ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

BÙI THÁI LONG

NGHIÊN CỨU MỘT SỐ PHƯƠNG PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN TRONG MẠNG MÁY TÍNH

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

Người hướng dẫn khoa học

PGS.TS Trịnh Nhật Tiến

Thái Nguyên – 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này của tự bản thân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến. Các chương trình thực nghiệm do chính bản thân tôi lập trình, các kết quả là hoàn toàn trung thực. Các tài liệu tham khảo được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Bùi Thái Long

LỜI CẢM ƠN

Tôi xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin – Viện Hàn lâm Khoa học và Công nghệ Việt Nam, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã dạy dỗ chúng tôi trong suốt quá trình học tập chương trình cao học tại trường.

Đặc biệt tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS Trịnh Nhật Tiến, Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội đã quan tâm, định hướng và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu cho tôi trong quá trình làm luận văn tốt nghiệp.

Cuối cùng, tôi xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với em trong suốt quá trình làm luận văn tốt nghiệp.

Thái Nguyên, ngày tháng năm 2015

HỌC VIÊN

Bùi Thái Long

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
LỜI MỞ ĐẦU 1
1. Lý do lựa chọn đề tài. 1
2. Đối tượng và phạm vi nghiên cứu 1
3. Hướng nghiên cứu của đề tài 2
4. Những nội dung nghiên cứu chính 2
Chương 1: CÁC HIỂM HỌA VỀ AN TOÀN THÔNG TIN TRÊN MẠNG MÁY TÍNH. 3
1.1. VẤN ĐỀ AN NINH MẠNG MÁY TÍNH. 3
1.1.1. An ninh hệ thống. 3
1.2. HIỂM HỌA VỀ AN NINH MẠNG. 6
1.2.1. Sử dụng gói số liệu quá lớn (Ping of Death) 6
1.2.2. Giả địa chỉ IP 6
1.2.3. Giả điều khiển TCP (TCP spoofing) 7
1.2.4. Session hijacking 7
1.2.5. Giả yêu cầu thiết lập kết nối 8
1.2.6. Tấn công phân đoạn IP 9
1.3. HIỂM HỌA ĐE DỌA DỊCH VỤ MẠNG MÁY TÍNH. 9
1.3.1. Hiểm họa dịch vụ thư điện tử. 9
1.3.2. Hiểm họa đe dọa dịch vụ Web 10
1.3.3. Hiểm họa dịch vụ Talnet 10
1.3.4. Hiểm họa dịch vụ FTP 11
1.3.5. Các lỗ hổng trên mạng 11
1.3.6. Ảnh hưởng của các lỗ hổng bảo mật trên mạng Internet 16
Chương 2: MỘT SỐ PHƯƠNG PHÁP BẢO VỆ THÔNG TIN TRÊN MẠNG MÁY TÍNH. 19
2.1. KIỂM SOÁT VÀ XỬ LÝ CÁC DẠNG TẤN CÔNG MẠNG 19
2.1.1. Tấn công giả mạo: Spoofing 19
2.1.2. Đánh hơi: Sniffing 22
2.1.3. Nghe lén: Mapping 24
2.1.4. Kiểu tấn công “Người đứng giữa”: Hijacking 25
2.1.5. Ngựa thành Trojan: Trojans 26

2.1.6. Tấn công từ chối dịch vụ: DoS 28
2.1.7. Tấn công từ chối dịch vụ phân tán: DDoS 29
2.1.8. Tấn công dựa trên yếu tố con người: Social engineering 31
2.2. DÙNG TƯỜNG LỬA. 32
2.2.1. Khái niệm tường lửa? 32
2.2.2. Ứng dụng của tường lửa 33
2.2.3. Chức năng chính của tường lửa 35
2.2.4. Phân loại tường lửa 35
2.2.5. Mô hình tường lửa 36
2.3. DÙNG CÔNG NGHỆ MẠNG RIÊNG ẢO. 37
2.3.1. Khái niệm mạng riêng ảo 37
2.3.2. Các loại mạng riêng ảo 39
2.3.3. Các thành phần cần thiết tạo nên một VPN 42
2.4. DÙNG CÔNG NGHỆ MÃ HÓA. 46
2.4.1. Mã hóa 46
2.4.2. Hệ mã hoá khoá công khai RSA 47
2.4.3. Chữ ký số 49
2.4.4. Hàm băm 52
2.4.5. Kỹ thuật mã khóa EC- ELGAMAL 53
Chương 3: THỬ NGHIỆM ỨNG DỤNG BẢO VỆ THÔNG TIN TRÊN MẠNG MÁY TÍNH 62
3.1. PHÁT BIỂU BÀI TOÁN 62
3.2. ĐỀ XUẤT GIẢI PHÁP 63
3.2.1. RSA + SHA-1 63
3.2.2. RSA + SHA-1 + EC-Elgamal 65
3.3. THIẾT KẾ PHẦN MỀM 68
3.4. GIAO DIỆN CHƯƠNG TRÌNH 68
3.4.1. Giao diện chương trình. 69
3.4.2. Kết quả 73
3.5. ĐÁNH GIÁ 73
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI 74
TÀI LIỆU THAM KHẢO 75

