NGHIÊN CỨU GIẢI PHÁP BẢO MẬT CHO DỊCH VỤ VOIP

Trần Thị Hiệp*, Vũ Thị Khánh Vân, Hà Thị Thu Hiền

Khoa Công nghệ Thông tin, Trường Đại học Công nghiệp Việt Trì

Email: hieptranit@gmail.com

Tóm tắt:

Hiện nay công nghệ 4.0 đang phát triển mạnh mẽ. VoIP là dịch vụ gọi nhóm nội bộ hoàn hảo áp dụng cho các công ty, doanh nghiệp. Tuy nhiên, việc bảo vệ gói dịch vụ này hiện vẫn còn nhiều lỗ hổng mà hacker dễ xâm nhập. Nhóm nghiên cứu xây giải pháp bảo mật cho dịch vụ VoIP, nhằm hạn chế thấp nhất những thiệt hại khi khách hàng sử dụng dịch vụ.

Từ khóa: *Công nghệ , VOIP, Open VPN, Firewall*

STUDYING SECURITY SOLUTIONS FOR VOIP SERVICES

Abstract:

Currently, technology 4.0 is developing strongly. VoIP is the perfect internal group calling service for companies and businesses. However, the protection of this service pack still has many vulnerabilities that hackers can easily penetrate. The research team builds a security solution for VoIP services, in order to minimize the damage when customers use the service.

Keywords: *Technology, VOIP, Open VPN, Firewall*

1. GIỚI THIỆU

Ngày nay, công nghệ thông tin được ứng dụng vào mọi mặt của đời sống, hoạt động trao đổi thông tin giữa các cá nhân, tổ chức, doanh nghiệp diễn ra mọi lúc mọi nơi. Việc trao đổi thông tin giữa các cá nhân và tập thể được thể hiện qua các hình thức cơ bản như: Dịch vụ điện thoại do một đơn vị cung cấp dịch vụ nhất định thực hiện; trao đổi qua thư điện tử; Gọi dịch vụ zalo…

Hiện nay hầu hết các trường đại học và trung học phổ thông, trung học cơ sở... đang sử dụng dịch vụ VnEdu của các nhà mạng như Viettel hoặc Vinaphone làm kênh chính thống để gửi các kết quả học tập và các thông báo về gia đình và học sinh theo kênh một chiều. Hiện các học sinh và phụ huynh đang phải đóng kinh phí là 100.000 đồng/ năm để chi trả cho dịch vụ này. Điều này chứng minh, hệ thống dịch vụ VoIP nếu triển khai được thì sẽ rất có lợi cho nhà trường nói riêng và các trường khác đóng trên địa bàn nói chung.

Cùng đó, VoIP mang lại nhiều lợi ích như: Khả năng linh hoạt cao, có thể kết nối bất cứ khi nào, bất cứ nơi đâu, chỉ cần ở đó có thể truy cập được Internet; Gọi nội bộ miễn phí giữa các giáo viên và sinh trong nhà trường với nhau, giá thành đầu tư hợp lý; Chất lượng cuộc gọi tốt, đảm bảo chất lượng trong khi hội thoại trực tuyến; Băng thông không bị hạn chế, chỉ phụ thuộc vào tốc độ đường truyền internet nhà trường đang sử dụng; Số lượng kết nối không bị hạn chế.

Tuy nhiên, việc thực hiện các giao dịch thông tin trên chưa hoàn toàn chủ động cho đơn vị và cá nhân, đồng thời độ bảo mật không cao vì dịch vụ cho quá nhiều đối tượng cùng lúc.

Do đó, việc nghiên cứu giải pháp bảo mật cho dịch vụ VOIP là vô cùng cần thiết:

1. Xây dựng mô phỏng trên phần mềm một hệ thống dịch vụ thoại VoIP dựa trên nền Internet, bằng hình thức cấp cho người dùng một tài khoản. Từ đó, người dùng có thể trao đổi thông tin với nhau thông qua dịch vụ này mà không mất phí cuộc gọi, tin nhắn. Thông tin có thể trao đổi hai chiều, dễ dàng cài đặt và sử dụng.

