị, phần mềm, các chi phí thông tin nâng cấp v.v. mà còn liên quan tới sự suy giảm tính thân thiện với người dùng. Những kiểm soát chính là:

- kiểm soát truy nhập;
- phát triển hệ thống;
- sao lưu dự phòng và khả năng mau hồi phục;
- mật mã và xác thực thông báo;
- các xem xét độc lập.

Có thể xem xét kiểm soát truy nhập dưới hai tiêu đề: truy nhập logic và

truy nhập vật lý. Có rất nhiều lớp người sử dụng với nhiều mức đặc quyền truy nhập trong các hệ thống VANS: những người lập trình hệ thống, kỹ sư bảo dưỡng, những người sử dụng, những khách hàng tiềm năng tại các cuộc thao diễn. Sự tuân thủ có tính nguyên tắc về mật khẩu, xóa các đặc quyền khi nhân viên thôi việc, không có sẵn các PIN ở dạng rõ trong khi truyền, xóa các mật khẩu đã dùng trong các cuộc thao diễn v.v. là tất cả những thao tác cần thiết để tuân thủ sự kiểm soát truy nhập logic.

Kiểm soát truy nhập vật lý đặc biệt quan trọng vì sự phá hoại có thể do những kẻ có chủ tâm, những kẻ khủng bố, những nhân viên bất bình... gây ra. Những người này không có kiến thức trước đó về hệ thống mà cũng chẳng tinh thông về máy tính. Các phím trên cạc, ti vi mạch kín, vị trí site của các thiết bị không giám sát, các hệ thống báo động cho các thiết bị không được giám sát, sự thu hồi các đặc quyền từ những nhân viên thôi việc... là những thành phần của một chiến lược kiểm soát truy nhập khôn ngoan.

Điều chủ yếu là giai đoạn phát triển hệ thống cần được chỉ đạo và được giám sát để tránh thiếu sót về mặt kỹ thuật cả do vô tình lẫn có chủ ý trên hệ thống tại chỗ. Nó bao gồm:

- Sử dụng các phương pháp luận phát triển bản thiết kế được cấu trúc thích hợp.
- Thực hiện các thủ tục kiểm soát chất lượng kể cả việc xem xét độc lập tất cả các modun phần mềm.
- Việc xem xét độc lập thiết kế hệ thống là do chuyên gia an toàn thực hiện.

Một dạng tấn công đơn giản và trực tiếp lên hệ thống là gây khó khăn hoặc gây nhiễu lên tuyến liên lạc. Nếu dữ liệu không đích thực được đưa vào một kênh liên lạc mang dữ liệu mã thì người thao tác có thể cho rằng, có một lỗi trong thiết bị mật mã và bỏ nó ra khỏi đường dây để duy trì dịch vụ. Những tùy chọn cần xem xét trong việc cung cấp các hệ thống dự phòng là:

- dùng một site chứa các bản dự phòng;
- phân phối các phương tiện xử lý trên một số nút để phòng ngừa rủi ro hỏng hóc trên toàn hệ thống do sự cố tại một site;
- dùng phần cứng có khả năng kháng lỗi;
- nhiều kiểu định tuyến các kênh liên lạc.

Có thể dùng mật mã để che dấu hay xác thực dữ liệu tài chính hoặc dữ liệu nhạy cảm. Những sơ đồ đó đòi hỏi khóa mã dùng cho các thông báo truyền đi phải thay đổi thường xuyên; các sơ đồ quản lý khóa kết hợp phải được thiết kế cho môi trường VANS, nơi các thiết bị đầu cuối thường không được giám sát và các vị trí không an toàn. Mật mã có lẽ không phải là một giải pháp tốt trong những ứng dụng VANS nào đó, chẳng hạn dịch vụ ngân hàng tại nhà, nơi các thiết bị đầu cuối của người dùng phải rẻ và thân thiện với người sử dụng. *Xem* access control, authentication, card key, CCTV, cryptography, disgruntled employee, EFTPOS, hacker, home banking, key management, VANS.

VAR ***VAR*** Viết tắt của Value Added Retailer (hãng bán lẻ giá trị gia tăng).

variable ***biến*** Trong lập trình, một đại lượng được đặt tên trong chương trình và có thể mang giá trị bất kỳ trong phạm vi giá trị hợp lệ với kiểu của nó và có thể được thao tác bởi toán tử hợp lệ bất kỳ đối với kiểu đó. Tên cho trước đối với một biến là một chuỗi các ký tự được dùng để biểu thị vị trí bộ nhớ cụ thể, nơi giữ giá trị hiện hành của biến. Bộ dịch của chương trình nguồn gán vị trí nhớ cho biến đã được đặt tên.

variable length record ***bản ghi độ dài thay đổi*** Trong các cấu trúc dữ liệu, một bản ghi có độ dài độc lập với độ dài của các bản ghi khác liên kết với nó. Một bản ghi như vậy có thể chứa các nhóm lặp. *So sánh với* fixed length record.

varying density holographic card ***các ảnh toàn ký mật độ thay đổi*** *Đồng nghĩa với* optical density card.

VASP *Xem* value added service provider.

V.bb ***chuẩn V.bb*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với một chỉ tiêu kỹ thuật cho việc truyền dữ liệu ở tốc độ 4800 bit/giây qua modem tương hợp với kênh điện thoại cấp tiếng nói. *Xem* voice grade channel, MODEM, V-series recommendations of CCITT.

Vcomm ***virut Vcomm*** Trong an toàn máy tính, một virut lây nhiễm các tệp EXE, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình và OVL và liên kết tệp. *Xem* virus names.

VDU ***khối hiển thị trực quan, thiết bị hiển thị trực quan*** *Xem* visual display unit.

vector ***vectơ*** (1) Một biến có cả độ lớn lẫn hướng. (2) Trong cấu trúc dữ liệu, một đại lượng được biểu diễn bởi một tập thứ tự các số, chẳng hạn mảng một chiều.

veincheck ***kiểm tra mạch*** Trong kiểm soát truy nhập, một kỹ thuật sinh trắc có thể quét các đường gân dưới da tay hay cổ tay của đối tượng. Thiết bị gồm một bộ quét tia hồng ngoại và một camera điện tử; đối tượng đặt tay vào bộ quét và hình ảnh các đường gân được camera ghi lại được số hóa và được so sánh với hình ảnh số hóa đã lưu tương đương. Tỷ lệ sai số không đổi yêu cầu cỡ 0.1%. *Xem* biometric, equal error rate.

verification ***(sự) xác minh, (sự) kiểm chứng*** (1) Trong an toàn máy tính, sự chứng minh bằng tài liệu về sự thâm nhập hay cố gắng thâm nhập vào hệ thống trực tuyến thực, phù hợp hoặc trái với những giả thuyết đã phát triển trong quá trình phân tích và xem xét hệ thống. (2) Trong an toàn máy tính, quá trình so sánh hai mức đặc tả hệ thống để có phù hợp (chẳng hạn, mô hình chính sách an toàn với đặc tả mức cao, TLS với mã nguồn hay mã nguồn với mã đối tượng). Quá trình này có thể hoặc không tự động hóa. *Xem* object code, source code, TLS.

verify ***xác minh, thẩm tra*** (1) Xác định xem một hoạt động hay thao tác trên dữ liệu có được thực hiện đúng không. (2) Trong tính toán, một phương

tiên xác minh xem dữ liệu được ghi lên đĩa có được ghi đúng không. Người sử dụng ra lệnh "Verify on" thì toàn bộ các hoạt động ghi lên đĩa sẽ được kiểm tra cho tới khi người dùng xóa bằng lệnh "Verify off".

Vernam cipher ***mã pháp Vernam*** Trong mật mã, một phép mã dòng trước đây được phát triển cho các máy điện báo in chữ vào năm 1917. Các ký tự của bản rõ được mã hóa thành dạng nhị phân và được đục lỗ lên băng giấy; một tập các số ngẫu nhiên cũng được biểu thị ở dạng nhị phân được đục lỗ tương tự lên băng giấy thứ hai. Hai băng giấy này được đọc đồng bộ, các số được cộng modulo 2 và nhờ thế tạo ra băng bản mã tương ứng. Bên thu được cung cấp một băng giấy chứa cùng dòng bit mã và bản rõ nhận được bằng phép cộng modulo 2 bản mã với dòng bit mã. *Xem* Vigenére cipher. *Xem* cryptographic bit stream, modulo arithmetic, stream cipher.

version number ***số hiệu phiên bản*** Trong tính toán, chỉ bản nâng cao chứa trong một sản phẩm cụ thể của một hệ điều hành.

vertical redundancy check ***kiểm tra dư thừa dọc*** *Xem* longitudinal redundancy check.

vibrating bell ***chuông rung*** Trong an toàn vật lý, một thiết bị báo động rung liên tục chừng nào còn có năng lượng hoạt động. *So sánh với* single stroke bell.

vibrating horn ***còi rung*** Trong an toàn vật lý, một kiểu còi điện từ tạo ra một tín hiệu báo động âm học do sự hoạt động của phần ứng rung động trước một màng ngăn kim loại.

vibration detector ***bộ phát hiện dao động, thiết bị phát hiện rung động*** Trong an toàn vật lý, một bộ cảm biến dùng âm thoa hoặc các tiếp xúc vòng hoặc thủy ngân rất thăng bằng mà khi được rung hay chuyển động sẽ gây tín hiệu báo động. Các thiết bị có âm thoa nhạy với các dao động đặc biệt, chẳng hạn những dao động do tiếng kính vỡ.

Victor ***virut Victor*** Trong an toàn máy tính, một loại virut làm chấm dứt hoạt động và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, làm hỏng các tệp chương trình, dữ liệu và OVL và các liên kết tệp. *Xem* virus names.

video motion detector ***bộ phát hiện chuyển động video*** Trong an toàn vật lý, một thiết bị được dùng cùng với hệ thống CCTV có thể phát hiện sự thay đổi trong hình ảnh thu được. Hình ảnh được mã số và được lưu lại, những thay đổi so với phần bất kỳ của hình ảnh được lưu kế cận sẽ chỉ ra một chuyển động trong vùng thuộc tầm nhìn.

video switcher ***bộ chuyển mạch video*** Trong an toàn vật lý, một thiết bị chuyển mạch CCTV để định tuyến lại các tín hiệu từ camera video đến các bộ giám sát. Bộ chuyển mạch cho phép người dùng quay camera theo kiểu nối tiếp hay bắc cầu. *Xem* bridging sequential switcher, CCTV, homing sequential switcher, sequential switcher.

videotex ***hệ hiển thị dữ liệu, hệ truyền văn bản video*** Một thuật ngữ

được dùng phổ dụng chỉ các dịch vụ điện toán cung cấp tin tức và các thông tin khác trên màn hình tivi (hay teletext). Hệ hiển thị dữ liệu được giới thiệu lần đầu tiên vào cuối những năm 1970 và một số dịch vụ công cộng đã được thực hiện. Công nghệ hệ hiển thị dữ liệu được thiết kế để tạo một kết nối giữa các thành viên của cộng đồng và một máy tính trung tâm. Ở dạng cao nhất, nó có thể cho phép đưa thư viện tra cứu cực lớn, năng lực máy tính và các tiện ích liên lạc mở rộng về nhà. Thuật ngữ videotext bao trùm hai phát triển công nghệ tách bạch: hiển thị dữ liệu và truyền văn bản (teletext). Trong trường hợp đầu, một liên kết với sự liên lạc hai chiều đơn giản thiết lập giữa người dùng và máy tính chủ thông qua mạng điện thoại. Với teletext, dòng thông tin là đơn công, phát rộng rãi qua các dải sóng tivi kết hợp với các chương trình vô tuyến. *Xem* viewdata, teletext.

videotext *văn bản video* Sự hiển thị tài liệu nguyên bản trên màn hình CRT hay màn hình tivi. *So sánh với* videotex.

Vienna/648 *virut Vienna/648* Trong an toàn máy tính, một virut lây nhiễm các tệp COM, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

view *khung xem, khung nhìn* (1) Trong các cơ sở dữ liệu, một chức năng đa trị từ một tập các quan hệ tới một quan hệ hay tập của nó. Thực tế, một khung nhìn tiết kiệm cho người sử dụng khỏi phải điều khiển dữ liệu được lưu. Ví dụ, nếu một cơ sở dữ liệu lưu trọng lượng của các mục hàng hóa riêng trong một khoang hàng hóa trên tàu và số lượng mỗi loại hàng, thì người dùng có thể yêu cầu xem trọng lượng tổng thể của hàng hóa như thể nó là một mục lưu hơn là phải gọi ra các mục dữ liệu riêng lẻ và thực hiện phép cộng. Biện pháp dùng khung nhìn gây ấn tượng cho người dùng là dữ liệu lấy ra được lưu trong cơ sở dữ liệu theo nghĩa thích hợp nhất đối với các yêu cầu của người dùng. *Xem* multilevel database security. (2) Trong các cơ sở dữ liệu, một tập con các cơ sở dữ liệu có sẵn đối với một người dùng cụ thể. *Xem* access control. (3) Trong các cơ sở dữ liệu, phần của cơ sở dữ liệu thỏa mãn các điều kiện một câu hỏi đưa ra.

viewdata *quan sát dữ liệu, hiển thị dữ liệu* Trong hệ hiển thị dữ liệu (videotex), một dịch vụ thông tin tương tác dùng kết nối điện thoại giữa người dùng và một máy tính chủ. Người sử dụng dùng một thiết bị đầu cuối đặc biệt hay một bộ thích ứng được liên kết với một máy thu vô tuyến nội địa. *Đồng nghĩa với* interactive videotex.

violation of transmission security *(sự) vi phạm an toàn truyền dẫn* *Đồng nghĩa với* traffic analysis.

Violator *virut Violator* Trong an toàn máy tính, một virut lây nhiễm các tệp COMMAND.COM và COM, tác động trong thời gian hoạt động, làm hỏng các tệp chương trình, OVL và các tệp dữ liệu. *Xem* virus names.

virtual *ảo* Trong kiến trúc và liên lạc dữ liệu, một mô tả của một phương tiện được cung cấp cho người dùng hay hệ thống như thể nó là một thực tại

vật lý. *So sánh với* transparent.

virtual call service ***dịch vụ gọi ảo*** Trong truyền thông dữ liệu, một dịch vụ chuyển mạch gói có thiết lập một kết nối logic trước khi chuyển đi. Các gói được chuyển trên kết nối logic, một số trong chúng không chứa dữ liệu song được dùng với mục đích giám sát. Trong giai đoạn chuyển dữ liệu, trình tự gói và các thao tác kiểm soát lưu lượng được thực hiện. *Xem* flow control, packet switching, packet switching network, virtual circuit.

virtual circuit ***mạch ảo*** Trong truyền thông dữ liệu, một mạch chứa một nhánh thiết lập từ nguồn tới đích trên mạng. Trong lúc gọi, tất cả các gói không lập địa chỉ riêng đều được truyền qua mạch ảo này và đến theo cùng trình tự như khi phân phối. *So sánh với* datagram, packet switching, packet switching network.

virtual machine ***máy ảo*** Trong tính toán, một phép mô phỏng máy tính và các thiết bị đi kèm theo thông qua một máy tính khác.

virtual memory ***bộ nhớ ảo*** (1) Trong tính toán, một kỹ thuật cho phép bộ xử lý dùng không gian địa chỉ đầy đủ của nó, thậm chí còn lớn hơn cả bộ nhớ vật lý chính có sẵn. Không gian nhớ ảo tồn tại trên đĩa nằm ngoài bộ nhớ chính khi bộ xử lý xác định địa chỉ một phần không gian địa chỉ của nó, phần cứng đặc biệt sẽ định vị trang cần thiết trên đĩa và chuyển nó tới một phân khu của bộ nhớ chính. *Xem* address space, page. (2) Trong an toàn máy tính, các hệ thống nhớ ảo cung cấp một cơ chế buộc tuân thủ sự kiểm soát truy nhập. Những người dùng dùng chung bộ nhớ vật lý, song có thể gán các trang nhớ ảo cho những người dùng hay quá trình riêng. Bảng các mục vào trang nhớ có thể chỉ ra kiểu truy nhập (đọc, ghi hay không) cho phép từ mỗi nút truy nhập. *Xem* access control.

virtual password ***mật khẩu ảo*** Trong kiểm soát truy nhập, một mật khẩu được tính toán từ một câu mật khẩu (passphrase), đáp ứng các yêu cầu của kho lưu mật khẩu (chẳng hạn 64 bit đối với DES). *Xem* passphrase, password.

virtual terminal ***thiết bị đầu cuối ảo*** Trong phần ngoại vi, một thiết bị đầu cuối lý tưởng được xác định như một chuẩn quản lý thống nhất các thiết bị đầu cuối thực sự. Bộ xử lý thiết bị đầu cuối sau đó sẽ chuyển các tín hiệu của thiết bị đầu cuối thực cho phù hợp với các chuẩn của thiết bị đầu cuối ảo. *Xem* terminal.

virtual terminal protocol ***giao thức đầu cuối ảo*** Trong truyền thông dữ liệu, một giao thức cho phép các chương trình truy nhập tới các thiết bị đầu cuối trên mạng độc lập với kiểu thiết bị đầu cuối đang dùng. *Xem* network virtual terminal, protocol.

virus ***virut*** (1) Trong an toàn máy tính, một dạng mã ác ý có tác động tới các chương trình khác bằng cách tự biến đổi để chèn bản sao có thể đã tiến hóa của chính nó. (2) Trong an toàn máy tính, một dạng mã ác ý kiểu "con ngựa thành Toroa tự lan truyền" bao gồm một thành phần thực thi nhiệm vụ,

một thành phần khởi sự và thành phần tự lan truyền. (3) Trong an toàn máy tính, một dạng mã ác ý:

- là một tập các lệnh lập trình hay dạng khác tự lan truyền qua các hệ thống máy tính và/hoặc các mạng và
- được thiết lập có chủ ý để thực hiện những hành vi mà những người chủ hợp pháp của những hệ thống đó không muốn.

Giới thiệu

Cohen đã công bố một công trình nghiên cứu về virut vào năm 1984 và trong công trình này, ông đã đưa ra một bản mô tả giả ngôn ngữ của một virut điển hình.

Hoạt động của chương trình virut là trước hết tìm kiếm một tệp khả thi khác và kiểm tra xem chuỗi dấu hiệu virut mà trong trường hợp này là chuỗi '1234567' có tại điểm bắt đầu của tệp không. Nếu dấu hiệu này có thì

```
program virus:=
{1234567;
subroutine infect-executable:=
{loop: file = random-executable;
if first-line-of-file = 1234567
then goto loop;
prepend virus to file;
}
subroutine do-damage:=
{whatever damage is design}
subroutine trigger-pulled:=
{return true on desired conditions}
main-program:=
{infect-executable;
if trigger-pulled then do damage;
}
next:}
```

Cohen Virus

tệp bị lây nhiễm và tệp khả thi tiếp theo trong thư mục bị xem xét. Nếu khi đó phát hiện ra một tệp chưa bị lây nhiễm thì mã virut được ghi lên phần bắt đầu của tệp.

Giai đoạn tiếp theo của hoạt động virut phụ thuộc vào sự hiện diện của bom logic hay bom thời gian trong mã virut. Cơ chế khởi sự được kiểm tra, chẳng hạn thời gian/ngày được kiểm tra xem có phải là 13 giờ ngày thứ sáu không; nếu đúng thì hoạt động gây hại được thực hiện, chẳng hạn định dạng đĩa theo quy định trong mã virut. Tệp khả thi bị lây nhiễm bởi virut có thể gây lây nhiễm bất cứ khi nào nó được thi hành.

Một virut không cần phải có bom logic/thời gian hay hoạt động ác ý đi theo. Tuy nhiên kinh nghiệm về các tấn công bằng virut cho thấy rằng, những tác động gây hại có thể phát triển khi các virut lan vào các môi trường mới, thậm chí khi không có mã ác ý gài trong đó.

Mã mô tả như trên chỉ là một lớp các virut có thể. Mã virut không nhất thiết gán vào phần đầu của các tệp khả thi, và lại mỗi lần mã virut thi hành, có hơn một tệp khả thi bị lây nhiễm.

Trong thảo luận về vấn đề lan truyền, phát hiện, chống... các virut, điều quan trọng là phân biệt giữa hành động của virut chỉ ra với hành vi của virut nào đó trên lý thuyết. Luôn có thể xử lý các virut đã biết vì nó có các tính chất và hành vi đặc trưng, chẳng hạn trong ví dụ ở trên, sự có mặt của virut có thể

phát hiện ra nhờ dấu hiệu '1234567' phần đầu của tệp.

Tuy nhiên, trong trường hợp chung nhất, người ta quy định cơ chế bảo vệ chống lại virut phải là cơ chế dựa trên thuộc tính nào đó của virut. Điều này có thể dẫn tới người viết virut tạo ra một chương trình làm nhiễm các chương trình khác song lại không có thuộc tính đó. Vào lúc này, không thể chỉ ra một thuộc tính phải luôn có mặt trong virut tùy ý và phải luôn không có mặt trong mã hợp pháp nào đó. Bởi vậy, không có thử nghiệm được biết đến nào có thể nhận diện một cách rõ ràng một virut và Cohen đã gợi ý rằng, về mặt lý thuyết không thể phát triển một thử nghiệm như vậy.

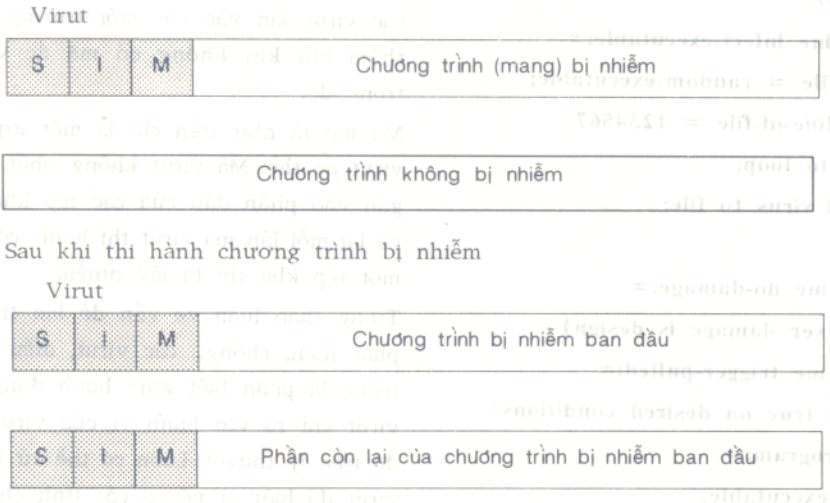
Sự lan truyền virut sẽ nhanh chóng qua một hệ thống máy tính vì mỗi chương trình bị nhiễm lại làm nhiễm tiếp các chương trình khác khi nó được thi hành. Thậm chí, nếu chỉ cho phép sự chia sẻ hạn chế thông tin trên hệ thống thì virut cũng sẽ lan truyền do bản chất bắc cầu của dòng thông tin. Như vậy, nếu A có thể chia sẻ thông tin với B thì tất cả thông tin có sẵn đối với A và tất cả thông tin có sẵn đối với B đều có thể bị lây nhiễm bởi virut bị thả đầu tiên trong các tệp của A, ngay cả khi chỉ có một tệp được chia sẻ giữa A và B. Tương tự, nếu B chia sẻ thông tin với C thì virut có thể ảnh hưởng tới tất cả các tệp của C.

Các kiểu virut

Các virut được phát triển đến nay có thể có một hay nhiều các thuộc tính: ghi đè, không ghi đè, mã nguồn, thường trú bộ nhớ, cung mồi và máy tính cá nhân. Virut thịnh hành nhất là các virut cung mồi (boot sector) tấn công các máy tính cá nhân.

Các virut ghi đè

Các virut ghi đè đến nay có tỷ lệ tương đối; hoạt động của nó được minh họa



virus: *virut.* Hình 1. Hành động của một virut ghi đè.

trên hình 1. Chương trình tải virut được đưa vào hệ thống máy tính vô tình hay cố ý. Phần virut của chương trình tải gồm ba phần:

- *S*, dấu hiệu virut.
- *I*, chương trình gây lây nhiễm.
- *M*, mã ác ý.

Khi chương trình mang được thi hành, virut bắt đầu hoạt động. Dấu hiệu *S* chỉ đơn giản một lệnh nhảy tới phần mã *I*; hoạt động đầu tiên của đoạn chương trình lây nhiễm là tìm tập tin khả thi và nạp nó vào bộ nhớ. Tệp khả thi nhờ quá trình thi hành để chuyển điều khiển tới byte đầu tiên. Chương trình lây nhiễm sau đó sẽ kiểm tra xem có dấu hiệu *S* không: nếu có thì đoạn chương trình lây nhiễm sẽ tìm một tệp khả thi khác và nạp nó từ kho lưu trữ thứ hai vào bộ nhớ chính. Nếu không có dấu hiệu *S* thì đoạn trình lây nhiễm sẽ ghi đè lên phần thứ nhất của mã thi hành cùng với 3 phần *S*, *I* và *M* rồi sau đó ghi tệp ngược trở về kho lưu trữ thứ hai.

Giai đoạn tiếp theo của virut phụ thuộc vào phần mã ác ý *M*. Nếu phần này có trong virut thì hoạt động ác ý, chẳng hạn biến đổi các tệp, có thể thực hiện vô điều kiện hoặc phụ thuộc vào cơ chế khởi sự, ví dụ bom logic hay bom thời gian. Sau đó điều khiển được chuyển tới phần còn lại của chương trình mang.

Khi chương trình lây nhiễm chạy, virut sẽ tìm cách lây nhiễm tới tệp khả thi khác, tuy nhiên, khi điều khiển được chuyển tới phần còn lại của chương trình người dùng thì chương trình này sẽ bị hỏng hoặc chạy một cách dị thường. Virut có thể che dấu tung tích của nó nhờ một thông báo lỗi, ví dụ lỗi chẵn lẻ và như vậy làm người dùng tin rằng có sự cố hệ thống nào đó.

Các virut ghi đè có hai đặc trưng quan trọng:

- độ dài của chương trình bị lây nhiễm không bị thay đổi bởi sự có mặt của virut.
- chương trình bị nhiễm sẽ hoạt động dị thường vào lúc thi hành hoặc gây nên thông báo lỗi.

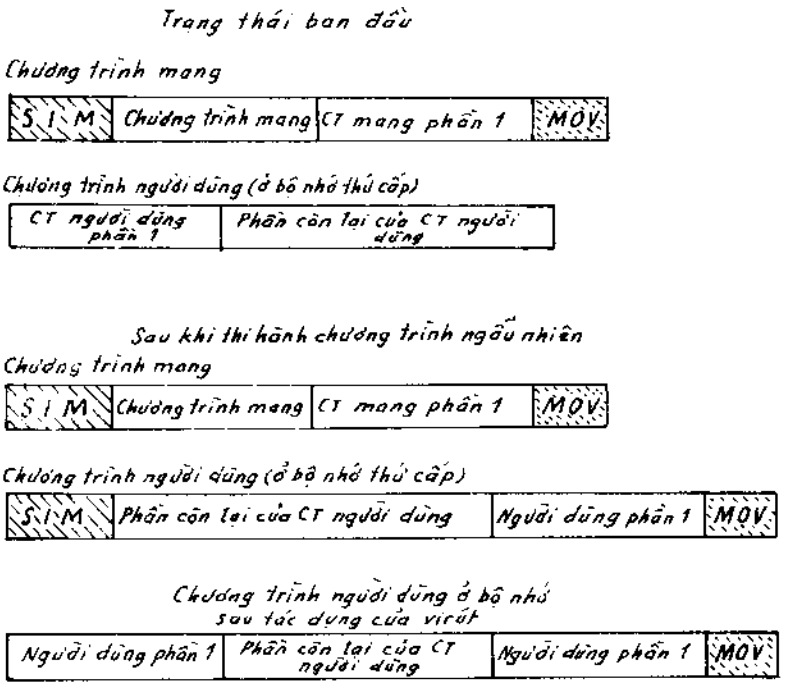
Các virut không ghi đè

Một virut không ghi đè thường sẽ làm tăng độ dài của các phần mềm bị nhiễm song nó có thể cho phép chương trình chạy một cách bình thường sau khi virut đã hoạt động. Hoạt động của virut không ghi đè được nêu trên hình 2.

Mã virut chứa ba phần *S*, *I* và *M* giống như virut ghi đè nêu trên. Ngoài ra nó còn có một lệnh MOV sao chép dữ liệu từ phần này sang phần khác của bộ nhớ.

Đầu tiên, virut tìm một tệp tin khả thi không chứa dấu hiệu *S*, tức nó chưa bị nhiễm. Sau đó virut chọn phần đầu tiên của tệp đó, Phần 1 trong biểu đồ có cùng độ dài đúng như các phần của virut *S*, *I* và *M*. Phần 1 này sau đó được sao chép lên phần cuối của của chương trình và đoạn mã MOV được gắn vào phần cuối của chương trình đó. Khi đó mã virut *S*, *I*, *M* được ghi vào phần đầu của tệp, đè lên Phần 1. Sau đó, virut chuyển điều khiển tới mã ác ý *M* của nó và từ đó tới chính chương trình mang.

Khi chương trình người dùng bị nhiễm được gọi đến, nó được sao chép vào bộ nhớ chính; mã virut *S*, *I* và *M* tiếp tục



virus: *virut*. Hình 2. Hoạt động của một virut không ghi đè. *S* - dấu hiệu virut; *I* - mã tác động của virut; *M* - mã tác động ác ý; MOV - mã chuyển động.

làm lây nhiễm và thực hiện hành động gây hại bất kỳ kèm theo *M*. Sau đó điều khiển được chuyển tới đoạn chương trình MOV tại phần cuối của chương trình. Đoạn chương trình MOV sẽ sao chép Phần 1 tại đoạn cuối chương trình lên phần đầu, ghi đè phần *S, I, M* của virut. Lúc này, điều khiển lại được chuyển tới phần đầu của chương trình người dùng, chương trình này thi hành bình thường.

Các virut không ghi đè có hai đặc trưng quan trọng:

- độ dài của các chương trình bị lây nhiễm thường bị tăng lên khi có virut;
- chương trình bị nhiễm vẫn có hành vi bình thường sau khi virut đã hành động. Nếu virut không gây nên hoạt động ác ý đáng lưu ý nào thì sự có mặt của nó sẽ được nguỵ trang.

Các virut mã nguồn

Một virut mã nguồn được ghi lên mã nguồn của một chương trình mang và tấn công lên mã nguồn của các chương trình khác. Một sinh viên chưa tốt nghiệp bất kỳ có thể viết một mã nguồn virut bằng ngôn ngữ BASIC. Hoạt động của một chương trình như vậy được mô tả như sau:

- Vào lúc chương trình virut chạy, nó kiểm tra thư mục xem có các tệp .BAS không;
- Virut đọc tên của tệp .BAS và kiểm tra nội dung của tệp có chứa tên các tệp bị nhiễm đến lúc đó không;
- Tệp chưa bị nhiễm được chọn sẽ được hợp nhất vào chương trình virut;
- Tệp chưa bị nhiễm bị ghi đè bằng chương trình hợp nhất nêu trên;
- Tên của tệp vừa bị nhiễm được ghi vào tệp chứa danh sách các tệp bị nhiễm.

Các virut mã nguồn có hai ưu điểm quan trọng, ít nhất là theo quan điểm của người phát triển virut:

- Chúng có thể di chuyển qua lại giữa các hệ điều hành;
- Kỹ thuật của các chương trình vô hiệu hóa virut thông thường bằng cách biên dịch lại sẽ không tác dụng.

Các virut thường trú bộ nhớ

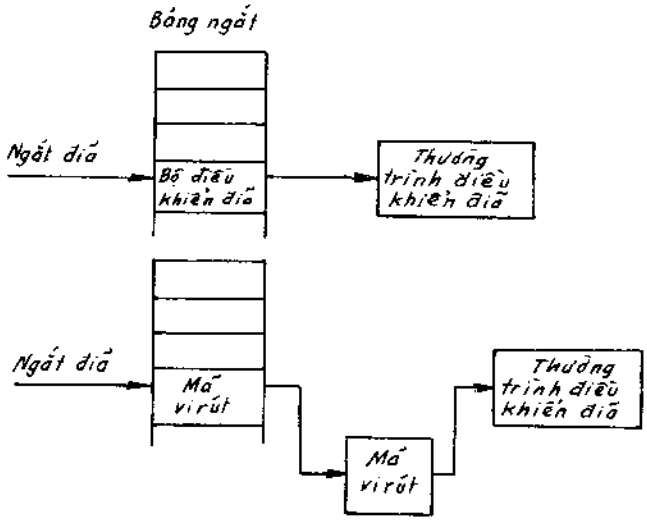
Những người thiết kế virut không chắc rằng, mã của họ được người dùng không nghi ngờ gọi ra trước khi chương trình người dùng đầu tiên bị lây nhiễm. Khi vượt qua được rào chắn này, thì sự lây nhiễm sẽ lan truyền khi người dùng gọi tới các chương trình bị nhiễm của mình.

Các virut thường trú bộ nhớ có thể khắc phục vấn đề về việc gọi tới lần đầu này bằng cách lợi dụng tính linh hoạt nội tại bên trong các kiến trúc của máy tính cá nhân. Một đặc điểm cơ bản của các máy tính là phương tiện ngắt, nó có thể gọi tới mã không thuộc phạm vi dãy các lệnh của một chương trình ứng dụng.

Khi một chương trình ứng dụng được thi hành, có sự giao tác giữa mã ứng dụng và mã hệ điều hành. Bất cứ khi nào chương trình ứng dụng giao tác với bộ phận nào đó của máy tính, ví dụ đọc đầu vào bàn phím, đưa dữ liệu ra máy in, đưa dữ liệu vào từ một đĩa từ... nó sẽ gọi phần mã hay một trình điều khiển trong hệ điều hành. Các chương trình ứng dụng phải biết nơi tìm trình điều khiển và khi hành động mà trình điều khiển yêu cầu hoàn thành thì hệ điều hành phải biết đoạn lệnh cần thi hành tiếp theo của chương trình ứng dụng. Sự bàn giao và sự chuyển ngược điều khiển này được thực hiện bởi kiến trúc ngắt của máy tính.

Khi chương trình ứng dụng yêu cầu dữ liệu từ đĩa, nó sẽ đơn giản tăng ngắt đĩa lên. Điều khiển được chuyển tới trình điều khiển đĩa và trạng thái của chương trình ứng dụng sẽ được bảo lưu trong khi thi hành mã của trình điều khiển. Khi trình điều khiển đĩa đã đọc xong dữ liệu từ đĩa, trạng thái của chương trình ứng dụng được phục hồi và tiếp tục quá trình của mình.

Trong các máy tính cá nhân, sự kết nối giữa một ngắt đĩa và trình điều khiển đĩa do một mục vào của bảng nằm trong RAM cung cấp. Như vậy, ngắt đĩa này làm một địa chỉ được đọc từ bảng ngắt và điều khiển được chuyển sang cho trình điều khiển đĩa lưu tại địa chỉ đó. Những người thiết kế virut khai thác tình huống này để bảo đảm việc gọi tới mã của họ (xem hình 3). Virut thay thế địa chỉ của trình điều khiển đĩa nằm trong bảng ngắt bằng địa chỉ của đoạn mã virut.



virus: *virut*. Hình 3. Virut chuyển điều khiển từ bộ điều khiển đĩa sang mã của virut.

Khi chương trình ứng dụng yêu cầu một thao tác trên đĩa, nó sẽ tạo ra một ngắt đĩa. Địa chỉ của đoạn mã virut trong mục vào của bảng ngắt được thay bằng địa chỉ của trình điều khiển đĩa. Như vậy, yêu cầu về đĩa sẽ gọi tới mã virut, khi virut thực hiện xong hành vi của mình, điều khiển được chuyển sang trình điều khiển đĩa sao cho người dùng không nhận ra có sự lây nhiễm.

Hành vi của virut thường trú bộ nhớ có thể được minh họa bằng giải mã:

Nếu virut không thường trú trong bộ nhớ thì nó sẽ:

thay thế ít nhất một ngắt, chấm dứt và nằm thường trú

thi hành chương trình nguyên thuỷ

Ngắt mới

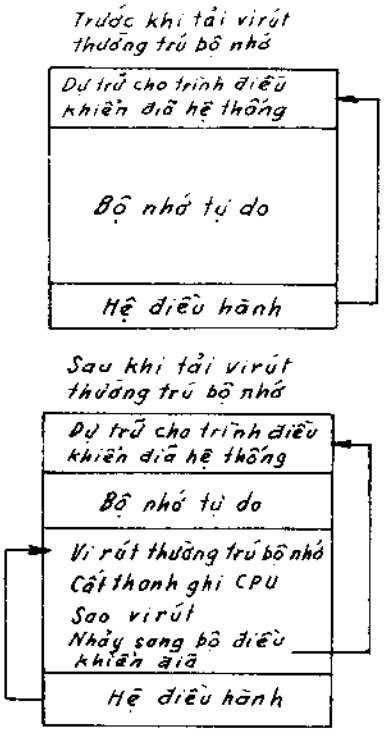
Nếu tìm thấy một tệp chưa bị lây nhiễm thì lây nhiễm tệp đó

Nếu điều kiện khởi sự thỏa mãn thì thực hiện hành động ác ý

Chuyển điều khiển tới chương trình ngắt ban đầu

Dạng chung của các virut thường trú bộ nhớ trong máy tính cá nhân là virut cung mồi (boot sector). Cung mồi là cung đầu tiên được đọc khi đĩa mềm hay cứng được khởi động; đoạn mã virut được lưu trên đĩa bởi vậy có thể giữ lấy quyền điều khiển trước hành động bất kỳ của người dùng. Sau đó virut sẽ tấn công lên hệ thống máy tính cá nhân (xem hình 4).

Một trong những virut cung mồi độc hại nhất là virut Brain hay virut Pakistani. Basit Alvit, một người bán hàng 19 tuổi người Pakistani đã tạo ra virut trong máy tính cá nhân và đã kết hợp nó vào thông báo về bản quyền khi đưa tên - Brain Computer Services, địa chỉ và số phôn vào trong mã virut. Alvit đã khai



virus: *virut*. Hình 4. Virut thường trú bộ nhớ.

là anh ta chỉ đưa ra một bản sao virut cho một người bạn. Bằng cách nào đó nó đã lan tới tận Mỹ và các phiên bản của nó đã xuất hiện tại các đại học Delaware, Pitsburgh, George Washington, Pennsylvania và Georgetown. Virut thông thường không có cơ chế gây hại mặc dù trong môi trường có tác động phụ nào đó, nó có thể phá hủy các secto dữ liệu trên đĩa. Có nhiều phiên bản của virut Brain khắp thế giới và người ta đã ghi lại được sự gây hại do sự biến đổi của nó. Virut Brain thường trú một phần trong bộ nhớ trong cung mồi của đĩa mềm và một phần ở ba liên cung được đánh dấu là những cung từ hỏng.

