

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN
THÔNG**

TRẦN THANH TÚ

**ĐẢM BẢO AN NINH CHO HỆ THỐNG
VOIP DI ĐỘNG**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên – 2014

MỤC LỤC

DANH MỤC CÁC HÌNH.....	3
DANH MỤC CÁC BẢNG.....	5
DANH MỤC CÁC TỪ VIẾT TẮT	6
MỞ ĐẦU.....	7
CHƯƠNG I: TỔNG QUAN VỀ VOIP VÀ VẤN ĐỀ ĐẢM BẢO AN NINH CHO HỆ THỐNG VOIP DI ĐỘNG	8
1.1. Tổng quan về VoIP:.....	8
1.1.1. Lợi ích của VoIP:	10
1.1.2. Những tồn tại của VoIP:.....	11
1.1.3. Cấu hình của mạng VoIP:	12
1.1.4. Một số giao thức trong VoIP:.....	17
1.2. Nguy cơ đối với hệ thống VoIP di động:.....	29
1.2.1. Các mối đe dọa đối với hệ thống VoIP:	29
1.2.2. Một số phương thức tấn công mạng VoIP:	30
1.3. Những nhu cầu về đảm bảo an ninh đối với hệ thống VoIP di động:	43
CHƯƠNG II: GIẢI PHÁP ĐẢM BẢO AN NINH CHO HỆ THỐNG VOIP DI ĐỘNG	45
2.1. Đảm bảo an ninh cho thông tin thiết lập cuộc gọi sử dụng TLS (Transport Layer Security):	46
2.1.1. Khả năng đảm bảo an ninh của TLS:.....	46
2.1.2. Quá trình bắt tay của TLS:.....	48
2.1.3. Thuật toán sử dụng trong quản lý trao đổi khóa và xác thực cho TLS:.....	50
2.2. Đảm bảo an ninh cho dữ liệu thoại sử dụng SRTP (Secure Real-time Transport Protocol):.....	57
2.2.1. Cấu trúc của gói dữ liệu SRTP:	57
2.2.2. Khả năng đảm bảo an ninh của SRTP:	57
2.2.3. Thuật toán sử dụng trong quản lý trao đổi khóa và xác thực cho SRTP:	61
CHƯƠNG III: XÂY DỰNG MÔ HÌNH ĐẢM BẢO AN NINH CHO HỆ THỐNG VOIP DI ĐỘNG.....	72
3.1. Cấu hình phần cứng, phần mềm:	72
3.1.1. Mô hình sơ đồ thiết bị triển khai:	72
3.1.2. Chuẩn bị phần cứng và phần mềm cài đặt:.....	73
3.2. Ứng dụng đảm bảo an ninh cho cuộc gọi VoIP từ các thiết bị di động:.....	78
3.2.1. Cuộc gọi VoIP ở chế độ không có bảo mật:.....	79
3.2.2. Cuộc gọi VoIP sử dụng TLS bảo mật cho SIP:	81
3.2.3. Cuộc gọi VoIP sử dụng SRTP mã hóa cho RTP:	82