2. Để bảo mật riêng cho hệ thống và cuộc gọi, tin nhắn của người dùng, nhóm tác giả đề xuất một số phương án bảo mật cho hệ thống, đồng thời xây dựng một hệ thống bảo mật sử dụng Open VPN và Firewall tích hợp nhằm đảm bảo an toàn trước nguy cơ tấn công mạng và ăn cắp thông tin

2. THỰC NGHIỆM

2.1 Cơ sở lý luận và thực tiễn

2.1.1. Hệ thống VoIP:

VoIP (Voice Over Internet Protocol) là công nghệ cho phép truyền thông tin giọng nói từ nơi này sang nơi khác thông qua các mạng sử dụng IP để truyền thông tin. VoIP cũng thường được biết đến dưới một số tên như điện thoại Internet, điện thoại IP, điện thoại băng thông rộng, v.v.

Ở điện thoại bình thường, tín hiệu thoại được lấy mẫu với tần số 8 KHz, sau đó được lượng tử hóa 8 bit / mẫu và được truyền ở tốc độ 64 KHz đến mạng chuyển mạch và sau đó được truyền đến mục tiêu. Ở phía máy thu, tín hiệu này sẽ được giải mã thành tín hiệu gốc.

Công nghệ VoIP không hoàn toàn khác với điện thoại thông thường. Đầu tiên, tín hiệu thoại cũng được số hóa, nhưng sau đó thay vì truyền qua PSTN (Public Switched Telephone Network -Mạng điện thoại chuyển mạch công cộng) qua các trường chuyển mạch, tín hiệu thoại được nén xuống thấp, sau đó được đóng gói, truyền qua mạng IP. Ở phía người nhận, các luồng thoại sẽ được giải nén thành các luồng PCM 64 (Pulse Code Modulation - Điều chế mã xung) và được truyền đến thuê bao được gọi.

2.1.2. Thực trạng sử dụng VoIP hiện nay

a. Các ứng dụng sử dụng VoIP

Các hình thức kết nối của Voip trong môi trường doanh nghiệp, công nghệ VoIP thường phổ biến dưới dạng kết nối phần cứng (thông qua điện thoại hoặc adapter) hoặc kết nối phần mềm (thông qua một số ứng dụng gọi điện thoại)

Phương pháp sử dụng Voip phổ biến nhất là với điện thoại truyền thống. Có nhiều cách để áp dụng công nghệ VoIP với điện thoại Analog truyền thống, điện thoại kỹ thuật số hay còn gọi là điện thoại VoIP.

- Voip với điện thoại Analog: Vì việc truyền giọng nói trong Voip diễn ra qua Internet, do đó một chiếc điện thoại thông thường không có khả năng VoIP. Tuy nhiên, có một adapter được gọi là Analog Telephone Adapter (ATA) hay còn gọi là gateway FSX có khả năng chuyển đổi tín hiệu điện thoại analog thành tín hiệu số có thể truyền qua Internet.

- VoIP với điện thoại IP bạn không cần phải mua adapter ATA để kết nối Internet, chỉ cần cắm điện thoại trực tiếp vào cổng Ethernet hỗ trợ mạng. Điện thoại sẽ giao tiếp từ Internet đến dịch vụ VoIP bạn đã đăng ký.

- VoIP với thiết bị chuyển đổi từ analog sang IP hay còn gọi là gateway FXO: Một số công ty sản xuất phần cứng có thể cắm vào jack cắm Ethernet trong nhà để chuyển đổi điện thoại tiêu chuẩn thành điện thoại có thể sử dụng Voip. Phần cứng này có một cổng web được sử dụng để xem các cuộc gọi, kiểm tra thư thoại và thiết lập tích hợp với các dịch vụ khác.

Cách rẻ nhất để sử dụng VoIp là kết nối tai nghe có micro với máy tính, nhưng yêu cầu phần mềm Voip để truyền giọng nói của người gọi đến người nhận sử dụng cùng phần mềm. Ngoài ra, có nhiều ứng dụng Voip có khả năng thực hiện các cuộc gọi điện thoại tiêu chuẩn. Một số ứng dụng phần mềm Voip phổ biến nhất: Skype, Jabber, Google Hangout, Google Voice.

