BCYCP
HVKTMM

BAN CƠ YẾU CHÍNH PHỦ

Học viện Kỹ thuật Mật mã

Báo cáo Tổng kết Khoa học và Kỹ thuật Đề tài:

NGHIÊN CỨU MỘT SỐ VẤN ĐỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN CHO CÁC MẠNG DÙNG GIAO THỨC LIÊN MẠNG MÁY TÍNH IP

TS Đào Văn Giá, TS. Trần Duy Lai

Hà Nội, 1-2005

BAN CƠ YẾU CHÍNH PHỦ

Học viện Kỹ thuật Mật mã

Báo cáo Tổng kết Khoa học và Kỹ thuật Đề tài:

NGHIÊN CỨU MỘT SỐ VẤN ĐỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN CHO CÁC MẠNG DÙNG GIAO THỨC LIÊN MẠNG MÁY TÍNH IP

TS Đào Văn Giá, TS. Trần Duy Lai

Hà Nội, 1-2005

Tài liệu này được chuẩn bị trên cơ sở kết quả thực hiện
Đề tài cấp Nhà nước, mã số KC.01.01

Danh sách những người thực hiện

Nhóm thứ nhất : Các nghiên cứu tổng quan, tìm hiểu giải pháp

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	PGS TS Hoàng Văn Tảo	Học viện Kỹ thuật Mật mã
2	PGS TS Lê Mỹ Tú	Học viện Kỹ thuật Mật mã
3	TS Nguyễn Hồng Quang	Phân viện NCKTMM- HVKTMM
4	ThS Đặng Hoà	Phòng QLNCKH- HVKTMM
5	TS Nguyễn Nam Hải	Trung tâm Công nghệ Thông tin
6	TS Đặng Vũ Sơn	Vụ Khoa học Công nghệ
7	TS Trần Duy Lai	Phân viện NCKHMM- HVKTMM
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	ThS Nguyễn Ngọc Điệp	Phòng QLNCKH- HVKTMM
2	ThS Nguyễn Đức Tâm	Khoa Tin học- HVKTMM
3	ThS Nguyễn Đăng Lực	Phân viện NCNVMM- HVKTMM
4	ThS Đoàn Ngọc Uyên	Khoa Tin học- HVKTMM
5	ThS Nguyễn Anh Tuấn	Phân viện NCKHMM- HVKTMM
6	KS Lê Khắc Lưu	Phân viện NCKTMM- HVKTMM
7	ThS Đào Hồng Vân	Trung tâm Công nghệ Thông tin
8	KS Nguyễn Cảnh Khoa	Phân viện NCKHMM-HVKTMM
9	KS Nguyễn Công Chiến	Phòng QLNCKH-HVKTMM

Sản phẩm đã đạt được:

- 07 báo cáo khoa học (các quyển 1A, 1B, 1C, 2A, 2B, 5A và 5B)

Nhóm thứ hai: Các phần mềm bảo mật gói IP

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Nguyễn Nam Hải	Trung tâm Công nghệ Thông tin
2	TS Đặng Vũ Sơn	Vụ Khoa học Công nghệ
3	TS Trần Duy Lai	Học viện Kỹ thuật Mật mã
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	KS Nguyễn Cảnh Khoa	Phân viện KHMM- HVKTMM
2	KS Nguyễn Quốc Toàn	Phân viện KHMM- HVKTMM
3	KS Đinh Quốc Tiến	Phân viện KHMM- HVKTMM
4	KS Nguyễn Tiến Dũng	Trung tâm Công nghệ Thông tin
5	KS Nguyễn Thanh Sơn	Khoa Mật mã- HCKTMM
6	KS Nguyễn Như Tuấn	Khoa Mật mã- HVKTMM

Sản phẩm đã đạt được:

- 03 báo cáo khoa học (các quyển 3A, 3B và 3C)
- 05 phần mềm bảo mật gói IP (01 trên Windows; 01 trên Solaris; 03 trên Linux)

Nhóm thứ ba: Cung cấp và sử dụng chứng chỉ số

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Trần Duy Lai	Phân viện NCKHMM-HVKTMM
2	PGS TS Lê Mỹ Tú	Học viện Kỹ thuật Mật mã
3	ThS Đặng Hoà	Phòng QLNCKH-HVKTMM
4	TS Nguyễn Hồng Quang	Phân viện NCKTMM-HVKTMM
B	**Những người tham gia một trong các kết quả nghiên cứu**	
1	ThS Hoàng Văn Thức	Phân viện NCKHMM-HVKTMM
2	KS Phạm Văn Lực	Phân viện NCKHMM-HVKTMM
3	KS Cao Thanh Nam	Phân viện NCKTMM-HVKTMM
4	ThS La Hữu Phúc	Phân viện NCKTMM-HVKTMM
5	ThS Trịnh Minh Sơn	Phân viện NCNVMM-HVKTMM
6	ThS Hoàng Thu Hằng	Phân viện NCNVMM-HVKTMM

Sản phẩm đã đạt được:

- 05 báo cáo khoa học (các quyển 6A, 7A, 8A, 8B và 9A)
- 03 phần mềm (cấp và thu hồi chứng chỉ số, thư viện chữ ký số, bảo mật Web dùng Proxy Server)
- 01 thiết bị phần cứng để ghi khoá có giao diện USB

Nhóm thứ tư: Đảm bảo toán học

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Lều Đức Tân	Phân viện NCKHMM-HVKTMM
2	TS Trần Văn Trường	Phân viện NCKHMM-HVKTMM
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	TS Nguyễn Ngọc Cương	Phân viện NCKHMM-HVKTMM
2	KS Trần Hồng Thái	Phân viện NCKHMM-HVKTMM
3	ThS Trần Quang Kỳ	Phân viện NCKHMM-HVKTMM
4	ThS Phạm Minh Hoà	Phân viện NCKHMM-HVKTMM
5	KS Nguyễn Quốc Toàn	Phân viện NCKHMM-HVKTMM
C	***Cộng tác viên***	
1	TS Nguyễn Lê Anh	Đại học Xây dựng
2	TSKH Phạm Huy Điển	Viện Toán học

Sản phẩm đã đạt được:

