

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

Lâm Anh Bình

**HỆ THỐNG VOIP
AN TOÀN VỚI CHUẨN BẢO MẬT H.235**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên – 2012

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên

<http://www.lrc-tnu.edu.vn>

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên

<http://www.lrc-tnu.edu.vn>

LỜI CẢM ƠN

Luận văn này được hoàn thành tại trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên. Dưới sự hướng dẫn của PGS.TS Nguyễn Văn Tam. Tác giả xin bày tỏ lòng biết ơn sâu sắc tới PGS.TS Nguyễn Văn Tam, người đã tận tình giúp đỡ, hướng dẫn tác giả hoàn thành luận văn này.

Với tình cảm chân thành và lòng biết ơn sâu sắc, cho phép tôi gửi lời cảm ơn đến các thầy cô giáo trong trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên, các Thầy giáo của Viện Công nghệ Thông tin, Viện Khoa học và Công nghệ Việt Nam đã tham gia quản lý, giảng dạy và giúp đỡ tác giả trong suốt quá trình học tập, nghiên cứu và làm luận văn.

Tôi xin chân thành cảm ơn sự ủng hộ, động viên giúp đỡ của Ban giám hiệu và các đồng nghiệp Trường Trung cấp nghề Cao Bằng.

Xin chân thành cảm ơn anh chị em học viên lớp CAO HỌC K9A đã giúp đỡ, động viên, khích lệ tác giả trong quá trình học tập và nghiên cứu.

Trong quá trình nghiên cứu, do khả năng có hạn và kinh nghiệm thực tế còn ít nên không tránh khỏi thiếu sót. Kính mong sự chỉ dẫn và góp ý của các thầy giáo, các bạn đồng nghiệp để công trình nghiên cứu tiếp theo được tốt hơn.

Thái Nguyên, tháng 11 năm 2012

Tác giả

Lâm Anh Bình

LỜI CAM ĐOAN

Tôi xin cam đoan đề tài của này là do chính bản thân Tôi thực hiện, với sự hướng dẫn của PGS.TS Nguyễn Văn Tam. Các dữ liệu, thông tin được thu thập từ những nguồn hợp pháp, nội dung nghiên cứu và kết quả trong đề tài này là trung thực.

Thái Nguyên, tháng 11 năm 2012

Tác giả

Lâm Anh Bình

MỤC LỤC

MỤC LỤC	iv
DANH MỤC CÁC CHỮ VIẾT TẮT	vi
DANH MỤC CÁC BẢNG	viii
DANH MỤC CÁC HÌNH.....	ix
MỞ ĐẦU	1
NỘI DUNG.....	3
Chương I: TỔNG QUAN VỀ BẢO MẬT CHO HỆ THỐNG VoIP[4]	3
1.1 Hệ thống VoIP là gì?	3
1.2 VoIP làm việc như thế nào?.....	4
1.3 Tiêu chuẩn và giao thức VoIP.	7
1.3.1 Tiêu chuẩn VoIP.....	7
1.3.2 Giao thức VoIP.....	7
1.4 Vấn đề an ninh của VoIP.	21
Chương II: GIẢI PHÁP BẢO MẬT VOIP SỬ DỤNG CHUẨN H.235[4].....	24
2.1 Vấn đề an ninh hiện nay và các mối đe dọa đến VoIP.	24
2.1.1 Vấn đề an ninh hiện nay trong VoIP	24
2.1.2 Các mối đe dọa đến VoIP.....	25
2.2 Các chuẩn H.323 và H.235.	28
2.2.1 Chuẩn H.323.	28
2.2.2 Chuẩn H.235.	36
2.3 Phương thức đảm bảo an ninh của H.235 đối với VoIP.	38
Chương III: TRIỂN KHAI THỬ NGHIỆM	47

3.1 Phương pháp thử nghiệm truyền thông VoIP an toàn.....	47
3.2 Những yếu tố cần thiết.....	47
3.2.1 H323 Phone.....	47
3.2.2 GNU Gatekeeper.....	48
3.2.3 Wireshark.....	49
3.3 Demo.....	50
3.3.1 Truyền trực tiếp và bắt gói tin.....	50
3.3.2 Truyền với chuẩn bảo mật H.235 qua GNU Gatekeeper.....	52
KẾT LUẬN.....	55
TÀI LIỆU THAM KHẢO.....	57