KẾT LUẬN	86
DANH MỤC TÀI LIỆU THAM KHẢO	87

DANH MỤC CÁC HÌNH

Hình 1.1. Lưu lượng thoại VoIP	9
Hình 1.2. Các Terminal của mạng IP có thể giao tiếp với các Telephone trong mạng SCN thông qua Gateway.....	10
Hình 1.3. Cấu hình của mạng VoIP	13
Hình 1.4. Cấu trúc gói tin RTP	18
Hình 1.5. Cấu trúc gói tin RTCP.....	20
Hình 1.6: Kiến trúc SIP	21
Hình 1.7. Sự hoạt động của trường hợp Proxy Mode.....	25
Hình 1.8 Sự hoạt động của trường hợp Redirect Mode.....	26
Hình 1.9: Call Flow của hệ thống	27
Hình 1.10: Luồng trao đổi thông thường	31
Hình 1.11: Luồng trao đổi bị tấn công DDoS.....	31
Hình 1.12: Tấn công DoS làm ngừng hoạt động của điện thoại IP	32
Hình 1.13: Máy tính tấn công ARP Spoofing.....	38
Hình 1.14: Tấn công ARP Spoofing làm đổi hướng ARP	39
Hình 2.1: Lớp bảo mật TLS cho giao thức SIP.....	47
Hình 2.2: Quá trình bắt tay giữa Client và Server.....	49
Hình 2.3: Dữ liệu lớp trên đóng gói bởi TLS/SSL.....	50
Hình 2.4: Cấu trúc gói tin SRTP	57
Hình 2.5: Lớp bảo mật SRTP cho giao thức RTP.....	58
Hình 2.6: Lược đồ mã hóa RTP payload sử dụng AES chế độ CTR.....	59
Hình 2.7: Xác thực gói SRTP	60
Hình 2.8: Cửa sổ trượt dùng để chống tấn công lặp gói	61
Hình 3.1: Mô hình sơ đồ triển khai hệ thống	73
Hình 3.2: Thông tin tổng đài FreePBX	73
Hình 3.3: Thông tin cấu hình user.....	74
Hình 3.4: Lựa chọn cài đặt bảo mật cho user.....	75
Hình 3.5: Cấu hình giao thức vận chuyển.....	76
Hình 3.6: Cấu hình phương thức mã hóa cho đa phương tiện	77
Hình 3.7: Phần mềm bắt gói tin Wireshark.....	78
Hình 3.8: Thực hiện cuộc gọi từ User 1002 đến User 1003	78
Hình 3.9: Thông tin cuộc gọi Wireshark bắt được.....	79
Hình 3.10: Thông tin của SIP ở chế độ không có bảo mật	80
Hình 3.11: Thông tin Voice mà RTP truyền bị Wireshark bắt được	81
Hình 3.12: Thông tin của SIP đã được mã hóa bởi TLS.....	82
Hình 3.13: Nội dung cuộc gọi vẫn không được mã hóa nếu chỉ dùng TLS	82

Hình 3.14: Thông tin tín hiệu cuộc gọi nếu chỉ dùng SRTP	84
Hình 3.15: Nội dung cuộc gọi được mã hóa bởi SRTP	85

DANH MỤC CÁC BẢNG

Bảng 1.1: Chức năng các thành phần của kiến trúc SIP	22
Bảng 1.2: Các yêu cầu SIP	23
Bảng 1.3: Các đáp ứng SIP	24
Bảng 1.4: Các cấp độ mà cấu trúc VoIP có thể bị tấn công.....	30
Bảng 2.1: Tổ hợp Khóa-khởi-vòng	62

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Nghĩa tiếng Việt
VoIP	Voice over Internet Protocol	Thoại trên giao thức Internet
PSTN	Public Switching Telephone Network	Mạng điện thoại chuyển mạch công cộng
SCN	Switching Circuit Network	Mạng chuyển mạch gói
RTP	Realtime Transport Protocol	Giao thức truyền tải thời gian thực
SRTP	Secure Realtime Transport Protocol	Giao thức truyền tải thời gian thực an toàn
SIP	Session Initiation Protocol	Giao thức tạo phiên
RTCP	Realtime Transport Control Protocol	Giao thức điều khiển truyền tải thời gian thực
ETSI	European Telecommunications Standards Institute	Viện tiêu chuẩn viễn thông Châu Âu
ISDN	Integrated Services Digital Network	Mạng số dịch vụ đa tích hợp
GSM	Global System for Mobile	Hệ thống di động toàn cầu
DECT	Digital Enhanced Cordless Telecommunications	Công nghệ truyền thông không dây số cải tiến
IETF	Internet Engineer Task Force	Tổ chức quản lý kỹ thuật
DoS	Denial of Service	Tấn công từ chối dịch vụ
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DNS	Domain Name System	Hệ thống phân giải tên miền
SSL	Secure Socket Layers	Lớp bảo mật lỗ hồng
SRTP	Secure Realtime Transport Protocol	Giao thức bảo mật tầng giao vận thời gian thực
TLS	Transport Layer Security	Giao thức bảo mật gói tin tầng giao vận
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ
PBX	Private Branch eXchange	Tổng đài nhánh riêng