Trong thực tế, các ứng dụng trong Voip như ứng dụng OTT (Over-the-top app) là thuật ngữ để chỉ các ứng dụng và các nội dung như âm thanh, video được cung cấp trên nền tảng Internet và không một nhà cung cấp hoặc bất kỳ cơ quan nào có thể can thiệp vào. Hầu hết các ứng dụng OTT đều sử dụng công nghệ VoIP để thực hiện cuộc gọi như: Zalo, facebook, viber, skype, telegram….

Bên cạnh các ứng dụng OTT thì công nghệ VoIP còn được ứng dụng để xây dựng trong hệ thống điện thoại VoIP. Các thiết bị đầu cuối như gateway, điện thoại IP, phần mềm softphone.

b. Đánh giá tính bảo mật của các ứng dụng sử dụng dịch vụ VoIP.

Các ứng dụng sử dụng dịch vụ này khá nhiều lỗ hổng khiến virus và ứng dụng độc hại dễ dàng xâm nhập. Đây cũng là điều kiện thuận lợi để hacker phá bỏ hệ thống bảo mật nhằm đánh cắp dữ liệu khách hàng. Với những hệ thống VoIP không có cơ chế mã hóa, VoIP miễn phí… thì hàng rào phòng thủ lại càng mỏng manh. Vì vậy, các nhà sản xuất phải thường xuyên đưa ra các phiên bản "vá" lỗi. Đó là cũng là lý do mà các doanh nghiệp, nhà sử dụng nên cập nhật thường xuyên bản quyền các phần mềm VoIP và chú trọng thay đổi phần cứng. Các phiên bản mới sẽ làm tốt chức năng bảo mật hệ thống VoIP hơn, tránh được các cuộc tấn công điều hướng cuộc gọi và đánh cắp thông tin người dùng.

Các thiết bị chạy VoIP thường là "con mồi béo bở" của virus, thường xuyên là đối tượng của các cuộc tấn công đánh cắp dữ liệu. Nguyên nhân gây ra tình trạng này một phần đến từ sự ảnh hưởng chung của các cuộc xâm nhập mạng lớn, cả virus và phần mềm độc hại đều có thể làm hại đến hệ thống VoIP. Hậu quả mang đến có thể là gây mất kết nối, mất dữ liệu hoặc làm lộ thông tin khách hàng vốn cần được bảo mật một cách nghiêm ngặt.

Chính vì vậy, cài đặt và sử dụng các phần mềm chống virus, phần mềm độc hại luôn là giải pháp đơn giản, hiệu quả và thiết thực nhất để tăng cường tính bảo mật hệ thống VoIP. Do đó, để đảm bảo an toàn, người sử dụng nên thiết lập các chính sách bảo mật nội bộ cho mình.

Tường lửa cũng là một giải pháp dễ thực hiện để ngăn chặn những truy cập trái phép từ bên thứ hai. Mặc dù không được đánh giá cao về hiệu quả, song tường lửa vẫn được nhiều doanh nghiệp lựa chọn vì chúng khá dễ cài đặt và không mất nhiều chi phí.

Do đó, nhóm nghiên cứu đã đề xuất giải pháp để bảo mật hệ thống VoIP, có thể kết hợp sử dụng tường lửa với các biện pháp khác như các chính sách nội bộ, giám sát các cuộc gọi đến và đi, nhận diện các truy cập trái phép... nhằm đảm bảo tối ưu nhất cho hệ thống.