DANH MỤC CÁC CHỮ VIẾT TẮT

Stt	Chữ viết tắt	Diễn giải	Ý nghĩa
1	AES	Advanced Encryption System	Hệ thống mã hóa nâng cao
2	ARC	Admission Confirm	Xác nhận nhập
3	ARJ	Admission Reject	Từ chối nhập
4	ARP	Address resolution protocol	Giao thức phân giải địa chỉ
5	ARQ	Admission Request	Yêu cầu nhập
6	ATM	Asynchronous Transfer Mode	Phương thức truyền không đồng bộ
7	BCF	Bandwidth Confirm	Xác nhận băng thông
8	BRJ	Bandwidth Reject	Từ chối băng thông
9	BRQ	Bandwidth Request	Yêu cầu băng thông
10	DoS	Denial of Service	Từ chối dịch vụ
11	ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông châu Âu
12	HTTP	Hypertext Transfer Protocol	Giao thức truyền siêu văn bản
13	IETF	Internet Engineering Task Force	Tổ chức làm nhiệm vụ kỹ thuật về Internet
14	IP	Internet Protocol	Giao thức Liên mạng
15	ISDN	Integrated Service Digital Network	Dịch vụ tích hợp mạng kỹ thuật số
16	ITU	International Telecommunication Union	Liên minh Viễn thông quốc tế

17	MAC	Media Access Control	Kiểm soát truy cập phương tiện truyền thông
18	MGCP	Media Gateway Control Protocol	Giao thức điều khiển công đa phương tiện
19	NAT	Network address translation	Dịch địa chỉ mạng
20	PBX	Private Branch Exchange	Tổng đài Nhánh Riêng
21	PSTN	Public Switched Telephone Network	Mạng điện thoại chuyển mạch kênh
22	QoS	Quality of Service	Chất lượng dịch vụ
23	RAS	Remote Access Services	Dịch vụ truy cập từ xa
24	RR	Receive Report	Nhận báo cáo
25	RTCP	Real Time Control Protocol	Giao thức điều khiển thời gian thực
26	RTP	Real Time Transport Protocol	Giao thức thời gian thực
27	SDES	Source Description Items	Mục Mô tả nguồn
28	SDP	Session Description Protocol	Giao thức mô tả phiên
29	SIP	Session Initiation Protocol	Giao thức phiên khởi đầu
30	SR	Sender Report	Gửi báo cáo
31	TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
32	TIA	Telecommunications Industry Association	Hiệp hội Công nghiệp Viễn thông
33	TLS	Transport layer security	An ninh lớp vận chuyển
34	UA	User Agents	Đại diện người dùng
35	UAC	User Agent Client	Đại diện người dùng khách
36	UAS	User Agent Server	Đại diện người dùng chủ
37	UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng

38	VoIP	Voice over Internet Protocol	Truyền tiếng nói qua giao thức Internet
----	-------------	------------------------------	---

DANH MỤC CÁC BẢNG

<i>Bảng 2-1 Cơ sở bảo mật hồ sơ H.235 v2 Phụ lục D</i>	<i>41</i>
<i>Bảng 2-2 Chữ ký bảo mật hồ sơ cá nhân của H.235 v2 Phụ lục E</i>	<i>42</i>
<i>Bảng 2-3 Thoại tùy chọn mã hóa H.235 v2 Phụ lục D.....</i>	<i>44</i>
<i>Bảng 2-4 Kết hợp hồ sơ cá nhân H.235 v2 Phụ lục F.....</i>	<i>45</i>
<i>Bảng 2-5 Tăng cường cơ sở hồ sơ cá nhân H.235 32 Phụ lục D.....</i>	<i>46</i>

DANH MỤC CÁC HÌNH

<i>H.1-1. Quá trình lưu chuyển giữ liệu giọng nói giữa các điểm cuối.</i>	6
<i>H.1-2. Giao thức tín hiệu VoIP</i>	7
<i>H.1-3. RTP dữ liệu trong gói tin IP.</i>	9
<i>H.1-4. Cổng H.323/PSTN.</i>	13
<i>H.1-5. Vùng H.323.</i>	14
<i>H.1-6. Kiến trúc mạng SIP.</i>	17
<i>H.1-7. Kiến trúc MGCP.</i>	20
<i>H.2-1. Kiến trúc mạng H.323.</i>	29
<i>H.2-2. Các giao thức hỗ trợ H.323.</i>	30
<i>H.2-3. Cuộc gọi H.323.</i>	33
<i>H.2-4. Thiết lập cuộc gọi vùng nội bộ.</i>	33
<i>H.2-6. Thiết lập cuộc gọi giữa các vùng.</i>	34
<i>H.2-5. Hủy kết nối cuộc gọi.</i>	36
<i>H.2-6. Phạm vi H.235.</i>	38
<i>H.3-1. Giao diện H.323 Phone gọi trực tiếp.</i>	50
<i>H.3-2. Giao diện chính của Wireshark đang bắt gói tin</i>	51
<i>H.3-3. Đồ thị truyền gói tin đã được bắt.</i>	52
<i>H.3-4. Giao diện GNU Gatekeeper</i>	52

<i>H.3-5. Giao diện chính của Wireshark đang bắt gói tin truyền qua GNU gatekeeper.</i>	<i>53</i>
<i>H.3-6. Đồ thị truyền gói tin đã được bắt truyền qua GNU gatekeeper..</i>	<i>54</i>