- 03 báo cáo khoa học (các quyển 3A, 3B và 3C)
- 02 phần mềm (sinh tham số an toàn cho hệ mật RSA và Elgamal)

Bài tóm tắt

Kết quả của đề tài KC.01.01 gồm 18 báo cáo khoa học và 10 sản phẩm phần mềm. Các quyển báo cáo khoa học đã được đánh số đề phù hợp với 9 mục sản phẩm như đã được đăng ký trong bản hợp đồng thực hiện đề tài. Tuy nhiên, xét về nội dung thì các sản phẩm đó có thể được xếp vào 4 nhóm sau:

- Nhóm thứ nhất: các nghiên cứu tổng quan, tìm hiểu giải pháp cho các cơ chế đảm bảo an ninh, an toàn mạng.
- Nhóm thứ hai: các sản phẩm bảo mật gói IP trên các hệ điều hành Linux, Solaris, Windows.
- Nhóm thứ ba: cung cấp và sử dụng chứng chỉ số.
- Nhóm thứ tư : nghiên cứu đảm bảo toán học về cách dùng và sinh tham số an toàn cho các hệ mật khoá công khai cũng như xây dựng hệ mã khối.

Đề tài đã tập trung giải quyết một số vấn đề về an ninh và bảo mật đối với thông tin được vận chuyển trên mạng dùng giao thức IP. Những kết quả nghiên cứu mang tính tổng quan, tìm hiểu giải pháp cho các cơ chế đảm bảo an ninh an toàn mạng bao gồm: quyển 1A „Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử“; quyển 1B „Nước Nga và chữ ký điện tử số“; quyển 1C „Tìm hiểu khả năng công nghệ để cứng hoá thuật toán mật mã“; quyển 2A“Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau“; quyển 2B “Tổng quan về an toàn Internet“; quyển 5A “An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux“; quyển 5B „Cơ chế an toàn của các hệ điều hành mạng, Network hacker, virut máy tính“.

Bài toán bảo mật gói IP đã được giải quyết khá triệt để, chúng tôi đã có các phần mềm mã hoá gói IP chạy trên 3 loại hệ điều hành mạng tiêu biểu, đó là Microsoft Windows, Sun Solaris và Linux. Đặc biệt, sử dụng khả năng mã nguồn mở của hệ điều hành Linux, chúng tôi đã tạo ra một họ các sản phẩm bảo mật gói IP. Ba báo cáo dành cho các phần mềm mã gói IP là: quyển 4A „Các phần mềm bảo mật gói IP trên hệ điều hành Linux“, quyển 4B „Hệ thống an toàn mạng trên môi trường mạng Sun Solaris“ và quyển 4C „Phần mềm bảo mật trên môi trường Windows“. Nếu như giải pháp bảo mật trên Linux là mã nguồn mở thì trên Windows là thay thế Winsock bằng winsock mật mã, còn trên Solaris là sử dụng công nghệ lập trình STREAMS để can thiệp vào chồng giao thức IP.

Thương mại điện tử là một trong những cái thể hiện xu hướng toàn cầu hoá trong tin học. Mật mã không những được sử dụng để bảo mật thông tin, mà một mặt ứng dụng rất được ưa chuộng của nó là ứng dụng để xác thực. Mật mã được dùng để xác thực là mật mã khoá công khai. Mỗi người sử dụng khoá công khai có một cặp khoá: một khoá bí mật và một khoá công khai. Người ta dùng khoá bí mật để ký văn bản còn dùng khoá bí mật của người khác để kiểm tra chữ ký mà người ký đã tạo ra. Khoá công khai thì có thể công bố công khai, bằng cách in như danh bạ điện thoại, nhưng lấy gì đảm bảo tính chân thực của những khoá công khai đã được công bố. Rất hay là chính bản thân mật mã khoá công khai lại được sử dụng để giải quyết bài toán này, người ta dùng chữ ký của CA (Certificate Authority) để ký vào một văn

bản đặc biệt bao gồm 2 thông tin chính là định danh của người sử dụng và khoá công khai của người đó. Cái đó được gọi là chứng chỉ số và góp phần tạo nên cơ sở hạ tầng khoá công khai (PKI- Public Key Infrastructure). Nhưng chứng chỉ số sinh ra cần phải được sử dụng vào các ứng dụng trên mạng, trong đó có các ứng dụng thương mại điện tử với hai dịch vụ cơ bản là Mail và Web. Một loạt các báo cáo đã tập trung giải quyết vấn đề này, đó là quyển 6A „Một hệ thống sinh chứng chỉ số theo mô hình sinh khoá tập trung"; quyển 7A „Một hệ chữ ký số có sử dụng RSA"; quyển 8A „Dùng chứng chỉ số với các ứng dụng Web và Mail"; quyển 8B „Bảo mật dịch vụ Web thông qua Proxy Server" và quyển 9A „Một số thiết bị được sử dụng để ghi khoá".

Trên đây đã điểm qua các kết quả nghiên cứu phát triển sản phẩm phần mềm trong 2 lĩnh vực là bảo mật gói IP được truyền thông trên mạng và bảo mật các dịch vụ Web và Mail trong thương mại điện tử. Thế nhưng cái lõi mật mã trong các sản phẩm ấy chính là các thuật toán, các tham số mật mã. Trong khuôn khổ phạm vi của đề tài cũng đã hoàn thành 3 kết quả nghiên cứu nhằm đảm bảo toán học cho độ an toàn mật mã, đó là: quyển 3A „Sinh tham số an toàn cho hệ mật RSA"; quyển 3B „Sinh tham số an toàn cho hệ mật Elgamal"; quyển 3C „Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả".

Hai nhóm sản phẩm về bảo mật gói IP và cung cấp/sử dụng chứng chỉ số đã được triển khai thử nghiệm. Có những sản phẩm sau đó đã được hoàn thiện nâng cấp để triển khai thực tế.