DANH SÁCH KÍ HIỆU, TỪ VIẾT TẮT

Viết tắt	Viết đầy đủ
CERT	Computer Emergency Reponse Team
CIAC	Department of Energy Computer Incident Advisory Capability
DARPA	Defense Advanced Research Projects Agency
FIRST	The Forum of Incident Response and Security Teams
PKI	Public Key Infrasture
RPC	Remote Procedure Call
SSL/TLS	Secure Socket layer/Transport Layer Security
VPN	Virtual Private Network

DANH MỤC CÁC HÌNH ẢNH

Hình 2-1: Tấn công Spoofing.....20
Hình 2-2: Tấn công Man-in-the-middle.....21
Hình 2-3: Tấn công giả mạo IP.....22
Hình 2-4 : Tấn công Mapping.....25
Hình 2-5 : Tấn công Hijacking.....26
Hình 2-6 : Tấn công Trojans.....26
Hình 2-7: Tấn công DDoS.....29
Hình 2-8: Tấn công Social engineering.....31
Hình 2.9 - Tường lửa cứng.....36
Hình 2.10 - Tường lửa mềm.....36
Hình 2.11 - Mô hình tường lửa TMG.....37
Hình 2-12 : Mạng riêng ảo truy cập từ xa.....40
Hình 2-13: Mạng riêng ảo Intranet.....41
Hình 2-14: Mạng riêng ảo Extranet.....41
Hình 2-15: Sử dụng kết nối VPN để kết nối từ xa đến Intranet.....42
Hình 2-16: Sử dụng kết nối VPN để kết nối 2 site ở xa.....42
Hình 2-17: Sử dụng kết nối VPN để kết nối tới mạng được bảo mật.....42
Hình 2.18: Phép cộng trên đường cong Elliptic.....57
Hình 2.19: Phép nhân đôi trên đường cong Elliptic.....58
Hình 3.1. Sơ đồ thuật toán RSA + SHA-1.....63
Hình 3.2. Sơ đồ tạo chữ ký số RSA + SHA-1.....63
Hình 3.3. Sơ đồ thẩm định chữ ký số RSA + SHA-1.....64
Hình 3.4. Giao diện chương trình chính.....69
Hình 3.5. Giao diện tạo khóa bằng nút *Tạo khóa*.....70
Hình 3.6. Giao diện tạo khóa bằng nút *Ngẫu nhiên*.....70
Hình 3.7. Giao diện quá trình mã hóa.....71
Hình 3.8. Giao diện quá trình nhận dữ liệu.....71
Hình 3.9. Giao diện giải mã dữ liệu.....72
Hình 3.10. Giao diện xác nhận dữ liệu.....72

LỜI MỞ ĐẦU

1. Lý do lựa chọn đề tài.

Trong những năm gần đây, sự bùng nổ của cách mạng thông tin đang diễn ra nhanh chóng trên phạm vi toàn thế giới. Sự phổ biến rộng rãi của Internet đã kết nối mọi người trên thế giới lại với nhau, trở thành công cụ không thể thiếu, làm tăng hiệu quả làm việc, tăng sự hiểu biết, trao đổi, cập nhật các thông tin nhanh chóng và tiện lợi.

Tuy nhiên, Internet là một mạng mở, nó cũng chứa đựng nhiều hiểm họa đe dọa hệ thống mạng, hệ thống máy tính, tài nguyên thông tin cá nhân của các tổ chức cá nhân hay doanh nghiệp. Như những tin tức quan trọng nằm ở kho dữ liệu hay trên đường truyền có thể bị tấn công, xâm nhập và lấy cắp thông tin. Do vậy, nảy sinh yêu cầu nghiên cứu các phương pháp bảo đảm an toàn thông tin như: Kiểm soát các lỗ hổng an ninh mạng, kiểm soát các dạng tấn công mạng nhằm mục đích ngăn chặn hạn chế các rủi ro đối với thông tin trong mạng máy tính.

Chính vì nhận thấy nhiệm vụ bảo vệ an toàn thông tin trong mạng máy tính, đặc biệt ở Việt Nam nên Em đã chọn đề tài "Nghiên cứu một số phương pháp bảo đảm an toàn thông tin trong mạng máy tính", đề tài này theo Tôi được biết là đã có một số Tổ chức, Doanh nghiệp, Viện, Trường Đại Học… nghiên cứu nhưng vẫn dừng ở một mức độ nhất định vì vậy Tôi vẫn quyết tâm nhận đề tài này với các nhiệm vụ cần đi sâu là nghiên cứu, đề xuất các giải pháp an toàn thông tin dựa trên kiến trúc tổng quan của mô hình an toàn thông tin trong mạng máy tính và vận dụng cơ sở lý thuyết mật mã ứng dụng vào an toàn thông tin.

2. Đối tượng và phạm vi nghiên cứu

- Đề tài nghiên cứu các phương pháp để thực hiện nhiệm vụ bảo mật và an toàn thông tin trong mạng máy tính, quá trình thực hiện và các kiến thức khoa học và thuật toán liên quan như: Xác thực, bảo mật, bảo toàn dữ liệu, mật mã, chữ ký số …

- Áp dụng các kết quả nghiên cứu để triển khai hệ thống bảo đảm an toàn thông tin trong mạng máy tính.