2.2. Thiết kế giải pháp bảo mật cho VoIP

2.2.1. Vấn đề bảo mật với VoIP

Những kẻ tấn công thường nhắm vào các hệ thống và ứng dụng phổ biến và được công bố rộng rãi nhất. VoIP đã trở thành một trong những ứng dụng như vậy. Trong phần này, trình bày các cuộc tấn công vào cơ sở hạ tầng VoIP. Các cuộc tấn công vào năm loại chính, bao gồm: DoS, nghe lén, Masquerading, gian lận và SPIT.

a. Tấn công DoS

Tấn công DoS là một loại tấn công gửi một lượng lớn yêu cầu đến dịch vụ cần bị tấn công, có thể dựa trên lỗi của mục tiêu. Tùy thuộc vào nguồn của các cuộc tấn công, nó được chia thành DoS và DDoS phổ biến. Mục đích là để làm cho mục tiêu bị dừng lại, không thể đáp ứng dịch vụ được gửi đến. Mức độ nghiêm trọng có thể gây ra sự cố hệ thống, sự cố cơ sở dữ liệu, v.v.

b. Nghe trộm

Nghe lén và phân tích dữ liệu trên đường truyền - Kẻ tấn công sẽ tìm cách thu thập thông tin nhạy cảm để chuẩn bị cho các cuộc tấn công tiếp theo. Trong VoIP hoặc trong các ứng dụng đa phương tiện trên Internet, kẻ tấn công có khả năng giám sát luồng tín hiệu hoặc dữ liệu không được mã hóa, trao đổi không được bảo vệ giữa người dùng. Phương pháp này nghe, lưu trữ, phân tích các gói hoặc giả thời gian thực trên đường truyền có thể là chủ động hoặc có thể bị động. Mục đích của kẻ tấn công là thông tin nhạy cảm như thông tin thẻ tín dụng, thông tin mật khẩu khác ..

c. Hóa trang

Là khả năng mạo danh người dùng, thiết bị hoặc dịch vụ để có quyền truy cập vào mạng, dịch vụ, thành phần mạng hoặc thông tin. Các cuộc tấn công giả mạo có thể được sử dụng để thực hiện hành vi gian lận, truy cập trái phép vào thông tin nhạy cảm và thậm chí làm gián đoạn dịch vụ. Mục tiêu của cuộc tấn công giả mạo là người dùng, thiết bị, các thành phần mạng.

d. Gian lận

Khả năng này xảy ra khi kẻ tấn công có một đặc quyền nhất định trong hệ thống, có

thể đó là kết quả từ các cuộc tấn công khác. Sau đó, kẻ tấn công có thể sử dụng kết quả có sẵn cho các mục đích cá nhân như ăn cắp phí, ăn cắp dịch vụ ... Đây là vấn đề nhà cung cấp dịch vụ, nhà phân phối quan tâm.

e. SPIT

Thư rác VoIP hay còn gọi là SPIT dự kiến sẽ là một vấn đề nghiêm trọng đối với các mạng VoIP. VoIP chưa phổ biến nhưng bắt đầu đặc biệt với sự xuất hiện của VoIP như một công cụ công nghiệp. Mỗi tài khoản VoIP có một địa chỉ IP được liên kết, những kẻ gửi thư rác dễ dàng gửi tin nhắn của họ đến hàng ngàn địa chỉ IP. Tin nhắn rác có thể mang virus và phần mềm gián điệp cùng với chúng. Điều này đưa chúng ta đến một nguy cơ khác của SPIT là lừa đảo qua VoIP. Tấn công lừa đảo bao gồm gửi thư thoại cho một người và giả mạo thông tin từ một bên đáng tin cậy đến người nhận như ngân hàng hoặc dịch vụ thanh toán trực tuyến, vì thư thoại thường yêu cầu dữ liệu bí mật như mật khẩu hoặc số thẻ tín dụng.

2.2.2. Giải pháp bảo mật cho VoIP

a. Giải pháp cho các cuộc tấn công DoS

Một số biện pháp đối phó để xử lý các cuộc tấn công DoS trong SIP.