Mục lục

Bảng chú giải các chữ viết tắt, ký hiệu, đơn vị đo,
từ ngắn hoặc thuật ngữ

ACL	Access Control List
AD	Active Directory
AH	Authentication Header
ARP	Address Resolution Protocol
AS	Autonomous System
ASET	Automated Security Enhancement Tool
ASIC	Application-Specific Integrated Circuit
ASN.1	Abstract Syntax Notation One
ASSP	Application-Specific Standard Product
BGP	Border Gateway Protocol
CA	Certificate Authority
CAD	Computer-Aided Design
CDFS	CDROM File System
CFS	Cryptographic Gile System
CIPE	Cryptographic IP Encapsulation
CLNP	Connectionless Network Protocol
CTL	Certificate Trust List
CRL	Certificate Revocation List
CRT	Chinese Residual Theorem
DAC	Discretionary Access Controls
DARPA	Defence Advanced Research Projects Agency
DSP	Digital Signal Processor
EDI	Electronic Data Interchange
EFS	Encryption File System
EGP	Exterior Gateway Protocol
ESP	Encapsulation Security Payload
FAT	File Allocation Table
FEK	File Encryption Key
FPGA	Field Programmable Gate Array
GGP	Gateway to Gateway Protocol
GSS-API	General Security Services Application Programming Interface
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPSEC	IP Security
ISAKMP	Intenet Security Association and Key Management Protocol
IKE	Internet Key Exchange
IHL	Internet Header Length
ITU	International Telecommunication Union
ISO	International Organization for Standardization
L2F	Layer 2 Forwarding
L2TP	Layer 2 Transfer Protocol
LDAP	Light Directory Access Protocol
LSA	Local Security Authority
MIME	Multipurpose Internet Mail Extensions

MSP	Message Security Protocol
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
NLSO	Network-Layer Security Protocol
NTFS	New Technology File System
PAM	Pluggable Authentication Module
PGP	Pretty Good Privacy
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
PPTP	Point to Point Transfer Protocol
RFC	Request For Comment
RISC/GPP	Reduced Instruction Set Computer/ General Purpose Processor
SET	Secure Electronic Transaction
SA	Security Association
S-HTTP	Secure Hyper Text Transfer Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
RAS	Remote Access Service
RPC	Remote Procedure Call
RSA	Rivest- Shamir- Adleman
SAM	Security Account Manager
SID	Security Identifier
SPI	Security Parameters Index
SRM	Security Reference Monitor
SSL	Secure Socket Layer
TCFS	Transparent Cryptographic File System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLSP	Transport Layer Security Protocol
TMĐT	Thương mại điện tử
TPDU	Transport Protocol Data Unit
UDP	User Datagram Protocol
VPN	Virtual Private Network

Lời mở đầu

Các nội dung mà đề tài đã tiến hành nhằm thực hiện 2 mục tiêu đã được đăng ký trong bản thuyết minh đề tài, đó là:

- Nghiên cứu một số công nghệ, giải pháp nhằm đảm bảo an toàn, an ninh thông tin cho các mạng dùng giao thức IP, từ đó đề xuất mô hình phù hợp đặc điểm sử dụng ở Việt Nam
- Phục vụ việc phát triển thương mại điện tử (TMĐT) của Việt Nam, hướng tới hội nhập khu vực

Sự phát triển của các mạng máy tính nói riêng và mạng Internet nói chung đã làm cho nhu cầu đảm bảo an ninh an toàn thông tin trên mạng ngày càng tăng. Có nhiều công nghệ mạng (ví dụ như Ethernet và Token Ring), có nhiều giao thức mạng (ví dụ như TCP/IP, IPX/SPX và NETBEUI,...), nhưng do sự phát triển vượt trội của giao thức IP so với các giao thức khác trên thế giới, và căn cứ vào đặc điểm công nghệ mạng được triển khai tại Việt Nam, chúng ta thấy rằng để có thể bảo đảm được an ninh an toàn cho hầu hết các dịch vụ mạng thì chỉ cần tập trung vào giải quyết các bài toán đối với giao thức IP. Nếu có giải pháp và sản phẩm bảo mật tốt cho môi trường IP, khi gặp phải các môi trường truyền thông khác chúng ta có thể dùng các thiết bị chuyển đổi (ví dụ như E1-IP) để sử dụng được các giải pháp và sản phẩm đã có.

Việt Nam đang trong quá trình hội nhập khu vực và hội nhập quốc tế. Thương mại điện tử chính là một công cụ đắc lực phục vụ cho quá trình hội nhập ấy. Ở trong nước cũng đang quá trình xây dựng chính phủ điện tử (đề án 112 của Chính phủ về Tin học hoá quản lý hành chính). Để cho thương mại điện tử cũng như chính phủ điện tử phát triển được đều cần có sự hỗ trợ của các công cụ/sản phẩm đảm bảo an ninh bảo mật thông tin trên các mạng truyền thông tin học.

Các sản phẩm của đề tài (báo cáo khoa học và phần mềm) đã đáp ứng đầy đủ các các nội dung đăng ký trong mục 16 „Yêu cầu khoa học đối với sản phẩm tạo ra“ của bản thuyết minh đề tài, cũng như bảng 2 „Danh mục sản phẩm khoa học công nghệ“ của bản hợp đồng thực hiện đề tài. Báo cáo khoa học của đề tài gồm 18 quyển như sau:

tt	Tên báo cáo
1	**Báo cáo cập nhật các kết quả mới trong lĩnh vực bảo mật mạng và thương mại điện tử:**
	Quyển 1A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử
	Quyển 1B: Nước Nga và chữ ký điện tử số
	Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã
2	**Mô hình bảo mật thông tin cho các mạng máy tính**
	Quyển 2A: Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau
	Quyển 2B: Tổng quan về an toàn Internet
3	**Nghiên cứu đảm bảo toán học**
	Quyển 3A: Sinh tham số an toàn cho hệ mật RSA
	Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal

	Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả
	Phụ lục: Một số nghiên cứu về hàm băm và giao thức mật mã
4	**Hệ thống phần mềm bảo mật mạng**
	Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux
	Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris
	Quyển 4C: Phần mềm bảo mật trên môi trường Windows
5	**An ninh, an toàn của các hệ điều hành mạng**
	Quyển 5A: An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux
	Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network Hacker, Virut máy tính
6	**Hệ thống cung cấp PKI**
	Quyển 6A: Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung
7	**Bộ chương trình cung cấp chữ ký điện tử**
	Quyển 7A: Một hệ chữ ký số có sử dụng RSA
8	**Hệ thống chương trình xác thực trong thương mại điện tử**
	Quyển 8A: Dùng chứng chỉ số với các dịch vụ Web và Mail
	Quyển 8B: Bảo mật dịch vụ Web thông qua Proxy Server
9	**Các sản phẩm nghiệp vụ và qui chế sử dụng**
	Quyển 9A: Một số thiết bị được sử dụng để ghi khoá