Các virut máy tính cá nhân

Những báo cáo đầu tiên về sự tấn công của virut xuất hiện trong khu vực máy tính cá nhân. Rõ ràng rằng, các máy tính cá nhân có rủi ro do các tấn công của virut lớn hơn nhiều so với các máy tính cỡ lớn vì các lý do sau:

- có sự dùng chung rộng rãi các đĩa mềm và các phần mềm giữa những người sử dụng máy tính cá nhân;
- số rất lớn người dùng một số hạn chế hệ điều hành, chẳng hạn MS.DOS;
- một người phát triển virut có vô số cơ hội truy nhập tới tất cả các bộ phận của hệ điều hành và có rất nhiều cơ hội thử nghiệm virut;

- nhiều người dùng máy tính cá nhân không hiểu biết thực sự về tính toán và không nghĩ gì đến việc phát hiện sớm các dấu hiệu về tấn công của virut;
- các máy tính cá nhân được sử dụng rộng rãi trong các trường học, một mảnh đất tốt cho những kẻ nghịch ngợm.

Virut Brain đã được chứng minh chỉ là một trong vô số virut máy tính cá nhân. Giữa năm 1988 và cuối năm 1990, đã có hàng ngàn báo cáo về những dạng virut mới có bí danh chung là: Macintosh, LeHigh, Amiga, Israeli, Bouncing Ball, Marijuana...

Hầu hết những virut này là các dạng khác nhau của virut cung khởi động. Vào giữa năm 1990, các báo cáo về một loại virut lén lút (stealth virus) mới đã được đưa ra, trong đó có virut 4096 hay 4k, virut IDF (lực lượng Quốc phòng Israen) và Frodo. Virut trộm đêm (stealth) tìm cách che dấu sự có mặt của mình bằng cách tiếp tục kiểm soát máy. Trong trường hợp virut 4096, virut thường trú vào bộ nhớ và sau đó bẫy các ngắt đĩa. Khi các tệp khả thi bị lây nhiễm, độ dài của nó được tăng tới 4096 byte. Virut sẽ thực sự tẩy mầm bệnh (disinfect) các tệp trên đường để che dấu việc gây lây nhiễm; nếu một tệp .COM bị nhiễm được sao chép tới một tệp có phần mở rộng khác thì tệp sẽ được tẩy mầm khi nó được sao chép, nhằm che dấu bằng chứng về sự lây nhiễm. Virut có bom thời gian thiết lập vào ngày bất kỳ giữa 22 tháng 9 tới 31 tháng 12. Ngày đầu là ngày sinh của Frodo, một nhân vật trong tiểu thuyết của Tolkien có tên "The Lord of the Rings". Virut làm hiển thị một thông báo 'Frodo lifes' khi bom thời gian khởi sự, song nó còn có một rệp chương trình (bug) làm treo máy.

Các virut trộm đêm có triển vọng trở nên tinh vi và lớn hơn. Chúng cho thấy mối nguy hiểm của việc chiếm lấy quyền kiểm soát máy tính trước khi sự tìm kiếm virut bắt đầu. *So sánh với* blob, check kiting, cookie monster, flying dutchman, french roundoff, logic bomb, stealth virus, time bomb, Trojan Horse, worm. *Xem* malicious logic, virus names.

Virus-90 ***virut 90*** Trong an toàn máy tính, loại virut chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COM, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

Virus-101 ***virut 101*** Trong an toàn máy tính, loại virut tự mã lên chính nó, chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, làm nhiễm các cung mồi (boot sector) của đĩa mềm, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

virus names ***(các) tên virut*** Trong an toàn máy tính, có 7 cách để đặt tên virut:

- các chuỗi văn bản đặt trong virut;
- mã nguồn ban đầu;
- kích thước các mã virut;
- tính tương tự;
- hành vi của virut;
- ngày khởi sự;
- sự phỏng đoán tốt nhất.

Một số virut có các chuỗi văn bản nằm trong mã virut, chẳng hạn, virut

Stoned chứa câu "your computer is now stoned". Trong những trường hợp khác, virut được đặt tên trong chính mã nguồn của nó, chẳng hạn, Dark Avenger. Nói chung virut được đặt tên theo đô dài của chúng, ví dụ virut 4096 làm tăng đô dài của tệp bị lây nhiễm tới 4096 byte. Nhiều virut là những dạng biến đổi của những phiên bản trước đó và được đặt tên tương tự. Ví dụ, những dạng biến đổi của virut Stoned được đặt tên là Stoned II, Stone A v.v.. Một số virut được đặt tên theo hành vi của nó: virut DIR-II tác động tới mục vào thư mục (directory) của tệp bị nhiễm, virut No-INT không khai thác các ngắt (INTerrupt) của DOS để làm lây nhiễm máy tính. Ngay khởi sự cho hành vi ác ý của virut nói chung được dùng làm tên virut và vì thế có tên virut là Friday 13^{th}. Cuối cùng người khám phá ra virut có thể quyết định theo sự phỏng đoán tốt nhất. Vì thế Michelangelo cũng được lấy làm tên vì ngày khởi sự ứng với ngày sinh của hoa sĩ Michelangelo. *Xem* virus.

visual display unit ***thiết bị hiển thị, thiết bị hiện hình*** Trong các thiết bị ngoại vi, thiết bị hiển thị đầu ra của máy tính ở dạng bản sao mềm. Các công nghệ hiển thị bao gồm CRT, LCD, LED và tấm plasma.

vocoder ***bộ mã tiếng nói*** Trong truyền thông, một thiết bị được dùng để giảm các yêu cầu về dải thông của các tín hiệu tiếng nói.

voice analysis ***phân tích tiếng nói*** Trong kiểm soát truy nhập, một kỹ thuật trắc sinh học dựa trên nhận dạng tiếng nói người dùng. Các hệ thống trắc sinh học nhận dạng người dùng bằng các mẫu tiếng nói của họ có hai ưu điểm chính. Trước hết chúng có thể chấp nhận phần lớn người dùng và thứ hai, chúng có thể lấy được tín hiệu của người dùng trên các mạng điện thoại. Nói chung người ta dùng các kỹ thuật mã dự đoán tuyến tính để xử lý dữ liệu tiếng nói, tạo nên mẫu số hóa. Thông thường, mẫu được lấy gồm việc lặp lại PIN hay khẩu lệnh ba lần. Khi yêu cầu truy nhập, người dùng nhắc lại khẩu lệnh và thời gian truy nhập theo lệnh là 20 giây. Hệ thống có thể điều chỉnh lại mẫu tiếng nói truy nhập thành công và như vậy, tận dụng được mẫu được lưu cùng với thói quen. Các nhà cung cấp dịch vụ máy tính yêu cầu tỷ lệ lỗi loại 1 và tỷ lệ lỗi loại 2 thấp khoảng 0,1% và 0,001%. *Xem* biometrics, Type 1 error, Type 2 error.

voice answer-back ***trả lời bằng tiếng nói*** Trong các thiết bị ngoại vi, một thiết bị trả lời bằng âm thanh có thể kết nối một hệ thống máy tính tới một mạng điện thoại để đưa các câu trả lời bằng tiếng nói theo yêu cầu. *Xem* speech synthesizer.

voice band ***dải tần tiếng nói, dải tiếng nói*** Trong truyền thông, dải tần số cho phép truyền rõ tiếng nói con người, thường trong khoảng từ 300 tới 3000 Hz. *Xem* voice scrambling.

voice bank ***ngân hàng tiếng nói*** Trong truyền thông, một hệ thống ghi âm có thể lưu các từ, câu có thể đọc lên nhằm mục tiêu truy nhập đọc.

voice grade channel ***kênh cấp tiếng nói*** Trong truyền thông, một kênh

phù hợp với sự truyền tín hiệu tiếng nói, fax, dữ liệu số hay tương tự ở dải tần tiếng nói, từ 300 tới 3000 Hz. *Xem* Hz, voice band.

voice mail ***thư tiếng nói*** Trong truyền thông, một hệ thống trong đó thông tin dạng tiếng nói được số hóa và được lưu trên bộ nhớ mạng, hoặc trên thiết bị thích hợp tại đích đến của thông báo. Thông báo dạng tiếng nói sau đó được bên được gọi truy lục đến. *Xem* voice store and forward, compare electronic mail.

voice print ***tín hiệu ghi giọng nói*** Trong kiểm soát truy nhập, tín hiệu được ghi âm dạng số để nhận dạng các đặc trưng của tiếng nói của một cá nhân được dùng cho mục đích nhận dạng. *Xem* voice analysis.

voice scrambling ***xáo trộn tiếng nói*** Trong an toàn liên lạc, phép mã hóa thông tin tiếng nói. Các kỹ thuật xáo trộn tiếng nói có thể được phân thành kỹ thuật tương tự và kỹ thuật số. Phép xáo trộn tiếng nói truyền thống được áp dụng cho các tín hiệu tương tự thông thường trên các đường điện thoại, song những phát triển theo công nghệ ISDN hiện tại lại cho phép truyền số các tín hiệu tiếng nói và sự phát triển này có những gợi ý quan trọng cho các bộ xáo trộn tiếng nói.

Phép xáo trộn tiếng nói tương tự xoay quanh việc biến đổi tín hiệu tương tự cần truyền đi và có thể xem xét phép biến đổi này hoạt động trong miền tần số hay thời gian hoặc cả hai.

Các bộ xáo trộn miền tần số

Các bộ xáo trộn miền tần số chứa các phép biến đổi các tần số hợp thành của tín hiệu tiếng nói. Phân phối tần số của tín hiệu vào nằm trong dải tần âm thanh, tức từ 300 - 3000Hz trong trường hợp liên lạc điện thoại, chúng (phân bố tần số) được biến đổi rồi truyền đi. Tại phía máy thu, phân bố tần số của tín hiệu thu được lại được đảo ngược lại để chuyển thành tín hiệu ban đầu.

Các kỹ thuật này có thể bảo vệ chống những kẻ nghe trộm vô tình hay cố ý song rất dễ bị tổn thương trước kẻ chặn bắt được trang bị tốt. Những khó khăn mà nhà thiết kế phải đối mặt về các thiết bị xáo trộn như vậy là độ dư cao trong tiếng nói thông thường, khả năng của người chặn bắt được đào tạo rút ra được thông tin có nghĩa từ sự truyền tiếng nói bị cắt xén nhiều, và đòi hỏi về việc quá trình xáo trộn không làm suy giảm đáng kể chất lượng truyền sau khi giải xáo trộn (giải mã).

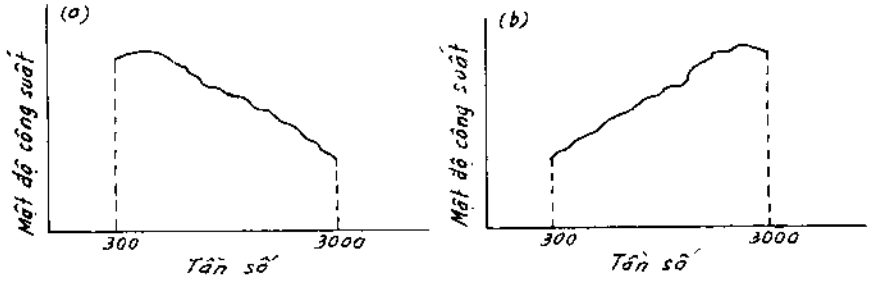
Ban đầu thiết bị xáo trộn là một bộ đảo tiếng nói, nó tạo ra khá hiệu quả hình ảnh phản chiếu của phổ tần số (xem hình 1). Xét hai tần số tại phần dải thấp (300 Hz) và phần dải cao (3000 Hz) của vùng tần số. Nếu biên độ của những tín hiệu này là V_I và V_{II} thì các tín hiệu được biểu diễn tương ứng là $V_I \sin(2\pi 300t)$ và $V_{II}\sin(2\pi 3000t)$. Bộ xáo trộn nhân tín hiệu tiếng nói với tín hiệu sóng mang $V_c\sin(2\pi f_c t)$ và hai tín hiệu kể trên được biến đổi thành:

$V_I \sin(2\pi 300t).\ V_c\sin(2\pi f_c t)$

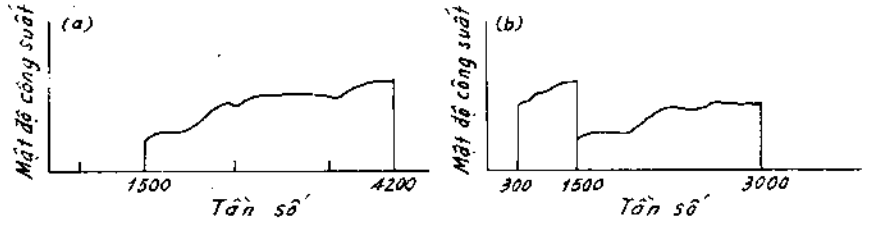
$V_{II}\sin(2\pi 3000t).V_c\sin(2\pi f_c t)$

Mỗi tín hiệu này chứa tần số biên thấp và tần số biên cao, như vậy:

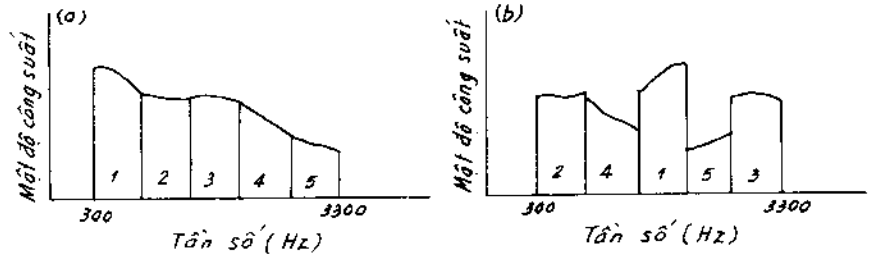
$V_I \sin(2\pi 300t).\ V_c\sin(2\pi f_c t)$ =



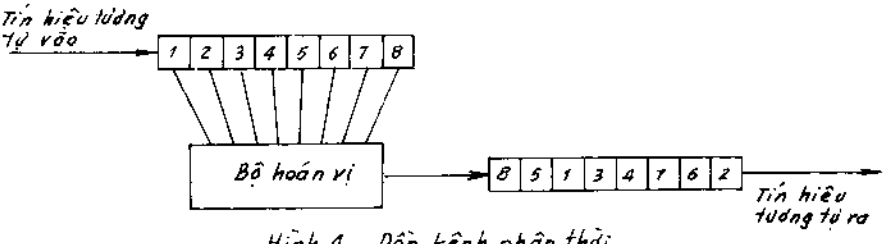
Hình 1. Đảo tần



Hình 2. Bộ đảo dịch dải



Hình 3. Bộ tách dải: a) sắp thứ tự dải con ban đầu; b) phổ xáo trộn



Hình 4. Đồn kênh phân thời

V

voice scrambling: *xáo trộn tiếng nói.*

$0.5V_L V_c((\cos(2\pi(f_c - 300)t) -$
$\cos(2\pi(f_c + 300)t))$

Các tần số biên cao hơn (tức $f_c + 300$) nằm phía trên dải tần số âm thanh và bị lọc đi. Nếu tần số sóng mang là 3300Hz còn biên độ sóng mang V_c bằng 2 thì hai tín hiệu tiếng nói ban đầu được biến đổi thành tín hiệu xáo trộn

$V_H((\cos(2\pi 300)t)$ và
$V_L(\cos(2\pi 3000)t)$

Tức là các biên độ tín hiệu tần số cao và thấp được đổi cho nhau ở đầu ra bộ xáo trộn.

Các bộ đảo tiếng nói đã làm méo tín hiệu song không cho độ mật thực sự vì người chặn bắt tín hiệu chỉ đơn thuần thực hiện quá trình xử lý tín hiệu tương tự như người nhận hợp pháp để nhận tín hiệu ban đầu.

Có thể dùng khái niệm về khóa mật dùng chung giữa người gửi và người nhận trong quá trình đảo tần nhờ các bộ đảo dịch tần. Trong trường hợp này, ta dùng tín hiệu mang ở tần số cao hơn để tín hiệu được đảo chứa các tần số trong dải từ 3000 tới $(f_c - 300)$ Hz, trong khi không có tín hiệu nào nằm trong dải từ 300 tới $(f_c - 3000)$ Hz. Dải phía trên của tín hiệu được đảo sau đó được dịch về phía phổ tần thấp hơn.

Ví dụ, nếu f_c là 4500 Hz thì tín hiệu được đảo nằm trong dải 1500 tới 4200 Hz. Dải từ 3000 - đến 4200 sau đó được dịch và lấp đầy dải từ 300 tới 1500 Hz (xem hình 2).

Trong bộ đảo dịch băng tần theo kiểu tuần hoàn, tần số sóng mang (f_c) được thay đổi mỗi lần khoảng 10 tới 20 miligiây theo tín hiệu ra của một bộ tạo số giả ngẫu nhiên. Người gửi và nhận chỉ cần thỏa thuận với nhau về bộ tạo số giả ngẫu nhiên, hạt giống của nó và sự đồng bộ những thay đổi tần số sóng mang.

Các bộ chặt băng (xem hình 3) cũng là một kiểu bộ xáo trộn băng tần, đưa ra các đoạn lớn hơn và sắp xếp lại phổ tín hiệu tiếng nói. Trong trường hợp này, phổ được chia thành một số dải tần độ rộng bằng nhau, những dải này có thể được sắp xếp lại và được đảo. Ví dụ, nó được chia thành 5 dải với số thứ tự ban đầu là 12345, thứ tự này được thay đổi bằng phép dịch tần thành 42153, ngoài ra, các dải 2 và 3 có thể được đảo lại. 5 dải này có 120 hoán vị có thể và với mỗi hoán vị, có 32 cách sắp xếp lại với các dải riêng biệt được đảo hoặc không. Như vậy, bộ xáo trộn có thể có 3840 = 120 x 32 cách sắp xếp tín hiệu tiếng nói khi chia phổ của nó thành 5 dải.

Tuy nhiên, nhiều cách trong số các cách sắp xếp tín hiệu nêu trên sẽ gần với tiếng nói ban đầu vì độ rõ còn lại sẽ cao tới mức không chấp nhận được. Ví dụ, các dải ứng với focman (formant) đầu tiên chứa tỷ lệ năng lượng tiếng nói cao, nếu người chặn tin định vị được hai dải này thì anh ta sẽ có cơ hội tốt hiểu được ý nghĩa của tiếng nói đã xáo trộn.

Có thể cải thiện việc thực hiện bộ chặt băng bằng cách chỉ chọn những tổ hợp kết hợp nào của phép đảo tần và sắp xếp lại che dấu hiệu quả nhất thông tin tiếng nói. Khi đó có thể lưu tập các phép hoán vị/đảo trong ROM và chọn dãy các tín hiệu ra khỏi ROM nhờ một bộ tạo số giả ngẫu nhiên ở những

khoảng thời gian một vài trăm miligiây. Số các hoán vị tiềm năng sẽ tăng lên khi tăng số các dải trong phổ, tuy nhiên việc chia nhỏ quá mức phổ tần tiếng nói có thể làm suy giảm tới mức không chấp nhận được đối với tín hiệu không được xáo trộn.

Nói chung, các kỹ thuật xáo trộn tần số dễ bị tổn thương trước tấn công xác định trước và khó bảo đảm rằng, độ rõ còn lại đủ thấp; bộ óc con người quá tinh tường trong việc rút ra những thông báo có nghĩa từ các tín hiệu tiếng nói bị bóp méo. Bởi vậy, những kỹ thuật này được dùng chủ yếu khi yêu cầu bộ xáo trộn có mức mật thấp (ở mức riêng tư).

Các bộ xáo trộn miền thời gian

Các bộ xáo trộn miền thời gian dùng các kỹ thuật dồn kênh chia thời gian để sắp xếp lại tín hiệu trong miền thời gian. Trong trường hợp này, tín hiệu tiếng nói được chia thành các khung (frame) thời gian và mỗi khung lại được chia nhỏ tiếp thành các đoạn.

Bộ xáo trộn tích một khung đầy đủ sau đó hoán vị các đoạn nhỏ riêng biệt và truyền tới máy thu, tại đây toàn bộ khung được xáo trộn theo phép hoán vị ngược lại và cho ra tiếng nói đã giải xáo trộn (xem hình 4).

Quá trình tích lại và sắp xếp lại trật tự các đoạn tín hiệu được thực hiện bằng cách lấy mỗi phần tín hiệu ứng với mỗi đoạn, chuyển từ dạng tương tự sang dạng số, lưu tập các bit nhận được và lặp lại quá trình cho tới khi tích được một khung hoàn chỉnh. Các số nhị phân biểu diễn mỗi đoạn sau đó được hoán vị trong thanh chứa và số các đoạn kết quả đưa ra theo trình tự lệ thuộc vào phép biến đổi số-tương tự và được truyền tới máy thu.

Việc thực hiện bộ xáo trộn phụ thuộc vào độ dài khung, số các đoạn trong khung và phép hoán vị các đoạn. Theo quan điểm an toàn, khung cần dài tới mức có thể; nếu độ dài khung này nhỏ hơn các thành phần tiếng nói có thể nhận dạng được thì độ rõ còn lại sẽ không đủ thấp. Mặt khác, quá trình xáo trộn sẽ tạo ra một trễ phụ dài cỡ 2 khung; trễ này có thể gây ra sự khó chịu cho những người sử dụng khi đang đàm thoại, sự khó chịu này tương tự với những cuộc đàm thoại thử nghiệm trên các kênh điện thoại vệ tinh nếu độ dài khung lớn hơn vài trăm miligiây.

Nguyên nhân trễ có thể minh họa qua phép xáo trộn dưới đây:

Đầu vào bộ xáo trộn	12345678
Đầu ra bộ xáo trộn	85134768
Đầu vào bộ giải xáo trộn	85134762
Đầu ra bộ giải xáo trộn	12345678

Nếu như trong trường hợp này, đoạn cuối cùng (8) cần được xáo trộn tới vị trí đầu của khung thì bộ xáo trộn phải thu thập toàn bộ khung trước khi đoạn đã xáo trộn đầu tiên (tức đoạn 8) được truyền đi. Tương tự, bộ giải xáo trộn phải tính tới khả năng đoạn cuối cùng của khung sẽ ứng với đoạn đầu tiên của khung đã giải xáo trộn và cũng lưu toàn bộ khung trước khi đưa ra đoạn đầu tiên. Trễ có thể giảm nếu dùng hệ thống trượt cửa sổ, hạn chế sự chuyển chỗ của một đoạn bất kỳ.

Số các đoạn phải đủ lớn để có số hoán vị lớn, trái lại kẻ chặn bắt có thể dễ

dàng giải xáo trộn (giải mã) thông báo nhờ kiểm tra vét cạn tập các hoán vị đầy đủ. Tuy nhiên, sự tăng số đoạn với độ dài khung cho trước sẽ làm giảm độ dài đoạn và điều này có thể làm giảm đáng kể chất lượng của thông báo đã giải xáo trộn.

Không phải tất cả các hoán vị phép xáo trộn đều đủ để che dấu thông báo trước kẻ chặn bắt có đào tạo. Tham số dịch là đại lượng đo sự đổi chỗ (displacement) trung bình của các đoạn hoán vị, đưa ra một chỉ số về mức xáo trộn. Ví dụ, trong phép hoán vị 12345678 thành 21345678 chỉ có 2 đoạn được đổi chỗ 1 vị trí sẽ cho hệ số dịch là 1/4. Phép hoán vị này rõ ràng sẽ cho độ rõ còn lại cao.

Việc đổi chỗ các cặp đoạn, việc đặt một hay nhiều đoạn giữa các cặp đoạn... cũng làm khung đã xáo trộn ở vào trạng thái bị nguy hiểm trước kẻ chặn bắt. Một số lớn các hoán vị được chứng minh là không đủ với mục đích bảo mật.

Số các hoán vị hiệu quả còn giảm hơn nữa do sự hạn chế các cặp hoán vị nào đó. Ta hãy xét ví dụ một cặp hoán vị:

TP1	TP2
1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
5 3 7 1 6 2 8 4	4 3 7 1 6 2 8 5

Máy thu phải chứa đảo của những hoán vị này để khôi phục thông báo đã xáo trộn trở về dạng ban đầu của nó. Các hoán vị đảo là:

RP1	RP2
1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
4 6 2 8 1 5 3 7	4 6 2 1 8 5 3 7

Kẻ chặn bắt có thể cũng lưu các hoán vị đảo và dùng âm phổ ký (sonograph) để thử tác động của những hoán vị đảo này lên tín hiệu bắt được. Nếu kẻ chặn bắt thử RP2 trên TP1 thì kết quả sẽ là 1 2 3 5 4 6 7 8. Kết quả này gần trùng với tín hiệu ban đầu (chỉ các đoạn 4 và 5 bị đảo nhau), khá đủ với mục tiêu bắt tín hiệu.

Rõ ràng là sẽ không thể dùng cả hai hoán vị TP1 và TP2 trong bộ xáo trộn. Các hoán vị bởi vậy sẽ được thử so với nhau để hủy những tổ hợp không thỏa mãn; kỹ thuật này gọi là phương pháp an toàn tương hỗ.

Bộ xáo trộn hoặc có thể tạo ra các hoán vị nhờ một kiểu bộ tạo số giả ngẫu nhiên nào đó và dùng một thuật toán để loại bỏ những hoán vị không đạt, hoặc lưu xen kẽ tất cả các hoán vị thỏa mãn trong ROM và chọn chúng theo kiểu ngẫu nhiên.

Nếu dùng phương pháp trước thì việc tạo, thử nghiệm, loại bỏ, tái tạo lại, thử lại v.v. phải được thực hiện trong vài trăm miligiây để đảm bảo có sẵn hoán vị cho khung tiếp sau. Ngoài ra, kỹ thuật này không thể dùng phương pháp an toàn tương hỗ để loại bỏ các cặp hoán vị không thỏa mãn.

Kỹ thuật dùng ROM đã hạn chế tổng số các hoán vị lưu một cách kinh tế, song không khắc phục được vấn đề chọn những hoán vị đạt yêu cầu trong thời gian thực và ngoài ra có thể dùng các phương pháp an toàn tương hỗ.

Máy thu không chỉ thực hiện phép hoán vị đảo mỗi khung mà còn phải đảm bảo chia tín hiệu nhận được tương ứng theo cùng các khung như các khung của máy phát. Bởi vậy phải truyền đi các

tín hiệu đồng bộ và chúng có thể là kiểu đồng bộ ban đầu hay đồng bộ liên tục.

Trong trường hợp đầu, tín hiệu đồng bộ chỉ gửi vào thời điểm bắt đầu của thông báo. Mặt khác, các tín hiệu đồng bộ liên tục được truyền liên tục suốt quá trình gửi thông báo. Những ưu điểm chính của đồng bộ liên tục là:

- máy thu có thể giải mã thông báo ngay cả khi đầu vào tới chậm, tức là không có điểm bắt đầu thông báo;
- máy thu có thể chuyển mạch tự động giữa thông báo rõ và thông báo mã (xáo trộn) nhờ phát hiện có tín hiệu đồng bộ hay không. Những tín hiệu này thường được đặt ở dải tần số hẹp và bởi vậy làm cho hệ thống dễ bị tổn thương trước kiểu tấn công từ chối dịch vụ.

Các bộ xáo trộn hai chiều

Các bộ xáo trộn có thể kết hợp các kỹ thuật xáo trộn miền thời gian và tần số. Một đoạn của thông báo tiếng nói cần xáo trộn được chia thành các phần tử thời gian/tần số. Những phần tử này sau đó được hoán vị trong khoảng thời gian/tần số (xem hình 5).

Các phần tử từ X11 tới X51 là 5 dải tần, tất cả nằm trong cùng phần tử thời gian X1. Phần tử thời gian X2 có 5 dải tần từ X12 tới X52.... Sau khi các phần tử thời gian/tần số được sắp xếp lại, tín hiệu kết quả được truyền đi thay cho tín hiệu gốc ban đầu.

Hình vẽ cho thấy các sắp xếp thời gian/tần số mới. Máy thu hợp pháp phải khôi phục lại các phần tử thời gian/tần số theo vị trí ban đầu của nó để giải xáo trộn thông báo tiếng nói. Những sơ đồ như vậy dẫn tới tiếng nói xáo trộn có độ rõ còn lại thấp và khó mã thám. Tuy nhiên, chất lượng của tiếng nói sau khi giải xáo trộn bị suy giảm do quá trình phân đoạn theo cả miền thời gian và tần số, làm gián đoạn và gây méo tiếng nói.

Bộ xáo trộn biến đổi Fourier rời rạc

Có thể dùng một phép biến đổi toán học gọi là biến đổi Fourier rời rạc (DFT) cho các bộ xáo trộn tiếng nói. Thông báo tiếng nói được số hóa và các mẫu tiếng nói nhận được sau đó được nhóm lại thành các khung có độ dài bằng nhau. Số các mẫu tiếng nói trong mỗi khung thường bằng lũy thừa của 2 để đơn giản hóa phép biến đổi; nó thường được chọn bằng 256. Mỗi khung được biến đổi trong miền tần số nhờ dùng DFT, tạo nên 256 thành phần biến đổi.

Các thành phần biến đổi này biểu thị tần số của khung tiếng nói, và những thành phần ứng với các tần số của dải thông của tuyến liên lạc và sẽ được hoán vị sau đó. Những thành phần còn lại cho bằng không. Điều này bảo đảm những thành phần tần số quan trọng không bị mất khi tín hiệu xáo trộn được truyền đi.

Số các thành phần biến đổi đã hoán vị thường theo bậc 88. Tiếp theo phép hoán vị, các thành phần biến đổi được biến đổi trở lại trong miền thời gian nhờ phép biến đổi Fourier đảo và các mẫu thời gian nhận được được chuyển từ dạng số sang dạng tương tự để truyền đi.

Máy thu đồng bộ hóa các khung tiếng nói đã xáo trộn vừa tới và thực hiện quá trình đảo ngược phép xáo trộn. Các

tín hiệu biến đổi Fourier đi qua phép hoán vị đảo và áp dụng phép biến đổi Fourier đảo một lần nữa để khôi phục lại các mẫu tiếng nói theo thời gian.

Bộ xáo trộn dùng biến đổi Fourier rời rạc có độ rõ còn lại thấp, tạo ra một tín hiệu xáo trộn khá giống với tiếng nói. Tuy nhiên, vẫn còn thông tin nào đó ở dạng biến thiên năng lượng tín hiệu tiếng nói. Có thể rút ra được độ rõ (nghe được) nào đó từ thông tin này. Chất lượng tiếng nói đã khôi phục rất tốt song có thể vẫn bị suy giảm trên kênh liên lạc tồi.

Với bộ xáo trộn DFT, số các hoán vị có thể rất cao với 88 thành phần biến đổi, có ưu thế vượt trội hơn so với các bộ xáo trộn kiểu chặt băng và phần tử thời gian vì những bộ này chỉ có hơn 32 hoán vị. Vì thế kỹ thuật DFT ít bị tổn thương trước kiểu tấn công mã thám dùng phép thử tất cả các hoán vị trong phép xáo trộn.

Các đặc trưng của các bộ xáo trộn tương tự

Một hệ thống xáo trộn tiếng nói hiệu quả sẽ tạo ra tiếng nói xáo trộn có độ rõ còn lại thấp. Tuy nhiên, các tín hiệu tiếng nói có độ dư cao và bộ não người rất thính trong việc rút ra độ rõ từ các tín hiệu tiếng nói đã bị làm méo. Ngoài ra, tiếng nói phục hồi từ các tín hiệu giải xáo trộn sẽ không bị suy giảm nhiều; người nghe tại máy thu sẽ chấp nhận nó và nhận ra người nói.

Trừ các bộ xáo trộn dùng tới các kỹ thuật xáo trộn hai chiều và biến đổi Fourier rời rạc, các bộ xáo trộn tương tự theo đặc trưng có độ rõ còn lại cao. Chất lượng tiếng nói sau khi khôi phục lại tốt nếu kênh liên lạc không quá xấu. Để bù trừ sai sót trên kênh, ta thường phải dùng phép hiệu chỉnh.

Các bộ xáo trộn mô tả ở trên có cùng thuật toán hoán vị xáo trộn là các phần tử miền tần số hoặc miền thời gian. Ở những nơi dùng phép hoán vị cố định, nhiều hệ thống như vậy đã bị mã thám nhờ lợi dụng độ dư của tiếng nói. Những tấn công tự động chỉ cần tiếng nói đã xáo trộn, có thể thực hiện trên bộ chặt băng tần, bộ xáo trộn DFT và xáo trộn các phần tử thời gian.

Nếu dùng ROM để lưu các hoán vị bị người mã thám khám phá ra thì với danh sách hạn chế, có thể tiến hành thử tất cả các hoán vị. ROM cũng đưa ra một cơ sở để so sánh khi kẻ chặn bắt bằng mã thám, có thể ước lượng phép hoán vị.

Các bộ xáo trộn số

Trong phép mật mã số trên một kênh tương tự, tín hiệu tương tự trước hết được số hóa (chuyển từ tương tự thành dạng số). Các bit số sau đó được nén qua bộ mã tạo nên một tín hiệu số tốc độ bit thích hợp. Phép mã nén tiếng nói lại để đảm bảo nó vẫn nằm trong vùng dải thông của kênh truyền. Chuỗi bit sau đó được mã mật và chuỗi kết quả nhận được được truyền qua kênh tiếng nói. Khi dùng kênh điện thoại tương tự chuẩn hóa, chuỗi bit mật mã được chuyển thành tín hiệu tương tự qua một modem. Tại máy thu, quá trình diễn ra ngược lại.

Bộ mã (coder) tiếng nói gây nên sự suy giảm chất lượng nào đó trong tiếng nói xáo trộn. Thuật toán mã mật dạng số điển hình là thuật toán mã dòng, chẳng

X51	X52	X53	X54	X55	X56	X57	X58
X41	X42	X43	X44	X45	X46	X47	X48
X31	X32	X33	X34	X35	X36	X37	X37
X21	X22	X23	X24	X25	X26	X27	X28
X11	X12	X13	X14	X15	X16	X17	X18

voice scrambling: *xáo trộn tiếng nói.* Hình 5. Ma trận phép xáo trộn hai chiều.

X43	X37	X25	X11	X17	X38	X22	X46
X26	X18	X36	X58	X48	X12	X33	X52
X53	X24	X14	X42	X28	X57	X31	X16
X41	X13	X56	X32	X51	X47	X15	X34
X35	X44	X21	X23	X54	X45	X27	X55

voice scrambling: *xáo trộn tiếng nói.* Hình 6. Một phép hoán vị xáo trộn hai chiều.

hạn mã khối trong chế độ phản hồi đầu ra hay chế độ phản hồi mã.

Phản hồi mã là tự đồng bộ song nó gây ra sự lan truyền sai số. Nếu dùng kênh liên lạc có tạp âm thì sự lan truyền sai số sẽ làm tăng tạp âm tại máy thu và điều này có thể làm tín hiệu ra sau khi giải mã khó nghe. Phản hồi đầu ra không gây sự lan truyền sai số và thích hợp cho các tín hiệu tiếng nói có độ dư cao, nơi các sai số trong các byte riêng lẻ có thể dễ dàng bỏ qua.

Tuy nhiên, dạng phản hồi đầu ra của phép mã dòng không tự đồng bộ và tạp âm các kênh liên lạc do mất đồng bộ sẽ lại làm tín hiệu ra khó hiểu. Bởi vậy cần có sự đồng bộ liên tục với tín hiệu đồng bộ được gửi theo những khoảng thời gian đều đặn hay ngẫu nhiên. Có thể dùng kỹ thuật bánh đà, cho phép máy thu suy ra cả thời gian điều tiết đồng bộ lẫn thông tin đồng bộ.

Các tín hiệu xáo trộn số sẽ có các đặc trưng của tạp âm trắng và máy phát có thể vẫn gửi các tín hiệu tạp âm trắng vào những lúc lưu lượng ít để không cho thông tin về lưu lượng tới kẻ chặn bắt. Mặt khác, kẻ chặn bắt có thể nhận thông tin rõ hữu ích từ tạp âm nền phù hợp bất kỳ, chẳng hạn tạp âm của máy điều hòa nhiệt độ ở phía máy phát. Tạp âm này sẽ được mã hóa ở những khoảng lặng trong tiếng nói và kẻ chặn bắt có thể nhận được lượng thông tin về bản rõ đáng kể và thông tin mã tương ứng.

Kẻ chan bắt cũng tận dụng được tính dư thừa cao trong các tín hiệu tiếng nói, trong phân tích tần số các thông báo được xáo trộn.

Việc thiết kế các bộ xáo trộn tiếng nói cho các mạch điện thoại thông thường bị ràng buộc bởi yêu cầu là: tín hiệu đã xáo trộn có dạng tín hiệu tương tự trong dải thông từ 300 - 3000 Hz. Với bộ xáo trộn số trên các mạng số dải rộng, như mạng ISDN dải rộng, có thể không cần nén tín hiệu trước khi mã hóa. Trên mạng thông tin như vậy, có thể thiết kế một bộ xáo trộn tiếng nói có độ rõ còn lại thấp, có chất lượng tiếng nói sau khi khôi phục lại rất tốt và an toàn chống lại sự mã thám. *Xem* band shift inventor, bandsplitter, carrier, cipher feedback, continuous synchronization, cryptographic bit stream, cyclical band shift inventor, denial of service, error propagation, fly wheeling, formant, Hz, initial synchronization, mutual security, output feedback, pseudorandom number, residual intelligibility, ROM, seed, self synchronizing, shift factor, sliding window-system, sonograph, speech invertor, time division multiplexing, time element scrambler, traffic analysis. *Đồng nghĩa với* speech scrambling.

voice store and forward ***lưu và chuyển tiếp tiếng nói*** Trong truyền thông, một hệ thống phát và lưu các thông báo tiếng nói để phát lại theo lệnh. *Xem* store and forward, voice mail.

volatile storage ***bộ nhớ khả biến*** Trong tính toán, phương tiện lưu trữ trong đó dữ liệu được lưu bị mất khi nguồn cung cấp bị ngắt. *So sánh với* nonvolatile storage.

volume ***tập (nhớ), volum*** Trong tính toán, một phương tiện lưu trữ giữ dữ liệu có thể lắp vào hay gỡ ra như một khối thiết bị hoàn chỉnh, ví dụ bộ đĩa.

volumetric sensor ***bộ cảm biến ba chiều*** Trong an toàn vật lý, nói tới một bộ cảm biến chống xâm nhập để phát hiện kẻ xâm nhập trong không gian ba chiều chỉ ra. *Xem* instrusion detector.

von Neumann ***kiến trúc von Neumann*** Trong tính toán, nói tới kiến trúc của một máy tính thông thường. Nó được đặc trưng hóa bởi một bộ xử lý kết hợp các phần tử tính toán đơn lẻ, sự truyền thông và bộ nhớ, sự tổ chức tuyến tính các ô nhớ kích thước cố định, một không gian địa chỉ một mức cho các ô, ngôn ngữ máy bậc thấp, sự điều khiển tính toán theo trình tự, tập trung hóa và các năng lực vào/ra cơ bản. *So sánh với* parallel processing.