MỞ ĐẦU

Hiện nay chúng ta có thể thấy được sự phát triển của công nghệ mạng điện thoại trên toàn thế giới, cùng với đó là Internet cũng ngày càng được phổ biến rộng rãi. Sự ra đời của truyền thoại qua giao thức Internet, Voice over Internet Protocol (VoIP), đã làm bộc lộ rõ những hạn chế của mạng điện thoại thông thường như chất lượng dịch vụ không cao, tài nguyên sử dụng còn hạn chế... VoIP là công nghệ truyền thoại dựa trên giao thức của mạng Internet. VoIP hiện nay đang ngày càng phát triển và dần thay thế mạng điện thoại truyền thống PSTN (Public Switched Telephone Network), vì ngoài việc thực hiện cuộc gọi thoại, VoIP còn truyền dữ liệu trên cơ sở mạng truyền dữ liệu.

Ngoài ra, trong những năm gần đây còn đánh dấu sự phát triển của điện thoại di động, đặc biệt là thế hệ điện thoại thông minh Smartphone. Người dùng điện thoại di động hiện nay hướng tới sử dụng các ứng dụng để ngoài việc nghe, gọi, còn có thể truyền tải dữ liệu như hình ảnh, video....

Cùng với sự phát triển của VoIP là vấn đề bảo mật cho hệ thống này. Hiện nay có rất nhiều hệ thống VoIP không được bảo mật, thông tin gửi đi không được mã hóa, dẫn đến việc bị tấn công làm lộ, làm mất dữ liệu. Do đó, việc làm thế nào để đảm bảo an ninh cho hệ thống VoIP, đặc biệt là hệ thống VoIP di động là hết sức quan trọng.

Việc đảm bảo an ninh cho hệ thống VoIP di động cũng có nhiều phương pháp. Trong nội dung luận văn sẽ tập trung vào các phương pháp đảm bảo an ninh cho những giao thức của hệ thống VoIP, và ứng dụng các phương pháp này trong quá trình thiết lập tổng đài cũng như khi thực hiện các cuộc gọi từ thiết bị di động.

CHƯƠNG I: TỔNG QUAN VỀ VOIP VÀ VẤN ĐỀ ĐẢM BẢO AN NINH CHO HỆ THỐNG VOIP DI ĐỘNG

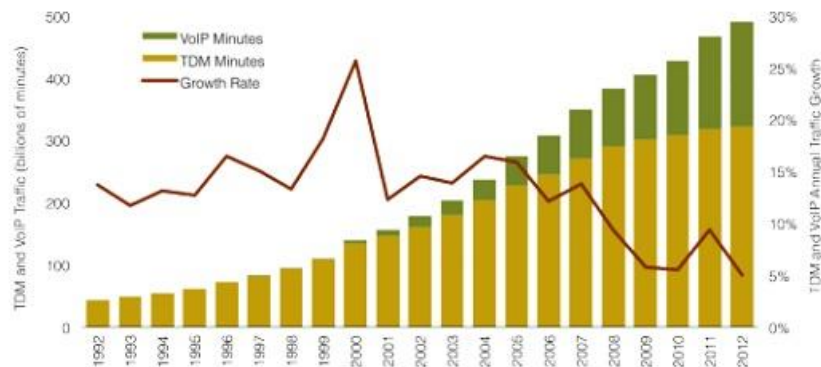
1.1. Tổng quan về VoIP:

Trong những bước phát triển của ngành viễn thông những năm gần đây, điện thoại IP được đánh giá là một bước tiến quan trọng về công nghệ. Hiện nay điện thoại IP đang là một mối quan tâm lớn trong bối cảnh phát triển mạnh mẽ của ngành viễn thông.