Các sản phẩm phần mềm/thiết bị bao gồm:

1	Phần mềm bảo mật gói IP: - Trên môi trường Windows (SECURE SOCKET) - Trên môi trường Linux (TRANSCRYPT, IP-CRYPTOR, DL-CRYPTOR)
2	Phần mềm về chứng chỉ số: - Sinh chứng chỉ số theo mô hình sinh khoá tập trung - Thư viện chữ ký số - Dùng chứng chỉ số để bảo mật dịch vụ Web thông qua Proxy Server
3	Phần mềm đảm bảo toán học: - Phần mềm sinh tham số an toàn cho hệ mật RSA - Phần mềm sinh tham số an toàn cho hệ mật Elgamal
4	Thiết bị nghiệp vụ: - Thiết bị ghi khoá với giao diện USB

TỔNG KẾT CÁC NỘI DUNG NGHIÊN CỨU VÀ KẾT QUẢ CHÍNH

1. Nhóm thứ nhất: Nghiên cứu tổng quan, tìm hiểu giải pháp cho các cơ chế đảm bảo an ninh an toàn mạng

1.1 Quyển 1 A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử. Chủ trì nhóm nghiên cứu: PGS. TS. Hoàng Văn Tảo

Tên của báo cáo đã thể hiện 3 nội dung sẽ được đề cập đến trong 3 chương. Toàn bộ báo cáo gồm 44 trang.

Chương 1 „Giới thiệu về IPSEC“ đã trình bày về một trong các công nghệ tạo nên mạng riêng ảo (VPN), các dịch vụ IPSEC cho phép bạn xây dựng các đường hầm an toàn thông tin qua các mạng không tin cậy (ví dụ như Internet) với cả hai khả năng xác thực và bảo mật. Các vấn đề đã được đi sâu là:

- Các đặc tính của IPSEC là: phân tách các chức năng xác thực và bảo mật (tất nhiên, chúng có thể kết hợp với nhau); được cài đặt ở tầng mạng; hỗ trợ 2 dạng kết nối là host-to-host và gateway-to-gateway; hỗ trợ khả năng quản lý khoá thuận tiện (khoá phiên có thể phân phối tự động hay thủ công)
- Các khái niệm cơ bản: Security Association (SA), Security Parameters Index (SPI), Authentication Header (AH), Encapsulation Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP),
- Những nơi có thể dùng được IPSEC (hay mô hình áp dụng), ưu điểm của IPSEC, các hạn chế của IPSEC (xác thực máy, không xác thực người dùng; không chống được tấn công từ chối dịch vụ, không chống được tấn công phân tích mạng), các mode dùng IPSEC (chỉ xác thực, mã hoá + xác thực)

Chương 2 có tên là „Phát hiện xâm nhập: làm thế nào để tận dụng một công nghệ còn non nớt“. Trong phần đặt vấn đề ở đầu chương đã nói rõ vì các bức tường lửa và các chính sách an ninh an toàn là chưa đủ để ngăn chặn mọi tấn công phá hoại, cho nên cần đến hệ phát hiện xâm nhập (IDS - Intrusion Detection System). Các vấn đề sau đã được trình bày:

- Phát hiện xâm nhập là gì? (nó bao gồm cả việc phát hiện sự lạm dụng của người ở trong cũng như người ngoài). Tại sao lại dùng tiện ích phát hiện xâm nhập? (nó thay cho nhiều con người, nó có thể phản ứng lại các xâm nhập). Cơ chế làm việc của các IDS.
- Các giải pháp phát hiện xâm nhập bao gồm: các hệ thống phát hiện dị thường; các hệ thống phát hiện lạm dụng; các hệ thống giám sát đích
- Những ưu điểm của IDS : giảm giá thành so với việc dùng con người, phát hiện ngăn chặn và khôi phục, nhật ký và khả năng pháp lý. Những nhược điểm: hãy còn *non nớt*, phát hiện sai, suy giảm hiệu suất, chi phí ban đầu,...
- Việc sử dụng IDS: nó có liên quan tới việc đánh giá rủi ro; khi mua một sản phẩm IDS cần chú ý tới chi phí, chức năng, khả năng mở rộng,...; khi sử dụng cần chú ý tới một khái niệm được gọi là „khai thác một kiến trúc phát hiện xâm nhập.

Chương 3 „Thương mại điện tử“ đã đề cập đến:

- Các hình thức hoạt động chủ yếu của TMĐT: thư, thanh toán điện tử, trao đổi dữ liệu, ..

- Tình hình phát triển TMĐT trên thế giới: quá trình phát triển có thể chia thành 3 giai đoạn; điểm qua tình hình phát triển TMĐT ở một số nước như Mỹ, Canada, Nhật, EU,...
- Tình hình phát triển TMĐT ở Việt Nam: môi trường đúng nghĩa cho TMĐT ở Việt Nam chưa hình thành; ở cuối chương có đề cập đến một số khuyến nghị trên con đường tiến tới TMĐT ở nước ta.
- An toàn trong TMĐT: đã điểm qua các mối đe doạ đến sự an toàn của TMĐT; những yêu cầu bảo vệ thông tin và giải pháp đảm bảo;

1.2 ***Quyển 1B: Nước Nga và chữ ký điện tử số.*** Chủ trì nhóm nghiên cứu: PGS. TS. Hoàng Văn Tảo

Ngày 10 tháng 1 năm 2002, tổng thống Nga V. Putin đã ký sắc lệnh liên bang về chữ ký điện tử số. Để đi tới Luật về chữ ký điện tử số, nước Nga đã có một quá trình chuẩn bị kỹ càng từ trước. Liên quan đến vấn đề này, trong báo cáo đã đề cập tới các nội dung sau:

- Bài viết của 3 chuyên gia FAPSI là tiến sĩ toán-lý A.C. Kuzmin, phó tiến sĩ kỹ thuật A.B. Korolkov và phó tiến sĩ toán-lý N.N. Murasov trong tạp chí chuyên ngành về an ninh thông tin "CBCNTVS MTPJGFCYJCNB" số ra tháng 2-3 năm 2001 "Những công nghệ hứa hẹn trong lĩnh vực chữ ký điện tử số": đề cập tới dự án chuẩn quốc gia mới của Nga về chữ ký số.
- Bài của các chuyên gia V. Miaxnhiankin và A. Mejutkov "Chữ ký điện tử hay con đường gian khổ thoát khỏi giấy tờ" trong tạp chí "CBCNTVS MTPJGFCYJCNB", số ra tháng 8-9 năm 2001: khác với chữ ký viết tay, chữ ký số phụ thuộc vào văn bản được ký.
- Vậy nước Nga đã dùng chuẩn chữ ký số nào? Chúng tôi đã mô tả: (1) chuẩn chữ ký số GOST P 34.10-94 ; (2) chuẩn chứ ký số GOST P 34.10-2001; (3) chuẩn hàm băm GOST P.34.11-94; (4) chuẩn mã khối GOST 24187-89 (do chuẩn hàm băm GOST P.34.11-94 có sử dụng thuật toán GOST 24187-89)
- Trong báo cáo chúng tôi đã dịch toàn bộ „*Bộ luật Liên bang về chữ ký điện tử*" gồm 5 chương và 21 điều.
- Để tiện so sánh, trong 5 phụ lục chúng tôi đã trình bày về: (1) mô tả thuật toán DSS của Mỹ, chuẩn này đã được công bố ngày 7 tháng 1 năm 2000 để thay cho chuẩn được đưa ra từ nhiều năm trước đây (1994); (2) mô tả họ các hàm băm SHA của Mỹ; (3) mô tả thuật toán mã khối Rijndael; (4) Giới thiệu bài báo của 2 tác giả người Nga so sánh thuật toán mã khối GOST 24187-89 của Nga và thuật toán Rijndael là thuật toán sẽ được chấp nhận là chuẩn mã dữ liệu mới của Mỹ (AES) thay cho DES; (5) Bên cạnh đó còn có một bài báo của tác C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini, Y. Zheng viết về chuẩn GOST 24187-89 của Nga.

1.3 Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã. Chủ trì nhóm nghiên cứu: Nguyễn Hồng Quang

Mật mã có thể thực hiện theo cách thủ công hoặc tự động với sự trợ giúp của máy móc. Trong thời đại điện tử, truyền thông và tin học ngày nay *các nguồn tin ngày càng đa dạng*; mọi *thông tin đều được số hóa* với khổng lồ trữ lượng tại chỗ và lưu lượng trên kênh; *đòi hỏi của người dùng ngày càng cao* về độ mật, tốc độ, độ an

toàn, tính tiện dụng... Trong tình hình đó, chỉ có một lựa chọn duy nhất là thực hiện mật mã với sự trợ giúp của máy móc.

Phần 1 "So sánh thực hiện mật mã bằng phần cứng và phần mềm" là để trả lời câu hỏi: nên thực hiện mật mã trên cơ sở phần cứng (hardware) hay phần mềm (software)? Để trả lời cho câu hỏi đó cần *phân tích các ưu nhược điểm* của hai platform này, xác định *những yêu cầu chung* cho một thiết bị điện tử và *yêu cầu riêng* mang tính đặc thù của thiết bị mật mã, các *yếu tố cần cân nhắc* khi sử dụng thực tế. Cuối phần 1 có so sánh về độ an toàn giữa 2 platform: sử dụng chung không gian nhớ RAM; đảm bảo toàn vẹn; thám ngược thiết kế; tấn công phân tích năng lượng; vấn đề lưu trữ khoá dài hạn; phụ thuộc vào độ an toàn của hệ điều hành.

Phần 2 "Lựa chọn công nghệ cho cứng hoá mật mã". Giả thiết yêu cầu đặt ra là bảo mật thông tin trong khu vực Chính phủ, An ninh và Quốc phòng ở đó đòi hỏi độ an toàn cao và tốc độ lớn, rõ ràng platform lựa chọn phải là hardware. Không như ở lĩnh vực khác chỉ cần chọn đúng công nghệ để thực hiện bài toán đặt ra sao cho tối ưu về giá thành, dễ phát triển, nhanh ra thị trường, có khả năng upgrade... là đủ. Với ngành mật mã, ngoài việc chọn công nghệ thích hợp cho *encryption*, cũng quan trọng không kém là công nghệ đó có bảo đảm *security* không. Cũng cần chú thích là trong số 7 công nghệ được phân tích, nhiều công nghệ là sự pha trộn giữa hardware và software trên cơ sở lập trình cho chip. Tuy nhiên khác với software như đã đề cập ở phần trước ở chỗ software cho chip thực hiện trên hardware được thiết kế riêng, chuyên dụng, đóng kín, không dùng chung bộ nhớ và hệ điều hành, được đốt vật lý trên chip. Và như vậy có thể xếp chúng vào hardware platform. Các công nghệ đã được đưa ra xem xét là: (1) ASIC (2) ASSP (Application-Specific Standard Product); (3) Configurable Processor; (4) DSP (Digital Signal Processor); (5) FPGA (Field Programmable Gate Array); (6) MCU (Microcontroller); (7) RISC/GPP (Reduced Instruction Set Computer/ General Purpose Processor). Các phương diện được so sánh là: (1) thời gian đưa sản phẩm ra thị trường; (2) năng lực thực hiện; (3) giá thành; (4) tính dễ phát triển; (5) năng lượng tiêu thụ; (6) tính mềm dẻo. Trong phần 2 cũng đã dành nhiều trang để trình bày kỹ về công nghệ FPGA, bởi vì *công nghệ thích hợp nhất để cứng hoá mật mã chính là FPGA*, đó là các nội dung: cấu trúc FPGA; khả năng cấu hình lại FPGA; những ưu điểm của FPGA đối với mật mã. Tiếp theo đã trình bày về việc dùng FPGA để cứng hoá các loại thuật toán mật mã khác nhau, đó là: (1) sinh khoá dòng; (2) các phép nhân và modulo; (3) mã khối (AES); (4) mật mã elliptic; (5) hàm hash; (6) sinh số ngẫu nhiên. Cuối phần 2 đã trình bày về độ an toàn mật mã dựa trên hardware: tấn công lên hardware nói chung và tấn công lên FPGA nói riêng (tấn công kiểu hộp đen; tấn công kiểu đọc lại; tấn công nhái lại SRAM FPGA; thám ngược thiết kế từ chuỗi bit; tấn công vật lý đối với các công nghệ SRAM FPGAS/ ANTIFUSE FPGAS/ FLASH FPGAS; tấn công side channel gồm có Simple Power Analysis và Different Power Analysis.