- Giám sát và tường lửa: Lọc lưu lượng không mong muốn. Duy trì danh sách những người dùng không được xác thực, nghi ngờ và từ chối những người dùng đó thiết lập các phiên

- Xác thực: Giải pháp là cấu hình xác thực trên ứng dụng VoIP. Để xác minh danh tính của người dùng trước khi chuyển tiếp tin nhắn của anh ấy / cô ấy. Xác thực có thể yêu cầu hai thiết bị VoIP giao tiếp để xác thực lẫn nhau trước khi bắt đầu giao tiếp thực tế. Việc xác thực lẫn nhau này có thể dựa trên một bí mật chung được biết trước khi giao tiếp, gây khó khăn nếu không kẻ tấn công giả mạo danh tính.

- Proxy không trạng thái: Để giảm nguy cơ tấn công cạn kiệt bộ nhớ (DoS), do đó có thể được sử dụng để thực hiện các kiểm tra bảo mật khác như xác thực người dùng, đăng ký bên thứ ba và lọc các nguồn spam.

- Thiết kế máy chủ (ví dụ: CPU, bộ nhớ và kết nối mạng) - là tuyến phòng thủ đầu tiên chống lại các cuộc tấn công DoS.

b. Giải pháp cho các cuộc tấn công nghe trộm

- Sử dụng phần cứng có chất lượng tốt.

- Đảm bảo rằng quyền truy cập vào tủ dây chỉ được giới hạn cho nhân viên có thẩm quyền.

- Thực hiện bảo mật địa chỉ MAC dựa trên cổng, trên bất kỳ điểm mạng dễ bị tổn thương nào.

- Bắt đầu một quy trình để thường xuyên quét mạng cho các thiết bị chạy ở chế độ không kiểm soát theo quy trình chặt chẽ.

- Mã hóa lưu lượng VoIP, đây là một phương pháp tốt để ngăn chặn nghe lén, tuy nhiên nó bổ sung thêm chi phí.

c. Giải pháp cho các cuộc tấn công giả mạo

Một mô-đun xác thực hiệu quả kết hợp với mã hóa sẽ là một giải pháp hiệu quả để giả mạo và giả mạo các cuộc tấn công

d. Giải pháp cho các cuộc tấn công gian lận

Các nhà cung cấp VoIP có thể ngăn chặn gian lận phí bằng cách cấu hình đúng tường lửa và bảo vệ các cổng. Các nhà cung cấp VoIP để bảo vệ chống lại mối đe dọa gian lận là thực hiện các quy tắc phát hiện sớm tinh vi cho phép họ tạm dừng dịch vụ trong thời gian thực khi phát hiện vi phạm. Các nhà cung cấp VoIP cũng phải chủ động theo dõi xem ai đang truy cập mạng của họ với tần suất nào và ai đang tạo ra loại lưu lượng nào

e. Giải pháp cho SPIT

- Lọc: Theo Brewton, cách hành động tốt nhất cho bất kỳ người dùng nào muốn bảo vệ hệ thống VoIP của mình là mua công nghệ lọc, nhưng trong khi các nhà cung cấp VoIP có thể giúp lọc SPIT, rõ ràng trước khi nó đi qua mạng và luôn có nguy cơ lưu lượng truy cập bất hợp pháp và không có khả năng bảo vệ hoặc truyền tin nhắn quy mô lớn vô tình gắn cờ là SPIT và ngăn không cho nguồn bảo vệ tiếp cận.

- Tường lửa: Tường lửa VoIP là một ứng dụng được điều khiển bởi chính sách bảo mật xác định xem có cho phép hoặc từ chối

một số cuộc gọi nhất định hay không. Quản trị viên đặt chính sách thông qua GUI. Cách tiếp cận phòng thủ chống lại các mối đe dọa, tường lửa phát hiện và ngăn chặn các cuộc tấn công VoIP DoS, tấn công SIP, gian lận phí, nhiễm virus và SPIT.