Dịch vụ điện thoại IP được xây dựng trên công nghệ VoIP. Đây là một công nghệ rất mới nhưng thu hút được rất nhiều sự quan tâm của các nhà khai thác và nhà sản xuất. VoIP được đánh giá là một bước đột phá trong công nghệ, nó sẽ là cơ sở để xây dựng một mạng tích hợp thực sự giữa thoại và số liệu. Đây là một hướng phát triển tất yếu của mạng viễn thông.

Do các ưu điểm giá thành rẻ và có nhiều dịch vụ mở rộng, điện thoại IP đã và đang tạo ra một thị trường rộng lớn gồm mọi đối tượng sử dụng gồm các thuê bao, các doanh nghiệp, các tổ chức và cơ quan nhà nước.

Để hiểu vấn đề này, chúng ta xem xét hệ thống điện thoại truyền thống, điển hình là PSTN (*Public Switching Telephone Network: Mạng thoại chuyển mạch công cộng*). Đó là kiểu mạng chuyển mạch kênh SCN (*Switching Circuit Network*) và được phát triển lên từ mạng analog, nghĩa là để thiết lập một cuộc gọi, cần phải có một kênh truyền riêng và giữ kênh truyền cho đến chừng nào cuộc nói chuyện kết thúc. Kiểu truyền thông như vậy không tận dụng một cách có hiệu quả băng thông hiện có, công suất giới hạn là 64kbit/s/kênh và thực hiện 30 cuộc điện thoại trên một đường E1.

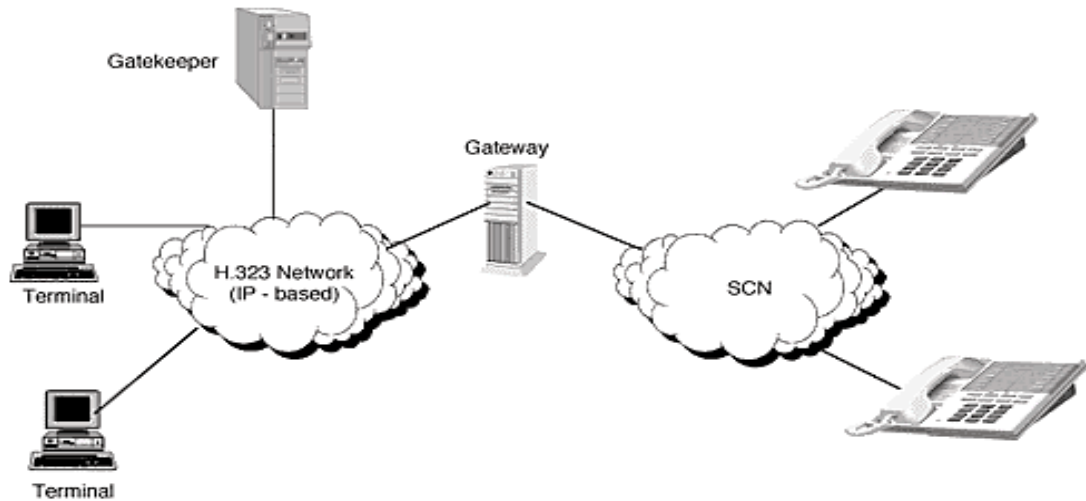


Hình 1.1. Lưu lượng thoại VoIP

Vậy VoIP khác với hệ thống điện thoại truyền thống thế nào? Tiếng nói thay vì được truyền qua mạng chuyên mạch kênh, thì lại được truyền qua mạng chuyên mạch gói phát triển lên từ mạng số, điển hình là mạng IP. Tiếng nói được số hoá, đóng gói, rồi được truyền đi như là các gói tin thông thường được truyền trên mạng IP. Dung lượng truyền dẫn được tất cả các thông tin chia sẻ và bằng cách đó băng thông được sử dụng có hiệu quả hơn mà không cần phải cung cấp cho từng kênh riêng lẻ. Mỗi kênh hoặc mỗi đường trung kế cung cấp nhiều khả năng ứng dụng như số liệu, thoại, fax và hội nghị video. Dễ dàng thấy công nghệ thoại này ưu điểm hơn hẳn công nghệ thoại truyền thống ở chỗ nó tận dụng được triệt để tài nguyên hệ thống, dẫn đến một điều chắc chắn là chi phí cho cuộc gọi được giảm đáng kể, đặc biệt là những cuộc gọi ở khoảng cách địa lý rất xa hiện nay vẫn còn quá đắt đỏ trong mạng điện thoại chuyên mạch kênh.