Phần 3 "Chuẩn bị để cứng hoá mật mã" xoay quanh FPGA. Hai nội dung đã được trình bày. Trước hết là những kiến thức cần thiết để thực hiện FPGA bao gồm: kiến thức về toán; kiến thức về kỹ thuật; kiến thức về công nghệ; kiến thức về thị trường vi mạch. Thứ hai là các công cụ cần thiết để thực hiện FPGA bao gồm: công cụ thiết kế (CAD); thiết bị (máy tính, bộ nạp); nhân lực. Cuối của phần này có giới thiệu một số hãng sản xuất FPGA như Xilinx và Altera cũng như tương lai của FPGA.

1.4 ***Quyển 2A: Giao thức TCP/IP và các giải pháp bảo mật ở các tầng khác nhau***.

Chủ trì nhóm nghiên cứu: ThS. Đặng Hoà

Muốn nghiên cứu giải pháp bảo mật cho giao thức IP thì cần phải hiểu rõ nó. Chính vì vậy mà báo cáo khoa học gồm có 2 phần, phần I „Giao thức mạng TCP/IP“ gồm có 9 chương, phần II „Giải pháp bảo mật“ gồm có 3 chương dành cho 3 tầng: tầng mạng, tầng giao vận và tầng ứng dụng. Chú ý rằng, khái niệm tầng ở 3 chương cuối lại theo mô hình ISO.

Chương 1 „Giới thiệu và khái quát“ đã trình bày lịch sử của TCP/IP, nó bắt đầu từ DARPA. 4 đặc tính của TCP/IP được nêu ra (không phụ thuộc hệ điều hành; không phụ thuộc phần cứng; chế độ đánh địa chỉ chung và chuẩn hoá các bộ giao thức ở tầng trên). Nó có các dịch vụ tiêu biểu ở tầng ứng dụng là thư điện tử, chuyển file, truy cập từ xa và www. Trong khi đó, các dịch vụ ở tầng mạng có thể chia làm 2 loại: dịch vụ không liên kết chuyển gói tin và dịch vụ vận tải dòng dữ liệu tin cậy. Các tài liệu chuẩn về TCP/IP ở dạng RFC, có thể tải xuống từ địa chỉ ftp://nic.ddn.mil/rfc/rfcxxxx.txt. Internet phát triển rất nhanh và tương lai của IP sẽ là IP v6.

Chương 2 „Cấu trúc phân tầng của mô hình TCP/IP“ nhằm trình về 4 tầng: tầng ứng dụng (Telnet, FTP,...); tầng vận tải (TCP, UDP,...); tầng Internet (IP) (hay còn gọi là tầng mạng); và tầng tiếp cận mạng (Ethernet, ATM,...). Trong tầng tiếp cận mạng cần chú ý việc chuyển đổi giữa địa chỉ IP và địa chỉ vật lý. Trong tầng Internet cần chú ý đến bài toán dẫn đường của gói tin (routing). Có hai biên địa chỉ quan trọng: (1) biên địa chỉ giao thức (ngăn cách địa chỉ của tầng thấp và tầng cao); (2) biên hệ điều hành (ngăn cách hệ thống với các chương trình ứng dụng).

Tầng	Biên
Tầng ứng dụng	Phần mềm ngoài hệ điều hành
Tầng vận tải	Phần mềm trong hệ điều hành
Tầng Internet	Chỉ sử dụng các địa chỉ IP
Tầng tiếp cận mạng	Sử dụng các địa chỉ vật lý
Phần cứng	

Chương 3 „Các địa chỉ Internet“ đã trình bày về 5 lớp địa chỉ mạng là A, B, C, D và E. Khái niệm mạng con (subnet) đi kèm với khái niệm địa chỉ mạng và subnet mask. Cách đánh địa chỉ Internet cũng có một số nhược điểm, đó là: địa chỉ hướng tới đường liên kết chứ không hướng tới máy; địa chỉ nhóm C chỉ gồm 255 máy nên khi vượt quá thì phải chuyển sang lớp B; đối với máy dùng nhiều địa chỉ IP (có nhiều card mạng chẳng hạn) thì việc vạch đường dẫn phụ thuộc vào địa chỉ được sử dụng.

Chương 4 có tên là „Tương ứng địa chỉ Internet với địa chỉ vật lý“. Do cuối cùng việc truyền thông phải được thực hiện trong mạng vật lý nhờ sử dụng địa chỉ vật lý mà phần cứng cung cấp nên phải có cách ánh xạ giữa địa chỉ IP và địa chỉ vật lý. Giao thức Giải quyết địa chỉ ARP đã cung cấp một cơ chế hiệu quả và dễ duy trì, đây là giải pháp giải quyết nhờ tương ứng động. Trong mỗi thiết bị mạng sẽ có một cache giải quyết địa chỉ.

Chương 5 „Giao thức Internet: chuyển gói tin không có liên kết“ trình bày về dịch vụ chuyển gói tin không liên kết (không chắc chắn, mỗi gói tin là độc lập với gói tin khác, dịch vụ được coi là chuyển cố gắng nhất). Trong chương này đã giới thiệu định dạng của gói tin IP (địa chỉ nguồn, địa chỉ đích, IHL, ...), có đi sâu vào một số trường như kích thước của gói tin, MTU và Fragmentation Offset. Trong hệ thống chuyển gói tin, việc vạch đường dẫn là quá trình chọn đường để gửi gói tin, và bộ định tuyến (router) là một máy tính bất kỳ làm chức năng vạch đường dẫn. Một vài giao thức dẫn đường đã được điểm qua: GGP, EGP, BGP.