Voronezh ***virut Voronezh*** Trong an toàn máy tính, một loại virut tự mã lên chính mình, làm chấm dứt và nằm thường trú trong bộ nhớ, lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, làm hỏng các tệp dữ liệu, OVL và chương trình. *Xem* virus names.

vostro account ***tài khoản của bạn, tài khoản vostro*** Một tài khoản ngân hàng tại một chi nhánh ngân hàng hay một ngân hàng đại lý ở một nước ngoài và được ghi bằng đồng tiền của nước người có tài khoản. Thuật ngữ này có

nghĩa là "tài khoản của bạn ở ngân hàng chúng tôi được ghi bằng đồng tiền của nước bạn".

V-Series recommendations of CCITT *(các) khuyến nghị xeri V của CCITT* Trong bộ các chuẩn, một xeri các khuyến nghị liên quan tới liên lạc dữ liệu trên các kênh tương tự. *So sánh với* X-Series recommendations of CCITT. *Xem* protocol standards.

VTP *Xem* virtual terminal protocol.

vulnerability *chỗ dễ bị tổn thương, điểm yếu* (1) Trong quản lý rủi ro, một điểm yếu trong các thủ tục an toàn của hệ thống tự động hóa, các kiểm soát về quản trị, các kiểm soát nội bộ v.v. có thể bị khai thác bởi mối đe dọa có sự truy nhập bất hợp pháp tới thông tin hay phá hỏng quá trình xử lý quan trọng. (2) Trong quản lý rủi ro, một điểm yếu có thể bị lợi dụng trong bố trí vật lý, trong tổ chức, các thủ tục, con người trong quản lý, quản trị, phần cứng, hay phần mềm làm thiệt hại tới hệ thống hay hoạt động ADP. Bản thân điểm yếu dễ tổn thương này không gây thiệt hại; đơn thuần nó là điều kiện hay tập các điều kiện làm hệ thống hay hoạt động của ADP bị tổn thất bởi cuộc tấn công. *Xem* ADP, technical vulnerability. (3) Trong quản lý rủi ro, điểm yếu hay kẽ hở về an toàn bất kỳ tồn tại trong hệ thống. Tính nhạy cảm của một hệ thống trước một hiểm họa tấn công chỉ ra, hay trước sự kiện bị tổn thất hoặc cơ hội tiềm ẩn trước một tác nhân hiểm họa để tạo nên cuộc tấn công đó. *So sánh với* safeguard, threat. *Xem* countermeasure, harmful event, matrix methodology, vulnerability assessment. (4) Trong an toàn thông tin, một thuộc tính an toàn hay điểm yếu của một mục tiêu đánh giá có thể bị khai thác nhằm vượt qua biện pháp đối phó. *Xem* construction vulnerability, exploitable vulnerability, information technology security evaluation criteria, operational vulnerability, potential vulnerability, target of valuation.

vulnerability assessment *đánh giá điểm yếu* (1) Trong quản lý rủi ro, sự xem xét tính nhạy cảm về sự mất mát hay sử dụng trái phép các tài nguyên, các sai sót trong các báo cáo và thông tin, các hành động bất hợp pháp hoặc không đúng quy tắc và/hoặc ý kiến công khai không có lợi hoặc có hại. (2) Trong quản lý rủi ro, sự đo lường khả năng dễ bị tổn hại bao gồm: (*a*) Tính nhạy cảm của một hệ thống cụ thể đối với một cuộc tấn công riêng. (*b*) Cơ hội có sẵn đối với tác nhân hiểm họa (phương pháp hoặc những phương tiện có thể dùng để khai thác khả năng dễ tổn thương như hỏa hoạn) để sắp đặt một cuộc tấn công. Luôn có thể chỉ ra một điểm yếu song nó có thể tồn tại độc lập với hiểm họa đã biết. Nói chung, một mô tả về điểm yếu sẽ tính đến những yếu tố này dưới sự kiểm soát thận thiên. *Xem* threat, threat agent, vulnerability. (3) Trong quản lý rủi ro, sự xem xét tính nhạy cảm đối với sự mất mát hay việc dùng trái phép các tài nguyên, sai sót trong các báo cáo và thông tin, các hoạt động bất hợp pháp hoặc không đúng quy tắc và ý kiến công khai không có lợi hay bất lợi. Các đánh giá về tính dễ tổn hại không đồng nhất với điểm yếu trước khi dẫn tới sự

lợi dụng. Chúng là cơ chế mà tổ chức có thể xác định nhanh chóng khả năng đối với những mất mát trong các chương trình hay các chức năng khác nhau của nó. Lịch trình xem xét lại kiểm soát bên trong sẽ được dựa trên các kết quả đánh giá các điểm dễ tổn hại. *Xem* internal control review.



W-13 *virut W-13* Trong an toàn máy tính, một virut lây nhiễm các tệp COM, tác động trong thời gian chạy, làm ngắt các tệp chương trình và OVL. *Xem* virus names.

WACK *tín hiệu WACK* Trong truyền thông dữ liệu, viết tắt của Wait before transmitting positive ACKnowledgement (đợi trước khi truyền báo nhận), một tín hiệu do phía máy thu gửi đi để báo rằng tạm thời nó chưa sẵn sàng nhận tín hiệu.

WADS *Xem* wide area data service.

WAN *Xem* wide area network.

warm site *địa điểm ấm, vị trí ấm* Trong quản lý rủi ro, một hệ thống tương tự với địa điểm nguội trừ việc nó có các phương tiện viễn thông. *So sánh với* cold site, hot site.

warm standby *dự phòng ấm* Theo độ tin cậy, một hệ thống sao chép dự phòng có thể được chuyển sang hoạt động trong vài giây khi hệ thống trục trặc. *So sánh với* cold standby, hot standby.

watermark tape *băng hình bóng* Trong kiểm soát truy nhập, một chất liệu được dùng cho các sọc từ, chúng làm cho việc sản xuất các thẻ từ giả mạo khó khăn hơn. Một hình bóng từ cố định được cảm ứng vào chất liệu bằng tác dụng của một từ trường thay đổi thích hợp trong khi các hạt có từ tính được giữ trong lớp sơn nhựa, sau đó nó được sấy khô nhờ thế cố định được hướng của các hạt từ tính. Một rãnh của thẻ được dùng để kiểm tra hình bóng từ và rãnh được chiếu từ trường không đổi trước khi đọc. Như vậy, nỗ lực bất kỳ nhằm giả mạo mẫu hình bóng bằng cách từ hóa một sọc từ thông thường sẽ bị cản trở bởi tác động xóa của từ trường không đổi. *So sánh với* sandwich tape. *Xem* magnetic stripe card.

wavelength division multiplexing *dồn kênh phân bước sóng* Trong truyền thông, một kỹ thuật đồng nhất với kỹ thuật dồn kênh phân tần. Thuật ngữ gắn với việc dùng các bước sóng khác nhau cho các tín hiệu ánh sáng đi dọc theo một cáp sợi quang. *Xem* fiber

optics, frequency division multiplexing.

WDM *Xem* wavelength division multiplexing.

weak bits *(các) bit yếu* Trong an toàn máy tính, một kỹ thuật trong đó, các bit có các giá trị phân cực trung gian giữa các bit 0 và 1 được ghi trước lên một đĩa mềm chủ cùng với phần mềm cần bảo vệ. Khi một bit yếu được đọc, trình điều khiển đĩa trên máy vi tính khi thì hiểu nó là bit 0, khi thì hiểu nó là bit 1. Một chương trình kiểm tra đặc biệt sẽ kiểm tra sự thay đổi thống kê này bằng cách đọc cung từ liên quan tới vài lần và bởi vậy sẽ xác định được liệu đĩa chủ có phải đang được dùng không. Nếu bit yếu được đọc và sau đó được sao chéo sang đĩa khác cùng với chương trình bảo vệ thì nó sẽ được ghi như một chữ số nhị phân thực sự và chương trình kiểm tra sẽ không phát hiện ra bất cứ sự thay đổi nào trong những lần đọc liên tiếp và bởi vậy suy ra rằng, bản sao đang được sử dụng; khi đó nó sẽ ngăn chương trình không cho thực hiện. *Xem* execute protection, fingerprint. *Đồng nghĩa với* fuzzy sector technique.

weak key *khóa yếu* Trong mật mã, là khóa DES tạo ra cùng phép biến đổi trong quá trình mã và giải mã, tức là phép mã hóa kép tạo lại bản rõ ban đầu. Các khóa yếu đối với DES là

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1,

F E F E F E F E F E F E F E F E

1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E và

E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1

Chú ý rằng, khi các bit chẵn lẻ bị khử khỏi các khóa này, cấu trúc đều đặn của chúng trở nên rõ ràng, ví dụ

0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

trở thành

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Một số sơ đồ quản lý khóa cung cấp cho người dùng các phương tiện mã hoặc giải mã hạn chế và các khóa yếu hay bán yếu có thể bị đối phương lợi dụng. *So sánh với* semiweak key. *Xem* DES, dual key, key management.

Whale *virut Whale* Trong an toàn máy tính, một loại virut trộm đêm tự mã lên chính mình, làm chấm dứt và nằm thường thú, làm lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, làm ngắt các tệp chương trình, các tệp dữ liệu và các liên kết tệp *Xem* virus names.

what if *điều gì xảy ra nếu* Trong các ứng dụng, một kỹ thuật ra quyết định lập trong đó, một hay nhiều biến độc lập trong mô hình có các giá trị đặc thù cho trước và đầu ra được tính toán. Các kết quả thường dẫn tới sự thay đổi trong chính mô hình.

White Book *Sách Trắng* *Xem* information technology security evaluation criteria.

white card fraud *lừa đảo thẻ trắng* (1) Trong hoạt động ngân hàng, một dạng lừa đảo thẻ tín dụng dùng thẻ tín dụng giả. Một thẻ bằng plastic trắng, rỗng có một sọc từ được sản xuất và sọc từ được mã theo các chi tiết chứa trong thẻ tín dụng của khách hàng thực sự; thông tin như vậy nhận được một cách bất hợp pháp từ cơ quan tài chính. Các thẻ sau đó được dùng để nhận tiền từ ATM (các máy trả tiền tự động). Thủ

phạm cũng có thể dập nổi số tài khoản hay thông tin khác lên thẻ. *Xem* ATM. (2) Trong hoạt động ngân hàng, một dạng lạm dụng trong đó thẻ tín dụng bị ăn cắp được đun nóng, chẳng hạn để trong nước sôi; các chữ số được dập nổi cũ sẽ bị ép xuống và các số mới được dập nổi lại.

white noise ***tạp âm trắng*** Trong truyền thông, một tín hiệu số ngẫu nhiên không mong đợi có năng lượng như nhau ở mọi tần số. *Xem* noise.

white noise emitter ***bộ phát tạp âm trắng*** Trong an toàn máy tính, một thiết bị bảo vệ chống sự phát xạ gây hại. Thiết bị đặt khít vào mặt sau của một VDU (thiết bị hiển thị) và phát ra các tín hiệu vô tuyến ngẫu nhiên. Tuy nhiên, thiết bị có thể gây nhiễu cho thiết bị điện tử khác trong vùng lân cận và kẻ nghe trộm có thể lọc tạp âm ra bằng các kỹ thuật tương ứng. *So sánh với* random line switching. *Xem* compromising emanations, van Eck phenomenon.

wide area data service ***dịch vụ dữ liệu diện rộng*** Trong truyền thông dữ liệu, một dịch vụ của hãng AT&T cho các thuê bao quay số điện thoại không hạn chế trên các mạch điện báo trong phạm vi một khu vực địa lý cụ thể, sẵn có cho thuê bao với lệ phí hàng tháng cố định.

wide area network ***mạng diện rộng*** Trong truyền thông dữ liệu, một mạng toàn diện nhiều chế độ nối với một số lớn các thiết bị đầu cuối và các máy tính trải ra trên một vùng rộng lớn. *So sánh với* local area network, municipal area network.

wideband channel ***kênh dải rộng*** Trong truyền thông dữ liệu, những kênh hoạt động tới 50 Kbit/giây, với các modem đặc biệt tốc độ có thể tăng lên tới 168 Kbit/giây. *Xem* bit, MODEM.

Wiegand effect ***hiệu ứng Wiegand*** Trong kiểm soát truy nhập, một hiệu ứng từ tính được dùng trong một số hệ thống kiểm soát truy nhập. Một dây sắt từ đặc biệt dạng cuộn xoắn ốc căng cố định sẽ được đảo đột ngột từ trường khi đặt vào một từ trường bên ngoài; sự đảo ngược như vậy có thể được chuyển thành các xung điện. *Xem* magnetically encoded card.

window ***cửa sổ*** (1) Trong tính toán, nói tới một kỹ thuật phần mềm nhằm chuyển dữ liệu thuận tiện giữa các gói chương trình. Nó cung cấp cho người dùng các hệ thống hết sức thân thiện, trên đó con người có thể nhìn thấy các nội dung của các gói phần mềm khác nhau trong các "cửa sổ" trên các màn hình VDU, cắt và dán thông tin từ cửa sổ này tới cửa sổ khác. (2) Trong truyền thông dữ liệu, *xem* sliding window protocol.

windows ***(các) cửa sổ*** *Xem* window.

wipe through card reader ***bộ đọc xóa thẻ đi qua*** Trong hoạt động ngân hàng và kiểm soát truy nhập, một bộ đọc thẻ trong đó thẻ bị xóa qua một khe mở trong thiết bị đầu đọc. *Xem* card reader.

wire center ***trung tâm nối dây*** Trong truyền thông dữ liệu, một thiết bị cho phép một mạng cục bộ có kiến trúc kiểu mạch vòng duy trì được sự

liên lạc hạn chế khi có sự hỏng cáp. Nếu phát hiện ra sự hỏng cáp, một rơle rẽ sẽ hoạt động trong trung tâm và cắt ngắn hiệu quả phần cáp và trạm bị tác động do hỏng cáp, cho phép các trạm còn lại trên vòng mạng tiếp tục liên lạc. *Xem* local area network, ring.

wired logic card ***thẻ logic nối mạch*** Trong kiểm soát truy nhập, một kiểu thẻ thông minh chứa mạch điện tử nằm trọn trên thẻ. *Xem* smart card.

wire service ***dịch vụ nối dây*** Trong truyền thông dữ liệu, là dịch vụ viễn thông bất kỳ mà các thuê bao có thể nhận các thông báo hay các cuộc truyền (ví dụ dịch vụ điện báo, TWX, SWIFT, BankWire, Fedwire). *Xem* banking network, BankWire, FedWire, SWIFT.

wiretap ***nghe trộm thông tin, nối trộm thông tin*** (1) Trong an toàn liên lạc, việc gắn một thiết bị trái phép như mạch nối rẽ, máy ghi băng hay thiết bị đầu cuối máy tính vào mạch liên lạc nhằm truy nhập tới dữ liệu. (2) Trong an toàn liên lạc, một kỹ thuật chặn một đường dây liên lạc để lấy thông tin. Việc nối trộm có thể thực hiện theo các chế độ chủ động hay thụ động:

- Chủ động: Gắn một thiết bị trái phép, chẳng hạn đầu cuối máy tính, vào mạch liên lạc nhằm truy nhập được tới dữ liệu nhờ tạo các thông báo hoặc tín hiệu kiểm soát sai, hoặc bằng cách thay đổi các cuộc liên lạc của người sử dụng hợp pháp.
- Thụ động: Sự giám sát và/hoặc ghi âm dữ liệu được truyền trên đường dây.

Xem active wiretapping, passive wiretapping. (2) Trong an toàn liên lạc, một biện pháp chặn bắt trái phép các thông báo. Mục đích của lấy trộm thông tin thụ động là làm lộ nội dung thông báo mã không bị phát hiện, trong khi đó, lấy trộm thông tin chủ động lại xoay quanh việc biến đổi cố ý các thông báo, đôi khi vì mục đích gài những thông báo sai lạc, gài các đoạn quay lại của các thông báo trước đó (ví dụ để lặp lại một giao dịch tín dụng) hoặc xóa các thông báo. Xác thực bảo vệ chống lại sự thay đổi thông báo và gài các thông báo sai bằng cách làm cho đối phương không thể biến đổi được hoặc tạo các thông báo đáp ứng tiêu chuẩn xác thực. *So sánh với* between-the-line entry, piggyback entry. *Xem* active wiretapping, browsing, passive wiretapping.

wiretapping ***(sự) lấy trộm thông tin*** *Xem* wiretap.

Wisconsin ***virut Wiscosin*** Trong an toàn máy tính, một loại virut tự mã lên chính mình, làm lây nhiễm các tệp COMMAND.COM, COM, EXE và OVL, tác động trong thời gian chạy, làm ngắt các tệp chương trình, các tệp dữ liệu và các tệp OVL. *Xem* virus names.

WNINTEL ***nguồn WNINTEL*** Trong an toàn dữ liệu, viết tắt của Warning Notice-Intelligence Sources or Methods Involved (các nguồn hay các phương pháp có liên quan cảnh báo thông cáo tin tức).

Wolfman Whale ***virut Wolfman Whale*** Trong an toàn máy tính, một loại virut làm chấm dứt và nằm thường thủ trong bộ nhớ, làm lây nhiễm các

tệp COMMAND.COM, COM và EXE, tác động trong thời gian chạy, làm ngắt các tệp chương trình và các tệp OVL. *Xem* virus names.

word *từ* Trong các cấu trúc dữ liệu, một nhóm các bit, các byte hay ký tự được xem như một thực thể và có khả năng lưu tại một vị trí trong bộ nhớ.

word-frame counter *bộ đếm khung từ* Trong truyền thông dữ liệu, một khối đếm số từ trong một khung khi nhận được chúng. Nó cũng có thể đếm số các khung. *Xem* frame, word.

word length *độ dài từ* Trong các cấu trúc dữ liệu, số các bit, byte hay ký tự trong một từ. *Xem* word.

work factor *hệ số làm việc* Trong an toàn máy tính, mức ước lượng về công sức hay thời gian chi phí mà người muốn xâm nhập bằng chuyên môn vào các tài nguyên phải bỏ ra để vượt qua một biện pháp bảo vệ. *Xem* resource.

workstation *trạm làm việc* Một thiết bị đầu cuối thông minh có các tiện ích được thiết kế cho các tác vụ định sẵn, chẳng hạn xử lý từ, thiết kế bằng máy tính.

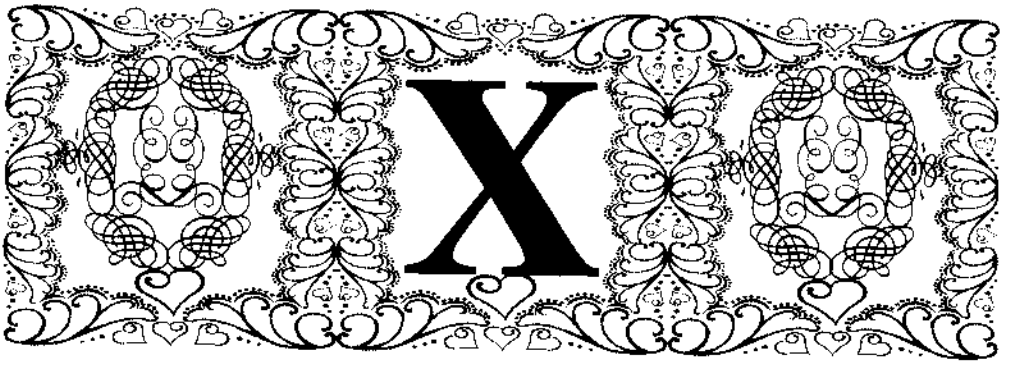
worm *sâu* (1) Trong an toàn máy tính, một dạng mã ác ý có thể tự nhân bản mà không cần một chương trình chủ để truyền nhiễm. Các mạng rất dễ tổn thương trước các tấn công của sâu. Một sâu khi vào được một nút mạng sẽ gây ra những vấn đề cục bộ tại nút và gửi các bản sao bản thân mình tới các nút lân cận. *So sánh với* virus. *Xem* malicious code, Morris worm. (2) Trong bảo vệ phần mềm, một chương trình do người sản xuất phần mềm viết ra, nó sẽ gọi phạt tiền nếu phát hiện ra việc sử dụng chương trình trái phép. Trường hợp tốt nhất, sâu sẽ làm treo chương trình được bảo vệ, còn trường hợp xấu nhất, nó sẽ gây ra một số sửa đổi sai lạc mỗi lần chạy và cuối cùng sẽ làm hỏng đĩa. Sâu rất nguy hiểm vì chúng có thể bị kích hoạt một cách ngẫu nhiên. *So sánh với* virus. *Xem* disk crash.

WORM *đĩa WORM, đĩa ghi một lần đọc nhiều lần* Trong các hoạt động ngoại vi, viết tắt của Write Once Read Many times, một đĩa compac quang cho phép dữ liệu mới được ghi lên bề mặt trống. Các máy tính cá nhân có thể chấp nhận được việc không có các tiện ích có khả năng xóa khi cho trước khả năng lưu trữ cao của đĩa. Những thiết bị này rất lý tưởng để lưu vết kiểm toán đầy đủ cho cả thông tin về tài chính lẫn thông tin về luật pháp.

worst case condition *điều kiện trường hợp xấu nhất* Trong mã thám, điều kiện trường hợp xấu nhất theo quan điểm của người lập mã là khi người mã thám biết đầy đủ về hệ thống mã, đã tích được lượng bản mã đáng kể và biết bản rõ tương đương với lượng bản mã nhất định.

write *ghi* Trong an toàn máy tính, một hoạt động cơ bản chỉ dẫn tới dòng thông tin từ một chủ thể tới một đối tượng. *So sánh với* read. *Xem* object, subject.

write access *truy nhập ghi* Trong an toàn máy tính, việc cho phép ghi lên một đối tượng. *So sánh với* read access. *Xem* object, write.



X ***chuẩn X*** Tiền tố trong tên các chuẩn của CCITT và ANSI. Trong cuốn từ điển này, các chuẩn CCITT được liệt kê dưới đây đều có tiền tố X, chẳng hạn X.25. Các chuẩn ANSI được liệt kê sau từ ANSI, ví dụ ANSI X9.9. *Xem* ANSI, X-Series recomendations of CCITT, XI.

X.1 ***chuẩn X.1*** Trong bộ các chuẩn, một khuyến nghị của CCITT cho các lớp người dùng dịch vụ quốc tế trên các mạng dữ liệu công cộng.

X.2 ***chuẩn X.2*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các phương tiện người dùng dịch vụ quốc tế trên các mạng dữ liệu công cộng.

X.3 ***chuẩn X.3*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với phương tiện ráp/gỡ gói tin (PAD) trên mạng dữ liệu công cộng. *Xem* PAD.

X.4 ***chuẩn X.4*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với cấu trúc chung của các tín hiệu mã chữ cái quốc tế No 5 cho truyền dữ liệu trên các mạng dữ liệu công cộng. *Xem* International Alphabet Number 5.

X.20 ***chuẩn X.20*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với giao diện giữa thiết bị đầu cuối dữ liệu (DTE) và thiết bị kết thúc mạch dữ liệu (DCE) cho các dịch vụ truyền dẫn khởi/ngừng trên các mạng dữ liệu công cộng. *Xem* DCE, DTE, public data network.

X.20 bis ***chuẩn X.20 lần hai*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với mạch phối ghép tương thích V.21 giữa thiết bị đầu cuối dữ liệu (DTE) và thiết bị kết thúc mạch dữ liệu (DCE) cho các dịch vụ truyền dẫn khởi/ngừng trên các mạng dữ liệu công cộng. *Xem* DCE, DTE, V.21.

X.21 ***chuẩn X.21*** Trong bộ các chuẩn, khuyến nghị của CCITT về đặc tả giao diện cho mạng dữ liệu công cộng dùng truyền đồng bộ trên mạng

điện thoại số và thiết bị liên lạc, sẽ tạo ra các tín hiệu định thời bit và byte. Đặc tả bao gồm các giao thức thiết lập và trả lời các cuộc gọi và để truyền và nhận dữ liệu khi dùng chế độ truyền đồng bộ song công. *Xem* byte, full duplex, synchronous transmission, X.26, X.27.

X.22 ***chuẩn X.22*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với mạch phối ghép DTE/DCE đồn kênh cho các lớp người dùng 3-6. *Xem* DCE, DTE.

X.24 ***chuẩn X.24*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các định nghĩa về các mạch trao đổi giữa DTE và DCE trên mạch dữ liệu công cộng. *Xem* DCE, DTE.

X.25 ***chuẩn X.25*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với mạch phối ghép giữa DTE và DCE cho các thiết bị đầu cuối hoạt động trong chế độ gói trên mạng dữ liệu công cộng. *Xem* data communications, DCE, DTE.

X.26 ***chuẩn X.26*** Trong bộ các chuẩn, khuyến nghị của CCITT về đặc trưng điện đối với X.21 tương ứng với RS-422A. *So sánh với* X.27. *Xem* CCITT, RS-422A, X.21.

X.27 ***chuẩn X.27*** Trong bộ các chuẩn, khuyến nghị của CCITT về đặc trưng điện đối với X.21 ứng với RS-423A. *So sánh với* X.26. *Xem* CCITT, RS-423A, X.21.

X.28 ***chuẩn X.28*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với mạch phối ghép DTE/DCE cho thiết bị đầu cuối dữ liệu ở chế độ khởi-ngừng tiếp cận tới phương tiện ráp/gỡ gói (PAD) trên mạng dữ liệu công cộng ở trong cùng một nước. *Xem* DCE, DTE, PAD.

X.29 ***chuẩn X.29*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các thủ tục trao đổi thông tin điều khiển và dữ liệu của người sử dụng giữa DTE chế độ gói và phương tiện ráp/gỡ gói. *Xem* DTE, PAD.

X.30 ***chuẩn X.30*** Trong bộ các chuẩn, khuyến nghị của CCITT để chuẩn hóa máy in trang chế độ cơ sở theo mã chữ cái quốc tế No 5. *Xem* International Alphabet Number 5.

X.31 ***chuẩn X.31*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các đặc trưng theo quan điểm truyền dẫn tại điểm trao đổi lẫn nhau giữa DTE và DCE khi thiết bị đầu cuối dữ liệu khởi/ngừng ở tốc độ 200 baud phù hợp với mã chữ cái quốc tế No 5. *Xem* DCE, DTE, International Alphabet Number 5.

X.32 ***chuẩn X.32*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các khối tự đáp cho các máy khởi-ngừng 200 baud theo mã quốc tế chữ cái No 5. *Xem* baud, International Alphabet Number 5.

X.33 ***chuẩn X.33*** Trong bộ các chuẩn, khuyến nghị của CCITT để chuẩn hóa văn bản quốc tế cho thước đo lề của máy khởi-ngừng phù hợp với mã chữ cái quốc tế No 5. *Xem* International Alphabet Number 5.

X.40 ***chuẩn X.40*** Trong bộ các chuẩn, khuyến nghị của CCITT để chuẩn hóa các hệ thống truyền được điều chế dịch tần nhằm cung ứng các kênh dữ liệu và điện báo nhờ sự chia tần số nhóm gốc.

X.50 ***chuẩn X.50*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các tham số cơ bản của sơ đồ dồn kênh để giao tiếp quốc tế giữa các mạng dữ liệu đồng bộ. *Xem* multiplexing, synchronous data network.

X.50 bis ***chuẩn X.50 lần hai*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các tham số cơ bản của sơ đồ truyền tín hiệu báo dữ liệu người dùng ở tốc độ 48 Kbit/giây để giao tiếp quốc tế giữa các mạng dữ liệu đồng bộ. *Xem* bit, synchronous data network.

X.51 ***chuẩn X.51*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các tham số cơ bản của sơ đồ dồn kênh để giao tiếp quốc tế giữa các mạng dữ liệu đồng bộ dùng các cấu trúc đường bao 10 bit. *Xem* bit, synchronous data network.

X.52 ***chuẩn X.52*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với phương pháp mã các tín hiệu không đồng bộ thành các vật mang tín hiệu đồng bộ của người dùng. *Xem* anisochronous transmission.

X.53 ***chuẩn X.53*** Trong bộ các chuẩn, khuyến nghị của CCITT về việc đánh số các kênh trên các đường kết nối đa lộ quốc tế ở tốc độ 64 Kbit/giây. *Xem* bit, multiplexing.

X.54 ***chuẩn X.54*** Trong bộ các chuẩn, khuyến nghị của CCITT về việc cấp phát các kênh trên các đường kết nối đa lộ quốc tế ở tốc độ 64Kbit/giây. *Xem* bit, multiplexing.

X.60 ***chuẩn X.60*** Trong bộ các chuẩn, khuyến nghị của CCITT về tín hiệu báo kênh chung cho các ứng dụng dữ liệu chuyển mạch.

X.61 ***chuẩn X.61*** Trong bộ các chuẩn, khuyến nghị của CCITT về hệ thống báo hiệu No 7 - phần người dùng dữ liệu.

X.70 ***chuẩn X.70*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với thiết bị đầu cuối và hệ thống báo hiệu điều khiển chuyển tiếp cho các dịch vụ khởi/ngừng trên các mạch quốc tế giữa các mạng dữ liệu không đồng bộ. *Xem* anisochronous data network.

X.71 ***chuẩn X.71*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với thiết bị đầu cuối không được tập trung và hệ thống báo tín hiệu điều khiển chuyển tiếp giữa các mạng dữ liệu đồng bộ. *Xem* synchronous data network.

X.75 ***chuẩn X.75*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các thủ tục kiểm soát gọi chuyển tiếp và kiểm soát đầu cuối và hệ thống chuyển dữ liệu trên các mạng quốc tế giữa các mạng dữ liệu chuyển mạch gói.

X.80 ***chuẩn X.80*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với sự hoạt động chung của các dịch vụ dữ liệu chuyển mạch dùng hệ thống báo hiệu qua lại.

X.87 ***chuẩn X.87*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các nguyên tắc và thủ tục để thực hiện các phương tiện người dùng quốc tế và các tiện ích mạng trong các mạng dữ liệu công cộng. *Xem* public data network.

X.92 ***chuẩn X.92*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với

các nối tham chiếu có tính giả thuyết cho các mạng dữ liệu đồng bộ công cộng. *Xem* synchronous data network.

X.93 ***chuẩn X.93*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các nối tham chiếu có tính giả thuyết cho các dịch vụ truyền dữ liệu chuyển mạch gói.

X.95 ***chuẩn X.95*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các tham số mạng trong các mạng dữ liệu công cộng. *Xem* public data network.

X.96 ***chuẩn X.96*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các tín hiệu xúc tiến cuộc gọi trong các mạng dữ liệu công cộng.

X.110 ***chuẩn X.110*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các nguyên tắc định tuyến cho các dịch vụ dữ liệu quốc tế công cộng qua các mạng dữ liệu chuyển mạch có cùng kiểu. *Xem* routing.

X.121 ***chuẩn X.121*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với kế hoạch đánh số quốc tế cho các mạng dữ liệu công cộng.

X.130 ***chuẩn X.130*** Trong bộ các chuẩn, khuyến nghị của CCITT cho các mục tiêu tạm thời đối với những thiết lập và gián đoạn cuộc gọi trong các mạng dữ liệu đồng bộ công cộng. *Xem* circuit switching, synchronous data network.

X.132 ***chuẩn X.132*** Trong bộ các chuẩn, khuyến nghị của CCITT cho các mục tiêu nhất thời để nâng cấp dịch vụ truyền thông dữ liệu quốc tế trên các mạng dữ liệu chuyển mạch công cộng.

X.150 ***chuẩn X.150*** Trong bộ các chuẩn, khuyến nghị của CCITT cho các mạch vòng kiểm định DTE và DCE đối với các mạng dữ liệu công cộng trong trường hợp phối ghép X.21 và X21 lần hai. *Xem* DCE, DTE, X.21, X.21 bis.

X.180 ***chuẩn X.180*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với các sắp xếp quản trị cho các nhóm người dùng quốc tế khép kín. *Xem* closed user group.

X.200 ***chuẩn X.200*** Trong bộ các chuẩn, khuyến nghị của CCITT đối với mô hình tham chiếu OSI cho các ứng dụng CCITT. *Xem* OSI.

X.210 ***chuẩn X.210*** Trong bộ các chuẩn, khuyến nghị của CCITT về quy tắc xác định Dịch vụ phân tầng OSI. *Xem* OSI.

X.400 ***chuẩn X.400*** Trong truyền thông dữ liệu, một chuẩn cho các hệ thống quản lý thông báo bao gồm các đặc tả về kiến trúc mạng, kiến trúc giao thức, chi tiết thực hiện, các phần tử chuyển thông báo và các giao thức nội dung. Chuẩn X.400 là tầng ứng dụng đã phát triển đầy đủ của mô hình kết nối các hệ thống mở và nó đưa ra khái niệm về các lớp con gọi là những bộ phận người dùng (user agent - UA) và những bộ phận chuyển thông báo (MTA).

Bộ phận người dùng tương tự với người dùng hệ thống bưu điện, người ghi địa chỉ và bỏ thư. Bộ phận chuyển thông báo là những văn phòng phân loại nhằm phân phối và chuyển giao thông báo. Các MTA giống như một

nhóm gọi là hệ thống chuyển phát thông báo (MTS).

Ba giao thức chính trong X.400 là giao thức tiếp sức P1 giao thức tiêu đề và thân thông báo P2 và giao thức nhiệm vụ con P3. Giao diện người dùng không được định nghĩa và do vậy, nó có tính linh hoạt tốt theo nghĩa ghi, hiển thị, lưu và truy lục thông báo.

Một thông báo điển hình có bao thư và nội dung chứa cả phần tiêu đề lẫn phần thân. Giao thức P2 chỉ tới phần tiêu đề thông báo với những yếu tố như người gửi, người nhận, chủ đề, người nhận thứ hai, chỉ dẫn trả lời cho ai, ai chỉ dẫn trả lời quyền ưu tiên, độ nhạy cảm, thời hạn hết hạn, bản sao kín chỉ tiết về thời gian phân phát, địa chỉ khai báo phân phối, chỉ dẫn tham khảo tới các địa chỉ khác, chuyển giải quyết khi thông báo lỗi thời, chuyển giải quyết thông báo trả lời tới ai. P2 cũng xác định các phần thân khác nhau của thông báo bao gồm điện báo, tiếng nói, fax, teletext, văn bản, video.

Giao thức P3 đề cập tới chuẩn về bọc gói để truyền giữa bộ phận người dùng và bộ phận chuyển phát thông báo. Như vậy, người dùng gửi phần thân thông báo và địa chỉ tới bộ phận người dùng, anh ta sẽ thêm tiêu đề P2 vào phần thân P2 và đặt nó vào bao P3.

Giao thức P1 chỉ tới chuẩn bọc gói khi thông báo được định tuyến từ bộ phận người dùng này tới bộ phận người dùng khác. MTA chấp nhận thông báo trong bao gói P3 từ UA và bỏ kèm tiêu đề P2 và phần thân vào bao P1 để chuyển tới MTA tiếp sau. Tại bên thu, MTA nhận bao P1 và chuyển tiêu đề P2 cùng phần thân vào bao P3 để chuyển tới UA. UA nhận bao P3 và chuyển phần thân P2 tới người nhận.

Vùng ứng dụng chính của chuẩn X.400 sẽ thuộc các hệ thống văn phòng dùng các kết nối giữa các máy tính cá nhân và các mạng.

Những ưu điểm đặc thù của X.400 đối với các OEM và các khách hàng của chúng được liệt kê dưới đây:

- Giá phát triển giảm dần do việc sử dụng các đặc tả được xác định rõ ràng.
- Việc mua phần mềm đóng gói có sẵn sẽ giảm được thời gian phát triển.
- Nhân viên OEM ít cần kiến thức chuyên sâu về quyền sở hữu các hệ thống thông tin.
- Những người sử dụng sẽ không bị gắn chặt vào các nhà sản xuất riêng lẻ.
- Loại bỏ được sự chuyển đổi lãng phí giữa các dịch vụ khác nhau.
- Phát triển theo dạng modun.
- Giảm bớt sử dụng điện thoại.
- Giảm bớt việc dùng giấy.

Xem application layer, blind copy, electronic mail, open systems interconnection, MTA, MTS, OEM, protocol, P1, P2, P3, UA.

X.435 ***chuẩn X.435*** Trong bộ các chuẩn, một chuẩn của CCITT về các dịch vụ và hệ thống thông báo EDI dùng để điều hành sự truyền các tài liệu EDI trên các hệ thống thư điện tử theo chuẩn X.400. *So sánh với* ANSI X.12. *Xem* EDI security, electronic mail, electronic data interchange, X.400.

Xmas tree ***cây Nôen*** Trong an toàn

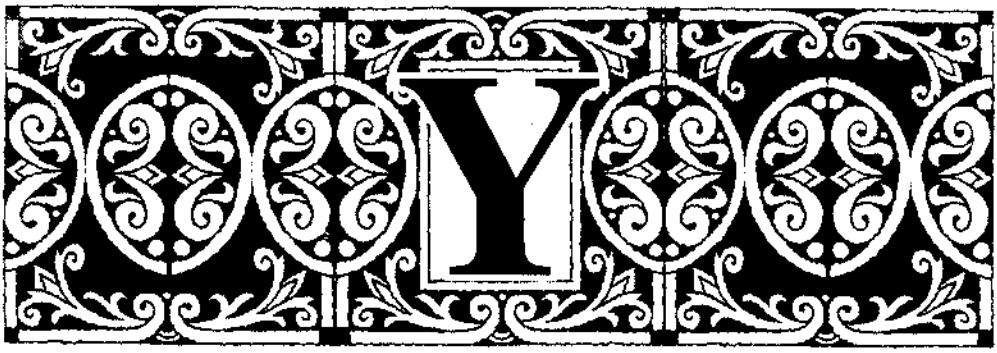
máy tính, một dạng tấn công kiểu sâu lên mạng thư điện tử của IBM, khi đó một cây Nôen xuất hiện trên màn hình của người sử dụng. *Xem* worm.

X-modem ***giao thức X-modem*** Trong phần mềm, một giao thức chuyển tệp không đồng bộ làm việc với hầu hết các máy vi tính và máy chủ. Giao thức thuộc khu vực công cộng và được sử dụng rộng rãi trên các hệ thống bảng thông báo. Dữ liệu cần truyền đi sẽ được ghép thành các khối 128 byte, khối cuối cùng được đệm các khoảng trống nếu cần. LRC được dùng để kiểm tra khối và mỗi khung có một số hiệu dãy để bên thu sẽ báo nhận và sau đó bỏ qua các khung đúp. *Xem* bulletin board, frame, LRC.