- VoIP SEAL: VoIP Seal là một công cụ mới nhắm mục tiêu các cuộc gọi bắt nguồn từ phần mềm tạo thư rác. SPIT được phát hiện và chặn dựa trên các mẫu liên lạc được quan sát trong suốt cuộc gọi. Nếu các cuộc gọi liên quan đến thư rác xuất hiện trong VoIP SEAL sẽ ngăn điện thoại đổ chuông.

f. Giải pháp sử dụng giao thức SRTP

Mục đích của SRTP là đảm bảo tính bảo mật của tải trọng RTP, bảo vệ tính toàn vẹn của toàn bộ gói RTP (bao gồm bảo vệ chống lại các gói RTP được phát lại) và xác thực ngầm định của tiêu đề. Bằng cách sử dụng các mật mã dòng stream có thể tìm kiếm, SRTP sẽ tránh được các cuộc tấn công từ chối dịch vụ có thể xảy ra đối với các mật mã luồng thiếu tính chất này.

SRTP lý tưởng để bảo vệ lưu lượng thoại qua IP vì nó có thể được sử dụng cùng với nén tiêu đề và không ảnh hưởng đến Chất lượng dịch vụ IP. Nó tạo ra một luồng khóa duy nhất cho mỗi gói RTP, do đó khiến cho những kẻ nghe trộm gần như không thể lấy được luồng RTP gốc từ luồng SRTP được mã hóa.

SRTP cũng cung cấp bảo vệ phát lại, điều này chắc chắn rất quan trọng đối với dữ liệu đa phương tiện. Nếu không có bảo vệ phát lại, một kẻ thù có thể thực hiện các thao tác đơn giản về bảo mật dữ liệu và lật đổ.

SRTP đạt được thông lượng cao và mở rộng gói thấp bằng cách sử dụng mật mã dòng nhanh để mã hóa, một chỉ mục ngầm để đồng bộ hóa và các hàm băm phổ quát để xác thực thư.

g. Giải pháp sử dụng giao thức ZRTP

ZRTP được phát triển bởi chính Phil Circle, Phil Zimmermann. Đây là một giao thức thỏa thuận khóa mật mã để đàm phán các khóa để mã hóa giữa hai điểm cuối trong một cuộc gọi điện thoại VoIP dựa trên RTP. Nó sử dụng trao đổi khóa Diffie mật Hellman và SRTP để mã hóa.

Giao thức ZRTP có một số tính năng mã hóa tốt đẹp thiếu nhiều cách tiếp cận khác đối với mã hóa VoIP. Mặc dù nó sử dụng thuật toán khóa công khai, nhưng nó tránh được sự phức tạp của PKI. Nó hoàn toàn không sử dụng khóa công khai. Nó sử dụng Diffie-Hellman phù du với cam kết băm và cho phép phát hiện các cuộc tấn công MiTM bằng cách hiển thị một chuỗi xác thực ngắn để người dùng so sánh bằng lời nói qua điện thoại. Nó có tính bảo mật hoàn hảo về phía trước, có nghĩa là các khóa bị phá hủy vào cuối cuộc gọi, điều này ngăn cản việc hủy bỏ cuộc gọi bằng cách tiết lộ trong tương lai của tài liệu chính.

ZRTP được thiết kế cho các phiên truyền thông unicast trong đó có một luồng phương tiện thoại. Đối với hội nghị an toàn nhiều bên, các phiên ZRTP riêng biệt có thể được đàm phán giữa mỗi bên và cầu hội nghị. ZRTP chỉ được thiết kế cho các cấu trúc liên kết điểm - điểm

2.2.3. Giải pháp bảo mật có sử dụng mô hình VPN kết hợp tường lửa.

Đây là mục tiêu chính của nhóm thực hiện đề tài, nhằm giới thiệu về hệ thống Elastix và đề xuất hai giải pháp bảo mật cho VoIP với mục đích bảo vệ tín hiệu truyền dẫn và ngăn chặn tin tặc xâm nhập hệ thống.

- Giải pháp đầu tiên sử dụng mô hình VPN nối tiếp khách hàng để bảo vệ tín hiệu truyền.

- Giải pháp thứ hai sử dụng VPN kết hợp tường lửa để ngăn chặn tin tặc xâm nhập hệ thống.

Để thực hiện hai giải pháp sử dụng mô hình VPN nối tiếp khách hàng để bảo vệ tín hiệu truyền và giải pháp sử dụng VPN kết hợp tường lửa để ngăn chặn tin tặc xâm nhập hệ thống, người dùng cần cài đặt hệ thống Elastix.