Chương 6 „Giao thức Internet: các thông báo điều khiển và báo lỗi“ thảo luận cơ cấu mà các cổng và các máy sử dụng để trao đổi sự điều khiển hoặc thông báo lỗi. Cơ cấu này được gọi là Giao thức Thông báo điều khiển Internet - Internet Control Message Protocol (ICMP). Giao thức này được coi là một phần của Giao thức Internet, và phải có trong mọi thực hiện của giao thức IP. Thông báo ICMP được bao bọc trong gói tin IP, đến lượt gói tin IP được bao bọc trong gói dữ liệu của mạng vật lý để truyền. Thông báo ICMP có định dạng như sau: TYPE (8 bit), CODE (8 bit), CHECKSUM (16 bit), header và 64 bit dữ liệu đầu của gói tin đã sinh ra lỗi. Một số chức năng chính của ICMP là: điều khiển dòng thông tin; phát hiện không tới được máy đích; chuyển đường; kiểm tra máy ở xa.

Chương 7 „Giao thức gói tin của người sử dụng UDP“ trình bày về định dạng của gói tin UDP, cách bọc gói tin UDP vào gói tin IP. Giao thức UDP chấp nhận các gói tin từ nhiều chương trình ứng dụng và chuyển chúng đến giao thức IP để truyền, và nó chấp nhận các gói tin UDP đến từ giao thức IP và chuyển chúng đến các chương trình ứng dụng thích hợp. Một cách khái niệm, toàn bộ việc phân cổng và hợp cổng giữa phần mềm UDP và chương trình ứng dụng xảy ra qua cơ chế cổng.

Chương 8 „Giao thức điều khiển truyền tin TCP“ nêu lên 5 tính chất của TCP: hướng đến dòng dữ liệu; liên kết mạch ảo; truyền có phần đệm; dòng dữ liệu không có cấu trúc; liên kết 2 chiều. Phải có một cơ chế giúp cho TCP cung cấp sự tin cậy, đó là xác nhận và truyền lại, đó là các cửa sổ trượt, thiết lập một liên kết TCP. Báo cáo cũng trình bày về khái niệm cổng của TCP, định dạng của đoạn TCP.

Chương 9 „Hệ thống tên vùng“ trình bày về các tên vùng quen thuộc như GOV, EDU, COM,..,; tương ứng giữa tên vùng và địa chỉ. Cơ cấu tên vùng để tương ứng các tên với các địa chỉ gồm các hệ thống hợp tác, độc lập gọi là các chương trình chủ cung cấp tên (name servers).

Chương 10 „An toàn tầng mạng“ đã đề cập tới :

- Phân biệt end system (hệ thống đầu cuối) và intermediate system (hệ trung gian).
- Connectionless Network Protocol (CLNP) cung cấp dịch vụ mạng kiểu không liên kết trong vai trò SNICP vai trò (subnetwork-independent convergence protocol)
- An toàn mức hệ thống cuối (end system-level security): nó liên quan tới hoặc Transport layer hoặc subnetwork-independent network layer protocol. Tuy nhiên, cài đặt an toàn cho hệ thống cuối ở tầng mạng là được ưu tiên hơn.
- An toàn mức mạng con (subnetwork-level security): khác với end system-level security.
- Network-Layer Security Protocol (NLSP) được công bố trong ISO/IEC 11577. Trong NLSP có hai giao diện: giao diện dịch vụ NLSP và giao diện dịch vụ mạng cơ sở (UN-underlying network). NLSP cũng cung cấp subnetwork level security.

Mô hình bảy tầng ISO

7	Tầng ứng dụng	PEM, S-HTTP, SET
6	Tầng trình diễn	
5	Tầng phiên	SSL
4	Tầng giao vận	IPSEC
3	Tầng mạng	PPTP, swIPe
2	Tầng liên kết dữ liệu	VPDN, L2F, L2TP
1	Tầng vật lý	Fiber Optics

Chương 11 „An toàn tầng giao vận“ đã trình bày về:

- Các thủ tục tầng giao vận gồm có: assignment to a network connection (gán liên kết mạng); transport protocol data unit transfer (truyền TPDU); segmentation and reasembling (phân đoạn và ráp lại); ...
- Transport Layer Security Protocol (TLSP) được mô tả ở chuẩn ISO/IEC 10736. Nó được đặt hoàn toàn trong tầng giao vận. TLSP được thiết kế để bổ sung vào các giao thức tầng giao vận thông thường mà không phải để thay đổi chúng.
- Các cơ chế an toàn: Hàm đóng gói của TLSP hỗ trợ việc cung cấp một vài dịch vụ an toàn và có thể kéo theo tổ hợp các cơ chế an toàn nào đó được yêu cầu. Các cơ chế này là nhãn an toàn, con trỏ hướng, giá trị kiểm tra toàn vẹn (ICV), đệm mã hoá (padding) và mã hoá.

Chương 12 „Các giao thức an toàn tầng ứng dụng của các mạng“ đã đi vào 3 lĩnh vực:

- Trao đổi tiền tệ. SET (giao dịch điện tử an toàn) là một giao thức an toàn căn cứ vào ứng dụng do Visa và MasterCard cùng nhau phát triển. Trong báo cáo đã trình bày kỹ 5 bước của SET. S/PAY được RSA Data Security phát triển là một cài đặt của SET
- Gửi thông báo điện tử: PEM, RIPEM, S/MIME, PGP
- Các giao dịch www: SSL, S-HTTP

1.5 ***Quyển 2B: Tổng quan về an toàn Internet.*** Chủ trì nhóm nghiên cứu: PGS. TS. Lê Mỹ Tú

Internet với chi phí thấp và tồn tại ở mọi nơi đã làm cho các ứng dụng thương mại điện tử trở nên khả thi. Thế nhưng, các rủi ro khi sử dụng Internet có thể gây ra hiện tượng nản chí. Chương 1 „An toàn Internet“ đã trình bày các vấn đề sau:

- Ba khía cạnh của bài toán „an toàn“ là: an toàn mạng (bao gồm Authentication and integrity, Confidentiality, Access control); an toàn ứng dụng và an toàn hệ thống
- An toàn giao thức mạng: hai kỹ thuật để an toàn IP đó là Authentication Header và Encapsulating Security Payload. ESP có 2 chế độ, đó là: tunnel mode và transport mode. Những nội dung được trình bày ở đây đã được trình bày ở chương 1 „Giới thiệu IPSEC“ ở quyển 1A.