XON-XOFF protocol ***giao thức XON-XOFF*** Trong truyền thông dữ liệu, một giao thức chuẩn dùng khi chuyển thông tin đi từ máy tính này tới máy tính khác hoặc tới các thiết bị ngoại vi. Giao thức thường đòi hỏi kết nối dữ liệu kép đầy đủ. Khi máy tính phía thu, hoặc ngoại vi có thể không còn nhận dữ liệu nữa, ví dụ khi cần một máy tính để phục vụ một nhiệm vụ có ưu tiên cao hơn, nó sẽ gửi một ký tự kiểm soát XOFF ASCII chỉ thị cho máy tính bên phát đợi ký tự XON. *Xem* ASCII, full duplex, priority, protocol.

XOR Xem EXCLUSIVE OR.

X-Series recommendations of CCITT ***(các) khuyến nghị xeri X của CCITT*** Trong bộ các chuẩn, một loạt các khuyến nghị về truyền dữ liệu trên các mạng dữ liệu công cộng. *So sánh với* V-Series recommendations of CCITT. *Xem* protocol standards.

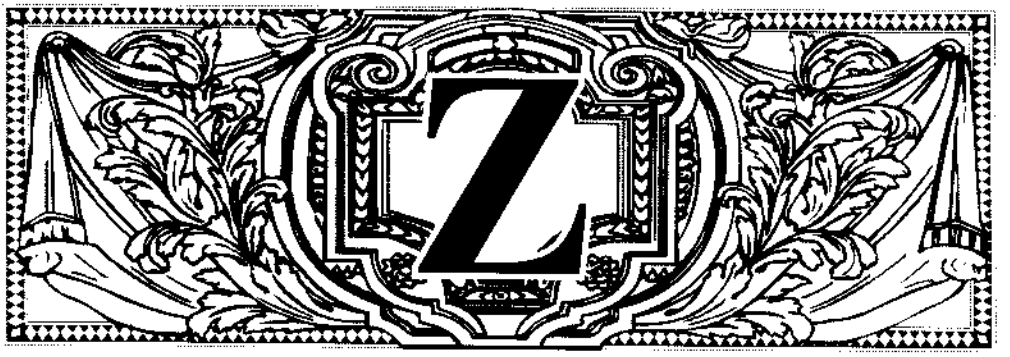


Yankee Doodle ***virut Yankee Doodle*** Trong an toàn máy tính, một loại virut làm chấm dứt và nằm thường trú trong bộ nhớ, làm lây nhiễm các tệp COM, EXE, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

Yankee-2 ***virut Yankee-2*** Trong an toàn máy tính, một loại virut làm lây nhiễm các tệp COM, EXE, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

Yellow Book ***Sách Vàng*** Trong an toàn máy tính, một cuốn sách về yếu tố kỹ thuật căn bản nằm sau CSC-STD-003-85 của Bộ Quốc phòng. Nó hướng dẫn việc áp dụng tiêu chuẩn TCSEC vào các môi trường đặc thù. *So sánh với* Blue Book, Orange Book, Red Book. *Xem* TCSEC, Rainbow Series.

Younger Committee ***Ủy ban trẻ*** Trong luật pháp, một Ủy ban của Mỹ đã xem xét các vấn đề bảo vệ và bí mật dữ liệu, đã được báo cáo năm 1972. *Xem* data protection, data protection - U.K., privacy.



Zero Bug *virut Zero Bug* Trong an toàn máy tính, một loại virut chấm dứt và nằm thường trú trong bộ nhớ, làm lây nhiễm các tệp COM, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

zero effort rate *tỷ lệ nỗ lực thấp nhất* Trong kiểm soát truy nhập, nói tới một thiết bị trắc sinh học được điều chỉnh tới điểm mà nó sẽ chấp nhận tín hiệu vào bất kỳ khi tín hiệu đó tương ứng với tín hiệu vào của người sử dụng hợp pháp. *So sánh với* equal error rate. *Xem* biometrics.

ZeroHunt *virut ZeroHunt* Trong an toàn máy tính, một loại virut tự mã lên chính mình, chấm dứt và nằm thường trú trong bộ nhớ, làm lây nhiễm các tệp COM, tác động trong thời gian chạy, làm hỏng các tệp chương trình và OVL. *Xem* virus names.

zeroization *đưa hết về số 0, zero hóa* Trong an toàn máy tính, một phương pháp khử từ, xóa hay ghi đè dữ liệu được lưu bằng điện tử. *Xem* degauss, overwriting.

zero knowledge proof *chứng minh tri thức không, chứng minh không để lộ thông tin* Trong mật mã, một phương pháp nhờ đó Alice thuyết phục được Bob rằng, cô ta biết sự việc nào đó mà không để lộ sự việc cho Bob; quả thực sẽ không thể thực hiện được về mặt tính toán đối với Bob nhằm xác định sự việc bằng thông tin do Alice cung cấp. *Xem* challenge/response, Fiat-Shamir Algorithm. *Đồng nghĩa với* minimum knowlegde proof.

zero order correlation immune *triệt tương quan bậc không* Trong mật mã, một dãy được lập nhờ một tổ hợp phi tuyến các dãy do một tập các thanh ghi dịch phản hồi tuyến tính tạo ra. Dãy được gọi là triệt tiêu tương quan bậc không nếu nó độc lập thống kê với một trong các dãy vào. *Xem* linear feedback

shift register.

zoning *(sự) phân vùng, (sự) chia vùng* Trong an toàn vật lý, một kỹ thuật xây dựng công trình có bảo vệ được chia thành các vùng; thiết bị khởi động tín hiệu báo động trong vùng như vậy có thể lập trình được để báo hiệu một mã nhận dạng và/hoặc chỉ ra trên bảng tín hiệu của vùng có hỏa hoạn.

ZSI *cơ quan ZSI* Viết tắt của Zentralstelle für Sicherheit in der Informationstechnik, Cơ quan an toàn thông tin của Đức.

PHẦN VIỆT - ANH

A

A A

AC AC

ADP ADP

AFR AFR

AIM AIM

AIS AIS

an toàn ADP ADP security

an toàn AMAIS AMAIS security

an toàn bắt buộc mandatory security

an toàn bức xạ emanation security

an toàn cá nhân personnel-sercurity

an toàn các hệ thống thông tin tự động và viễn thông telecommunications and automated information systems security

an toàn cơ sở dữ liệu database security

an toàn cơ sở dữ liệu nhiều mức multilevel database security

an toàn dữ liệu data security

an toàn dữ liệu thao tác operational date security

an toàn EDI EDI security

an toàn EEPROM EEPROM security

an toàn hành chính administrative security

an toàn hệ thống ADP ADP system security

an toàn hệ thống thông tin information system security

an toàn hệ thống thông tin và viễn thông Quốc gia của Mỹ NTISS

an toàn hệ thống tự động hóa automated system security

an toàn kết nối các hệ thống mở OSI security

an toàn khi có sự cố fail mafe

an toàn không điều kiện unconditionally secure

an toàn không tùy ý non-discretionary security

an toàn kỹ thuật technical security

an toàn LAN LAN security

an toàn logic logical security

an toàn luồng thông tin traffic flow security

an toàn mạng network security

an toàn mạng cục bộ LAN security

an toàn mạng nội hạt LAN security

an toàn máy tính computer security

an toàn máy tính cá nhân personal ,computer security

an toàn mềm fail soft

an toàn ngân hàng tại nhà home banking security

an toàn nhân sự personnel sercurity

an toàn nhiều mức multilevel secure, MLS

an toàn phát xạ emission security
an toàn phần cứng hardware security
an toàn phần mềm software security
an toàn tài sản thông tin information asset security
an toàn tăng cường add-on security
an toàn tệp file security
an toàn thông tin information security
an toàn thủ tục procedural security
an toàn thư điện tử electronic mail security
an toàn tính toán computationally secure
an toàn truyền thông communications security
an toàn tùy ý discretionary security
an toàn tự động hóa automation security
an toàn tương tác mutual security
an toàn VANS VANS security
an toàn vận hành OPSEC (OPerations SECurity)
an toàn vật lý physical security
an toàn về mặt lý thuyết theoretically secure
an toàn xử lý từ xa teleprocessing security
ảnh toàn ký hologram
ánh xạ mapping
ánh xạ ký tự character mapping
ảo virtual
API API
API mật mã cryptographic API
AR AR
ARPA ARPA
ARU ARU
ASIS ASIS
ATTT INFOSEC (Information Security)
AU AU
autoclap autoclave
ăn cắp phần mềm softlifting
âm không chạm kiss off tone
âm phổ ký sonograph
ấn phẩm FIPS FIPS PUB (Federal Information Processing Standard Publication)
ấn phẩm FIPS 65 FIPS Pub 65

B

bai byte

bài poke trí tuệ mental poker

bài toán loga rời rạc discrete logarithm problem

bài toán ngày sinh birthday problem

(các) bài toán TOCTTOU TOCTTOU problems

(sự) bám sát locking

ban DG XIII DG XIII

ban OIS 21 OIS 21

Ban phối hợp bang của Liên bang Federal State Joint Board

bàn điều khiển console

bản ghi record

bản ghi (nhật ký) an toàn security log

bản ghi cắm planted record

bản ghi chép theo dõi logging

bản ghi độ dài cố định fixed length record

bản ghi độ dài thay đổi variable length record

bản ghi kết thúc trailer

bản ghi logic logical record

bản ghi vật lý physical record

bản gốc plaintext

bản gốc chọn trước chosen plaintext

bản kê treo suspense account

bản mã cryptogram, cryptotext

bản mã tín hiệu ciphertext

bản phân định kiểm soát truy nhập access control roster

bản quyền copyright

bản quyền phần mềm software license

bản rõ cleartext, plaintext

bản rõ biết trước known plaintext

bản rõ đã biết known plaintext

bản tóm lược thông báo message digest

bản chạy COTS

bán song công half duplex

bảng table

bảng chữ cái quốc tế số 5 international alphabet number 5

bảng dữ liệu data tablet

bảng điều khiển control panel

bảng định tuyến routing table

bảng thập phân hóa decimalization table

bảng thông báo bulletin board

bảng viết điện tử electronic blackboard

bảo dưỡng maintenance

bảo dưỡng phần mềm software maintenence

bảo đảm cung cấp delivery assurance

bảo đảm điểm tới điểm end-to-end assurance

bảo đảm phân phát delivery assurance

(sự) bảo mật privacy

bảo mật dòng lưu lượng traffic flow confidentiality

bảo trì maintenance

bảo trì có hiệu chỉnh corrective maintenance

bảo trì phần mềm maintenance

bảo trì phòng ngừa preventive maintenance

bảo trì tệp file maintenance

bảo vệ guard

(sự) bảo vệ protection

bảo vệ bộ nhớ memory protection, storage protection

bảo vệ chạy chương trình execute protection

bảo vệ chống rò rỉ bức xạ emanation security

(được) bảo vệ chống sao chép copy protected

bảo vệ chống sao chép copy protection, execute protection

bảo vệ dữ liệu data protection

bảo vệ dữ liệu - Ailen data protection - Ireland

bảo vệ dữ liệu - Aixolen data protection - Iceland

bảo vệ dữ liệu - Đan Mạch data protection - Denmark

bảo vệ dữ liệu - Đảo Guernsey data protection - Guernsey

bảo vệ dữ liệu - Đảo Jersey data protection - Jersey

bảo vệ dữ liệu - Đảo Man data protection - Isle of Man

bảo vệ dữ liệu - Áo data protection - Austria

bảo vệ dữ liệu - Bỉ data protection - Belgium

bảo vệ dữ liệu - Bồ Đào Nha data protection - Portugal

bảo vệ dữ liệu - Canada data protection - Canada

bảo vệ dữ liệu - EC data protection - EC

bảo vệ dữ liệu - Hà Lan data protection - Netherlands

bảo vệ dữ liệu - Hoa Kỳ data protection - USA

bảo vệ dữ liệu - Hội đồng Châu Âu data protection - Council of Europe

bảo vệ dữ liệu - Hy Lạp data protection - Greece

bảo vệ dữ liệu - Israen data protection - Israel

bảo vệ dữ liệu - Liên hiệp Anh data protection - UK

bảo vệ dữ liệu - Lucxămbua data protection - Luxembourg

bảo vệ dữ liệu - Na Uy data protection - Norway

bảo vệ dữ liệu - Nhật Bản data protection - Japan

bảo vệ dữ liệu - Niu Di Lân data protection - New Zealand

bảo vệ dữ liệu - OECD data protection - OECD

bảo vệ dữ liệu - Pháp data protection - France

bảo vệ dữ liệu - Phần Lan data protection - Finland

bảo vệ dữ liệu - Sip data protection - Cyprus

bảo vệ dữ liệu - Slovenia data

protection - Slovenia

bảo vệ dữ liệu - Tây Ban Nha data protection - Spain

bảo vệ dữ liệu - Thụy Điển data protection - Sweden

bảo vệ dữ liệu - Đức data protection - Germany

bảo vệ dữ liệu - Ôxtrâylia data protection - Australia

bảo vệ đầu ra output protection

bảo vệ đối tượng object protection

bảo vệ hạn chế limited protection

bảo vệ khu vực area protection

bảo vệ mật privacy protection

bảo vệ phần mềm software protection

bảo vệ phụ thuộc dữ liệu data-dependent protection

bảo vệ tệp file protection

bảo vệ theo điểm point protection

bảo vệ tìm nạp fetch protection

bảo vệ trường lựa chọn selective field protection

bảo vệ tùy ý discretionary protection

bảo vệ vùng space protection

(sự) bão hòa từ magnetic saturation

báo cáo đánh giá kỹ thuật evaluation technical report

báo cáo về không nhất quán discrepancy reports

báo cáo về sai lệch discrepancy reports

báo động bắt buộc duress alarm

báo động chéo cross alarm

báo động hông hóc nuisance alarm

báo động kép double drop

báo động mạch kín closed circuit alarm

báo động ngắt break alarm

(các) báo động phối hợp combined alarms

báo động trước pre-alarm

báo hiệu signalling

báo hiệu số digital signalling

báo hiệu tấn công attack signalling

báo hiệu trong dải in band signalling

báo không công nhận negative acknowledgement

báo nhận acknowledgement

báo phủ nhận NAK, negative acknowledgement

bát phân octal

baud baud

băm khóa key hashing

băng (từ) tape

băng an toàn tape

băng hình bóng watermark tape

băng khóa key tape

băng lớp kẹp sandwich tape

băng từ magnetic tape

(sự) bắt chước simulation

bắt dữ liệu data capture

(ký tự) bắt đầu phần tiêu đề start of header

(ký tự) bắt đầu văn bản start of text

bậc order

bấm manip dịch tần frequency shift keying

bất biến invariant

bẫy trapdoor

bẫy dây cord trap

BBS BBS

ben bel

bên bồi hoàn reimbursement party

bên có credit party

bên nhận receiver
bên nhận thẻ card acc
bên nợ debit party
bên thanh toán instructing party
bên trả reimbursement party
(sự) bí mật secrecy
bí mật Confidential
bí quyết know how
bị bao hàm contained
bị giới hạn contained
bìa mở rộng expansion card
biển thủ embezzlement
biến variable
biến cố có hại harmful event
biến đổi dòng thông báo message stream modification
biến đổi tệp file conversion
biến khởi đầu initializing variable
biến mật mã cryptographic variable
biến thể khóa key variant
biến toàn cục global
(các) biện pháp an toàn security measures
(các) biện pháp chống virut anti-viral measures
biện pháp đối phó countermeasure
(các) biện pháp đối phó bằng quét điện tử electronic countermeasures sweeping
biện pháp ECM ECM
(các) biện pháp kiểm soát truy nhập access control measures
biểu đồ âm thanh sonogram
biểu đồ mạng network diagram
biểu thức expression
biểu thức logic logical expression
bit bit
bit bổ sung overhead bit
bit bội ba tribit
bit chẵn lẻ parity bit
bit cờ flag bit
bit cực phải least significant bit
(các) bit dữ liệu data bits
bit dừng caboose, stop bit
bit đôi dibit
bit đồng bộ sync bit
bit khởi đầu start bit
bit kiểm tra check bit
bit nhỏ nhất least significant bit
bit nội dịch overhead bit
bit song song bit parallel
bit tạo khung framing bits
bit trên giây bits per second
bit trên inso bits per inch
(các) bit yếu weak bits
bo mạch circuit board
bo mạch in printed circuit board
bo mạch mã encrypter board
bo mạch mở rộng expander board, expansion card
bỏ delete
bỏ ký tự rỗng null suppression
bỏ qua jump out
bó tin packet
bóc (thư) stripping
(sự) bọc gói encapsulation
bọc gói số digital enveloping
bom hẹn giờ time bomb
bom logic logic bomb
bom thời gian time bomb

bom thư letter bomb

bổ sung bit bit stuffing

bổ sung ký tự character stuffing

bố cục tệp file layout

bộ ba bit tribit

bộ ba chữ trigram

bộ ba ký tự trigram

bộ báo vệ chống hồ quang đánh thủng arc-breakdown protector

bộ biên dịch compiler

bộ biến hoán điệu MODEM

bộ bù trễ pha delay equalizer

bộ cảm biến ba chiều volumetric sensor

bộ cảm biến để sàn floor sensor

bộ cảm biến điện dung capacitance sensor

bộ cảm biến điện trường electric field sensor

bộ cảm biến (phát hiện) động đất seismic sensor

bộ cảm biến đường truyền line sensor

bộ cảm biến kháng lại sự thay đổi inertia sensor

bộ cảm biến khoảng cách span sensor

bộ cảm biến khói ion hóa ionization smoke sensor

bộ cảm biến quán tính inertia sensor

bộ cảm biến quang điện photoelectric sensor

bộ cảm biến quang điện điều chế modulated photoelectric sensor

bộ cảm biến rada radar sensor

bộ cảm biến thụ động passive sensor

bộ cảm biến trường tĩnh điện electrostatic field sensor

bộ cảm biến từ magnetic sensor

bộ cảm biến vi ba microwave sensor

bộ cảm biến vi ba lưỡng ổn bistatic microwave sensor

bộ cảm biến (bắt buộc) xách tay portable duress sensor

bộ cản deterrent

bộ chặt dải bandsplitter

bộ chỉ thị đệm ký tự padding indicator

bộ chọn đường router

bộ chuyển đổi (mã) converter

bộ chuyển mạch cầu nối tuần tự bridging'sequential switcher

bộ chuyển mạch tự báo động auto-alarming switcher

bộ chuyển mạch về (vào) tự hoàng sequential switcher

bộ chuyển mạch video video switcher

bộ chuyển tiếp transponder

bộ chương trình ACF2 ACF2

bộ chương trình an toàn dữ liệu data security package

(các) bộ chương trình hỏi kiểm toán máy tính computer audit enquiry packages

(các) bộ chương trình kiểm toán máy tính computer audit packages

bộ cuộn băng từ chạy suốt tape streamer

bộ dịch translator

bộ dò nhiệt heat detector

bộ dò rung điện tử electronic vibration detector

bộ dồn kênh multiplexer, MUX

bộ dồn ký tự characterplexer

bộ dữ liệu khoảng cách hạn chế LDDS (Limited Distance Data Set)

bộ đa hợp multiplexer

bộ đảo dịch dải tần band shift invertor

bộ đảo dịch dải tần theo vòng cyclical band shift invertor

bộ đảo tiếng nói speech invertor

bộ đếm counter

bộ đếm khung từ word-frame counter

bộ đệm buffer

bộ đệm PIN PIN pad

bộ đĩa disk pack

bộ điều biến modulator

bộ điều chế modulator

bộ điều chế-giải điều chế MODEM

bộ điều khiển controller, handler

bộ điều khiển chùm cluster controller

bộ điều khiển đường truyền line driver

bộ điều khiển liên kết truyền thông communication link controller

bộ điều khiển tích hợp integral controller

bộ định danh thông báo MID

bộ định tuyến router

bộ đọc các gián tiếp off line card reader

bộ đọc sọc từ stripe reader

bộ đọc thẻ badge reader

bộ đọc thẻ có khả năng loại bỏ single voiding card reader

bộ đọc thẻ gần proximity card reader

bộ đọc thẻ hệ thống system card reader

bộ đọc thẻ thông minh intelligent card reader

bộ đọc thẻ trực tuyến on line card reader

bộ đọc thẻ tuần tự sequential card reader

bộ đọc vạch từ stripe reader

bộ đọc xóa thẻ đi qua wipe through card reader

bộ đôi bigram

bộ đổi giao thức protocol converter

bộ đổi quy cách protocol converter

bộ đồng xử lý coprocessor

bộ gá truy nhập dữ liệu data access arrangement

bộ ghép âm acoustic coupler

bộ ghép bus dữ liệu data bus coupler

bộ ghép dữ liệu data coupler

bộ giải điều (chế) demodulator

bộ giải mã decoder

bộ giải mã văn bản từ xa teletext decoder

bộ giám sát an toàn security monitor

bộ giám sát tham chiếu reference monitor

bộ giao thức protocol suite

bộ góp dữ liệu data sink

bộ gỡ rối debugger

bộ hợp dịch assembler

bộ khóa giao dịch transaction key set

bộ khởi đầu initiator

bộ khử từ degausser

bộ kiểm soát truy nhập đầu cuối terminal access controller

bộ ký tự character set

bộ ký tự chữ cái alphabetic character set

bộ ký tự mã hóa coded character set

bộ lập - giải mã CODEC

bộ lập biểu ưu tiên priority scheduler

bộ LDDS LDDS (Limited Distance Data Set)

bộ lọc filter

bộ lọc an toàn security filter

bộ lọc an toàn trước front end security filter

bộ lọc ngoại vi front end security filter

bộ logic logical unit

bộ mã chuẩn công nghiệp SIC

bộ mã hóa thẻ card encoder

bộ mã SIC SIC

bộ mã tiếng nói vocoder

bộ mắc trộm điện thoại telephone tap

bộ mô phỏng emulator

bộ mô tả descriptor

bộ mô tả tệp file descriptor

bộ (quan hệ) n n-tuple

bộ ngăn chặn arrester

bộ nhận dạng tiếng nói speech recognizer

bộ nhập/xuất input/output unit

bộ nhớ bất biến nonvolatile storage

bộ nhớ chỉ đọc read-only memory

bộ nhớ chỉ đọc được lập trình xóa được erasable programmed read only memory

bộ nhớ chỉ đọc lập trình bằng điện electrically programmable read only memory

bộ nhớ chỉ đọc lập trình được PROM

bộ nhớ chỉ đọc thay đổi bằng điện electrically alterable ROM

bộ nhớ chính main memory

bộ nhớ dự phòng backing storage

bộ nhớ đĩa cố định fixed disk storage

bộ nhớ đĩa cố định và đổi được fixed and exchangeable disk storage

bộ nhớ đĩa quang optical disk storage

bộ nhớ đĩa thay đổi được exchangeable disk storage

bộ nhớ khả biến volatile storage

bộ nhớ mở open storage

bộ nhớ PROM PROM

bộ nhớ quang optical memory

bộ nhớ tệp file storage

bộ nhớ truy nhập ngẫu nhiên random access memory

bộ nhớ xóa được erasable storage

bộ nối BNC BNC connector

bộ phát đáp transponder

bộ phát hiện áp điện piezoelectric detector

bộ phát hiện chuyển động motion detector

bộ phát hiện chuyển động bằng siêu âm ultrasonic motion detector

bộ phát hiện chuyển động bằng tần số vô tuyến radio frequency motion detector

bộ phát hiện chuyển động video video motion detector

bộ phát hiện dao động vibration detector

bộ phát hiện dao động điện tử electronic vibration detector

bộ phát hiện khói smoke detector

bộ phát hiện lửa bằng tia cực tím ultraviolet fire detector

bộ phát hiện sự có mặt presence detector

bộ phát hiện tín hiệu qua đường dây thu received line signal detector

bộ phát tạp âm trắng white noise emitter

bộ phân biệt cảnh báo alarm discriminator

bộ phân tich chương trình program analyzer

bộ phân tich mã nguồn source code

analyzer

bộ phần mềm software package

bộ phận bảo vệ không thực negative safeguard

bộ phận chuyển mạch switching office

bộ phận chuyển thông báo message transfer agent

bộ phận mật mã cryptographic device

bộ phận người dùng user agent

bộ phận thu phát transceiver

bộ phận trả tiền remitter

bộ phục vụ tệp file server

bộ phục vụ truyền thông communication server

bộ quan hệ tuple

bộ quản handler

bộ quản thiết bị đầu cuối terminal handler

bộ quay số dialer

bộ quay số bằng số digital dialer

bộ quay số điện thoại telephone dialer

bộ quét truyền thông communication scanner

bộ sao bit bit copier

bộ sắp hàng ưu tiên priority scheduler

bộ SCOMP SCOMP

bộ sinh an toàn nhiều mức MLS

bộ tách dải bandsplitter

bộ tạo đồng dư tuyến tính LCG, linear congruential generator

bộ tạo khóa key generator

bộ tạo khóa dòng key stream generator

bộ tập trung concentrator

bộ tập trung dây chủ động active wire concentrator

bộ theo dõi tracker

bộ thích ứng giao diện truyền thông không đồng bộ asynchronous communications interface adaptor

bộ tiền xử lý front end processor

bộ tiền xử lý mạng front end network processor

bộ tổng hợp tiếng nói speech synthesizer

bộ triệt tín hiệu đội echo suppressor

bộ truyền tin số digital communicator

bộ tự động định danh autoidentifier

bộ VAD VAD

bộ vi xử lý microprocessor

bộ xác thực thẻ bài token authenticator

bộ xáo trộn scrambler

bộ xáo trộn dải tần bandscrambler

bộ xáo trộn DFT DFT scrambler

bộ xáo trộn dùng phép biến đổi Fourier rời rạc discrete Fourier transform scrambler

bộ xáo trộn điện thoại telephone scrambler

bộ xáo trộn hai chiều two-dimensional scrambler

bộ xáo trộn phần tử thời gian time element scrambler

bộ xử lý processor

bộ xử lý giao diện interface processor

bộ xử lý liên lạc an toàn SCOMP

bộ xử lý mảng array processor

bộ xử lý mạng truyền thông communications network processor

bộ xử lý ngoại vi mạng front end network processor

bộ xử lý thông báo giao diện interface message processor

bộ xử lý trung tâm central processing unit

bộ xử lý truyền thông communication processor
bộ xử lý trước front end processor
bội số chung nhỏ nhất least common multiple
bốn mắt four eyes
bốt baud
bới rác dumpster diving, scavenging
bromclodiflometan bromochlorodifluoromethane
BSCNN LCM
bù complement; equalization
bus bus
bus dùng thẻ bài token bus
bức điện message
bức tường chống lửa fire walls
bức tường lửa fire walls
bức xạ EMI/RF EMI/RF radiation
bức xạ rò emanation
bưu phẩm PIN PIN mailer
byte byte, octet
byte bao envelope
byte nối tiếp byte serial

C

C2 năm 92 C2 by 92

cạc ảnh toàn ký mật độ thay đổi varying density holographic card

cạc chấm từ magnetic spot card

cạc chip chip card

cạc mã chính master code card

cạc mở rộng expansion card

cạc thông minh không tiếp xúc contactless smart card

cạc vạch từ magnetic stripe card

cạc vi mạch microcircuit card

cạc vi xử lý microprocessor card

cách bố trí tệp file layout

cách ly isolation

cách ly điều khiển được controllable isolation

(sự) cài bẫy entrapment

cài đặt implementation

cài đặt/bỏ cài đặt install-deinstall

cài mã encipher, encrypt

(sự) cài mã encryption

cải tiến amend

cái là đặc tính người dùng something the user is

cái người dùng biết something the user knows

cái người dùng sở hữu something the user has

(bộ) cảm biến chủ động active sensor

cảm biến quang photosensor

cảm ứng từ dư remanence

camera ngân hàng bank camera

cáp bọc shielded cable

cáp chắn shielded cable

cáp đồng trục coaxial cable

cáp quang nhiều chế độ multimode fiber

cáp xoắn đôi twisted pair

căn nguyên thủy primitive root

cặp chữ bigram

cặp khóa mã khóa key-encrypting key pair

cặp liên lạc communicating pair

cặp truyền thông communicating pair

cấm sao chép copy protection

(sự) cấm sử dụng interdiction

(làm) cân bằng balancing

cân đối theo lô batch balancing

cần thì biết need to know

cấp an toàn security level

cấp dịch vụ grade of service

cấp dữ liệu data level

cấp đường truyền line level

cấp mạch điện circuit grade

(sự) cấp nguồn source authorization

cấp phát kênh thích ứng adaptive

channel allocation

(sự) cấp phép authorization

(sự) cấp quyền authorization

(sự) cấp quyền truy nhập access authorization

cập nhật tệp file updating

cất trữ ngoài vị trí off site storage

câu kết collusion

câu lạc bộ Chaos Chaos Club

câu lệnh statement

câu lệnh khuyến cáo caution statement

câu mật khẩu passphrase

(các) câu truy vấn mẫu ngẫu nhiên random sample queries

cầu bridge

cầu nối bridge

cầu dẫn router

cấu hình mạng network topology

cấu trúc cây tree structure

cấu trúc dữ liệu data structure

cấu trúc liên kết topology

cấu trúc mạng network structure

cây tree

cây gom sink tree

cây góp sink tree

cây liên kết threaded tree

cây Nôen Xmas tree

cây sự cố fault tree

chạm đường hit on the line

chạm khóa key collision

chạy chương trình hiệu đính editing run

chạy soạn thảo editing run

chạy (chương trình) tạo sản phẩm production run

chẵn lẻ khối block parity

chẵn lẻ ngang horizontal parity

chắn dẫn conductive shielding

chặn (thu) intercept

chặn in print suppress

chẩn đoán sự cố fault diagnosis

chấp nhận acceptance

chất lượng phần mềm software quality

chất lượng phần mềm máy tính computer software quality

che giấu covert

chen gói packet interleaving

chèn gói packet interleaving

chèn thanh ghi register insertion

chế độ mode

chế độ an toàn chia ngăn compartmented security mode

chế độ an toàn có kiểm soát controlled security mode

chế độ an toàn dành riêng dedicated security mode

chế độ an toàn hệ thống cao system high security mode

chế độ an toàn khoanh vùng compartmented security mode

chế độ an toàn nhiều mức multilevel security mode

chế độ byte byte mode

chế độ chuyên dụng dedicated mode

chế độ cục bộ local mode

chế độ dành riêng dedicated mode

chế độ dồn kênh multiplex mode

chế độ dùng thẻ card based mode

chế độ điều khiển control mode

chế độ hoạt động an toàn nhiều người sử dụng multi-use security mode of operation

chế độ không trong suốt nontransparent

mode

chế độ nóng hot mode

chế độ riêng native mode

chế độ tại chỗ local mode

chế độ truy nhập access mode

chế độ truy nhập an toàn tới các hệ xử lý tự động hạn chế limited ADP access security mode

chệnh biased

chi phí phân phối hoàn toàn fully distributed costs

chi phối dominate

(các) chỉ báo cho các hoạt động an toàn operations security indicators

chỉ lệnh instruction

chỉ mục index

chỉ mục trù mật dense index

chỉ nhận receive only

chỉ số index

chỉ số không trù mật nondense index

chỉ số so sánh rủi ro risk index

chỉ thị instruction

Chỉ thị 42 về an ninh Quốc gia National Security Directive-42

Chỉ thị 4 về an ninh thông tin Quốc gia National Communications Security Directive 4

chỉ thị đặc quyền privilege instructions

chỉ thị NSDD NSDD

chỉ thị NSDD-145 NSDD-145

Chỉ thị về an toàn hệ thống thông tin và viễn thông Quốc gia của Mỹ NTISSD

chỉ thị về giữ bí mật secrecy order

chỉ thu receive only

(sự) chia ngăn compartmentalization

chia sẻ tài nguyên resource sharing

chia sẻ thời gian time sharing

(sự) chia tải load sharing

(sự) chia vùng zoning

chìa khóa được mã coded key

chiếm đường truyền seize

chính sách policy

chính sách an toàn security policy

chính sách an toàn bắt buộc mandatory security policy

chính sách an toàn dựa trên danh tính identity based security policy

chính sách an toàn dựa trên quy tắc rule-based security policy

chính sách an toàn tập thể corporate security policy

chính sách an toàn tùy ý discretionary security policy

chính sách giữ bí mật secrecy policy

chính sách kỹ thuật technical policy

chính sách NTISSP-200 NTISSP-200

chính sách toàn vẹn integrity policy

(sự) cho phép permissions

(sự) cho phép truy nhập access permission

chọn selection

(sự) chọn đường routing

chọn đường thích ứng adaptive routing

chọn số mò blind dialing

(tín hiệu) chọn tốc độ báo hiệu dữ liệu data-signalling rate selector

chỗ dễ bị tổn thương vulnerability

chỗ dễ tổn thương kết cấu construction vulnerability

chồng đĩa disk pack

chống chuyển ngược anti-passback

chống nghẽn anti-jam

chống Tempest Tempest proofing

chống theo dõi anti-surveillance

chu kỳ khóa mã cryptoperiod

chu kỳ lưu giữ retention period

chu kỳ mật mã cryptographic period

chu kỳ truy nhập access period

chu kỳ xác thực authentication period

chu trình chứng từ document cycle

chu trình ghi đè overwrite cycle

chu trình hoạt động ngân hàng banking cycle

chu trình kinh doanh ngân hàng banking cycle

chu trình phát triển phần mềm software development life cycle

chu trình thanh toán payment cycle

chu trình thương mại trade cycle

chu vi an toàn security perimeter

chủ dữ liệu data owner

chủ sự principal

chủ thể subject

chủ thể dữ liệu data subject

chủ thể mạng nhiều mức multilevel network subject

chủ thể nội bộ internal subject

chủ thể tin cậy trusted subject

(các) chuẩn standards

chuẩn reference

chuẩn ANSI X.12 ANSI X.12

chuẩn ANSI X3.92 - 1981 ANSI X3.92 - 1981

chuẩn ANSI X3.105 - 1983 ANSI X3.105 - 1983

chuẩn ANSI X3.106 - 1983 ANSI X3.106 - 1983

chuẩn ANSI X3.118 - 1984 ANSI X3.118 - 1984

chuẩn ANSI X9.2 - 1980 ANSI X9.2 - 1980

chuẩn ANSI X9.3 - 1981 ANSI X9.3 - 1981

chuẩn ANSI X9.5 - 1988 ANSI X9.5 - 1988

chuẩn ANSI X9.7 - 1988 ANSI X9.7 - 1988

chuẩn ANSI X9.8 - 1982 ANSI X9.8 - 1982

chuẩn ANSI X9.9 - 1986 ANSI X9.9 - 1986

chuẩn ANSI X9.12 - 1983 ANSI X9.12 - 1983

chuẩn ANSI X9.13 - 1983 ANSI X9.13 - 1983

chuẩn ANSI X9.14 - 1983 ANSI X9.14 - 1983

chuẩn ANSI X9.16 - 1984 ANSI X9.16 - 1984

chuẩn ANSI X9.17 - 1985 ANSI X9.17 - 1985

chuẩn ANSI X9.18 - 1986 ANSI X9.18 - 1986

chuẩn ANSI X9.19 - 1986 ANSI X9.19 - 1986

chuẩn ANSI X9.20 - 1986 ANSI X9.20 - 1986

chuẩn ANSI X9.21 - 1986 ANSI X9.21 - 1986

chuẩn ANSI X9.22 - 1986 ANSI X9.22 - 1986

chuẩn ANSI X9.23 - 1988 ANSI X9.23 - 1988

chuẩn AS 2805 AS 2805

chuẩn AS 3801 - 1989 AS 3801 - 1989

chuẩn AS 3802 - 1989 AS 3802 - 1989
chuẩn AS 3803 - 1989 AS 3803 - 1989
chuẩn AS 3804 - 1989 AS 3804 - 1989
chuẩn Bell 103 Bell 103
chuẩn Bell 212A Bell 212A
chuẩn chữ ký số digital signature standard
chuẩn cứ criteria
chuẩn DEA 1 DEA 1
chuẩn điều khiển liên kết dữ liệu data link control standard
chuẩn EDIFACT EDIFACT
(các) chuẩn giao thức protocol standards
chuẩn IEEE 802 IEEE 802
chuẩn IEEE 802.3 IEEE 802.3
chuẩn IEEE 802.4 IEEE 802.4
chuẩn IEEE 802.5 IEEE 802.5
chuẩn IEEE 802.6 IEEE 802.6
chuẩn ISO 7498 ISO 7498
chuẩn ISO 7810 ISO 7810
chuẩn ISO 7811 ISO 7811
chuẩn ISO 7816 ISO 7816
chuẩn ISO 7982-1 ISO 7982-1
chuẩn ISO 8372 ISO 8372
chuẩn ISO 8583 ISO 8583
chuẩn ISO 8730 ISO 8730
chuẩn ISO 8731 ISO 8731
chuẩn ISO 8732 ISO 8732
chuẩn ISO 9564 ISO 9564
chuẩn ISO 9735 ISO 9735
chuẩn ISO 9992 ISO 9992
chuẩn ISO 9807 ISO 9807
chuẩn ISO 10126 ISO 10126
chuẩn ISO 10202 ISO 10202
(các) chuẩn lập trình programming standards
chuẩn mã dữ liệu data encryption standard
chuẩn mã dữ liệu quốc tế IDEA
chuẩn modem Hayes Hayes
chuẩn RS-232 RS-232
chuẩn RS-366 RS-366
chuẩn RS-449 RS-449
chuẩn RS-422A RS-422A
chuẩn RS-423A RS-423A
chuẩn RS-232C RS-232C
chuẩn thực hiện performance standard
chuẩn V.1 V.1
chuẩn V.2 V.2
chuẩn V.3 V.3
chuẩn V.4 V.4
chuẩn V.5 V.5
chuẩn V.6 V.6
chuẩn V.10 V.10
chuẩn V.11 V.11
chuẩn V.13 V.13
chuẩn V.15 V.15
chuẩn V.16 V.16
chuẩn V.19 V.19
chuẩn V.20 V.20
chuẩn V.21 V.21
chuẩn V.22 V.22
chuẩn V.23 V.23
chuẩn V.24 V.24
chuẩn V.25 V.25
chuẩn V.26 V.26
chuẩn V.27 V.27
chuẩn V.28 V.28
chuẩn V.29 V.29
chuẩn V.30 V.30

chuẩn V.31 V.31
chuẩn V.32 V.32
chuẩn V.35 V.35
chuẩn V.36 V.36
chuẩn V.37 V.37
chuẩn V.40 V.40
chuẩn V.41 V.41
chuẩn V.50 V.50
chuẩn V.51 V.51
chuẩn V.52 V.52
chuẩn V.53 V.53
chuẩn V.54 V.54
chuẩn V.55 V.55
chuẩn V.56 V.56
chuẩn V.22 bis V.22 bis
chuẩn V.22 lần hai V.22 bis
chuẩn V.26 lần hai V.26 bis
chuẩn V.27 lần hai V.27 bis
chuẩn V.27 ter V.27 ter
chuẩn V.bb V.bb
chuẩn X X
chuẩn X.1 X.1
chuẩn X.2 X.2
chuẩn X.3 X.3
chuẩn X.4 X.4
chuẩn X.20 X.20
chuẩn X.21 X.21
chuẩn X.22 X.22
chuẩn X.24 X.24
chuẩn X.25 X.25
chuẩn X.26 X.26
chuẩn X.27 X.27
chuẩn X.28 X.28
chuẩn X.29 X.29
chuẩn X.30 X.30
chuẩn X.31 X.31
chuẩn X.32 X.32
chuẩn X.33 X.33
chuẩn X.40 X.40
chuẩn X.50 X.50
chuẩn X.51 X.51
chuẩn X.53 X.53
chuẩn X.54 X.54
chuẩn X.60 X.60
chuẩn X.61 X.61
chuẩn X.70 X.70
chuẩn X.71 X.71
chuẩn X.75 X.75
chuẩn X.80 X.80
chuẩn X.87 X.87
chuẩn X.92 X.92
chuẩn X.93 X.93
chuẩn X.95 X.95
chuẩn X.96 X.96
chuẩn X.110 X.110
chuẩn X.121 X.121
chuẩn X.130 X.130
chuẩn X.132 X.132
chuẩn X.150 X.150
chuẩn X.180 X.180
chuẩn X.200 X.200
chuẩn X.210 X.210
chuẩn X.400 X.400
chuẩn X.435 X.435
chuẩn X.20 lần hai X.20 bis
chuẩn X.50 lần hai X.50 bis
chùm cluster
chùm lỗi error burst
chuỗi string
chuỗi dữ liệu data chain

chuỗi khóa key stream

chuỗi rỗng null string

chuỗi xung pulse train

chuông một tiếng single stroke bell

chuông rung vibrating bell

chuyên dụng dedicated

chuyên gia an toàn máy tính computer security specialist

chuyên gia bảo vệ có chứng chỉ Certified Protection Professional

chuyên viên kiểm toán audit expert

chuyển đổi mã code conversion

chuyển giao công nghệ DOD DOD Technology Transfer

(sự) chuyển khoản transfer

(sự) chuyển mạch switching

chuyển mạch circuit switching

chuyển mạch đường ngẫu nhiên random line switching

chuyển mạch gói packet switching

chuyển mạch khung frame switching

chuyển mạch kiểm soát truy nhập được phép authorized access control switch

chuyển mạch ngày-đêm Day-Night switch

chuyển mạch nối nhanh fast connect circuit switching

chuyển mạch phân khoảng space division switching

chuyển mạch phân thời time division switching

chuyển mạch số digital switching

chuyển mạch thông báo message switching

chuyển nhanh điện tử electronic vaulting

chuyển nợ debit transfer

chuyển quỹ ngược reverse funds transfer

chuyển tác chuyển tiền funds transfer transaction

chuyển thanh toán cho bên thứ ba third party transfer

(sự) chuyển tiền funds transfer

chuyển tiền điện tử electronic funds transfer

chuyển tiền qua sổ sách book transfer

chuyển tiếp relay

chuyển tiếp định danh tin cậy trusted identification forwarding

chuyển tiếp khung frame relay

chuyển, truy nhập và quản lý tệp file transfer, access and management

chuyển và xử lý công việc job transfer and manipulation

chữ - số alphanumeric

chữ ký (số) signature

chữ ký đã qua trọng tài arbitrated signature

chữ ký điện tử electronic signature

chữ ký Lamport Diffie Lamport Diffie signature

chữ ký phổ dụng universal signature

chữ ký Rabin Rabin signature

chữ ký số digital signature

chữ ký số ElGamal ElGamal digital signature

chữ số có trọng số nhỏ nhất least significant digit

chữ số kiểm tra check digit

chữ số nhị phân binary digit

chức năng an toàn security function

(các) chức năng giao diện phần mềm

software interface functions

(các) chức năng giao tiếp của con người human interface functions

chức năng phân tán distributed function

(tính) chức năng tin cậy trusted functionality

(các) chức năng tới hạn critical functions

chứng chỉ certificate

chứng minh hình thức formal proof

chứng minh không để lộ thông tin zero knowledge proof

chứng minh tính đúng đắn correctness proof

chứng minh tính đúng đắn của chương trình proof of program correctness

chứng minh tri thức không zero knowledge proof

chứng minh với tri thức tối thiểu minimum knowledge proof

chứng thực notarization

chứng thực an toàn phần mềm software security certification

chứng thực thông báo message certification

chương trình program

chương trình an toàn máy tính xếp vào loại mật classified computer security program

chương trình COMPUSEC COMPUSEC

chương trình Comsec Comsec

chương trình con subroutine

chương trình con đệ quy recursive subroutine

chương trình CSTVRP CSTVRP

(các) chương trình của người dùng user programs

chương trình duy trì đánh giá rating maintenance program

chương trình dự phòng bất ngờ contingency program

chương trình đối tượng object program

chương trình GIDEP GIDEP

chương trình khắc phục bảo vệ unprotect

chương trình kiểm soát mạng network control program

chương trình lừa mật khẩu spoofing program

chương trình nạp khóa key loader

chương trình nguồn source program

chương trình nhái mocking brid

chương trình nhận dạng khóa keying identifier

chương trình phân tích độ phức tạp FORTRAN FORTRAN Complexity Analysis Program

chương trình phân tích rẽ nhánh logic logic path analysis program

chương trình SIOP-ESI SIOP-ESI

chương trình tạo khóa key generator

(các) chương trình truy nhập đặc biệt special access programs

chương trình TTAP TTAP

chương trình ứng dụng application program

chương trình ưu tiên foreground program

chương trình xác nhận an toàn truyền thông thương mại Commercial COMSEC Endorsement Program