Nhưng như vậy không phải là điều dễ dàng. Ta biết rằng thoại là một ứng dụng mang tính thời gian thực, nghĩa là yêu cầu dòng tiếng nói phải được truyền đi tới phía nhận một cách gần như tức thì. Trong mạng chuyên mạch kênh điều đó là đơn giản vì mỗi cuộc thoại không phải chia sẻ với các ứng dụng khác, đường truyền nói chung luôn được đảm bảo thông giữa hai đầu dây, hiếm khi xảy ra những trục trặc như tắc nghẽn hay bị mất thông tin. Còn với mạng chuyên mạch gói như IP thì sao? Mạng IP được xem như là mạng truyền số liệu, nghĩa là thông tin dữ liệu tới đích không có yêu cầu về mặt thời gian thực. Và lại trên mạng IP, do đường truyền được chia sẻ bởi nhiều ứng dụng, hoặc bản thân các gói tin tiếng nói lại đi theo nhiều con đường khác nhau tới đích, tình trạng tắc nghẽn, trễ, mất dữ liệu thường xuyên xảy ra. Những điều đó nếu không được giải quyết tốt sẽ gây ảnh hưởng rất lớn đến chất lượng tiếng nói nhận được. Đây là vấn đề hết sức quan trọng trong công nghệ VoIP.

Ngoài ra mạng IP và mạng chuyên mạch kênh còn có thể giao tiếp với nhau thông qua Gateway, cho phép một đầu cuối ở mạng này có thể thoại với một đầu cuối của mạng kia (hình 1.2), mà vẫn trong suốt đối với người sử dụng, sự phát triển này đem lại khả năng tích hợp nhiều dịch vụ của hai loại mạng với nhau.



Hình 1.2. Các Terminal của mạng IP có thể giao tiếp với các Telephone trong mạng SCN thông qua Gateway.

1.1.1. Lợi ích của VoIP:

- Giảm cước phí truyền thông. Đặc biệt là các cuộc gọi đường dài cũng như tận dụng hiệu quả hơn tài nguyên giải thông đường truyền. Đây là yếu tố quan trọng nhất thúc đẩy sự phát triển của công nghệ VoIP.

- Hợp nhất hóa. Hệ thống mạng chuyển mạch kênh rất phức tạp, cần phải có một đội ngũ nhân viên vận hành và giám sát hoạt động của nó. Với một cơ sở hạ tầng tích hợp các phương thức truyền thông cho phép hệ thống được chuẩn hóa tốt hơn, hoạt động hiệu quả hơn và giảm tổng số thiết bị, nhân lực cần thiết. Điều này cũng làm giảm thiểu sai sót trên hệ thống hiện thời.

- Sử dụng công nghệ thoại trên IP đem lại nhiều lợi ích thiết thực cho các nhà truyền tải:

- + Triệt và nén im lặng: Được sử dụng khi có khoảng nghỉ ngơi trong cuộc nói chuyện. Khoảng nghỉ này có thể lên tới 50-60% một cuộc gọi. Vì thế, ta có thể tiết kiệm được giải thông tiêu tốn, nhất là với hội thoại nhiều người. Không giống như mạng chuyển mạch kênh, VoIP triệt im lặng qua các liên kết toàn cầu tại các điểm đầu cuối. Mạng IP thích hợp cho việc ghép kênh, giảm bớt giải thông tiêu thụ toàn mạng. Sự triệt im lặng và bù nén làm cũng tăng hiệu quả sử dụng mạng.

- Chia sẻ thuận lợi:

- + Đặc trưng của mạng IP là chia sẻ tài nguyên mạng. Các kênh truyền thông không được tạo ra cố định và riêng biệt như trong mạng chuyển mạch kênh, mà nó được dùng chung cho nhiều ứng dụng khác.