3. KẾT QUẢ VÀ THẢO LUẬN

3.1. Đánh giá mô hình triển khai

Mục đích của công việc là đề xuất các giải pháp bảo vệ đường dây tín hiệu cho hệ thống VoIP cho phép ngăn chặn các cuộc tấn công từ bên ngoài. Đồng thời, mang lại hiệu quả kinh tế và an ninh.

Giải pháp phù hợp với nhiều loại thiết bị khách: PC, Laptop, Smartphone ... Đồng thời, chạy trên các hệ điều hành Windows, Mac, Linux, Android và iOS.

Mục đích chính của đề tài đề xuất hai giải pháp bảo mật cho VoIP với mục đích truyền tín hiệu bảo vệ và ngăn chặn tin tặc xâm nhập hệ thống. Giải pháp đầu tiên sử dụng mô hình VPN nối tiếp khách hàng để bảo vệ tín hiệu truyền. Giải pháp thứ hai sử dụng VPN kết hợp tường lửa để ngăn chặn tin tặc xâm nhập hệ thống. Trên máy chủ Elastix, cài đặt OpenVPN và tường lửa.

✓ Giải pháp đầu tiên có những ưu điểm sau:

- Tín hiệu được mã hóa.
- Thích hợp cho nhiều loại thiết bị và hệ điều hành.
- Chặn các cuộc tấn công: người trung gian ...
- Ẩn địa chỉ thật của máy chủ.

✓ Giải pháp thứ hai có những ưu điểm sau:

- Tín hiệu được mã hóa.
- Thích hợp cho nhiều loại thiết bị và hệ điều hành.
- Chặn các cuộc tấn công: người trung gian ...
- Ẩn địa chỉ thật của máy chủ.
- Chặn DoS và DDoS.
- Chỉ cho phép các đối tượng sử dụng VPN và chặn các đối tượng không phải VPN.

3.2. Đánh giá của bộ môn chuyên môn

Qua một thời gian tìm hiểu, cài đặt và định hướng, thiết lập demo một số biện pháp bảo mật cho hệ thống VoIP, nhóm nghiên cứu đã đưa vấn đề này ra bàn luận ở bộ môn Mạng máy tính và truyền thông thuộc khoa Công nghệ thông tin - Đại học Công nghiệp Việt Trì. Trên cơ sở nhận được sự đóng góp tích cực của các thầy cô ở khoa công nghệ thông tin và các đóng góp chuyên sâu của các giảng viên thuộc bộ môn chuyên môn, các buổi sinh hoạt học thuật xoay quanh phạm vi nghiên cứu của đề tài. Nhóm nghiên cứu được bộ môn đánh giá cao về hàm lượng khoa học, tính thiết thực của đề tài ứng dụng trong cuộc sống và trong giảng dạy chuyên môn.

Nhóm đã đưa ra được một số biện pháp chống tấn công hệ thống. Đồng thời mô phỏng giả lập cho hai biện pháp được cho là đánh giá trong hệ thống bảo mật hiện nay.

4. KẾT LUẬN

Trên cơ sở nghiên cứu thực tế việc sử dụng các dịch vụ VnEdu tại các cơ sở giáo dục về chi phí và tính bảo mật. Trên cơ sở nghiên cứu các tài liệu, kế thừa kết quả xây dựng hệ thống đã có, chúng tôi đã tiến hành nghiên cứu và đề xuất giải pháp bảo mật cho dịch vụ VoIP tại trường Đại học Công nghiệp Việt Trì.

Tài liệu tham khảo

1. Thomas Porter, Jan Kanclirz, Andy Zmolek, Antonio Rosela, Michael Cross, Larry Chaffin, Brian Baskin, Choon Shim (**2004**), Practical VoIP Security,.

2. Jianqiang Xin (**2007**), Security Issues and countermeasure for VoIP.

3. Santi Phithakkitnukoon, Ram Dantu, and Enkh-Amgalan Baatarjav (**2008**), VoIP Security - Attacks and Solutions.