CIA CIA

có bán COTS

có chặn truy nhập access barred
có khả năng phá mã breakable
có phạm vi rộng lớn galactic
có thể chuyển giao deliverable
có thể giải được tractable
có thể kiểm soát được tractable
codec CODEC
còi rung vibrating horn
con dấu mật mã cryptographic seal
con ngựa (thành) Tơroa Trojan Horse
con rệt điện tử bug
con trỏ pointer
con trỏ ngăn xếp stack pointer
cống thêm piggyback
(sự) cống thêm piggybacking
Consocxiom chứng nhận an toàn hệ thống thông tin quốc tế International Information Systems Security Certification Consortium
(tính) công bằng impartiality
công chứng notarization
công chứng khóa key notarization
công cụ mật mã cryptographic device
công cụ mẫu stub
công cụ phần mềm software tool
(các) công cụ và thiết bị ST&E ST&E tools and equipment
công nghệ technology
công nghệ bảo vệ dữ liệu data protection engineering
công nghệ quan trọng critical technology
công nghệ quân sự quan trọng military critical technology
công nghệ sinh trắc biometrics
công nghệ thông tin information technology
công nghệ tới hạn critical technology
công nghệ tri thức knowledge engineering
công nhận accreditation
(sự) công nhận tác quyền type accreditation
công ty bưu chính viễn thông Post Telegraph and Telephone
công ty bưu điện Post Telegraph and Telephone
công ty truyền thông đa tạp công cộng miscellaneous common carrier
Công ước hỗ trợ hành chính lẫn nhau trong các vấn đề về thuế Convention on Mutual Administrative Assistance in Tax Matters
công việc phụ background job
công việc thứ cấp background job
cổng port
cổng chọn số công cộng public dial port
cổng chọn số riêng private dial port
cổng nối gateway
cổng truy nhập access port
cổng vào gateway
(các) cơ cấu kiểm soát truy nhập access control mechanisms
cơ chế an toàn security mechanism
cơ chế an toàn tỏa khắp pervasive sercurity mechanism
cơ chế chung ít nhất least common mechanism
cơ chế phê chuẩn tham chiếu reference validation mechanism
(các) cơ chế tới hạn an toàn security critical mechanisms
Cơ quan an ninh Quốc gia/Dịch vụ an

toàn trung tâm National Security Agency/Central Security Service

cơ quan cấp chứng chỉ certification authority

cơ quan chứng nhận certification body

cơ quan DARPA DARPA

cơ quan điều chỉnh cước regulatory agency

Cơ quan hàng không và vũ trụ Quốc gia (Hoa Kỳ) National Aeronautics and Space Agency

cơ quan OCI OCI (Office of Computer Information)

cơ quan OPM OPM (Office of Personnel Management)

cơ quan OPNAVINST OPNAVINST

cơ quan OTP OTP

cơ quan ZSI ZSI

cơ số base, radix

cơ số 8 octal

cơ sở base

cơ sở chứng nhận certification authority

cơ sở dữ liệu database

cơ sở dữ liệu AVLOS AVLOS

cơ sở dữ liệu dạng cây tree databases

cơ sở dữ liệu logic logical database

cơ sở dữ liệu mạng network database

cơ sở dữ liệu phân cấp hierarchical database

cơ sở dữ liệu phân tán distributed database

cơ sở dữ liệu quan hệ relational database

cơ sở dữ liệu thống kê statistical database

cơ sở dữ liệu tích hợp integrated database

cơ sở dữ liệu vật lý physical database

cơ sở đánh giá an toàn công nghệ thông tin information technology security evaluation facility

cơ sở hạ tầng khóa công khai PKI

cơ sở kiến thức knowledge base

cơ sở nhận acquirer

cơ sở phát hành thẻ card issuer

cơ sở tài chính financial institution

cơ sở thông tin quản lý an toàn secure management information base

cơ sở tính toán tin cậy trusted computing base

cơ sở tính toán tin cậy mạng network trusted computing base

cơ sở tri thức knowledge base

cờ flag

cỡ từ dữ liệu data word size

crakơ cracker

CSM CSM

cú pháp syntax

cửa sổ truyền transmission window

Cục an ninh Quốc gia NSA (National Security Agency)

cung (từ) sector

cung không chuẩn nonstandard sector

cuộc gọi call

cuộn scrolling

cuộn nhóm rolling up

cửa sau backdoor

cửa sập trapdoor

cửa sổ window

cứng hóa hardwired

cước phí tariff

cường độ từ trường magnetic field intensity

D

DAA DAA

DAC DAC

dải bảo vệ guard band

dải gốc baseband

dải hẹp narrow band

dải ranh giới demarcation strip

dải rộng broadband

dải tần band

dải tần tiếng nói voice band

dải thông bandwidth, passband

dải thông cần thiết neccesary bandwith

dải thông hẹp narrow band

dải tiếng nói voice band

dàn xếp hoàn toàn complete mediation

dạng chuẩn normal forms

dạng chuẩn thứ ba third normal form

dạng chuẩn thứ hai second normal form

dạng chuẩn thứ nhất first normal form

dạng số digital

dạng thông thường normal forms

dạng thức lệnh instruction format

danh mục index

danh mục đầu tư portfolio

danh mục lệnh instruction repertoire

danh mục năng lực capability list

danh mục trù mật dense index

danh mục list

danh pháp nomenclature

danh sách list

danh sách sản phẩm Tempest đã phê duyệt Endorsed Tempest Product List

danh sách đen blacklist

danh sách hỏi lần lượt polling list

danh sách hỏi vòng polling list

danh sách hủy bỏ chứng chỉ certificate revocation list

danh sách khóa key list

danh sách kiểm soát truy nhập access control list

danh sách sản phẩm đã đánh giá Evaluated Products List

danh sách sản phẩm ưu tiên Preferred Products List

danh sách thẻ nóng hot card list

danh sách thu hồi chứng chỉ certificate revocation list

danh sách truy nhập access list

(các) danh sách vắn tắt brevity lists

danh tính thông báo message identifier

dành riêng dedicated

dãy cờ flag sequence

dãy giám sát supervisory sequence

dãy m m-sequence

dãy siêu tăng superincreasing series

dẫn tốc độ pacing

dấu mark
dấu ấn cơ thể body print
dấu báo trước xử lý handling caveats
dấu cách space
dấu đánh dấu burn mark
dấu đốt burn mark
dấu hiệu flag
dấu hiệu mark
dấu hiệu thâm nhập penetration signature
dấu phân tách delimeter
dấu tách delimeter
dấu tách trường field separator
dấu thời gian time stamp
dấu xác thực authenticator
dB db
dB decibel
DBA database administrator
DBMS database management system
DCD data carrier detect
DCE data circuit terminating equipment
DCID DCID
DDL DDL
DDN DDN
DDP DDP
DDS DDS
DEA data encryption algorithm
DEA 2 DEA 2
DEE DEE
DEL delete character
DES data encryption standard
DGP DGP
DGT DGT
(kỹ thuật) di chuyển migration
(phép) dịch shift
dịch vị offset
dịch vụ an toàn security service
dịch vụ BankWire BankWire
(các) dịch vụ cải tiến enhanced services
dịch vụ CashWire CashWire
dịch vụ chuyển mạch gói quốc tế International Packet Switched Service
dịch vụ chuyển thông báo MTS
dịch vụ chữ ký signature service
dịch vụ cơ bản basic service
dịch vụ Data-Star Data-Star
dịch vụ dữ liệu diện rộng wide area data service
dịch vụ đáp lại yêu cầu request reply service
dịch vụ định hướng kết nối connection oriented service
dịch vụ được xác nhận confirmed service
dịch vụ EMS EMS
dịch vụ gói dữ liệu datagram service
dịch vụ gọi ảo virtual call service
dịch vụ Keberos Keberos
dịch vụ không được xác nhận unconfirmed service
dịch vụ không kết nối connectionless service
dịch vụ mạng giá trị gia tăng value added network service
dịch vụ mở open shop
dịch vụ MTS MTS
dịch vụ nối dây wire service
dịch vụ SWFT SWFT
dịch vụ thanh toán payment service
dịch vụ thư điện tử an toàn privacy enhanced mail
dịch vụ trả tiền payment service

dịch vụ truyền thông communication service

(các) dịch vụ viễn tin học teleinformatic services

diễn dịch mạng tín nhiệm TNI

(sự) dịu thêm piggybacking

DIVA data input voice answerback

DML data manipulation language

DMS digital multiplex switching system

dò chất lượng tín hiệu signal quality detector

dò lỗi bằng tín hiệu dội echoplex

dò tìm âm thanh audio detection

dò tìm ngược backtracking

DOD DOD

DODCSC DODCSC

DOE DOE

DON DON

dọn dẹp purging

dọn dẹp tệp file tidying

dọn rác garbage collection

dọn rác liệu garbage collection

dọn tệp file cleanup

dòng line

dòng (ký tự) string

dòng bit bit stream

dòng bit mật mã cryptographic bit stream

dòng dữ liệu data stream

dòng dữ liệu vượt đường biên transborder data flow

dòng đầu trang header

dòng khóa key stream

dồn kênh multiplex

(sự) dồn kênh multiplexing

dồn kênh dữ liệu dataplex

dồn kênh đồng tính homogeneous multiplex

dồn kênh không đồng nhất heterogeneous multiplex

dồn kênh phân bước sóng wavelength division multiplexing

dồn kênh phân khoảng space division multiplexing

dồn kênh phân tần frequency division multiplexing

dồn kênh phân tần frequency multiplexing

dồn kênh phân thời time division multiplexing

dồn kênh phân thời thống kê statistical time division multiplexing, statmux

dồn kênh theo nhu cầu demand multiplexing

dồn kênh thuần nhất homogeneous multiplex

DP DP

DPCM differential PCM

DSA DSA

DTE data terminal equipment

DTI DTI

DTR data terminal ready

dung lượng kênh channel capacity

dùng chung tài nguyên resource sharing

dùng lại đối tượng object reuse

DUV data under voice

duy nhất thống kê statistically unique

(sự) duyệt browsing

duyệt lại mã code review

duyệt qua scan

dư thừa redundancy

dư thừa bảo vệ protective redundancy

dư thừa cấu trúc structural redundancy

dư thừa kép dual redundancy

dư thừa lai hybrid redundancy

(sự) dư thừa mạng network redundancy

dư thừa modun modular redundancy

dư thừa mô đun bội ba triple modular redundancy

dư thừa N modun NMR

dư thừa phần cứng hardware redundancy

dư thừa phần mềm software redundancy

dư thừa thông tin information redundancy

dư thừa thời gian time redundancy

dữ liệu data

dữ liệu bị hạn chế RD (Restricted data)

dữ liệu cá nhân personal data

dữ liệu chỉ dùng chính thức For Official Use Only data

dữ liệu chủ chốt essentiality

dữ liệu (truyền) dạng tiếng nói data in voice

dữ liệu đặc quyền privileged data

dữ liệu được phát đi transmitted data

dữ liệu được tiếp nhận received data

dữ liệu kiểm toán audit data

dữ liệu kiểm tra test data

dữ liệu kinh doanh nhạy cảm sensitive business data

dữ liệu kỹ thuật technical data

dữ liệu nhạy cảm sensitive data

dữ liệu riêng proprietary data

dữ liệu rõ clear data

dữ liệu sai lạc corrupt data

dữ liệu sở hữu proprietary data

dữ liệu tạo khóa keying material

dữ liệu thô raw data

dữ liệu/thông tin xếp vào loại mật classified data/information

dữ liệu thu nhận acquired data

dữ liệu thử nghiệm test data

dữ liệu tiếng data in voice

dữ liệu tĩnh static data

dữ liệu ủy nhiệm credentials

dự án FC-FIPS FC-FIPS

dự kiến tổn thất hằng năm annual loss expectancy

(chế độ) dự phòng standby

dự phòng ấm warm standby

dự phòng cấp một hot standby

dự phòng không gian spatial redundancy

dự phòng mạng chuyển mạch switched network backup

dự phòng nguội cold standby

dự phòng nóng hot standby

dự phòng phần cứng hardware redundancy

dự phòng phần mềm software redundancy

dự phòng/phục hồi backup/restore

dự phòng thứ cấp cold standby

Đ

đa dụng general purpose

(sự) đa hợp multiplexing

đa hợp multiplex

đa liên kết multilink

đa năng general purpose

đa truy nhập cảm biến sóng mang có dò xung đột carrier sense multiple access - collision detection

đa truy nhập phân thời time division multiple access

đa truy nhập phân tần frequency division multiple access

đa tuyến multipath

daemon daemon

đài báo động alarm station

đại diện lưu giữ escow agent

đại lý chuyển thông báo message transfer agent

đại lý người sử dụng user agent

đại số Boole Boolean algebra

đại số logic Boolean algebra

đại số quan hệ relational algebra

đàm thoại conversation

đám cluster

đan xen bit bit interleaving

đan xen ký tự character interleaving

(sự) đánh dấu marking

đánh dấu đặc biệt special marking

(sự) đánh giá evaluation

đánh giá điểm yếu vulnerability assessment

đánh giá mức nhạy cảm sensitivity assessment

đánh giá rủi ro risk assessment

đánh giá tĩnh static evaluation

đánh giá về mặt kinh tế economic assessment

(sự) đánh lừa spoofing

đánh tín hiệu dịch tần frequency shift keying

(sự) đảo inversion

đạo luật 1974 về tính riêng tư privacy Act 1974

đạo luật Quản lý xuất khẩu 1979 Export Administration Act of 1979

đáp answering

(bộ) đáp tự động auto answer

đáp tự động automatic answering

đáp ứng dữ liệu đã nhận đủ positive response

đáp ứng khẩn cấp emergency response

đáp ứng xác thực positive response

đáp ứng yêu cầu request response

đặc quyền privilege

đặc quyền tối thiểu least privilege

đặc tả specification

(các) đặc tả an toàn security specifications

(bản) đặc tả chương trình program specification

đặc tả hình thức mức cao nhất formal top-level specification

đặc tả mô tả mức cao nhất descriptive top-level specification

đặc tả mức cao top-level specification

đăng ký phần mềm software license

đăng nhập log in

đăng nhập log on

đắp vá patch

(sự) đặt bẫy entrapment

(tiền) đặt cọc bổ sung replenishment deposit

(sự) đặt phụ tải loading

đầu cuối terminal

đầu cuối cấu hình không thông minh configurably dumb terminal

đầu cuối chế độ khuôn dạng form mode terminal

đầu cuối chế độ mẫu biểu form mode terminal

(tín hiệu) đầu cuối dữ liệu sẵn sàng data terminal ready

đầu cuối đáp âm thanh audio response terminal

đầu cuối không thông minh dumb terminal

đầu cuối ký tự character terminal

đầu cuối POS point-of-sale terminal

(thiết bị) đầu cuối thông minh smart terminal

đầu ra output

đầu ra thời gian thực realtime output

đầu vào thời gian thực realtime input

đe dọa ngẫu nhiên accidental threat

(chương trình) demon demon

dexiben decibel

để phòng can thiệp tamper-proof

(sự) để lộ compromise, disclosure

đệm padding

đệm báo động trộm burglar alarm pad

đệm dò xâm nhập đường dây chôn buried-line intrusion pad

đệm lưu lượng traffic padding

đĩa cứng hard disk

đĩa đầu cố định fixed head disk

đĩa ghi một lần đọc nhiều lần WORM

đĩa mềm diskette, floppy, floppy disk

đĩa quang optical disk

đĩa quang số optical digital disk

đĩa từ magnetic disk

đĩa WORM WORM

địa chỉ address

địa điểm ấm warm site

địa điểm tách split site

đibit dibit

đích object

đích an toàn security target

đích phản xạ retro target

điểm bán hàng chuyển tiền điện tử electronic funds transfer point of sale

điểm bảo vệ point protection

điểm có phòng máy shell site

điểm cuối bán hàng point of sale

điểm dễ tổn thương có thể khai thác được exploitable vulnerability

điểm không cố định anti-fixed point

điểm kiểm tra checkpoint

điểm lạnh cold site

điểm nguội cold site

(địa) điểm nóng hot site

(địa) điểm nóng khép kín closed hot site

điểm nóng mở open hot site

điểm nối điểm point-to-point

điểm POB POB

điểm POS POS

điểm sự cố quan trọng single point of failure

điểm thanh toán ngân hàng POB

điểm tới điểm point-to-point

điểm trả tiền point of sale

điểm yếu vulnerability

điểm yếu có thể khai thác exploitable vulnerability

điểm yếu hoạt động operational vulnerability

điểm yếu tiềm ẩn potential vulnerability

điểm yếu về cấu trúc construction vulnerability

điểm yếu về kỹ thuật technical vulnerability

điểm yếu xã hội societal vulnerability

điện mật cryptogram

điện thoại chia ô cellular telephone

điện thoại di động cellular radio, cellular telephone

điện thoại và điện báo Post Telegraph and Telephone

(cái) điện trở cuối đường end-of-line resistor

điều biên amplitude modulation

điều biên vuông góc quadrature amplitude modulation

điều biên xung pulse amplitude modulation

(sự) điều biến modulation

điều biến biên độ amplitude modulation

điều biến biên độ vuông góc quadrature amplitude modulation

điều biến biên độ xung pulse amplitude modulation

điều biến dịch pha phase shift keying

điều biến denta delta modulation

điều biến độ rộng xung pulse width modulation

điều biến mã xung pulse code modulation

điều biến mã xung vi sai differential PCM

điều biến pha phase modulation

điều biến tần số frequency modulation

điều biến thời khoảng xung pulse duration modulation

điều biến vị trí xung pulse position modulation

điều biến xung pulse modulation

(sự) điều chế modulation

điều chế mã xung pulse code modulation

điều chế mã xung vi sai differential PCM

điều chế xung pulse modulation

điều gì xảy ra nếu what if

(sự) điều hòa reconciliation

điều khiển đẳng trị isarithmic control

điều khiển liên kết chế độ cơ bản basic mode link control

điều khiển liên kết dữ liệu bậc cao high-level data link control

điều khiển liên kết dữ liệu đồng bộ synchronous data link control

điều khiển liên kết dữ liệu nâng cao advanced data link control

điều khiển luồng flow control

điều khiển luồng thông tin information flow control

(ký tự) điều khiển thiết bị device control

điều khiển tốc độ pacing

(các) điều khoản provisions

điều khoản đổi mới tự động automatic renewal clause

điều kiện dẫn precondition

điều kiện lỗi error condition

điều kiện sau postcondition

điều kiện trước precondition

điều kiện trường hợp xấu nhất worst case condition

điều pha phase modulation

điều phối conditioning

điều tần frequency modulation

điều tra máy tính - 1980 computer inquiry 1980

điều tra nghiên cứu investigation

digital digital

định dạng format

(sự) định dạng formatting

định danh identification

định danh duy nhất unique identification

định danh người dùng mạng network user identification

(sự) định danh thiết bị đầu cuối terminal identification

định giá giá trị của dịch vụ value of service pricing

định giá theo mức độ sử dụng usage sensitive pricing

(sự) định hướng orientation

định hướng thuê nhân công mới new hire orientation

định luật giao hoán commutative law

định luật kết hợp associative law

định luật phân phối distributive law

định luật Shannon Shannon's Law

định lý an toàn cơ bản basic security theorem

định lý Fermat Fermat's Theorem

định lý phần dư Trung Hoa Chinese Remainder Theorem

định lý Trung Hoa Chinese Theorem

định thời clocking

định thời bên ngoài external timing

định thời mạng network timing

định thời phần tử tín hiệu nhận receiver signal element timing

định thời phần tử tín hiệu phát transmitter signal element timing

(sự) định tuyến routing

định tuyến bội multiple routing

định tuyến cấp thời hot potato routing

định tuyến denta delta routing

định tuyến theo thư mục directory routing

định tuyến theo trọng số tối thiểu minimum weight routing

định tuyến thích ứng adaptive routing

định tuyến thích ứng phân tán distributed adaptive routing

định tuyến thích ứng tách ly isolated adaptive routing

định tuyến thích ứng tập trung centralized adaptive routing

định vị thông tin navigation
dịu thêm piggyback
(sự) dịu thêm điện tử electronic piggybacking
đo từ xa telemetering
đỏ red
đoạn segment
đoạn đầu header
đoạn khóa shadow
đoạn mã sửa chương trình program patch
đoạt seize
đọc read
đọc có xóa destructive readout
đọc mật mã decipher
(sự) đọc mật mã decipherment
đọc phá hủy destructive readout
đọc ra không xóa nondestructive readout
đọc/ghi R/W (Read/Write)
đòi hỏi/đáp ứng challenge/response
(sự) đóng dấu endorsement
đóng giả impersonation
(sự) đóng kín encapsulation
đóng lại lockout
(sự) đóng ngắt mạch circuit switching
độ bảo đảm assurance
độ bất định equivocation
độ bất định khóa key equivocation
độ bền strength
độ bí mật confidentiality
độ bí mật ứng dụng application confidentiality
độ cách ly kênh channel isolation
độ cảm ứng từ dư magnetic remanence
độ chi tiết granularity
độ dài bản ghi record length
độ dài đệ quy recursion length
độ dài từ word length
độ đầy đủ logic logical completeness measure
độ kết hạt granularity
độ kháng (từ) coercivity
độ kháng từ cao hico
độ kín confidentiality
độ lệch bias, offset
độ lệch PIN PIN offset
độ mập mờ equivocation
độ mật hoàn thiện perfect secrecy
độ nhạy sensitivity
độ phức tạp complexity
độ phức tạp tuyến tính linear complexity
độ rõ còn lại residual intelligibility
độ rủi ro risk
độ sâu phòng thủ defensive depth
độ tin cậy dependability, reliability
độ tin cậy của dịch vụ reliability of service
độ trễ vào entrance delay
độ từ kháng loco
độ từ kháng cao high coercivity
độ từ kháng thấp low coercivity
độ ưu tiên priority
(tính) độc lập dãy bit bit sequence independence
độc lập dữ liệu vật lý physical data independence
độc lập với máy machine independence
đối chiếu matching
(bên) đối tác counterparty
đối thoại bằng mật khẩu password dialogue

đối tượng object
đối tượng ẩn hidden object
đối tượng khuất hidden object
đối tượng lưu trữ storage object
đối tượng ổn định persistent object
đội chống hiểm họa threat team
đội con cọp tiger team
đội dẫn đường escorts
đội hộ tống escorts
đội phản ứng khẩn cấp máy tính Computer Emergency Response Team
đồng bộ sync, synchronous
đồng bộ bên ngoài external timing
đồng bộ hóa liên tục continuous synchronization
đồng bộ khởi đầu initial synchronization
đồng dư congruent
đồng nguyên tố mutually prime
đồng suất lỗi equal error rate
đồng thủ tục coroutine
đồng thường trình coroutine
(sự) đột nhập penetration
đột nhập qua điện thoại telephone intrusion
đơn công simplex, SPX
đơn cực unipolar
đơn vị dữ liệu datagram
đơn vị dữ liệu dịch vụ service data unit
đơn vị dữ liệu giao diện interface data unit
đơn vị dữ liệu giao thức protocol data unit
đơn vị khởi đầu originator
đơn vị logic logical unit
đơn vị nguyên thủy primitive
đơn vị thuê bao subscriber's unit
đưa hết về số 0 zeroization
đưa ra dump
được kiểm soát bởi người khởi đầu ORCON
(sự) được phép clearance
được tin cậy trusted
được tín nhiệm trusted
đường bao envelope
đường chính bus
đường chủ bus
đường cơ sở baseline
đường dẫn path
đường dây line
đường dây an toàn security line
đường dây báo động reporting line
đường dây không chuyển mạch nonswitched line
đường dây liên kết tie line
đường dây riêng private line
đường nối connection
đường thay thế alternate route
đường thiết bị facility line
đường thuê bao leased line
đường trễ delay line
đường trục chính trunk
đường trục liên kết tie trunk
đường trung chuyển trunk
đường truy nhập access line
đường truyền line
đường truyền tiền mặt cash highway
đường về riêng homerun

E

E0 E0

E1 E1

E2 E2

E3 E3

E4 E4

E5 E5

E6 E6

EAPROM EAPROM

EAROM electrically alterable ROM

ECC error correction code

ECCM ECCM

EDC error detection code

EDP EDP

EDP electronic data processing

EEPROM EEPROM

EFT electronic funds transfer

EIA EIA

EIA Electronic Industries Association

EM electronic mail

EMI electromagnetic interference

EMS EMS

ENQ enquiry character

entropy entropy

EOA end of address

EOB end of block

EOF end of file

EOM end of message

EOT end of transmission

EPOS EPOS (Electronic point of sale)

EPROM electrically programmable read only memory

EPROM EPROM (Erasable Programmed Read Only Memory)

EPROM xóa bằng KEEPROM

EROM EROM (Erasable Read Only Memory)

ESC escape code

ETX end of text

(mạng) Euronet Euronet

EXCLUSIVE OR EXCLUSIVE OR

F

fax facsimile

FC FC

FCC Federal Communication Commission

FD full duplex

FDM frequency division multiplexing

FDMA frequency division multiple access

FDS fixed disk storage

FDX full duplex

FEC forward error correction

FEDS fixed and exchangeable disk storage

FEP front end processor

FIFO first in first out

file bō father file

FIMAS FIMAS (Financial Institution Message Authentication Standard)

FINS FINS (Financial Institution Numbering System)

FIPS FIPS (Federal Information Processing Standard)

floppy floppy

flops flops

FM frequency modulation

FM facilities management

FNF first normal form

FNP front end network processor

foeman formant

FOI FOI (freedom of information)

format format

FRC FRC (Federal Radio Commision)

FRD FRD (Formerly Restricted Data)

FRR FRR

FS field separator

FSK frequency shift keying

FTP FTP (File Transfer Program)

G

G G

galactic galactic

(sự) gán địa chỉ addressing

gán thiết bị device assignment

(sự) gánh thêm điện tử electronic piggybacking

GAO GAO (General Accounting Office)

gần tự an toàn fail soft

(sự) gây mập mờ confusion

gây nhiễu jamming

(sự) gây nhiễu perturbation

(sự) gây nhiễu bằng dữ liệu ngẫu nhiên random data perturbation

(phép) gây nhiễu dựa trên bản ghi record based perturbation

gây nhiễu dựa trên kết quả result-based perturbation

(sự) gây xáo trộn confusion

GF(p) GF(p)

ghép kênh phân thời thống kê statistical time division multiplexing

ghi write

(sự) ghi đè overwriting

ghi lại record

(sự) ghi mật mã encryption

ghi nợ trực tiếp direct debit

GHz GHz

(sự) gia cảm loading

gia công processing

giả danh masquerading

giả mạo forgery, mimicking

(sự) giả mạo masquerade

giả thuyết về kẽ hở flaw hypothesis

giá cước tariff

giá trị đúng good value

giá trị kiểm chứng PIN PIN verification value

giá trị kiểm tra khóa key check value

giá trị kiểm tra mật mã cryptographic checkvalue

giá trị kiểm tra tính nguyên vẹn integrity check value

giá trị mã code value

giá trị mốt mode

giá trị xác minh thẻ card verification value

giai đoạn ngừng (hoạt động) outage

(các) giai đoạn xử lý periods processing

giải điều (chế) demodulation

giải mã decode

giải mã bằng khóa không xác thực spurious key decipherment

giải mật mã decipher, decrypt

(sự) giải mật mã decipherment, decryption

giải phóng vật mang tin ADP clearing ADP media

giải thuật algorithm

(sự) giảm điện áp brownout

(sự) giảm mức (phân loại) sanitization

giảm mức degradation

giám đốc các hệ thông tin information systems director

(sự) giám sát monitoring, supervision

giám sát an toàn sẵn sàng tự động hóa availability-automated security monitoring

giám sát an toàn tự động hóa automated security monitoring

giám sát chuyển tiếp forward supervision

giám sát cuối đường end-of-line supervision

giám sát hiểm họa threat monitoring

giám sát ngược backward supervision

giám sát nhân viên employee monitoring

giám sát tham chiếu mạng network reference monitor

giám sát tham chiếu thành phần component reference monitor

giám sát thuận forward supervision

giám sát tính phần trăm percentage supervision

giám sát từ xa telemonitoring

giám sát xuôi forward supervision

gian lận dữ liệu data diddling

giàn lattice

gián tiếp off line

giành điều khiển bid

giao dịch transaction

giao dịch chuyển tiền funds transfer transaction

giao dịch dữ liệu phân tán bằng sợi quang fiber distributed data interface

giao dịch địa phương local transaction

giao dịch nối gián tiếp indirectly connected transaction

giao dịch nối trực tiếp directly connected transaction

giao dịch trao đổi interchange transaction

giao diện interface

giao diện chương trình ứng dụng application program interface

giao diện nhập/xuất input/output interface

giao diện nối tiếp serial interface

giao diện vào/ra input/output interface

giao tác transaction

giao tác cục bộ local transaction

giao tác nối trực tiếp directly connected transaction

giao thức protocol

giao thức bậc cao high-level protocol

giao thức cảm biến sóng mang carrier sense protocol

giao thức chuyển thư đơn giản simple mail transfer protocol

giao thức cửa sổ trượt sliding window protocol

giao thức DQDB DQDB

giao thức dừng và đợi stop-and-wait protocol

giao thức đầu cuối ảo virtual terminal protocol

giao thức định hướng ký tự character oriented protocol

giao thức đường truyền line protocol
giao thức hướng bit bit oriented protocol
giao thức Internet Internet protocol
giao thức kênh line protocol
giao thức kiểm soát sự truyền dữ liệu transmission control protocol
giao thức kỹ thuật và văn phòng technical and office protocol
giao thức LAP LAP
giao thức MOTIS MOTIS
giao thức NIFTP NIFTP
giao thức P1 P1
giao thức P2 P2
giao thức P3 P3
giao thức TCP/IP TCP/IP
giao thức TELNET TELNET
giao thức truy nhập liên kết LAP
giao thức tự động hóa sản xuất manufacturing automation protocol
giao thức X-modem X-modem
giao thức XON-XOFF XON-XOFF protocol
giấu ô cell suppression
giấu (thông) tin information hiding
giấy báo có credit advice
giấy báo nợ debit advice
giấy phép bọc ni lông shrink-wrapped license, tear-me-open
giấy phép nhị phân binary license
giga giga
GIGO garbage in garbage out
giờ Greenwich trung bình Greenwich Mean Time
giờ quốc tế phối hợp Co-ordinated Universal Time
(sự) giới hạn confinement
giới hạn bảng table restriction
(các) giới hạn bộ nhớ memory bounds
giới hạn xử lý handling restrictions
GISA GISA (German Information Security Agency)
GMT GMT
gói chương trình an toàn dữ liệu data security package
gói dò dấu vết trace packet
gói dữ liệu datagram
gói phần mềm software package
gói rỗng empty slot
gói SMF SMF
gói tin packet
gói UCCI UCCI
gói vạch vết trace packet
gọi ảo có chuyển mạch switched virtual call
gọi chuông trở lại ring back
gọi có lựa chọn selective calling
gọi dữ liệu thường xuyên permanent data call
gọi ngược call back
gọi tự động automatic calling
gốc base
gỡ (bỏ) stripping
gỡ rối debug

H

hacko hacker

hacko Hanover Hanover Hacker

hàm băm hash function

hàm băm một chiều one-way hash function

hàm cửa sập một chiều trapdoor one-way function

hàm Euler Euler totient function

hàm hash hash function

hàm hash một chiều one-way hash function

hàm kiểm tra mật mã cryptographic checkfunction

hàm một chiều one-way function

hàm Snefru Snefru

hàm tuyến tính linear function

hạn chế ô cell restriction

(các) hạn chế vượt đường biên transborder restrictions

hàng đợi queue

hãng AT&T AT&T

hãng Bundespost Bundespost

hãng Datasolve Datasolve

hãng phần mềm software house

hãng truyền thông chuyên dụng specialized common carier

hãng truyền thông công cộng common carrier

hạng category, rank

hạng một one category

(các) hạng mục tiện ích quân sự bên trong Items of Intrinsic Military Utility

hạng truy nhập access category

hartley hartley

hạt giống seed

hatli hartley

HD half duplex

HDLC high-level data link control

HDX half duplex

hec hertz

hệ system

(các) hệ an toàn cài sẵn building security systems

hệ AOSS AOSS

hệ báo cháy bổ trợ auxiliary fire alarm system

hệ báo động lớp A Class A alarm system

hệ báo động lớp B Class B alarm system

hệ báo động mã hóa coded alarm system

hệ biểu đồ chỉ báo graphic annunciator

hệ CHAPS CHAPS

hệ chẩn đoán diagnostics

hệ che giấu concealment system

hệ chỉ báo annunciator

hệ CHIPS CHIPS

(các) hệ chuyên gia expert systems

hệ chuyển mạch dồn kênh số digital multiplex switching system

hệ chuyển tải dữ liệu data transport system

hệ CISA CISA

hệ công dụng kép dual use system

hệ CRAMM CRAMM

hệ dữ liệu (bên) dưới tiếng nói data under voice

hệ dữ liệu (bên) trên tiếng nói data above voice

hệ dựa trên tri thức thông minh intelligent knowledge based system

hệ đánh giá cảnh báo alarm assessment system

hệ đĩa chủ disk server

hệ đĩa secvơ disk server

hệ điện thoại vô tuyến cellular radio

hệ điều hành operating system

hệ điều hành an toàn secure operating system

hệ điều hành an toàn chứng minh được PSOS

hệ điều hành an toàn nhân hóa KSOS

hệ điều hành Unix Unix

hệ điều vận bằng toàn tác transaction driven system

hệ độc lập mã code independent system

hệ được nhúng embedded system

hệ EFTS EFTS

hệ gia dụng tích hợp integrated home system

hệ giám sát kép double-supervised system

hệ giao tác dẫn hướng transaction driven system

hệ Guardwire Guardwire

hệ halon halon system

hệ hiển thị dữ liệu videotex

hệ hỗ trợ quyết định decision support system

hệ IDES IDES

hệ không mã noncoded system

hệ KNS KNS (key notarization system)

hệ KSOS KSOS

hệ logic phân tán distributed logic

hệ lõng embedded system

hệ mã code system

hệ mã hóa coded system

hệ mã khóa không đối xứng asymmetric key system

hệ mật khẩu password system

hệ mật mã không đối xứng asymmetric cryptosystem

hệ MMS MMS

hệ mở open system

hệ MVS MVS

hệ PACX PACX

hệ phát hiện đột nhập intruder detector system

hệ phương pháp luận giả thuyết về kẽ hở flaw hypothesis methodology

hệ phương pháp luận phát triển hình thức Ina Jo Ina Jo Formal Development Methodology

hệ phương pháp luận phát triển phân cấp hierarchical development methodology

hệ phương pháp RISKCALC RISKCALC

hệ PSOS PSOS

hệ quản lý cơ sở dữ liệu database management system

hệ SAGITTAIRE SAGITTAIRE

hệ SAISS SAISS

hệ sóng mang carrier system

hệ số dịch chuyển shift factor

hệ số làm việc work factor

hệ số năng suất mật mã cryptographic throughput factor

hệ SPEED SPEED

hệ thanh toán điện tử electronic system for payments

hệ thống báo dựa trên máy tính computer based message system

hệ thống tin information system

Hệ thống tin tự động hóa Automated Information System

hệ thống system

hệ thống bảo vệ bằng khóa và chìa lock-and-key protection system

Hệ thống báo cáo những vụ việc liên quan tới thi hành luật Law Enforcement Incident Reporting System

hệ thống báo cháy tại chỗ local fire alarm system

hệ thống báo động tại chỗ local alarm system

hệ thống báo hỏa riêng proprietary fire alarm system

hệ thống báo hỏa từ xa remote station fire alarm system

hệ thống báo trước presignal system

hệ thống Buddy The Buddy System

hệ thống chìa khóa trao tay turnkey system

hệ thống con được bảo vệ protected subsystem

hệ thống công chứng khóa KNS (key notarization system)

hệ thống cục bộ local network

hệ thống cửa sổ trượt sliding window system

hệ thống dịch vụ thanh toán bù trừ tự động hóa của các ngân hàng Bankers Automated Clearing Services

hệ thống dựa trên quy tắc rule-based system

hệ thống đĩa tháo gỡ được removable cartridge disk

hệ thống điện thoại an toàn secure telephone system

hệ thống được giám sát supervised system

hệ thống FedWire FedWire

hệ thống giám sát đơn single supervised system

hệ thống khóa đối xứng symmetric key system

hệ thống khóa giao dịch transaction key system

hệ thống không quy tắc noncoded system

hệ thống kiểm soát mạng network control system

hệ thống kiểu McCulloh McCulloh-type system

hệ thống mã chính master code system

hệ thống mã đối xứng one key cryptosystem

hệ thống mã đối xứng symmetric cryptosystem

hệ thống mã hai khóa two-key cryptosystem

hệ thống mã hóa cipher system

hệ thống mã lựa chọn selective coded system

hệ thống mã một khóa one key cryptosystem

hệ thống mạng network system

hệ thống máy tính dùng chung tài nguyên resource sharing computer system

hệ thống máy tính dùng chung tài nguyên truy nhập được từ xa remotely accessed resource-sharing computer system

hệ thống máy tính tin cậy trusted computer system

hệ thống mật mã cryptographic system, cryptosystem

hệ thống MC MC system

(các) hệ thống mở open systems

(các) hệ thống nhạy cảm sensitive systems

hệ thống phát hiện cơ động portable detector system

hệ thống phân tán có bảo vệ protected distribution system

hệ thống phân tán nối dây có bảo vệ protected wireline distribution system

hệ thống phê chuẩn tính hợp lệ MAC MVS

hệ thống quản lý mạng network management system

hệ thống STU-III STU-III

Hệ thống Thông báo Quân sự MMS

hệ thống tin cậy trusted system

hệ thống trạm xa remote station system

hệ thụ động slave

hệ thức truy toán tuyến tính linear recurrence relation

hệ truyền số digital transmission system

hệ truyền văn bản video videotex

hệ xử lý dữ liệu tự động Automatic Data Processing System

hết giờ time out

hiểm họa threat

(các) hiểm họa an toàn security threats

hiểm họa bị động passive threat

hiểm họa chủ động acvite threat

hiểm họa có chủ tâm deliberate threat

hiểm họa giả định postulated threat

hiểm họa logic logical threat

hiểm họa tình cờ accidental threat

hiểm họa vật lý physical threat

hiển thị dữ liệu viewdata

hiện tượng van Eck van Eck phenomenon

hiệp hội AFCEA AFCEA

hiệp hội ASA ASA

Hiệp hội bảo vệ điện trạm trung tâm Central Station Electrical Protection Association

Hiệp hội công nghiệp điện tử Electronic Industries Association

hiệp hội FIU FIU (Federation of Information Users)

Hiệp hội máy tính Association for Computing Machinery

Hiệp hội quốc tế về thẻ vi mạch International Association for Microcircuit Cards

Hiệp ước giúp tuân thủ luật pháp chung Mutual Legal Assistance Treaty, MLAT

Hiệp ước hỗ trợ luật pháp lẫn nhau MLAT

Hiệp ước Schengen Treaty of Schengen

hiệu chỉnh phòng lỗi forward error correction

hiệu quả effectiveness

hiệu quả che chắn shielding effectiveness

hiệu ứng Wiegand Wiegand effect

(sự) hình thành dữ liệu data origination

hình thức formal

hmc one-way function

họ family

hỏa hoạn lớp A Class A fire

hỏa hoạn lớp B Class B fire

hỏa hoạn lớp C Class C fire

hoán vị permutation

hoạt động activity

hoạt động đại lý agency activity

hoạt động hỗ trợ housekeeping

(sự) hoạt động liên tục continuity of operations

hoạt động mật mã ngoại tuyến off line crypto-operation

hoạt động mật mã trực tuyến on line crypto-operation

hoạt động ngân hàng từ xa telebanking

hoạt động song song parallel operation

hoạt động thời gian thực realtime operation

hoạt động tình báo espionage

học trở ngược backwards learning

hỏi gọi xoay vòng roll call polling

hỏi riêng ad hoc enquiry

hỏi vòng trung tâm hub polling

hỏi vòng tự động automatic polling

hỏi vòng vị trí site polling

hỏi/đáp challenge/response, inquiry/response

hỏng hóc bug

hồ sơ đặc quyền privilege profile

hồ sơ kiểm soát nội bộ internal control documentation

hồ sơ lược tả profiles

hồ sơ người sử dụng user profile

hồ sơ thâm nhập penetration profile

hỗ trợ an toàn add-on security

hỗ trợ nội bộ internal reciprocal

hồi tiếp bản mã cipher feedback

hồi tiếp mã theo byte byte cipher feedback

hồi tiếp xuất output feedback

hội AFNOR AFNOR

hội IERE IERE (Institution of Electronic and Radio Engineers)

hội nghị CEPT CEPT

hội nghị từ xa teleconferencing

hội sở phát hành issuer

hội thoại conversation

hộp nắp trong suốt hat box

hộp P P box

hộp S S box

hộp thay thế substitution box

hộp thư điện tử electronic mailbox, mail box

hở vòng loophole

hợp đồng gói gọn shrink-wrapped license

hợp mạng hệ mở open systems interconnection

hợp ngữ assembly language

hợp số composite

(sự) hủy bỏ cancellation

hủy cuộc gọi cancel call

hủy nối kết aborted connection

hủy vô tình dữ liệu accidental destruction

hư hỏng corruption

hướng dẫn DODD DODD

I

I-4 I-4

I&A I&A

IA5 IA5

IAC IAC

IC integrated circuit

ID ID

ID identification character

ID người dùng user id

IDA IDA

IDE IDE

IEC IEC

IEE IEE (Institution of Electrical Engineers)

IEEE IEEE (Institute of Electrical and Electronics Engineering)

IFIP IFIP

IIL integrated injection logic

IIS I Inf Sc (Institute of Information Scientists)

INWG International Network Working Group

INTAMIC International Association for Microcircuit Cards

(mạng) Internet Internet

I/O điều khiển bằng ngắt interrupt controlled I/O

IPSE IPSE

IPSS International Packet Switched Service

IR information retrieval

ISDN integrated services digital network

ISN ISN (Input Sequence Number)

ISO-7 ISO-7

ISOA ISOA (Information Security Officer's Assistant)

ISSA ISSA (Information Systems Security Agency)

ISSO ISSO (Information Systems Security Officer)

IT information technology

ITAR ITAR (International Traffic in Arms Regulations)

ITB intermediate text block

ITU International Telecommunications Union

IV&V Independent Verification ard Validation

K

kẻ đột nhật intruder

kẻ lạm dụng điện thoại phreak

kẻ lạm dụng điện thoại - máy tính phracker

kẻ phá hoại crasher

kẻ phá hoại hệ thống system saboteur

kẻ phá khóa cracker

kẻ tấn công attacker

kẻ trộm thiết bị đầu cuối terminal thief

kẻ xâm nhập intruder

kẽ hở flaw

kẽ hở an toàn breach, security breach

kẽ hở giả pseudo-flaw

kế hoạch an toàn máy tính computer security plan

(các) kế hoạch bất thường contingency plans

kế hoạch dự phòng backup plan

kế hoạch dự phòng người dùng user alternative plan

kế hoạch đáp ứng khẩn cấp emergency response plan

kế hoạch hóa khôi phục kinh doanh business recovery planning

kế hoạch hóa phục hồi kinh doanh business resumption planning

kế hoạch khẩn cấp emergency plan

kế hoạch khôi phục sau sự cố disaster recovery plan

kế hoạch khôi phục thảm họa ứng dụng application disaster recovery plan

kế hoạch phòng sự cố disaster plan

kế hoạch thay thế cho người dùng user alternative plan

kênh an toàn secure channel

kênh analog analog channel

kênh bí mật covert channel, secure channel

kênh bộ chọn selector channel

kênh cấp tiếng nói voice grade channel

kênh chuyên dụng dedicated channel

kênh chuyển tiếp forward channel

kênh công khai overt channel

kênh dải rộng wideband channel

kênh dẫn xuất theo thời gian time-derived channel

kênh dồn byte byte multiplex channel

kênh dồn khối block multiplexer channel

kênh dữ liệu data channel

kênh định thời bí mật covert timing channel

kênh định thời ngầm covert timing channel

kênh được giám sát supervised line

kênh hạn chế confinement channel

kênh khai thác được exploitable channel

kênh lân cận adjacent channel

kênh logic logical channel

kênh mang thông tin information bearer channel

kênh ngầm covert channel

kênh ngược backward channel

kênh nhập/xuất input/output channel

kênh nhớ bí mật covert storage channel

kênh nhớ ngầm covert storage channel

kênh phụ secondary channel

kênh phương tiện facility line

kênh thông cao bearer

kênh thuận forward channel

kênh thứ cấp secondary channel

kênh tin cậy trusted channel

kênh truyền thông communication channel

kênh tuân thủ an toàn security compliant channel

kênh tương tự analog channel

kênh xuôi forward channel

kết nhóm grouping

kết nối connection

kết nối chung các hệ thống mở open systems interconnection

kết nối dữ liệu data connection

kết nối vi khối chính micro mainframe link

kết thúc địa chỉ end of address

kết thúc khối end of block

kết thúc tệp end of file

kết thúc thông báo end of message

kết thúc truyền end of transmission

kết thúc văn bản end of text

kết xuất dump

kết xuất chọn lọc selective dump

(sự) kết xuất đã định dạng formatted dump

kết xuất phòng sự cố rescue dump

kết xuất tĩnh static dump

khả năng capability

khả năng bảo trì maintainability

khả năng bị tấn công tiềm ẩn potential vulnerability

khả năng chấp nhận của người dùng user acceptability

khả năng cùng hoạt động interoperability

khả năng dùng lại reusability

khả năng kháng lỗi fault tolerance

khả năng lặp lại repeatability

khả năng liên vận hành interoperability

khả năng tái tạo reproducibility

khả năng truy nhập kiểm soát được controlled accessibility

khách hàng customer

khai thác dữ liệu data mining

khái niệm đỏ/đen red/black concept

khái niệm giám sát tham chiếu reference monitor concept

khảo sát investigation

khắc phục trót lọt defeat

khẳng định nhận affirmative acknowledgement

khe thông báo message slot

khe trống empty slot

kho lưu archive

kho lưu trữ mở open storage

khóa key, lock

khóa bản ghi record lock

khóa bán yếu semiweak key

khóa chạy running key
khóa chạy thử test key
khóa chặn lockout
khóa chính master key, primary key
(được) khóa chống sao chép copy protected
khóa chống sao chép copy protection
khóa con sub-key
khóa công khai public key
khóa dài long key
khóa dấu xác thực authenticator key
khóa dữ liệu data key
khóa dự phòng candidate key
khóa đối ngẫu palindromic key
(các) khóa gắn nhãn tagged keys
khóa giao dịch transaction key
khóa kép dual key
khóa khử ghép decoupling key
khóa kiểm tra check key
khóa liên động interlock
khóa mã dữ liệu data-encrypting key
khóa mã đơn cho mạng netkey
khóa mã khóa key-encrypting key
khóa mật secret key
khóa mật mã cryptographic key, crypto-key
khóa nguyên vẹn integrity locking
khóa nhận dạng thực thể entity identifier
khóa phần cứng dongle
khóa phiên session key
khóa phụ secondary key
khóa riêng native key, private key
khóa tách riêng decoupling key
khóa terminal terminal key
khóa tệp file lock
khóa thẻ card key
khóa thiết bị đầu cuối terminal key
khóa thứ cấp candidate key, secondary key
khóa tìm kiếm search key
khóa trao đổi interchange key
khóa tự đối ngẫu anti-palindromic key
khóa xác thực authentication key
khóa yếu weak key
khoản item
khoang compartment
khoảng range
(các) khoảng có hệ thống systematic ranges
khoảng duy nhất unicity distance
khoảng lệch offset
khoảng trống space
(sự) khoanh vùng compartmentalization
(sự) khôi phục recovery
khôi phục rollback*
khối block
khối cuối mạng network termination unit
khối dồn kênh channel bank
khối điều khiển truyền thông communications control unit
khối hiển thị trực quan VDU
khối logic logical unit
khối lượng công việc/tháng man month
khối mật mã cipher block
khối thích ứng đường truyền line adaptor unit
khối tín hiệu burst
khối xác thực thông báo message authentication block
khối xếp heap

không cân xứng biased
không chối bỏ nonrepudiation
không đồng bộ asynchronous
không giải được intractable
không gian bản mã cryptogram space
không gian địa chỉ riêng private address space
không gian được kiểm soát controlled space
không gian khóa key space
không gian kiểm soát vật lý physical control space
không gian thông báo message space
không hợp đồng no contract
không khả quyết undecidable
không mật unclassified
không nhận denial
không phân mức truy nhập uncleared
không phổ biến ra nước ngoài NOFORN
không thể thực hiện về mặt tính toán computationally infeasible
không tin cậy untrusted
không trở về không nonreturn to zero, NRZ
không từ chối nonrepudiation
không tương thích noncompatibility
không xếp vào loại mật unclassified
khống chế suy luận inference control
(sự) khởi đầu kết hợp sai spurious association initiation
khởi động lại reset
khởi động lại nguồn power restart
khởi động lại ở điểm kiểm tra checkpoint restart
khởi động nguội cold start
khởi nhập sign in, sign on
khởi sinh dữ liệu data origination
khớp nối interface
khu vực bảo vệ protection pattern
khung (bit) frame
khung báo nhận acknowledgement frame
khung dữ liệu data frame
khung nhìn view
khung trang page frame
khung xem view
khuôn format
khuôn lệnh instruction format
khuôn mẫu template
khuôn (thức) thông báo message format
khuôn thức format
(các) khuyến nghị xeri V của CCITT V-Series recommendations of CCITT
(các) khuyến nghị xeri X của CCITT X-Series recommendations of CCITT
khử phân loại các phương tiện nhớ từ tính declassification of magnetic storage media
khử từ degauss, deperm
kích cỡ khối block size
kích hoạt activation
kích thước khối block size
kích thước từ dữ liệu data word size
(sự) kiểm chứng verification
kiểm chứng cài đặt implementation verification
kiểm chứng chữ ký động dynamic signature verification
kiểm chứng hình thức formal verification
(sự) kiểm chứng thiết kế design

verification

kiểm dư vòng cyclic redundancy check

kiểm định thâm nhập penetration testing

kiểm định tính an toàn security testing

(các) kiểm soát an toàn đường cơ sở baseline security controls

(các) kiểm soát an toàn nội bộ internal security controls

kiểm soát cấu hình configuration control

kiểm soát chống lặp overlap control

kiểm soát dựa trên kiểm toán audit based control

kiểm soát điểm tới điểm end-to-end control

kiểm soát định tuyến routing control

kiểm soát đối ngẫu dual control

kiểm soát đường truyền line control

(các) kiểm soát EDP EDP controls

kiểm soát hỏi vòng polling

kiểm soát kép dual control

kiểm soát không nhớ memoryless control

kiểm soát kích thước tập câu truy vấn query set size control

kiểm soát luồng dữ liệu data flow control

kiểm soát luồng thông tin information flow control

kiểm soát lừa đảo máy tính computer fraud control

kiểm soát mật mã cryptographic control

(các) kiểm soát nội bộ internal controls

kiểm soát quay số dial-up control

kiểm soát suy luận inference control

kiểm soát sự cố failure control

kiểm soát theo tuyến path scrutiny

(sự) kiểm soát thứ tự order control

kiểm soát tiên nghiệm a priori control

kiểm soát tranh chấp contention control

kiểm soát truy nhập bắt buộc mandatory access control

kiểm soát truy nhập dựa trên danh tính identity based access control

kiểm soát truy nhập dựa trên quy tắc rule-based access control

kiểm soát truy nhập hướng người dùng user-directed access control

kiểm soát truy nhập hướng người sử dụng UDAC

kiểm soát truy nhập access control

kiểm soát truy nhập kiểu lấy - cấp take-grant access control

kiểm soát truy nhập logic logical access control

kiểm soát truy nhập máy chủ host access control

kiểm soát truy nhập phụ thuộc ngữ cảnh context dependent access control

kiểm soát truy nhập phụ thuộc nội dung content dependent access control

kiểm soát truy nhập theo hành chính administratively directed access control

kiểm soát truy nhập trung gian medium access control

kiểm soát truy nhập tùy ý discretionary access control

kiểm soát truy nhập tùy ý mạng network discretionary access control

kiểm soát truy vấn ngầm định implied

queries control

kiểm soát tương đối giới hạn bảng relative table size control

kiểm soát và phân phối khóa key distribution and control

kiểm soát luồng flow control

kiểm toán audit

(sự) kiểm toán auditing

kiểm toán an toàn security audit

kiểm toán an toàn ngoài external security audit

kiểm toán an toàn nội bộ internal security audit

kiểm toán định kỳ periodic audit

kiểm toán lồng sẵn embedded audit

kiểm toán lồng trong embedded audit

kiểm toán nội bộ internal audit

kiểm toán tính an toàn hệ thống system security audit

kiểm toán tự động hóa automated audit

kiểm toán viên nội bộ internal auditor

kiểm tra audit

kiểm tra bằng tín hiệu đội echocheck

kiểm tra các giới hạn bộ nhớ memory bounds checking

kiểm tra chẵn lẻ dọc longitudinal party check

(phép) kiểm tra dư thừa redundancy checking

kiểm tra dư thừa dọc longitudinal redundancy check, LRC, vertical redundancy check

kiểm tra giới hạn bounds checking

kiểm tra hệ thống tệp file system check

kiểm tra ký tự khối block character check

kiểm tra mạch veincheck

kiểm tra modulo N modulo N check

kiểm tra nghiệm thu acceptance inspection

kiểm tra nội bộ internal audit

kiểm tra tại bàn desk checking

kiểm tra tham số không đầy đủ incomplete parameter checking

kiểm tra thâm nhập penetration testing

kiểm tra thiết bị equipment check

kiểm tra thông tin từ giấy loại dumpster diving

kiểm tra tính chẵn lẻ odd even check

kiểm tra tính chẵn lẻ parity checking

kiểm tra tính đầy đủ completeness check

kiểm tra tính hợp lệ validity checking

kiểm tra tính hợp lệ của dữ liệu nhập input data validation

kiểm tra tính hợp lý reasonableness check

kiểm tra tính liên tục continuity check

kiểm tra tính phù hợp compliance testing

kiểm tra tính tuân thủ compliance testing

kiểm tra tổng khối block sum check

kiểm tra tổng số summation check

kiểm tra tuần tự trung tâm hub polling

kiểm tra tư cách cá nhân personal verification

kiểm tra và đánh giá tính an toàn security test and evaluation

kiểm tra viên nội bộ internal auditor

kiểm tra vòng lặp loop checking

kiểm truy access control

kiến trúc architecture

kiến trúc an toàn security architecture

kiến trúc an toàn dữ liệu data security architecture

kiến trúc an toàn hệ thống số phân tán digital distributed system security architecture

kiến trúc an toàn mạng network security architecture

kiến trúc hai tầng two-layer architecture

kiến trúc khóa ba lớp three-layer architecture

kiến trúc kiểu vỏ hành onion skin architecture

kiến trúc mạng network architecture

kiến trúc mạng hệ thống system network architecture

kiến trúc mật mã phổ biến common cryptographic architecture

kiến trúc phân tầng onion skin architecture

kiến trúc von Neumann von Neumann

kiểu mode; type

kiểu dịch vụ service type

kiểu dữ liệu data type

kiểu dữ liệu trừu tượng abstract data type

kiểu khách hàng customer type

kiểu sản phẩm product type

kiểu tấn công mode of attack

kiểu tiền funds type

kiểu truy nhập access type

kỳ hạn term

kỹ thuật băm hashing

kỹ thuật cung mờ fuzzy sector technique

kỹ thuật DMA direct memory access

kỹ thuật liên kết phần cứng hardware handshaking

kỹ thuật MICR MICR

kỹ thuật phân tích ngược reverse engineering

kỹ thuật phần mềm software engineering

kỹ thuật salami salami technique

ký hiệu định danh identifier

ký hiệu MID MID

ký hiệu nhận dạng identifier

ký hiệu nhận dạng cá nhân personal identifier

ký hiệu nhận dạng chứng nhận certificate identifier

ký hiệu nhận dạng khóa keying identifier

ký hiệu nhận dạng thông báo message identifier

ký hiệu nhận dạng thông báo MID

ký pháp cú pháp trừu tượng 1 abstract syntax notation 1

ký tự character

ký tự báo nhận acknowledge character

ký tự DEL delete character

ký tự điền fill character

ký tự điều khiển control character

ký tự điều khiển gọi call control character

ký tự định danh identification character

ký tự đồng bộ SYN

ký tự hỏi enquiry character

ký tự hủy cancel character

ký tự hủy khối block cancel character

intermediate text block

ký tự không hợp pháp illegal character

ký tự khởi đầu thông báo SOM

ký tự lấp đầy fill character

ký tự mở rộng mã code extension character

ký tự nhắc chú ý attention character

ký tự nhận dạng identification character

ký tự rỗi idle character

ký tự rỗi đồng bộ synchronous idle character

ký tự sai illegal character

ký tự SYN SYN

ký tự tách bản ghi record separator character

ký tự thay thế substitute character

ký tự thoát escape character

ký tự trên giây, cps, CHPS characters per second

ký tự trống space

ký tự xóa khối block cancel character

L

lá an toàn foil

lá chắn mạng network guard

(sự) lách qua mạng network weaving

(sự) làm cho khớp reconciliation

làm giảm mức sanitizing

làm hay mua make v. buy

làm lại khóa re-key

(sự) làm lộ compromise, disclosure

(sự) làm lộ không được phép unauthorized disclosure

làm mịn đúng correct refinement

làm sạch purging

làm tròn có hệ thống systematic rounding

làm tròn có kiểm soát controlled rounding

làm tròn kiểu Pháp French roundoff

làm tròn ngẫu nhiên random rounding

lạm dụng hệ thông tin information system abuse

lạm dụng máy tính computer abuse

lan truyền lỗi error propagation

lát thời gian time slice

lắp dư modun modular redundancy

lắp/gỡ gói tin packet assembler/disassembler

lặp iteration

(phát) lặp lựa chọn selective repeat

lần ngược backtracking

lập bảng thông báo điện tử electronic messaging

lập chỉ mục index build

lập chỉ số index build

lập danh sách list

lập địa chỉ address

(sự) lập địa chỉ addressing

lập kế hoạch phòng sự cố disaster planning

(sự) lập mô hình modeling

(sự) lập ngày tháng sử dụng aging

lập trình programming

lập trình tự gói packet sequencing

lấy mẫu enrolment, sampling

(sự) lấy trộm thông tin wiretapping

(sự) len lỏi qua mạng network weaving

lệch bias

lệnh instruction

lệnh ác ý malicious code

lệnh bảo vệ safeguarding statement

lệnh cập nhật commit

(câu) lệnh chương trình program statement

lệnh đặc quyền privilege instructions

lệnh hỏi tuyến tính linear query

lệnh mã máy machine code instruction

lệnh nhập/xuất input/output statement
lệnh rút tiền draw down
lệnh SOW SOW (Statement of Work)
lệnh SON SON (Statement of Need)
lệnh truy vấn tuyến tính linear query
liếc trộm qua vai shouldering, shoulder surfing
liên cụm cluster
Liên đoàn viễn thông quốc tế International Telecommunications Union
(mệnh đề) liên hệ relationship
liên hiệp AFIPS AFIPS
liên kết chaining
liên kết chức năng binding of functionality
liên kết dồn kênh tốc độ cao high-speed multiplex link
liên kết dữ liệu data link
liên kết khối mật mã cipher block chaining
liên kết mã dòng stream cipher chaining
liên kết mạng Internetworking
liên kết mật mã khối block cipher chaining
liên kết truyền thông communication link
liên lạc communication
liên lạc dữ liệu data communications
liên lạc giữa các quá trình interprocess communication
liên lạc hữu tuyến line communications
liên lạc song song parallel communication
liên lạc viễn thông telecommunications
(sự) liên tục của các hoạt động continuity of operations
liệt kê list
linh động tần frequency agility
loại category
loại hình bội multiple categories
loại hình category
Loại I Type I
loại một one category
loại phương tiện facility type
loạt xung pulse train
(phép) lọc filtering
(sự) lọc xóa scrubbing
loga logarithm
(mạch) logic logic
(thuộc) logic logical
logic ác ý malicious logic
logic độc hại malicious logic
lõi core
lõi sợi quang core
(sự) lộ bí mật cá nhân personal disclosure
(sự) lộ bí mật phủ nhận negative disclosure
lỗi error
lỗi cứng hard error
lỗi loại 1 Type 1 error
lỗi loại 2 Type 2 error
lỗi mềm soft error
lỗi nhẹ soft error
lỗi phụ thuộc mẫu pattern sensitive fault
lỗi rồi bug
lỗi thất thường intermittent error
lớp dịch vụ class of service
lớp đa thức không tất định nondeterministic polynomial class
lớp F-AV F-AV

lớp F-B1 F-B1

lớp F-B2 F-B2

lớp F-B3 F-B3

lớp F-C1 F-C1

lớp F-C2 F-C2

lớp F-DC F-DC

lớp F-D1 F-D1

lớp F-DX F-DX

lớp F-IN F-IN

lớp NP NP Class

lớp P P Class

Luật an toàn máy tính 1987 Computer Security Act of 1987

Luật an toàn máy tính 1988 Computer Security Act of 1988

luật Bundesdatenschutzgesetz Bundesdatenschutzgesetz

luật cấm blocking law

luật ngăn chặn blocking law

Luật về lạm dụng máy tính 1990 Computer Misuse Act 1990

lục rác scavenging

luồng bit bit stream

luồng dữ liệu data stream

lũy thừa power

lừa đảo thẻ trắng white card fraud

lực kháng từ coercive force

lược đồ schematic

lược đồ chia sẻ khóa mật secret sharing scheme

lược đồ con subschema

lược tả profile

lược tả GOSIP GOSIP

lược tả người dùng user profile

lưới lattice

lưới cảm biến grid sensor

lưỡng cực bipolar

lượng công việc xử lý dữ liệu tới hạn critical data processing workload

lượng logic logical

lượng thông tin information content

lượng tiền lưu chuyển hiện tại current utilization

lượng tiền sử dụng hiện thời current utilization

lượng tử phổ dụng universal quantifier

lượng tử hóa quantize

lưu lượng tin traffic

lưu lượng tới incoming traffic

lưu trữ archive

lưu và chuyển tiếp store and forward

lưu và chuyển tiếp tiếng nói voice store and forward

lý thuyết thông tin information theory

lý thuyết truyền thông communication theory

M

ma trận matrix

mã code

mã ác ý malicious code

mã ASCII ASCII

mã ba lô knapsack cipher

mã Baudot Baudot code

mã biến cố event code

mã Caesar Caesar cipher

mã chẩn đoán diagnostic code

mã chu trình cyclic code

mã chuẩn của Mỹ để trao đổi thông tin USASCII

mã chuyển vị transposition cipher

mã chứng nhận certificate

mã "con quỷ bánh bao" cookie monster

mã cộng additive cipher

mã cờ flag code

mã DC1 DC1

mã DC4 DC4

mã dịch shift code

mã dòng stream cipher

mã dòng đồng bộ synchronous stream cipher

mã dư redundant code

mã dữ liệu quân sự field data code

mã đa biểu polyalphabetic cipher

mã đa thức polynomial code

mã điều khiển control token

mã định danh người sử dụng mạng network user identity

mã đối tượng object code

mã đồng nhất identity

mã EBCDIC EBCDIC code

mã ElGamal ElGamal cipher

mã giao tác transaction code

mã Gray Gray code

mã Hamming Hamming code

mã hệ thống system code

mã hóa encipher, encode, encrypt

(phép) mã hóa encryption

mã hóa dạng mắt cáo trellis coding

mã hóa điểm tới điểm end-to-end encryption

mã hóa khóa mật secret key encryption

mã hóa không đảo được irreversible encryption

mã hóa Manchester Manchester encoding

mã hóa mạng network encryption

mã hóa trực tuyến on line encryption

mã hợp pháp authorization code

mã Huffman Huffman code

mã kết nối link encryption

mã kết thúc tail

mã khách hàng customer code

mã kiểm chứng khóa key verification code

mã kiểm tra test

mã knapsack knapsack cipher

mã ký tự character code

mã lại thành khóa chính re-encipher to master key

mã lại từ khóa chính re-encipher from master key

mã liên kết link encryption

mã liên kết dữ liệu data link encryption

mã MDC MDC

mã N sai M bit M out of N code

mã nằm chờ ambush code

mã nguồn source code

mã nhận dạng identifier code

mã nhận dạng cá nhân PIC

mã nhận dạng thẻ card identification code

mã nhị phân binary code

mã pháp cipher

mã pháp ba lô Graham-Shamir Graham-Shamir knapsack cipher

mã pháp ba lô Merkle-Hellman Merkle-Hellman knapsack cipher

mã pháp dạng ống pipeline cipher

mã pháp dòng stream cipher

mã pháp dùng khóa một lần one-time pad

mã pháp đối xứng symmetric cipher

mã pháp đơn biểu monoalphabetic cipher

mã pháp ElGamal ElGamal cipher

mã pháp Feistel Feistel cipher

mã pháp không thể phá được unbreakable cipher

mã pháp knapsack Merkle-Hellman Merkle-Hellman knapsack cipher

mã pháp Lucipher Lucipher

mã pháp một chiều one-way cipher

mã pháp ngẫu nhiên random cipher

mã pháp Pohlig-Hellman Pohlig-Hellman cipher

mã pháp Schnorr Schnorr cipher .

mã pháp thay thế substitution cipher

mã pháp tịnh tiến translation cipher

mã pháp tự sinh khóa từ bản mã ciphertext key auto-key cipher

mã pháp Vernam Vernam cipher

mã phát hiện lỗi error detection code

mã phát hiện lỗi kép hiệu chỉnh lỗi đơn SECDEC

mã phát hiện thao tác MDC

mã phát hiện thay đổi MDC

mã phương tiện facility code

mã qua các điểm kết nối link to link encryption

mã SECDEC SECDEC

mã sửa lỗi error correction code

mã tàu ma flying dutchman

mã thám cryptanalysis

mã thoát escape code

mã thử nghiệm test

mã tích product cipher

mã tiền tố prefix

mã toàn tác transaction code

mã toàn vẹn thông báo message integrity code

mã toàn vẹn thông báo MIC

mã truyền thông dữ liệu trong suốt transparent data communication code

mã tuần hoàn cyclic code

mã tự hiệu chỉnh self-correcting code
mã tự phụ thuộc autoclave
mã tỷ số không đổi constant ratio code
mã ủy quyền authorization code
mã xác minh khóa key verification code
mã xác thực tệp file authentication code
mã xác thực thông báo message authentication code
mã xyclic cyclic code
MAB message authentication block
mạch circuit
mạch ảo virtual circuit
mạch ảo thường trực permanent virtual circuit
mạch bốn dây four-wire circuit
mạch cân bằng balanced circuit
mạch chồng chập superimposed circuit, superposed circuit
mạch dữ liệu data circuit
mạch đa điểm multipoint circuit
mạch điện circuit
mạch được chấp nhận approved circuit
mạch ghép nối interface
mạch ghép nối nối tiếp serial interface
mạch hai dây two-wire circuit
mạch logic logic circuit
mạch logic phun tích hợp integrated injection logic
mạch nhiều điểm multidrop circuit, multipoint circuit
mạch quang tích hợp integrated optical circuit
mạch song công duplex circuit
mạch thuê bao leased circuit
mạch tích hợp integrated circuit
mạch tích lũy accumulator circuit
mạch trễ delay circuit
mạch tự kiểm tra self-checking circuit
mạch xáo trộn mã code scrambling circuit
màn báo động alarm screen
màn cảnh báo alarm screen
màn chắn EMI/RF EMI/RF shield
màn hình tinh thể lỏng liquid crystal display
màng array
mạng network
mạng Aloha Aloha
mạng ARPA ARPANET
mạng Arpanet ARPANET
mạng BITNET BITNET
mạng cắt lát slice network
mạng "chuyên chế" despotic network
mạng chuyển mạch switched network
mạng chuyển mạch công cộng public switched network
mạng chuyển mạch gói packet-switching network
mạng chữ T T network
mạng Cirrus Cirrus
mạng có đệm buffered network
mạng cục bộ LAN, local area network, local network
mạng dân chủ democratic network
mạng DIANE DIANE
mạng diện rộng wide area network
mạng dữ liệu Bell Bell Data Network
mạng dữ liệu có quản lý managed data network
mạng dữ liệu công cộng public data network
mạng dữ liệu đồng bộ synchronous data

network

mạng dữ liệu quốc phòng Defense Data Network

mạng địa phương local area network

mạng đối chiếu matching network

mạng Ethernet Ethernet

mạng Euro Euronet

mạng hình sao star

mạng khu vực thủ đô metropolitan area network

mạng khu vực trung tâm metropolitan area network

mạng kỹ thuật số tích hợp integrated digital network

mạng LAN LAN, local area network

(các) mạng lập sẵn scheduled circuits

mạng máy tính computer network

mạng máy tính không đồng nhất heterogeneous computer network

mạng máy tính phân cấp hierarchical computer network

mạng máy tính phi tập trung decentralized computer network

mạng máy tính tập trung centralized computer network

mạng máy tính thuần nhất homogeneous computer network

mạng mắt lưới mesh

(các) mạng ngân hàng banking networks

mạng NIIT NIIT

mạng nối đầy đủ fully connected network

mạng nối hoàn toàn fully connected network

mạng nội bạt LAN

mạng phân cấp hierarchical network

mạng phân tán distributed network

mạng phiến slice network

mạng phủ overlay network

mạng quân sự Milnet

mạng SITA mức cao SITA high level network

mạng so khớp matching network

mạng số dịch vụ tích hợp integrated services digital network

mạng số kết hợp integrated digital network

mạng số phục vụ kết hợp integrated services digital network

mạng tầm xa long haul network

mạng thành phố municipal area network

mạng theo lịch biểu scheduled circuits

(các) mạng thông tin information networks

Mạng tin học Châu Âu European Information Network

mạng Tymnet Tymnet

mạng vòng dùng thẻ bài token ring

mạng vòng lặp loop network

mạng vô tuyến gói packet radio

mạng vùng LAN

mạng xếp chồng overlay network

mánh lấu cá kiting

mạnh về tính toán computationally strong

mạo nhận impersonation

máy ảo virtual machine

máy chính host, mainframe

máy chủ host

máy (tính) chủ server

máy chủ truyền thông communication

server

máy chủ xác thực authentication server

máy dịch vụ service machine

máy dò detector

máy dò chuyển động dùng hồng ngoại infra red motion detector

máy dò nhiệt kiểu lưỡng kim bimetallic-type heat detector

máy đọc thẻ card reader

máy mã Enigma Enigma machine

máy phát transmitter

máy phát hiện khói kết hợp combination smoke detector

máy rút tiền mặt cash dispenser

máy thu receiver

máy thu báo động alarm receiver

máy thu địa chấn geophone

máy thu phát transceiver

máy tính computer

máy tính cá nhân personal computer

máy tính chủ host computer

máy tính Colossus Colossus

máy tính cỡ lớn mainframe

máy tính cỡ nhỏ microcomputer

máy tính đa dụng general purpose computer

máy tính đa năng general purpose computer

máy tính điện tử số electronic digital computer

máy tính nối tiếp serial computer

máy tính nút node computer

máy tính song song parallel computer

máy tính trung tâm mainframe

máy tính truyền thông communications computer

máy tính tuần tự serial computer

máy trả nhận tiền tự động automated teller machine, automatic teller machine

máy vi tính microcomputer

mắc mạch kép double circuiting

mầm seed

mất mát do uốn cong nhiều macrobend loss

mất mát do uốn cong vi mô microbend loss

mất mát thông tin information loss

mất nguồn blackout

mật Confidential

mật độ nén packing density

mật khẩu keyword, password

mật khẩu ảo virtual password

mật khẩu cá nhân personal password

mật khẩu dài passphrase

(các) mật khẩu dùng một lần one-time passwords

mật khẩu động dynamic password

mật khẩu hết hiệu lực expired password

mật khẩu hợp lệ valid password

mật khẩu phụ thuộc thời gian time-dependent password

mật khẩu quá hạn expired password

mật khẩu truy nhập access password

mật mã cipher

mật mã học cryptology

mật mã khóa công khai public key cryptography

mật mã khối block cipher

mật mã không đối xứng asymmetric cipher

mật mã không khóa keyless

cryptography

mật mã cipher

mật mã mạng network encryption

mật mã nút node encryption

mật mã riêng private cryptography

mật mã thực genuine

mật mã ủy nhiệm escrow cryptography

mẫu template

mẫu bản ghi record layout

mẫu tạo khung framing pattern

méo distortion

méo do trễ delay distortion

méo điều biến tương hỗ intermodulation distortion

(sự) móc nối linkage

móc nối quan hệ phần cứng hardware handshaking

móc xích chaining

móc xích mã dòng stream cipher chaining

modem MODEM

modem an toàn secure module, security modem

modem chip chip modem

modem dải gốc baseband modem

modem đồng bộ synchronous modem

modem khoảng cách hạn chế limited distance modem

modem quay số tự động auto dial modem

modem rỗng null modem

modem tích hợp integrated modem

modem trống null modem

modulo 2 modulo 2

modulo n modulo n

modun an toàn security module

modun chống can thiệp tamper-resistant module

modun chuyển khóa key transport module

modun COMSEC của NSA NSA COMSEC module

mô hình model

mô hình an toàn security model

mô hình an toàn mạng network security model

mô hình Bell-La Padula Bell-La Padula model

mô hình Biba Biba model

mô hình chính sách an toàn security policy model

mô hình chính sách an toàn hình thức formal security policy model

mô hình Clark-Wilson Clark-Wilson model

mô hình giàn lattice model

mô hình hóa dữ liệu data modelling

mô hình ma trận truy nhập access matrix model

mô hình toán học mathematical model

mô hình Vạn lý trường thành Chinese Wall model

(sự) mô phỏng simulation

mô phỏng song song parallel simulation

mô hình an toàn của Landwehr cho các hệ thống quân sự Landwehr's security model for military message systems

mốc an toàn thấp low water mark

môi trường environment

môi trường an toàn khép kín closed security environment

môi trường an toàn mở open security environment

môi trường đe dọa thù địch hostile threat environment

môi trường điểm tới điểm point-to-point environment

môi trường khép kín closed environment

môi trường truyền thông communications medium

môi trường từ tính loại 1 Type 1 magnetic media

môi trường từ tính loại 2 Type 2 magnetic media

mối đe dọa threat

mối đe dọa logic logical threat

một cực unipolar

mở (thư) stripping

mở khóa decrypt

mở rộng lỗi error extension

mở rộng sai lệch garble extension

mời gọi invitation

(sự) mũ hóa exponentiation

mục item

(các) mục ẩn hidden sections

mục cuối tail

mục dữ liệu data element, data item, datum

mục dữ liệu không bị giới hạn UDI

mục dữ liệu không bị ràng buộc unconstrained data item

mục dữ liệu ràng buộc constrained data item

mục nhập entry

mục quản handler

mục tiêu an toàn security objective

mục tiêu bảo vệ object of defense

mục tiêu đánh giá target of evaluation

mục tiêu đặc biệt special purpose

mức level

mức an toàn security level

mức an toàn chủ thể subject security level

mức an toàn phiên session security level

mức ảnh hưởng impact

mức cấp quyền authorization level

mức cha parent

mức cốt yếu essentiality

mức độ sử dụng usage

mức đường truyền line level

mức (an toàn) hệ thống cao system high

mức (an toàn) hệ thống thấp system low

mức linh hoạt flexibility

mức lộ exposure

mức mã code level

mức nhiễu của mạch circuit noise level

mức ồn mạch circuit noise level

mức phân loại classification level

mức phơi bày exposure

mức rủi ro chấp nhận được acceptable level of risk

mức thông clearance, clearance level

mức thông mật confidential clearance

mức thông tối mật top secret clearance

mức thông tuyệt mật secret clearance

mức tin cậy degree of trust

mức toàn vẹn integrity level

mức truy nhập access level, clearance, clearance level

mức truy nhập mật confidential clearance

mức truy nhập tối mật top secret

clearance

mức truy nhập tuyệt mật secret clearance

mức truy nhập vật chứa cần thiết container clearance required

mức ủy quyền authorization level

mức va chạm impact

N

nạp load

nạp chương trình ban đầu initial program load

nạp mẫu enrolment

năm chuẩn cứ Shannon Shannon's five criteria

năm tiêu chí Shannon Shannon's five criteria

nắm bắt handled by

năng lực capability

năng suất throughput

nâng cấp lại regrade

né tránh circumvention

nén dữ liệu data compression

nén văn bản text compression

ngày chuyển posting date

ngày có giá trị value date

ngày hợp lệ value date

ngày khởi đầu thông báo MOD

ngày tháng nhập entry date

ngày thanh toán pay date

ngày thiết lập thông báo date of message origination

ngày trả tiền pay date

ngày và thời gian phát hành release time and date

ngăn compartment

ngăn chặn lockout

ngăn chặn arrest

ngăn chứa container

ngăn xếp stack

ngắt interrupt

ngắt chùm beam break

ngắt đảo ngược reverse interrupt

ngắt hạn chế thời gian time limit cutout

ngắt mềm software interrupt

ngắt ngoài external interrupt

ngắt phần cứng hardware interrupt

ngầm covert

ngầm định default

ngầm định từ chối truy nhập default to denial of access

ngầm hiểu default

ngân hàng bank

ngân hàng bỏ túi pocket banking

ngân hàng bồi hoàn reimbursement bank

ngân hàng của người khởi đầu originator's bank

ngân hàng dữ liệu databank

(các) ngân hàng đại lý correspondent banks

ngân hàng đại lý của người gửi sender's correspondent bank

ngân hàng gửi sending bank

ngân hàng môi giới intermediary bank

ngân hàng nhận receiving bank

ngân hàng phục vụ tài khoản account servicing bank

ngân hàng sở hữu tài khoản account owner bank

ngân hàng tại nhà home banking

ngân hàng thanh toán instructing bank

ngân hàng tiếng nói voice bank

ngân hàng trung gian intermediary bank

ngân hàng tự hoạt động self-banking

ngân hàng tương ứng của người nhận receiver's correspondent bank

ngẫu nhiên random

nghe âm thanh audio listen in

nghe lén eavesdropping

nghe lén âm thanh acoustic eavesdropping

nghe lén điện tử electronic eavesdropping

nghe trộm eavesdropping

nghe trộm điện tử electronic eavesdropping

nghe trộm thông tin wiretap

nghe trộm thụ động passive wiretapping

nghi ngờ lẫn nhau mutually suspicious

nghiệm sai false solution

nghiệm thu acceptance

nghiên cứu ngược backwards learning

nghiên cứu thâm nhập penetration study

nghiên cứu tính khả thi về an toàn security feasibility study

nghiên cứu về các hệ điều hành an toàn Research in Secured Operating Systems

ngoại mạch off line

ngoại tuyến off line

ngoại vi peripheral

ngôn ngữ language

ngôn ngữ bậc cao high-level language

ngôn ngữ bậc thấp low level language

ngôn ngữ chuyển tiếp trạng thái Estelle Estelle State Transition Language

ngôn ngữ chương trình program language

ngôn ngữ Claims Claims Language

ngôn ngữ cơ sở dữ liệu database language

ngôn ngữ định hướng thủ tục procedure oriented language

ngôn ngữ đối tượng object language

ngôn ngữ FORTRAN FORTRAN

ngôn ngữ Gypsy Gypsy

ngôn ngữ hình thức formal language

ngôn ngữ khai báo declarative language

ngôn ngữ không thủ tục nonprocedural language

ngôn ngữ kiểu vỏ hành onion skin language

ngôn ngữ máy machine language

ngôn ngữ mô tả dữ liệu data description language

ngôn ngữ nguồn source language

ngôn ngữ Special Special

ngôn ngữ thao tác dữ liệu data manipulation language

ngôn ngữ thế hệ thứ tư fourth generation language

ngôn ngữ thủ tục procedural language

ngôn ngữ truy vấn query language

ngôn ngữ tự nhiên natural language

ngôn ngữ xử lý dữ liệu data manipulation language
nguồn (tin) source
nguồn dữ liệu data source
nguồn đối xứng nhị phân binary symmetric source
nguồn ngoài outsourcing
nguồn WNINTEL WNINTEL
nguồn yếu brownout
nguy cơ sự cố hazard
(sự) nguỵ trang masking
nguỵ trang ký steganography
nguyên lý khả chấp acceptability principle
nguyên tắc cơ chế chung tối thiểu principle of least common mechanism
nguyên tắc dàn xếp hoàn toàn principle of complete mediation
nguyên tắc đặc quyền tối thiểu principle of least privilege
nguyên tắc môi trường kín principle of closed environment
nguyên tố cùng nhau coprime, mutually prime, relatively prime
(tính) nguyên vẹn integrity
ngữ nghĩa học semantics
ngữ pháp grammar
ngừng thử lại pause retry
người bán lẻ retailer
người bán lẻ gian lận fraudulent retailer
người có thẩm quyền phê duyệt chỉ định designated approving authority
người dùng user
người dùng dịch vụ service user
người dùng dữ liệu data user
người dùng siêu đặc quyền superuser
người dùng thẻ retailer
người đánh giá evaluator
người điều hành hệ thống SYSOP
người được ủy nhiệm lưu giữ escow agent
người giữ dữ liệu data keeper
người giữ thẻ card holder
người gửi sender
người hưởng banecifiary
người hưởng cuối cùng ultimate beneficiary
người khởi đầu originator
người kiểm toán EDP EDP auditor
người kiểm toán ngoài external auditor
người kiểm tra ngoài external auditor
người mua thường xuyên frequent buyer
người nhận recipient
người phát originator
người quản lý hệ thống system manager
người quản trị cơ sở dữ liệu database administrator
người sở hữu dữ liệu data owner
người sử dụng user
người sử dụng dữ liệu data user
người sử dụng đầu cuối end user
người sử dụng hệ thống system user
người sử dụng trái phép UU
người sử dụng trực tiếp end user
người tạo ra cơ sở dữ liệu database producer
người tháng man month
người thao tác operator
người trả tiền nặc danh anonymous refunder
người trông coi dữ liệu custodian of data

người vận hành operator

ngưỡng threshold

nhà bảo trợ mạng network sponsor

nhà cung cấp dịch vụ giá trị gia tăng value added service provider

nhà sản xuất thiết bị gốc original equipment manufacturer

nhà sản xuất tương hợp giắc cắm plug compatible manufacturer

nhà sản xuất tương thích phích cắm plug compatible manufacturer

(sự) nhái spoofing

nhãn (kiểm) ticket

nhãn label

nhãn an toàn security label

nhãn đầu header label

nhãn đuôi trailer

nhãn ngoài external label

nhãn nhạy cảm sensitivity label

nhãn tiêu đề header label

nhãn truy nhập access label

nhãn trường field tag

nhảy điện tử electronic vaulting

nhân kernel

nhân an toàn security kernel

(được) nhân hóa kernelized

nhân tử factor

nhân viên an toàn ADP ADP security staff

nhân viên an toàn dữ liệu data security officer

nhân viên bất bình disgruntled employee

nhân viên không trung thực dishonest employee

nhận dạng identification

nhận dạng cá nhân personal identification

nhận dạng cá nhân tự động automatic personal identification

nhận dạng dấu hiệu bằng quang học optical mark recognition

nhận dạng ký tự bằng quang học optical character recognition

nhận dạng ký tự nhờ mực từ tính MICR

nhận dạng tài khoản account identification

(sự) nhận dạng thiết bị đầu cuối terminal identification

nhận dạng và xác thực identification and authentication

nhận diện duy nhất unique identification

nhận diện người sử dụng mạng network user identification

nhập công việc từ xa remote job entry

nhập trước xuất trước first in first out

nhật ký journal

nhị phân binary

nhiệm vụ task

nhiệt độ tạp âm noise temperature

nhiệt độ tiếng ồn noise temperature

nhiều thể hiện polyinstantiation

nhiễu interference, noise

nhiễu cảm ứng induced interference

nhiễu cảm ứng crossfire

nhiễu chạm đường truyền hit

nhiễu điện từ electromagnetic interference

nhiễu tần số vô tuyến radio frequency interference

nhìn lén qua vai shouldering

nhóm group

nhóm CESG CESG

nhóm chức năng functional group

nhóm con TCB TCB Subset

nhóm đối tác counterparty group

nhóm GSIS GSIS (Group for the Standardization of Information Services)

nhóm (ký tự) khởi-ngừng start-stop envelope

nhóm làm việc mạng quốc tế International Network Working Group

nhóm lặp repeating group

nhóm logic logical party

nhóm người dùng users group

nhóm người dùng khép kín closed user group

nhóm TC 97/SC 17/WG4 TC 97/SC17/WG4

nhóm TC97/SC20 TC 97/SC20

nhóm tin tặc Milwauke 414 Milwauke 414

nhóm trao đổi interchange group

nhóm truy nhập access group

nhồi bit bit stuffing

nhớ và chuyển tiếp store and forward

nhu cầu cần biết need to know

nible nibble

nòng phun khóa key gun

nối cứng hardwired

nối kết đa điểm multipoint connection

nối kết mạng vòng daisy chain

nối lén chủ động active wiretapping

(sự) nối liền linkage

nối mạch phản hồi bussback

(sự) nối mạng network connection

nối ra - vào bussback

nối tới cảnh sát police connect

nối trộm thông tin wiretap

nội dịch housekeeping

nội dung thông báo message text

nội dung thông tin information content

nơi cung cấp dịch vụ service provider

nơi dữ liệu trú ẩn data haven

nơi đến thứ cấp secondary destination

nơi gom (dữ liệu) sink

nơi gom dữ liệu data sink

nơi nhận recipient

NP đầy đủ NP complete

n-trả lời, k% lợi thế n-respondent, k%-dominance

núm thoát exit button

nút node

nút chuyển mạch gói packet switch node

nút lá leaf

nửa byte nibble

nước cư trú country of residence

nước sở tại country of domicile

O, Ô, Ơ

octet octet

OWF one-way function

ô dữ liệu data cell

ô nhiễm contamination

(sự) ô nhiễm dữ liệu data contamination

ổ dữ liệu dataplug

ổ đĩa disk drive

ổ đĩa mềm floppy disk drive

ống bit số digital bit pipe

ống dẫn ánh sáng light conduit

ống dẫn sáng light guide

ống kim loại bảo vệ electrical metallic tubing

ở xa remote

oristic heuristic

Ostet Oe

Ostet oersted

P

PAN primary account number

phá bẫy capture

phá chữ ký signature deconstruction

(sự) phá hoại sabotage

(sự) phá hỏng destruction

(sự) phá hủy destruction

phá rối jamming

phạm vi range

phạm vi công nhận accreditation range

phản hồi đầu ra output feedback

phản ứng khẩn cấp emergency response

phản ứng thời gian thực realtime reaction

(sự) phát transmission

(sự) phát hành PIN PIN issuance

phát hành trực tiếp con ngựa Tơroa Trojan Horse direct release

phát hiện âm thanh audio detection

phát hiện chuyển động ở dải vi ba microwave motion detection

phát hiện có đối trọng balanced detection

phát hiện thao tác manipulation detection

phát hiện xâm nhập intrusion detection

phát lại relay

(các) phát lộ compromising emanations

phát qua dẫn điện conductive radiation

phát rộng broadcast

phát tán diffusion

phát tán điện từ electromagnetic emanations, electromagnetic emissions

phát xạ âm thanh acoustic emission

phát xạ điện từ electromagnetic emanations; electromagnetic emissions

(các) phát xạ gây hại compromising emanations

(các) phát xạ tần số vô tuyến radio frequency emissions

phân bố Gauss Gaussian distribution

phân bố Poisson Poisson distribution

phân cấp T T carrier

phân chia có kiểm soát controlled sharing

phân định trách nhiệm cá nhân individual accountability

phân hệ an toàn máy tính computer security subsystem

phân hoạch khóa key partitioning

phân hoạch NTCB NTCB partition

phân kênh demultiplexing

phân loại mật secrecy classification

phân loại ngầm định default classification

(sự) phân loại theo thời hạn sử dụng aging

phân phối hạn chế LIMDIS

phân phối khóa công khai public key distribution

(sự) phân tách thời gian temporal separation

phân tán diffusion

phân thời time sharing

phân tích analysis

phân tích cấu trúc structure analysis

phân tích chi phí - rủi ro cost-risk analysis

phân tích chữ ký signature analysis

phân tích dãy biến cố event sequence analysis

phân tích dấu vân tay fingerprint analysis

phân tích đệ quy recursion analysis

phân tích độ phức tạp complexity analysis

phân tích động dynamic analysis

phân tích động sự gõ phím keystroke dynamics analysis

phân tích hệ thống system analysis

phân tích hiểm họa threat analysis

phân tích hình học tay hand geometry analysis

phân tích in dấu tay palmprint analysis

phân tích ký tự character disassembly

phân tích liên kết binding analysis

phân tích luồng flow analysis

phân tích luồng dữ liệu data flow analysis

phân tích luồng điều khiển control flow analysis

phân tích luồng thông tin information flow analysis

phân tích lưu lượng traffic analysis

phân tích lưu lượng an toàn security flow analysis

phân tích mã code analysis

phân tích mạch ghép nối mođun module interface analysis

phân tích mật mã cryptanalysis

phân tích mức ảnh hưởng impact analysis

phân tích phần mềm software analysis

phân tích rủi ro risk analysis

phân tích rủi ro định lượng quantitative risk analysis

phân tích rủi ro định tính qualitative risk analysis

phân tích theo thứ bậc hierarchical decomposition

phân tích tiếng nói voice analysis

phân tích tĩnh static analysis

phân tích trực tiếp mẫu pattern directed analysis

phân tích vết kiểm toán audit trail analysis

phân tích viễn cảnh scenario analysis

phân tích võng mạc mắt eye retina analysis

(sự) phân vùng zoning

Phần A Division A

Phần B Division B

(các) phần bảo vệ trọng yếu của TCB protection-critical portions of the TCB

phần bổ sung add-in

phần bù khóa key offset

Phần C Division C

phần cuối drop

phần cứng hardware
Phần D Division D
phần dư redundancy, residue
phần dư MAC MAC residue
phần dự phòng redundancy
phần đen black
phần ghép aggregation
phần gộp aggregation
phần mềm software
phần mềm ác ý malware
phần mềm an toàn không nhân non-kernel security-related software
phần mềm có đóng shareware
phần mềm không được chấp thuận unapproved software
phần mềm nhạy cảm sensitive software
phần mềm phá hoại vandalware
phần mềm thường trú resident software
phần mềm tin cậy trusted software
phần mềm từ xa telesoftware
phần mềm tự nguyện shareware
phần mềm ứng dụng application software
phần mở rộng extension
phần sụn firmware
phần trăm từ chối percent denial
phần tử element
phần tử cha parent
phần tử dữ liệu data element
phần tử dừng stop element
phần tử khởi đầu start element
phần tử tín hiệu signal element
phần tử xác thực authentication element
phép biến đổi dòng thông báo MSM
phép biến đổi mật privacy transformation
phép biến đổi MSM MSM
phép chia division
phép chiếu projection
phép đảo inversion
phép đo từ xa telemetry
phép gán set
phép ghi mật mã cryptography
phép gộp aggregation
phép kiểm tra tổng thể substantive testing
phép kiểm tra trọng yếu substantive testing
phép lập mã cryptography
phép lấy phần dư n mod n
phép loại trừ - hoặc EXCLUSIVE OR
phép mã biến đổi transformational coding
phép mã có thể đảo được reversible encryption
phép mã DES bội multiple DES encipherment
phép mã điểm tới điểm end-to-end encipherment
phép mã gián tiếp off line encryption
phép mã hóa encipherment
phép mã khóa riêng private key encryption
phép mã lũy thừa exponentiation cipher
phép mã mũ hóa exponentiation cipher
phép mã ngoại mạch off line encryption
phép tính quan hệ relational calculus
phép toán một ngôi unary operation
phép tra thực hiện lại reperformance test
phép tuyển loại EXCLUSIVE OR
phép viễn trắc telemetry

phê chuẩn cho hoạt động approval to operate

phê chuẩn / chứng nhận approval/accreditation

phê chuẩn dữ liệu data validation

phê chuẩn dữ liệu nhập input data validation

(sự) phê chuẩn hợp lệ validation

phê chuẩn nhận dạng identity validation

phê chuẩn PIN PIN validation

(sự) phê duyệt endorsement

phê duyệt tạm thời interim approval

(sự) phê duyệt truy nhập hình thức formal access approval

(sự) phê duyệt validation

(lệ) phí charges

phích dữ liệu dataplug

phiên (làm việc) session

phiên bản KVM/370 KVM/370

phong tỏa tài khoản account freezing

phòng điều khiển control cabinet

phòng kiểm soát control cabinet

phòng sai guarding

phòng thanh toán bù trừ tự động hóa Automated Clearing House

Phòng thí nghiệm của tổ chức ký nhận Underwriter's Laboratory

phòng thủ mạng network guard

phòng vệ safeguard

(các) phòng vệ an toàn security safeguards

phổ biến dissemination

phracd phracker

(sự) phụ thuộc dependence

(sự) phụ thuộc bắc cầu transitive dependence

(sự) phụ thuộc hàm functional dependence

phụ thuộc hàm hoàn toàn fully functional dependent

(sự) phụ thuộc liên ký hiệu intersymbol dependence

(sự) phụ thuộc liên ký hiệu mạnh strong intersymbol dependence

phục hồi rollback

(sự) phục hồi recovery

phương pháp CRC cyclic redundancy check

phương pháp Diffie-Hellman Diffie-Hellman technique

phương pháp EDAC EDAC

phương pháp luận Affirm Affirm

phương pháp luận LAVA LAVA

phương pháp luận ma trận matrix methodology

phương pháp luận phân tích rủi ro risk analysis methodology

phương pháp phân tích rủi ro Marion Marion

phương pháp phòng sạch cleanroom approach

phương pháp thông báo method of advice

phương pháp từ trên xuống top down method

phương thức mode

phương thức DAC discretionary access control

phương thức không trong suốt nontransparent mode

phương thức tấn công mode of attack

phương tiện facility

phương tiện công chứng khóa KNF (Key

Notarization Facility)

phương tiện công nghệ thông tin information technology facility

phương tiện dự phòng standby facility

phương tiện đánh giá đã đăng ký thương mại commercial licensed evaluation facility

phương tiện kiểm soát truy nhập tài nguyên RACF

phương tiện KNF KNF (Key Notarization Facility)

phương tiện máy tính computer facility

phương tiện máy tính trung tâm central computer facility

phương tiện mật mã cryptographic facility

phương tiện mở open shop

phương tiện năng lượng cao high energy media

phương tiện quản lý khóa key management facility

phương tiện truyền thông communications medium

PIN chuẩn reference PIN

PIN dẫn xuất derived PIN

Q

quá giờ time out

quá tải kênh channel overload

quá trình process

quá trình cấp phép authorization process

quá trình đemon demon

quá trình giản lược summary processing

quá trình không tin cậy untrusted process

quá trình mật mã cryption

quá trình ngẫu nhiên random process

quá trình tin cậy trusted process

quá trình ứng dụng application process

quá trình xác thực authentication process

quan chức an toàn hệ thống System Security Officer

quan chức công nhận accreditation authority

quan hệ relation

quan hệ lập khóa keying relationship

quan sát dữ liệu viewdata

quản lý an toàn security management

quản lý cấu hình configuration management

quản lý cấu hình an toàn secure configuration management

quản lý dữ liệu data management

(sự) quản lý khóa key management

quản lý mạng network management

quản lý mật mã cryptomanagement

quản lý ngẫu nhiên contingency management

quản lý phương tiện facilities management

quản lý rủi ro risk management

quản lý tài nguyên thông tin information resources management

quản lý tệp file management

quản lý thẻ bài token management

quản lý thông tin information management

quản lý truy nhập dữ liệu data access management

quản lý và an toàn PIN PIN management and security

Quản trị dịch vụ chung General Services Administration

quang nhận dạng dấu hiệu optical mark recognition

quang nhận dạng ký tự optical character recognition

quang sợi fiber optics

quảng bá broadcast

quay số ngược dial back

quay số tự động auto dial

quay vòng rotation

quay vòng nhiệm vụ rotation of duties

(sự) quét scanning

quét hack hack, sweeping

quét chống phá điện tử electronic countermeasures sweeping

quét scan

quy định PIN PIN assignment

quy định Telpak Telpak

quy tắc policy

quy tắc bình lặng tranquility

quy tắc kỹ thuật technical policy

quỹ biên giới điện tử electronic frontier foundation

quỹ có sẵn available funds

quỹ cùng ngày same day funds

quỹ đã bù trừ cleared funds

quỹ liên bang federal funds

quỹ ngày hôm sau next-day funds

quyền sở hữu ownership

quyền truy nhập access right

(các) quyền truy nhập cho phép permissions

quyền ủy thác authorization

quyết định động formulary

R

ra khỏi mạng log off

rác garbage

rác liệu garbage

rào chắn ngoại vi perimeter barrier

rào chắn vành đai perimeter barrier

rào chắn vật lý physical barrier

ráp ký tự character assembly

RDC remote diagnostic center

REL REL (Releasable)

RF RF (Radio Frequency)

(sự) riêng tư privacy

(sự) rò rỉ leakage, seepage

rò rỉ dữ liệu data leakage

rò rỉ thông tin do con ngựa Tơroa Trojan horse leakage

ROM xóa được bằng điện electrically erasable ROM

rời hệ thống log off, log out

rời ra disjoint

rủi ro chấp nhận được acceptable risk

rủi ro còn lại residual risk

rủi ro đối tác counterparty risk

rủi ro lan truyền từ các nguồn bất lợi diffuse risk from adversarial source

rủi ro nhận dạng identification risk

rủi ro tiết lộ disclosure risk

rủi ro tín dụng credit risk

rút gọn dữ liệu data reduction

S

Sách Da Cam Orange Book

sách hướng dẫn đánh giá an toàn công nghệ thông tin information technology security evaluation manual

Sách Đỏ Red Book

Sách Trắng White Book

Sách Vàng Yellow Book

Sách Xanh Blue Book

sai chức năng malfunction

sai hỏng nhạy mẫu pattern sensitive fault

sai lạc corruption

(sự) sai lạc dữ liệu data corruption

sai sót fault

sai số error

sai số tương đối relative error

sai thủ tục flaw

san bằng equalization

sản phẩm product

sản phẩm mật mã loại 1 Type 1 cryptographic product

sản phẩm mật mã loại 2 Type 2 cryptographic product

sản phẩm RACF RACF

(các) sản phẩm tin cậy trusted products

sàng Eratosthenes sieve of Eratosthenes

sanon Shannon

sao chép bất hợp pháp piracy

sao hoàn toàn full duplex

sao lậu phần mềm software crèep

(tính) sẵn sàng ADP ADP availability

sắp thứ tự gói packet sequencing

sắp xếp hồ sơ điện tử electronic filing

sắp xếp lưu trữ điện tử electronic filing

sâu worm

sâu Moriss Moriss worm

secto sector

secto không chuẩn nonstandard sector

secvơ server

secvơ tệp file server

secvơ xác thực authentication server

shanon Shannon

(sự) si mê điện thoại phone phreaking

siêu dữ liệu metadata

siêu mã superencipherment

siêu máy tính supercomputer

siêu xóa superzapping

so khớp hit, matching

so khớp máy tính computer matching

soạn thảo edit

song ánh bijection

song công duplex

song công (hoàn toàn) full duplex

sóng liên tục continuous wave

sóng mang carrier

sổ hướng dẫn khôi phục sau sự cố disaster recovery manual
sổ mã code book
sổ mã điện tử electronic codebook
sổ nhật ký log
sổ tay an toàn địa điểm vận hành operational site security manual
số number
(thuộc) số digital
số bù complement
số dư tài khoản account balance
số giả ngẫu nhiên pseudorandom number
số hiện tại nonce
số hiệu dãy ra OSN
số hiệu dãy thông báo message sequence number
số hiệu giao dịch transaction number
số hiệu nhận dạng cá nhân PIN
số hiệu nhận dạng người dùng user id
số hiệu phiên bản version number
số hiệu PIN PIN
số hiệu thông báo message numbering
số học modulo modulo arithmetic
số học nhị phân binary arithmetic
số hữu tỷ rational number
số liệu nhận dạng tệp tin file descriptor
số lượng number
số mũ exponent
(các) số ngẫu nhiên random numbers
số nguyên integer
số nguyên ngẫu nhiên đặc trưng cho thông báo message specific random integer
số nguyên tố prime number
số nguyên tố an toàn safe prime
số nguyên tố Fermat Fermat prime
số nguyên tố lẻ odd prime
số nguyên tố Mersenne Mersenne prime
số nhận dạng cá nhân personal identification number
số nhận dạng cá nhân dẫn xuất derived PIN
số nhị phân binary number
số nonce nonce
số tài khoản gốc primary account number
số tham chiếu hệ thống SRN
số thứ tự ordinal
số thứ tự hệ thống SSN
số thực real number
sơ đồ schema
sơ đồ bản ghi record layout
sơ đồ mạch số chuyển mạch circuit switched digital circuitry
sơ đồ ngoài external schema
sơ đồ tệp file layout
sợi quang đơn kiểu monomode fiber
sợi tinh quái rogue fiber
sơn phun pray paint
spufinh spooling
SRN SRN
SSN SSN
ST&E security test and evaluation
stub stub
suất loại bỏ sai false rejection rate
suất lỗi khối block error rate
suất nghiệm thu sai false acceptance rate
suất tin rate
suất tin tuyệt đối absolute rate
súng gài khóa key gun

(sự) suy giảm attenuation

suy luận inference

suy rộng Euler Euler's Generalization

sử dụng nội bộ internal use

sự cố fault, malfunction

sự cố an toàn security incident

sự cố an toàn máy tính computer security incident

sự cố đầu từ head crash

sự cố đĩa disk crash

sự kiện liên quan tới an toàn security relevant event

sửa đổi amend

sửa đổi câu truy vấn query modification

sửa đổi dữ liệu data modification

sửa đổi nhỏ hệ thống các bản ghi minor change to a system of records

sửa lỗi tiến forward error correction

sửa lỗi trước forward error correction

sửa lỗi tự động hóa automated error correction

sửa tạm patch

SYSOP SYSOP

T

tác nhân gây hiểm họa threat agent

tác vụ task

tách bạch đặc quyền separation of privilege

tách bạch nhiệm vụ hoặc chức năng separation of duties or functions

(nguyên tắc) tách bạch và dàn xếp separate and mediate

tách ký tự character disassembly

tách ra disjoint

tai biến crash

tài khoản của bạn vostro account

tài khoản của bên thứ ba loro account

tài khoản của chúng tôi nostro account

tài khoản loro loro account

tài khoản nostro nostro account

tài khoản vostro vostro account

tài liệu material

tài liệu ISRD ISRD (Information System Requirements Document)

tài liệu mã hóa cryptogram

tài liệu tạo khóa keying material

tài nguyên resource

tài sản asset

tải load

tải đường truyền line load

tải lên upload

tải ra upload

tải vào kênh down line load

tải xuống down line load

tải xuống download

tái cấu trúc tệp file restructuring

tái định hướng cuộc gọi call redirection

tái tạo regeneration

tám bit octet

tạm ngắt break

tạm ngừng break

tán sắc kiểu mode dispersion

tạo đà flywheeling

(sự) tạo khóa key generation

tạo khuôn format

(sự) tạo khuôn formatting

tạo lại regeneration

tạo mẫu ký tự character assembly

tạo nguồn phụ second sourcing

tạo nguồn thứ cấp second sourcing

tạo ống dẫn pipelining

tạo séc không check kiting

tạo thẻ chủ card mastering

tạo thẻ gốc card mastering

tạp âm noise

tạp âm lượng tử hóa quantizing noise

tạp âm nhân tạo man-made noise

tạp âm trắng white noise

tạp nhiễu xung impulsive noise

tắc nghẽn deadlock
tâm nucleus
tấm mạch circuit board
tấm mạch mã hóa encrypter board
tấm mạch ranh giới demarcation strip
tần số cắt cutoff frequency
tần suất lỗi error rate
tấn công attack
tấn công bản mã chọn trước chosen cryptogram attack
tấn công báo phủ nhận NAK attack
tấn công chỉ có bản mã ciphertext only
tấn công chủ động active attack
tấn công chuyển tiếp replay
tấn công công nghệ technological attack
tấn công dùng từ điển dictionary attack
tấn công gặp điểm giữa meet in the middle
tấn công không đồng bộ asynchronous attacks
tấn công lúc nửa đêm midnight attack
tấn công phân tích analytical attack
tấn công theo kiểu đào hầm tunneling attack
tấn công thụ động passive attack
tấn công toàn diện exhaustive attack
tấn công tráo đổi replay
tấn công vét cạn exhaustive attack
tấm mạch mở rộng expansion board, expansion card
(sự) tận dụng bộ xử lý processor utilization
tận dụng khoản vay loan utilization
tầng biểu diễn presentation layer
tầng liên kết dữ liệu data link layer
tầng mạng network layer
tầng phiên session layer
tầng ứng dụng application layer
tầng vận tải transport layer
tầng vật lý physical layer
tập (nhớ) volume
tập phổ biến universal set
tập bố father file
tập con subset
tập con ký tự character subset
tập dữ liệu dat set
tập dữ liệu khóa mật mã cryptographic key data set
tập đầy đủ số dư complete set of residues
tập giao tác transaction set
tập hợp set
tập hợp câu truy vấn query set
tập hợp lệnh instruction set
tập khóa giao tác transaction key set
tập mã code set
tập quen ngược backwards learning
tập rút gọn các phần dư reduced set of residues
tập vạn năng universal set
(sự) tẩy erasure
TCB đơn khối monolithic TCB
Telecom của Anh British Telecom
tem ngày/giờ date/time stamp
tem thời gian time stamp
tem thời gian - ngày tháng time-date stamp
Tempest Tempest
tera tera
(tín hiệu) terminal dữ liệu sẵn sàng data terminal ready
terminal ký tự character terminal

terminal thông minh intelligent terminal

tên tệp file name

(các) tên virut virus names

tệp file

tệp âm negative file

(các) tệp ẩn hidden files

tệp chủ master file

tệp có đánh chỉ số indexed file

tập con TCB dự phòng candidate TCB subset

tệp dữ liệu ngoài external data file

tệp dữ liệu vi mô microdata file

tệp đảo inverted file

tệp được lập danh mục indexed file

tệp hai chiều flat file

tệp lược tả đặc quyền privilege profile

tệp nóng hot file

tệp ông grandfather file

tệp phẳng flat file

tệp theo dõi log

tệp treo suspense file

thác khóa bản mã key ciphertext avalanche

thác rõ mã plaintext ciphertext avalanche

tham chiếu reference

tham số parameter

tham số an toàn security parameter

tham số ủy quyền authorization parameter

thảm báo động area mat

thanh ghi register

thanh ghi dịch shift register

thanh ghi dịch phản hồi tuyến tính linear feedback shift register, LSFR

thanh ghi giới hạn bounds register

thanh ghi khóa key register

thanh ghi LSFR LSFR

(sự) thanh lọc sanitization

(sự) thanh toán payment

thanh toán settlement

thanh tra an toàn security inspection

thành phần component

thành phần khóa key component

thành phần mạng network component

thành tố formant

thao tác bản rõ cleartext operation

thao tác mật mã cryption, crypto-operation

thao tác nội dịch red tape operation

thao tác riêng privity

tháo dồn kênh demultiplexing

thay đổi quan trọng significant modification

thăm dò trạng thái status poll

thặng dư residue

thặng dư bậc hai quadratic residue

thặng dư MAC MAC residue

(sự) thâm nhập penetration

(sự) thâm nhập hệ thống system penetration

thẩm tra verify

thẩm tra cá nhân personal verification

thẩm tra PIN PIN verification

thẩm tra và phê duyệt độc lập Independent Verification and Validation

thân thiện với người dùng user friendly

thập lục phân hexadecimal

thập phân được mã (theo hệ) nhị phân binary coded decimal

thập phân mã hóa nhị phân binary coded decimal

thất thoát loss

(sự) thất thoát compromise

thẻ ticket

thẻ âm negative card

thẻ bài token

thẻ bài điện tử electronic token

thẻ bài điều khiển control token

thẻ bài thông minh intelligent token

thẻ dập nổi embossed card

thẻ điện tử thụ động passive electronic card

thẻ độ đen optical density card

thẻ ghi nợ debit card

thẻ kiểm soát token

thẻ logic nối mạch wired logic card

thẻ mã bằng từ tính magnetically encoded card

thẻ mã hóa bằng điện dung capacitively coded card

thẻ mạch được điều hưởng tuned circuit card

thẻ mật độ quang optical density card

thẻ ngân hàng pocket banking

thẻ nhận dạng identity token

thẻ siêu thông minh supersmart card

thẻ sọc từ magnetic stripe card

thẻ sọc từ mag stripe card

thẻ thông minh smart card

thẻ thông minh không tiếp xúc contactless smart card

thẻ tin dụng credit card

thẻ truy nhập access card

thẻ từ kháng cao high coercivity card

thẻ vệt từ magnetic spot card

thế hệ generation

thi hành cách ly isolation enforcement

thiết bị bảo vệ cổng port protection device

thiết bị báo động bằng âm thanh audible alarm device

thiết bị chỉ thị cảnh báo alarm indicating device

thiết bị chống nghe lén anti-eavesdrop device

thiết bị chủ chốt keystone equipment

thiết bị chuyển hướng tuần tự sequential switcher

thiết bị chuyển tiếp repeater

thiết bị COAM COAM

thiết bị cuối đường truyền line termination equipment

thiết bị cuối mạng network termination unit

thiết bị DASD DASD

thiết bị DEA DEA device

thiết bị dữ liệu dat set

thiết bị dự phòng standby equipment

thiết bị đáp responder

thiết bị đáp âm thanh audio response unit

thiết bị đầu cuối terminal

thiết bị đầu cuối ảo virtual terminal

thiết bị đầu cuối ảo trên mạng network virtual terminal

thiết bị đầu cuối chế độ cuộn scroll mode terminal

thiết bị đầu cuối cho phép truy nhập bội multiple access rights terminal

thiết bị đầu cuối chuyển theo gói packet terminal

thiết bị đầu cuối có bộ đệm thiết bị unit buffer terminal

thiết bị đầu cuối dữ liệu data terminal equipment

thiết bị đầu cuối đường dây LTE

thiết bị đầu cuối ở chế độ trang page mode terminal

thiết bị đầu cuối tại điểm trả tiền point-of-sale terminal

thiết bị đầu cuối thông minh intelligent terminal

thiết bị điều khiển chùm cluster control unit

thiết bị ghi khóa key gun

thiết bị gọi tự động automatic calling unit

thiết bị gửi sender

thiết bị hai đầu two-end device

thiết bị hiển thị visual display unit

thiết bị hiển thị trực quan VDU

thiết bị hiện hình visual display unit

thiết bị kết thúc mạch dữ liệu data circuit terminating equipment

thiết bị khách hàng COAM

thiết bị không thông minh dumb device

thiết bị khởi báo bằng tay manual alarm initiating device

thiết bị khởi phát báo động tự động automatic alarm initiating device

thiết bị LTE LTE

thiết bị lưu trữ dung lượng lớn mass storage device

thiết bị mật mã cryptographic equipment

thiết bị một đầu one end device

thiết bị một mức single-level device

thiết bị nạp khóa key loader

thiết bị nghe lén điện tử electronic listening device

thiết bị ngoại vi an toàn security peripheral

thiết bị người dùng đầu cuối end user device

thiết bị nhập input device, input unit

thiết bị nhập/xuất input/output device

thiết bị nhiều mức multilevel device

thiết bị phát hiện detector

thiết bị phát hiện chuyển động nhờ âm thanh sonic motion detector

thiết bị phát hiện khói bằng tín hiệu quang điện photoelectric beam smoke detector

thiết bị phát hiện rung động vibration detector

thiết bị phát hiện thâm nhập intrusion detector

thiết bị phát hiện từ xa remote detector panel

thiết bị phát hiện xâm nhập bằng laze laser intrusion detector

thiết bị phụ ancillary equipment, auxiliary equipment

thiết bị quản lý khóa key management device

thiết bị quay số băng từ tape dialer

thiết bị quét scanner

thiết bị tạo khóa key generator

thiết bị thông minh intelligent device

thiết bị trạm cảnh sát police station unit

thiết bị truy nhập dữ liệu trực tiếp direct data access arrangement

thiết bị vào input unit

thiết bị vào/ra input/output device

thiết bị vòng loop plant

thiết bị xác thực authentication equipment

thiết bị xác thực đầu cuối terminal authentication device

thiết kế đối chiếu reverse engineering

thiết kế khái niệm conceptual design

thiết kế không mật nonsecret design

thiết kế mạng rẻ nhất least cost network design

thiết lập quan hệ handshaking

thỏa thuận khóa key agreement

thỏa thuận mua bán deal

(sự) thông clearance

thông báo message

(thư) thông báo advice

thông báo chứng nhận certificate

thông báo cũ stale message

thông báo dịch vụ service message

thông báo dịch vụ đáp response service message

thông báo dịch vụ khóa key service message

thông báo dịch vụ khôi phục lỗi error recovery service message

thông báo dịch vụ lỗi error service message

thông báo dịch vụ mật mã cryptographic service message

thông báo dịch vụ ngắt disconnect service message

thông báo đáp lại dịch vụ yêu cầu response to request service message

thông báo đến địa chỉ duy nhất single address message

thông báo ghi nhận memo advice

thông báo giao dịch/thanh toán Transaction/Payment Message

thông báo lỗi error message

thông báo nhàm chán stale message

thông báo song song parallel messages

thông báo tài chính financial message

thông báo thanh toán payment message

thông báo tới incoming message

thông báo trả tiền payment message

thông báo và đánh giá advice and assessment

thông báo yêu cầu dịch vụ request for service message

thông đồng collusion

thông lượng từ magnetic flux

thông suốt dãy bit bit sequence transparent

thông suốt dữ liệu data transparency

thông tin information

thông tin an ninh Quốc gia của Mỹ NSI (National Security Information)

thông tin chia ngăn nhạy cảm sensitive compartmented information

thông tin chính phủ nước ngoài Foreign Government Information

thông tin chưa xếp vào loại mật unclassified information

thông tin công nghiệp quốc phòng defense industry information

thông tin cốt lõi essential elements of friendly information

thông tin khoa học và kỹ thuật scientific and technical information

thông tin mở đầu header

thông tin ngân hàng - ngân hàng bank to bank information

thông tin nhạy cảm sensitive information

thông tin nội dịch housekeeping information

thông tin PROPIN PROPIN

thông tin quốc phòng nhạy cảm sensitive defense information

thông tin về tài khoản gốc primary account information

thông tin xác thực authentication information

thống kê nguồn lỗi error source statistics

thống kê nhạy cảm sensitive statistic

thông dải bandpass

thời gian ấn định time out

thời gian bảo vệ cover time

thời gian bảo vệ tối thiểu minimal cover time

thời gian cài đặt installation time

thời gian chạy máy uptime

thời gian dừng dwell time

thời gian đa thức polynomial time

thời gian đáp ứng response time

thời gian hàng đợi queuing time

thời gian hiệu lực an toàn security life

thời gian khôi phục trung bình mean time to recover

thời gian lưu (dữ liệu) retention period

thời gian ngừng downtime

thời gian rỗi idle time

thời gian sẵn sàng available time

thời gian sống trung bình mean life

thời gian sửa chữa trung bình mean time to repair

thời gian tốn thêm cho hỏi vòng polling overhead

thời gian trễ trên mạng network delay

thời gian trung bình giữa các sự cố mean time between failure

thời gian vận hành operating time, uptime

thời hạn khóa cryptoperiod

thời lượng time slice

thu điều khiển phát pacing

thu gom dữ liệu hỏng garbage collection

thu gom rác garbage collection

thu nạp dữ liệu data capture

thu nhận dữ liệu data acquisition

thu thập dữ liệu data collection

thu thập tự động automatic capture

thủ quỹ không trung thực sharp eyed cashier

thủ quỹ ranh ma sharp eyed cashier

thủ tục procedure

(các) thủ tục procedures

thủ tục biến đổi transformational procedure

thủ tục con subroutine

(các) thủ tục dự phòng backup procedures

thủ tục dự phòng fall back

thủ tục đệ quy recursive routine

thủ tục điều khiển cuộc gọi call control procedure

thủ tục ghi đè overwrite procedure

(các) thủ tục khôi phục recovery procedures

thủ tục kiểm soát truyền dữ liệu nâng cao advanced data communications control procedure

thủ tục móc nối quan hệ handshaking

procedure

thủ tục phê chuẩn tính toàn vẹn integrity validation procedure

thủ tục thiết lập quan hệ handshaking procedure

(các) thủ tục toàn vẹn hệ thống system integrity procedures

thụ động passive

thuận lợi cho người dùng user friendly

thuật ngữ nomenclature, term

thuật phỏng đoán heuristic

thuật toán algorithm

thuật toán Berlekamp-Massey Berlekamp-Massey algorithm

thuật toán Data Seal Data Seal

thuật toán đối xứng symmetric algorithm

thuật toán Euclid Euclid's algorithm

thuật toán Fiat Shamir Fiat Shamir algorithm

thuật toán Guillou-Quisquater Guillou-Quisquater

thuật toán khóa mật secret key algorithm

thuật toán không đối xứng asymmetric algorithm

thuật toán mã dữ liệu data encryption algorithm

thuật toán mã dữ liệu nhanh fast data encipherment algorithm

thuật toán mã dữ liệu quốc tế IDEA

thuật toán mã dựa trên mật khẩu password based encryption algorithm

thuật toán mã hóa encryption algorithm

thuật toán mật mã cryptographic algorithm

thuật toán RSA RSA

thuật toán xác thực authentication algorithm

thuật toán xác thực thông báo message authentication algorithm

thuộc tính attribute

thuộc tính an toàn sao star security property

thuộc tính cơ sở prime attribute

thuộc tính phụ nonprime attribute

thuộc tính sao star property

thư điện tử electronic mail

thư mục directory

thư mục phân cấp hierarchical directory

thư tiếng nói voice mail

thư viện khóa key library

thử beta beta testing

thử chấp nhận acceptance testing

thử chức năng functional testing

thử động dynamic testing

thử mạch ngược vòng loopback test

thử mức bão hòa saturation testing

thử nghiệm thu acceptance testing

thử tràn flood testing

thứ tự ưu tiên priority

thừa nhận nonrepudiation

thừa số factor

thực hiện implementation

thực thể entity

thực thể ngang hàng peer entity

thường trình đệ quy recursive routine

thường trình kết nối link

(cảm biến) tia hồng ngoại thụ động PIR

tia kinh tuyến meridional ray

tích kê ticket

tích vô hướng scalar product

tiền điện tử electronic coin

tiền liên bang federal funds

tiền tố RS RS

tiền trực tiếp immediate funds

tiền tức thời immediate funds

tiến trình process

tiến trình thực hiện chứng nhận certification path

tiện cho người dùng user friendly

(các) tiện ích so sánh chương trình program comparison utilities

tiếng chuông chime

tiếng đáp lại dữ liệu nhập data input voice answerback

tiếng ồn noise

tiếng ồn xung impulsive noise

tiếp âm relay

tiết kiệm cơ câu economy of mechanism

tiết lộ disclosing

(sự) tiết lộ âm negative disclosure

tiết lộ do sơ suất inadvertent disclosure

(sự) tiết lộ trái phép unauthorized disclosure

tiêu chí criteria

(các) tiêu chí an toàn của DOD DOD security criteria

tiêu chí đánh giá an toàn máy tính tin cậy trusted computer security evaluation criteria

tiêu chuẩn criteria

(các) tiêu chuẩn cân đối hóa harmonized criteria

tiêu chuẩn DIN DIN

tiêu chuẩn DIS DIS

tiêu chuẩn DOD 5200.28-STD DOD 5200.28-STD

(các) tiêu chuẩn đánh giá an toàn công nghệ thông tin information technology security evaluation criteria

(các) tiêu chuẩn, liên bang Federal Criteria

tiêu chuẩn thiết kế design standard

tiêu đề header

tiêu đề thông báo message heading

tiểu ban 11 TC 11

tiểu ban 68/SC2 TC 68/SC2

tìm kiếm bản mã ciphertext searching

tìm kiếm khóa bội multiple key retrieval

tìm kiếm thông tin information retrieval

tìm rệp debug

(sự) tin cậy trust

tin tặc hacker

tin tình báo qua truyền thông COMINT

tin tức intelligence

tin tức tình báo intelligence

tín hiệu signal

tín hiệu analog analog signal

tín hiệu báo chuông ring indicator

tín hiệu báo động alarm signal

tín hiệu báo thiết bị dữ liệu sẵn sàng data set ready

tín hiệu báo trục trặc trouble signal

tín hiệu chấp nhận cuộc gọi call accepted signal

tín hiệu chờ ring back

tín hiệu DCD data carrier detect

tín hiệu dị thời anisochronous signal

tín hiệu dò sóng mang carrier detect

tín hiệu dò sóng mang dữ liệu data carrier detect

tín hiệu điều biến modulating signal

tín hiệu điều khiển gọi call control signal

tín hiệu ghi giọng nói voice print
tín hiệu giám sát supervisory signal
tín hiệu gửi clear to send
tín hiệu hồi đáp answer back
tín hiệu không nhận cuộc gọi call not accepted signal
(các) tín hiệu làm lộ compromising emanations
tín hiệu ra output
tín hiệu ROS ROS
tín hiệu số digital signal
tín hiệu thông clear to send
tín hiệu tiến hành cuộc gọi call progress signal
tín hiệu tương tự analog signal
tín hiệu WACK WACK
tín hiệu xen vào intervention signal
tín hiệu yêu cầu gửi request to send
(sự) tín nhiệm trust
tinh chỉnh tuning
tình thế gây sự cố trouble condition
tính an toàn safety, security
tính an toàn đơn simple security property
tính bí mật của dữ liệu data confidentiality
tính chắc chắn safety
tính chẵn even parity
tính chẵn lẻ parity
tính chất giới hạn confinement property
tính chính xác accuracy
tính cơ động portability
tính dễ bị chặn interceptability
tính dễ tổn hại về mặt kỹ thuật technical vulnerability
tính dễ tổn thương vận hành operational vulnerability
tính đáng tin cậy dependability, trustworthiness
tính độc lập dữ liệu data independence
tính độc lập dữ liệu logic logical data independence
tính đơn giản simplicity
tính đúng đắn correctness
tính khả chuyển portability
tính khả dụng usability
tính khả quy trách nhiệm accountability
tính khách quan objectivity
tính không nhất quán khi cập nhật update inconsistency
tính không thể đảo ngược noninvertibility
tính lặp lại repeatability
tính lẻ odd parity
tính linh hoạt portability
tính nghiêm trọng materiality
tính nhạy cảm sensitivity
tính nhạy cảm susceptibility
tính nhạy cảm và mức nguy cấp sensitivity and criticality
tính nhất quán consistency
tính phân định trách nhiệm accountability
tính sẵn sàng availability
tính thông minh intelligence
tính toàn vẹn dữ liệu data integrity
tính toàn vẹn thông tin information integrity
tính toán cá nhân personal computing
tính toán phía người sử dụng end user computing
tính toán tích hợp integrated computing

tính toán tương tác interactive computing
tính tới hạn criticality
toàn tác transaction
(tính) toàn vẹn integrity
toàn vẹn hệ thống system integrity
toàn vẹn ứng dụng application integrity
toán hạng operand
toán tổ hợp combinatorics
toán tử operator
toán tử Boole Boolean operator
toán tử hợp join
toán tử logic logical operator
toán tử nối join
toán tử quan hệ relation operator
topo topology
topo mạng network topology
tổ chức CCTA CCTA
tổ chức CLODO CLODO
tổ chức ECMA ECMA
tổ chức ECOMA ECOMA
tổ chức ECSA ECSA
tổ chức ISO International Standards Organization
tổ chức ODETTE ODETTE
tổ chức tạo ra cơ sở dữ liệu database producer
Tổ chức tiêu chuẩn hóa quốc tế International Standards Organization
tổ hợp bị cấm forbiden combination
tổ hợp sai forbiden combination
tốc độ báo hiệu dữ liệu data-signalling rate
tốc độ bit bit rate
tốc độ cao high-speed
tốc độ chuyển dữ liệu data transfer rate
tốc độ chuyển dữ liệu thực actual data transfer rate
tốc độ dữ liệu data rate
tốc độ điều biến modulation rate
tốc độ kênh truyền line speed
tốc độ lặp xung pulse repetition rate
tốc độ thấp low speed
tốc độ thông tin information rate
tốc độ trung bình medium speed
tốc hoạt khóa key crunching
tốc hoạt số number crunching
tối mật Top Secret
tội phạm máy tính computer crime
tổn hao loss
tổn hao do cong nhẹ microbend loss
tổn hao dan xen insertion loss
tổn thất thông tin information loss
tổng băm hash total
tổng chạy - chạy run to run totals
tổng đài chuyển mạch dữ liệu data-switching exchange
tổng đài chuyển mạch gói packet-switching exchange
tổng đài máy tính tự động dành riêng PACX
tổng đài nhánh máy tính hóa computerized branch exchange
tổng đài nhánh tự động riêng private automatic branch exchange
tổng đài tự động nội bộ private automatic branch exchange
tổng kiểm tra checksum, hash total
tổng kiểm tra mật mã cryptographic checksum
tổng lô batch total
tổng thử test amount

trả bảo lãnh cover payment

trả lời answering

trả lời bằng tiếng nói voice answer-back

trả lời nhập dữ liệu bằng tiếng nói data input voice answerback

trả về số không có phân cực polarized return to zero

trạm station

trạm báo cháy dùng tín hiệu mã không nhiễu cục bộ local noninterfering coded station

trạm báo cháy không đập vỡ kính nonbreak glass station

trạm báo hỏa được mã liên tiếp và không can thiệp positive noninterfering and succession coded station

trạm chính primary station

trạm chính master station

trạm dịch vụ server

trạm dữ liệu data station

trạm điều khiển control station

trạm giám sát monitoring station

trạm kéo pull station

trạm kết hợp combined station

trạm kiểm soát mạng network control station

trạm làm việc workstation

trạm nóng mở open hot site

trạm ở xa remote station

trạm phụ secondary station

trạm phụ tributary station

trạm tách split site

trạm thứ cấp secondary station

trạm trung tâm central station

trạm trung tâm cấp A grade A central station

trạm trung tâm cấp AA grade AA central station

trạm trung tâm cấp B grade B central station

trạm vận hành báo động arming station

trang nhớ page

trạng thái state

trạng thái an toàn secure state

trạng thái điều hành executive state

trạng thái giám sát supervisor state

trạng thái sẵn sàng ready state

trạng thái thi hành executive state

trạng thái treo lock up

tranh chấp contention

tránh trót lọt defeat

trao đổi interchange

trao đổi dữ liệu data exchange

trao đổi dữ liệu điện tử electronic data interchange

trao đổi văn bản định hướng thông báo message oriented text exchange

trao đổi văn bản định hướng thông báo MOTIS

trao đổi xác thực authentication exchange

treo lock up

trễ do tranh chấp contention delay

trễ pha phase delay

trệch bias

tri thức phân tích split knowledge

trì hoãn/từ chối phục vụ delay/denial of service

trí tuệ intelligence

trí tuệ nhân tạo artificial intelligence

triết lý bảo vệ protection philosophy

triệt ký tự rỗng null suppression

(sự) triệt nguồn (phát xạ) source suppression

triệt ô cell suppression

triệt tương quan bậc không zero order correlation immune

triệu lệnh/giây MIPS

trình biên dịch compiler

trình biến đổi vị ngữ predicate transformer

trình dịch vụ tệp file server

trình phân tích chương trình program analyzer

trình phục vụ đĩa thông minh intelligent disk server

trình sao bit bit copier

trình theo dõi tracker

trình tự thanh toán payment order

trình tự xác thực authentication sequence

trong suốt transparent

trong suốt dãy bit bit sequence transparent

(độ) trong suốt mật mã cryptographic transparency

trọng tài arbiter

trội hơn dominate

trộm cắp burglary

(sự) trộn dãy multiplexing

trở kháng đường dây line impedance

trở kháng đường truyền line impedance

trở lại n bước go back n

trợ giúp help

trục trặc malfunction

Trung tâm An toàn Máy tính Quốc gia National Computer Security Center

trung tâm cấp chứng chỉ khóa key certification center

trung tâm CCETT CCETT

trung tâm chẩn đoán từ xa remote diagnostic center

trung tâm chuyển mạch switching center

trung tâm chuyển mạch thông báo message switching center

trung tâm chuyển mạch thông báo tự động automatic message switching center

trung tâm chuyển tiếp relay center

trung tâm chứng nhận khóa key certification center

trung tâm dịch khóa key translation center

trung tâm điều hành mạng network operating center

trung tâm NCC NCC

trung tâm NCIC NCIC

trung tâm NCSC NCSC

trung tâm nối dây wire center

trung tâm phát triển development center

trung tâm phân phối khóa key distribution center

Trung tâm phân tích thông tin Bộ quốc phòng Hoa Kỳ DOD Information Analysis Center

trung tâm thông tin information center

Trung tâm thông tin về tội phạm Quốc gia National Crime Information Center

trung tâm tính toán khép kín closed shop

truy cập access

truy lục dữ liệu data mining

truy lục dữ liệu data retrieval

truy lục khóa bội multiple key retrieval

truy nhập bộ nhớ trực tiếp direct memory access

truy nhập có kiểm soát controlled access

truy nhập dành riêng dedicated access

truy nhập do sự cố failure access

truy nhập đọc read access

truy nhập ghi write access

truy nhập gián tiếp indirect access

truy nhập hạn chế limited access

truy nhập ngẫu nhiên random access

truy nhập nối đuôi tailgating

truy nhập qua quay số dial access

truy nhập tệp file access

truy nhập thông tin access to information

truy nhập access

truy nhập trực tiếp direct access

truy nhập từ xa remote access

truy tìm dữ liệu data retrieval

(sự) truyền transmission

truyền analog analog transmission

truyền cân bằng balanced transmission

truyền dải gốc baseband

truyền dị thời anisochronous transmission

truyền dữ liệu data transmission

truyền đa kiểu multicast

truyền đẳng thời isochronous transmission

truyền đồng bộ synchronous transmission

(giao thức) truyền đồng bộ nhị phân binary synchronous communications

truyền đồng thời simultaneous transmission

truyền hình khép kín closed circuit television

truyền không cân bằng unbalanced transmission

truyền không đồng bộ asynchronous transmission

truyền nối tiếp các byte byte serial transmission

truyền song song parallel transmission

truyền thông communication

truyền thông dữ liệu data communications

truyền thông hữu tuyến line communications

truyền thông liên quá trình interprocess communication

truyền thông song song parallel computer

truyền thông theo lô batched communication

truyền thông tuần tự serial communication

truyền tới tấp flooding

truyền tràn flooding

(sự) truyền tuần tự serial transmission

truyền tương tự analog transmission

truyền văn bản từ xa teletext

trực tiếp on line

trực tuyến on line

trường mục treo suspense account

trường field

trường dữ liệu thẻ khác other card data

trường E/E field

trường Galois Galois field

trường OCD OCD

TSW telesoftware

TTKĐB async

(sự) tuân thủ cách ly isolation enforcement

tuổi thọ an toàn security life

tuổi thọ thiết bị load life

tuổi thọ trung bình mean life

tùy chọn optional

tùy ý optional

tuyến an toàn secure path

tuyến báo động alarm line

tuyến liên kết tie line

tuyến liên kết link

tuyến liên lạc tin cậy trusted communications path

tuyến tấn công attack path

tuyến thay thế alternate route

tuyến tin cậy trusted path

tuyệt mật Secret

tư liệu material

tư liệu khu vực công cộng public domain

tư liệu tạo khóa mật mã cryptographic keying material

từ word

(sự) từ chối repudiation

từ chối denial

từ chối dịch vụ thông báo denial of message service

từ dữ liệu data word

từ điển dữ liệu data dictionary

từ điển mã code book

từ khóa keyword, lockword

từ thông magnetic flux

từ xa remote

tự an toàn fail mafe

tự chỉnh balancing

tự do thông tin FOI, freedom of information

tự đồng bộ self-synchronizing, self-synchronous

tự động hóa văn phòng OA (Office Automation)

tự khóa fail secure

tự khôi phục auto restore

tương đương tuyến tính linear equivalence

tương hoán reciprocal

tương hỗ reciprocal

tương tác interactive

(tính) tương thích compatibility

(tính) tương thích hướng lên upward compatibility

tương tự analog

tỷ lệ lỗi error rate

tỷ lệ lỗi khối block error rate

tỷ lệ lỗi sót residual error rate

tỷ lệ nỗ lực thấp nhất zero effort rate

tỷ số s/n signal to noise ratio, s/n ratio

tỷ số tín trên tạp signal to noise ratio

U

UA UA

ủy ban ANSI X3.T1 ANSI X3.T1

ủy ban CCIR CCIR

ủy ban CNIL CNIL

ủy ban CNPDPI CNPDPI

ủy ban CoCom CoCom

ủy ban Lindop Lindop Committee

ủy ban NTISSC NTISSC (National Telecommunications and Information System Security Committee)

Ủy ban Quốc gia về xử lý và tự do dữ liệu National Commission on Data Processing and Freedom

ủy ban trẻ Younger Committee

ủy ban truyền thông liên bang Federal Communications Commission

ủy ban tư vấn quốc tế về điện báo và điện thoại Comité Consultatif Internationale de Télégraphie et Téléphonie

ủy nhiệm delegate

(sự) ủy nhiệm lưu giữ mã nguồn source code escrow

(sự) ủy quyền nguồn source authorization

ứng dụng nhạy cảm sensitive application

(sự) ước lượng evaluation

ước lượng tĩnh static evaluation

ước số chung lớn nhất greatest common divisor

USCLN GCD

ưu tiên xử lý processing priority

V

va đường truyền hit on the line
vacxin vaccine
vành ring
vành bảo vệ protection ring
vành đai (bảo vệ) perimeter
vành đai trong inside perimeter
vào cổng sau piggyback entry
vào giữa chừng between-the-lines entry
vào giữa đường between-the-lines entry
vào mạng log on
vào rác ra rác garbage in garbage out
vào sau ra trước last in first out, LIFO
vào trước ra trước first in first out
VAR VAR (Value Added Retailer)
văn bản text
văn bản thông báo message text
văn bản viđeo videotext
văn phạm grammar
văn phòng dịch vụ service bureau
văn phòng gián tiếp back office
văn phòng hỗ trợ back office
văn phòng máy tính computer bureau
văn phòng OMB OMB
văn phòng OUSD&E OUSD&E
văn phòng tính toán computer bureau
văn phòng trực tiếp front office
(các) vấn đề để sót residue problems
vấn tin đặc biệt ad hoc enquiry
vấn tin không theo thể thức ad hoc enquiry
vận hành song lộ diplex operation
vận hành song tin diplex operation
vật chứa container
vẽ hoa pray paint
vectơ vector
vectơ điều khiển control vector
vectơ khởi đầu initialization vector
vectơ trễ delay vector
vét cạn khóa key exhaustion
vét cạn thông báo message exhaustion
vết giao dịch transaction trail
vết kiểm toán audit trail
vết loang blob
vết sự cố fault trace
vệt kiểm toán an toàn security audit trail
vi phạm an toàn security breach
(sự) vi phạm an toàn truyền dẫn violation of transmission security
vi phạm bản quyền piracy
vi phạm bản quyền phần mềm software piracy
vi phạm quy chế cần biết need to know violation
(sự) vi phạm tính an toàn security

violation

ví điện tử electronic purse, electronic wallet

(câu lệnh) vị ngữ predicate

vị thế mở open position

vị trí ấm warm site

vị trí có phòng máy shell site

vị trí nóng hot site

vị trí nóng khép kín closed hot site

vị trí tách split site

videotex tương tác interactive videotex

viễn thông telecommunications

viễn truyền văn bản teletext

viện ASET ASET

viện IInfSc IInfSc (Institute of Information Scientists)

Viện IRE IRE (Institute of Radio Engineers)

Viện khoa học và công nghệ Quốc gia National institute for Science and Techology

Viện tiêu chuẩn Anh British Standards Institution

Viện tiêu chuẩn Hợp chủng Quốc Hoa kỳ USASI

Viện tiêu chuẩn quốc gia Hoa Kỳ American National Standards Institute

Viện toàn vẹn thông tin quốc tế International Information Integrity Institute

virut virus

virut 90 Virus-90

virut 101 Virus-101

virut W-13 W-13

virut 13 tháng 7 July 13th

virut 16 tháng Sáu June 16th

virut AGI AGI

virut AGI-Plan AGI-Plan

virut Aids Aids

virut AirCop AirCop

virut Alabama Alabama

virut Alameda Alameda

virut Amstrad Amstrad

virut Anthrax-Boot Anthrax-Boot

virut Anthrax-File Anthrax-File

virut Arab Arab Virus

virut Armageddon Armageddon

virut BeBe BeBe

virut Beeper Beeper

virut Best Wish Best Wish

virut Black Monday Black Monday

virut Blood-2 Blood-2

virut Bloody Bloody

virut Boot Boot

virut Brain Brain

virut Brain Slayer Brain Slayer

virut Burger Burger

virut Cancer Cancer

virut Carioca Carioca

virut Cascade Cascade

virut Casino Casino

virut Casper Casper

virut Chaos Chaos

virut Christmas - J Christmas-J

virut Christmas Violater Christmas Violater

virut Chúc mừng năm mới Happy New Year

virut Course Boot Curse Boot

virut cung khởi động boot sector virus

virut Dark Avenger Dark Avenger

virut Datacrime datacrime

virut Datacrime II Datacrime II
virut Datacrime II-B Datacrime II-B
virut Datacrime-B Datacrime-B
virut DataLock DataLock
virut Dbase Dbase
virut Den Zuk Den Zuk
virut Destructor Destructor
virut Devil's Dance Devil's Dance
virut Dir-Vir Dir-Vir
virut Disk killer Disk killer
virut Do-Nothing Do-Nothing
virut Doom2 Doom2
virut Dot killer Dot killer
virut EDV EDV
virut Empire Empire
virut Enigma Enigma
virut Father Christmas Father Christmas
virut Fellowship Fellowship
virut Fish-6 Fish-6
virut Flash Flash
virut Flip Flip
virut F-Word F-Word
virut Form Form
virut Frere Jacques Frere Jacques
virut Frogs Frogs
virut Fu Manchu Fu Manchu
virut ghi đè overwriting virus
virut Ghost Boot Ghost Boot
virut Ghost COM Ghost COM
virut Guppy Guppy
virut Happy Day Happy Day
virut Whale Whale
virut Holocaust Holocaust
virut Hybrid Hybrid
virut Hymn Hymn
virut Hymn-2 Hymn-2
virut Icelandic Icelandic
virut IKV528 IKV528
virut Invader Invader
virut Iraqi Warrior Iraqi Warrior
virut Wiscosin Wisconsin
virut ItaVir ItaVir
virut Jeff Jeff
virut Jerusalem Jerusalem
virut JoJo JoJo
virut Joker Joker
virut Joshi Joshi
virut Justice Justice
virut Kakuturbo Kukaturbo
virut ké phá đĩa Disk killer
virut Kennedy Kennedy
virut Keypress Keypress
virut không ghi đè nonoverwriting virus
virut Korea Korea
virut Label Label
virut Lazy Lazy
virut Leapfrog Leapfrog virus
virut Lehigh Lehigh
virut Leprosy Leprosy
virut Leprosy-B Leprosy-B
virut Liberty Liberty
virut Lisbon Lisbon
virut Little Pieces Little Pieces
virut Mardi Bros Mardi Bros
virut máy tính computer virus
virut MGTU MGTU virus
virut Michelangelo Michelangelo
virut Microbes Microbes
virut Mirror Mirror

virut MIX1 MIX1
virut MIX2 MIX2
virut Monxla Monxla
virut Murphy Murphy
virut Musis Bug Musis Bug
virut New Sunday New Sunday
virut Nina Nina
virut Nomenclature Nomenclature
virut Off Stealth Off Stealth
virut Wolfman Whale Wolfman Whale
virut Ontario Ontario
virut Oropax Oropax
virut PI PI
virut Paris Paris
virut Parity Parity
virut Payday Payday
virut Pentagon Pentagon
virut Perfume Perfume
virut Phantom Phantom
virut Ping Pong-B Ping Pong-B
virut Plague Plague
virut Plastique Plastique
virut Polimer Polimer
virut Polish 2 Polish-2
virut Polish 217 Polish 217
virut Print Screen Print Screen
virut RedX RedX
virut S-847 S-847
virut Saddam Saddam
virut Swap Boot Swap Boot
virut Saturday 14 Saturday 14th
virut Scott's Valley Scott's Valley
virut Sentinel Sentinel
virut Shake Shake
virut Swiss 143 Swiss 143
virut Skism Skism
virut Slow Slow
virut Solano Solano
virut Sorry Sorry
virut Spyer Spyer
virut Staf Staf
virut Star Dot Star Dot
virut Stealth Stealth virus
virut Stone-90 Stone-90
virut Stoned Stoned
virut Stricker Stricker
virut Subliminal Subliminal
virut Sunday Sunday
virut SURIV01 SURIV01
virut SURIV02 SURIV02
virut Sverdlov Sverdlov
virut Sylvia/Holland Sylvia/Holland
virut Syslock Syslock
virut Taiwan Taiwan
virut Taiwan3 Taiwan3
virut Taiwan4 Taiwan4
virut Teror Teror
virut Tester Tester
virut thứ bảy ngày 14 Saturday 14th
virut Thứ sáu ngày 13 Friday 13th
virut Tiny Tiny
virut Tiny-133 Tiny-133
virut Traceback Traceback
virut Tunes Tunes
virut Typo Boot Typo Boot
virut Typo/Fumble Typo/Fumble
virut USSR USSR
virut V-299 V-299
virut V-555 V-555
virut V800 V800

virut V-801 V-801
virut V-961 V-961
virut V2000 V2000
virut V2100 V2100
virut Vacsina Vacsina
virut Vcomm Vcomm
virut Victor Victor
virut Vienna/648 Vienna/648
virut Violator Violator
virut Voronezh Voronezh
virut Yankee-2 Yankee-2
virut Yankee Doodle Yankee Doodle
virut Zero Bug Zero Bug
virut ZeroHunt ZeroHunt
vít mũ có vấu clutch head screw
volum volume
vòng loop, ring
vòng bảo vệ tệp file protect ring
Vòng Cambridge Cambridge Ring
vòng có khe slotted ring
vòng lặp an toàn security loop
vòng lặp loop
vọng cục bộ local echo
vọng mềm cục bộ local software echo
vọng tại chỗ local echo
vô cùng infinity
vô hướng scalar
vùng band
vùng an toàn security area
vùng bị hạn chế restricted area
vùng chéo cross zone
vùng chết dead zone
vùng địa chỉ address space
vùng được kiểm soát controlled area
vùng giao nhau cross zone
vùng khoanh compartment
vùng không nhạy dead zone
vùng kiểm soát control zone
vùng kiểm soát Tempest Tempest control zone
vùng làm việc an toàn secure working area
vùng nhớ heap heap
vùng phím đa tần MF keypad
vùng phím số digital keyad
vùng quang clear zone
vùng trống trải clear zone
vùng truy nhập có kiểm soát controlled access area

X

xác định đặt quan hệ handshaking

xác lập lại reset

(sự) xác minh verification

xác minh verify

xác minh hình thức formal verification

(sự) xác nhận tính hợp lệ validation

xác nhận tính hợp lệ dữ liệu data validation

xác thực authenticate

(sự) xác thực authentication

xác thực cá nhân personal authentication

xác thực danh tính identity authentication

xác thực đối tượng object authentication

xác thực hệ thống system authentication

xác thực hỏi và đáp challenge and reply authentication

xác thực lẫn nhau mutual authentication

xác thực mật mã cryptographic authentication

xác thực nguồn gốc dữ liệu data origin authentication

xác thực người sử dụng user authentication

xác thực người sử dụng authentication of users

xác thực thông báo message authentication

xác thực thực thể ngang hàng peer entity authentication

xáo trộn tiếng nói speech scrambling

xáo trộn tiếng nói voice scrambling

xâm nhập intrusion

xâm phạm intrusion

xâu string

xâu bit bit string

xâu rỗng null string

xây dựng chỉ mục index build

xây dựng chữ ký signature construction

xé để mở tear-me-open

xem lại mã code review

xem lướt browsing

xem nhanh snapshot

xem trộm browsing

xen kẽ bit bit interleaving

xén bớt bản mã ciphertext stealing

xeri chuẩn Rainbow Rainbow series

xét duyệt kiểm soát nội bộ internal control review

xếp hạng rank

xích khối mã cipher block chaining

xích mã khối block cipher chaining

xích vòng daisy chain

xóa delete, clearing

(sự) xóa erasure

xóa hẳn degauss

xóa ký tự delete character

(quá trình) xóa mức cao superzapping

xóa tệp file cleanup

xóa về zero clearing

XOR EXCLUSIVE OR

xổ để cứu rescue dump

xuất exportation

xuất bản điện tử electronic publishing

xung chuyển tiếp đường dây line transient

xung đánh dấu mark

(các) xung đồng bộ synchronization pulses, sync pulses

xuống cấp degradation

xuống cấp nhẹ graceful degradation

xuyên âm crosstalk

xuyên âm đa nguồn babble

xuyên âm rõ intelligible crosstalk

xuyên âm sợi quang fiber cross-talk

xử lý processing

xử lý dư redundant processing

xử lý dữ liệu data processing

xử lý dữ liệu điện tử electronic data processing

xử lý dữ liệu phân tán distributed data processing

xử lý đặc quyền privileged process

xử lý giao tác transaction processing

xử lý ống dẫn pipelining

xử lý phân tán distributed processing

xử lý phía người dùng end user computing

xử lý quan trọng critical processing

xử lý song song parallel processing

xử lý tệp file processing

xử lý theo lô từ xa remote batch processing

xử lý tới hạn critical processing

xử lý trục trặc troubleshoot

xử lý tùy ý discretionary processing

xử lý từ xa teleprocessing

xử lý ưu tiên priority processing

Y, Z

yêu cầu requirement

(các) yêu cầu an toàn security requirements

(các) yêu cầu bảo đảm an toàn tối thiểu MSAR

yêu cầu bắt đầu dịch vụ request service initiation

(các) yêu cầu chức năng an toàn tối thiểu MSFR

yêu cầu gọi call request

(các) yêu cầu không gian và thời gian time and space requirements

yêu cầu MSAR MSAR

yêu cầu MSFR MSFR

yêu cầu thông ngăn chứa container clearance required

yêu cầu truyền lại tự động automatic retransmission request

zero hóa zeroization

TÀI LIỆU THAM KHẢO

1. Information Security
   Dictionary of concepts, standards and terms
   MacMillan Publishers Ltd. 1992
2. McGraw-Hill Dictionary of Scientific and Technical Terms
   Fifth edition, New York, San Francisco Washington D.C. London, Sydney..., 1994
3. IBM Dictionary of Computing
   McGraw-Hill, Inc., New York, London, Tokyo, 1994
4. Computer Dictionary
   Microsoft Press, Second edition, 1994
5. The American Heritage Illustrated Encyclopedic Dictionary
   Hougston Mifflin Company-Boston, 1987
6. Dictionary of Computer and Internet Terms
   Melody Convington and Douglas Dowing, Barron; 1998
7. The Free On-line Dictionary of Computing
   Editor Denis Howe, 1998
8. MacMillan Dictionary of Information technology
   London, 1989
9. Từ điển Công nghệ thông tin - Điện tử - Viễn thông Anh - Việt
   Nhà xuất bản Khoa học và Kỹ thuật, Hà Nội - 2000
10. Các từ điển chuyên ngành và đa ngành
    Nhà xuất bản Khoa học và Kỹ thuật, Hà Nội, 1961 - 2000
11. Từ điển tiếng Việt
    Nhà xuất bản Khoa học Xã hội, Hà Nội, 1988.

BAN TỪ ĐIỂN
NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

TỪ ĐIỂN
AN TOÀN THÔNG TIN
ANH - VIỆT VÀ VIỆT- ANH

Chịu trách nhiệm xuất bản PGS. TS TÔ ĐĂNG HẢI
Biên tập TRẦN HÒA, ĐẶNG VĂN SỬ, VŨ TRUNG THÀNH
Sửa chế bản HÒA - SỬ - THÀNH
Vẽ bìa HƯƠNG LAN

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT
70 Trần Hưng Đạo - Hà Nội

In 2.000 cuốn, khổ 16 x 24 cm tại Công ty Liksin số 701 Kinh Dương Vương Q.6 TP. Hồ Chí Minh, ĐT : 751 2562. Mã số in : SC 0103, số in : 672/01.
Giấy phép xuất bản số 123/ CXB Cục xuất bản cấp ngày 18/1/2001
In xong và nộp lưu chiểu tháng 8 năm 2001.



Cuốn từ điển này bao quát
các chủ đề quan trọng của
AN TOÀN THÔNG TIN gồm:

* Phân tích rủi ro
* Các chuẩn
* An toàn cơ sở dữ liệu
* Máy tính cá nhân
* Quản lý khóa
* Virut
* Các hệ tin cậy
* Vấn đề xác thực
* Kiểm soát truy nhập

*Mỗi thuật ngữ tiếng Anh đều
có thuật ngữ tiếng Việt đối chiếu
và có phần giải thích súc tích
kèm theo

*Các hình minh họa gọn và rõ ràng
giúp hiểu chính văn tốt hơn

8 935048 910412

Giá: 165.000 đ