- Các bước tường lửa đảm bảo an toàn hệ thống: điểm qua một số khái niệm như Screening routers, Proxy servers, Perimeter network.
- Trong phần trình bày về An toàn dịch vụ gửi tin đã đề cập đến: Các dịch vụ bảo vệ thông báo (Message origin authentication –Xác thực nguồn gốc của thông báo; Content integrity-Toàn vẹn nội dung; Content confidentiality-Sự tin cậy của nội dung; Non-repudiation of origin-Chống chối bỏ nguồn gốc) và Các dịch vụ xác nhận (confirmation service) (Proof of delivery –Chứng minh sự chuyển giao; Proof of submission –Chứng minh sự xem xét; Non-repudiation of delivery-Chống chối bỏ sự chuyển giao; Non-repudiation of submission- Chống chối bỏ sự xem xét). Có 6 ứng dụng có bảo mật được đề cấp đến là: (1) PEM (Privacy Enhanced Mail); (2) MIME (Multipurpose Internet Mail Extensions) với Security Multipats for MIME và MIME Object Security Services (MOSS); (3) S/MIME với Signed data, Enveloped data và Signed and Enveloped data; (4) PGP (Pretty Good Privacy); (5) X.400 Security; (6) MSP (Message Security Protocol)
- An toàn Web: Phần này trình bày 3 vấn đề là: (1) SSL; (2) S-HTTP và (3) Phần mềm có khả năng tải xuống. SSL cung cấp hàng loạt các dịch vụ an toàn cho các *client-server session*: Server authentication; Client authentication; Integrity và Confidentiality. SSL gồm có 2 giao thức nhỏ: SSL Record Protocol và SSL Handshake Protocol. S-HTTP được thiết kế như là một mở rộng an toàn cho HTTP, về bản chất nó là một giao thức *giao dịch yêu cầu-đáp ứng*. Các dịch vụ an toàn được S-HTTP cung cấp giống với các dịch vụ được SSL cung cấp. Các chương trình Java, được gọi là các applet, được tải xuống một cách tự động từ một máy chủ thông qua việc truy nhập vào các trang Web có sẵn, sau đó được các *browser* của các máy khách thông dịch và biểu diễn. Hệ thống ActiveX của Microsoft cũng có khả năng tải xuống. Các hệ thống dành cho việc xác thực nguồn của phần mềm có khả năng tải xuống cũng đã và đang được phát triển , ví dụ, hệ thống ***Authenticode*** của Microsoft.
- An toàn đối với các ứng dụng thương mại điện tử : trình bày 3 vấn đề là (1) An toàn EDI (Electronic Data Interchange); (2) Giao thức SET cho thanh toán thẻ ngân hàng và (3) Các mô hình thanh toán an toàn khác trên Internet (Cyber Cash, CheckFree, First Virtual, DigiCash, Mondex,...)
- Các thoả thuận của các nhà cung cấp dịch vụ Internet bao gồm: sử dụng và chấp nhận; các định nghĩa dịch vụ; sử dụng hợp pháp và kiểm soát của các nhà cung cấp dịch vụ đối với nội dung thông tin; chất lượng của thông tin; an toàn mật khẩu; sự lạm dụng; ...

Chương 2 „Nhu cầu thực tế về bảo mật “ đã đề cập tới các vấn đề: Tình hình phát phát triển của CNTT trên thế giới; Tình hình phát triển CNTT trong nước; Mô tả kết quả mạng của Bộ Tài chính (tuy rằng số liệu tương đối cũ). Có thể nói tóm lại, với sự triển khai của các đề án 112 và 47 thì nhu cầu bảo mật các dịch vụ mạng trong nước ta ở thời điểm này là rất lớn.

1.6 Quyển 5A : An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux. Chủ trì nhóm nghiên cứu: TS. Nguyễn Nam Hải, ThS. Đặng Hoà, TS. Trần Duy Lai

Báo cáo gồm có 3 phần: phần I dành cho Linux (các trang 1 –48), phần II dành cho Solaris (các trang 49-140) và phần III dành cho họ Microsoft Windows (các trang 141-167)

Phần I. An toàn của hệ điều hành Linux

Chương 1 „Linux Security“ được viết theo các tài liệu dạng HOWTO của Linux:

- Với phương pháp bảo vệ vật lý cũng có khá nhiều cái phải làm, đó là: khoá máy tính; dùng các lựa chọn của BIOS; bảo vệ trình Boot Loader là LILO (thông qua các tham số trong file lilo.conf); khoá màn hình bằng xlock và vlock.
- An toàn tài khoản truy nhập: Bảo vệ bằng cách phân quyền tối thiểu; tránh đăng nhập với tài khoản root hay su
- An toàn file và hệ thống file: thiết lập umask; phân biệt rõ owner/group/other; Các thuộc tính: read/write/Execute/Save/SUID/SGID
- An toàn mật khẩu: /etc/passwd và /etc/shadow
- Mã hoá: Linux hỗ trợ PGP, SLL, S-HTTP, S/MIME, IPSEC, ssh, stelnet, PAM, CIPE, Kerberos, CFS và TCFS
- An toàn giao diện đồ hoạ: khác với Microsoft Wimdows, Xwindow trong Linux chạy như một ứng dụng. Chính vì vậy mà có khá nhiều cái mất an toàn từ đó có thể. Những cái cần quan tâm tới gồm có X11, SVGA và GGI (Generic Graphic Interface).
- An toàn nhân: có nhiều tuỳ chọn khi dịch nhân có liên quan đến khả năng an ninh an toàn, ví dụ như CONFIG_FIREWALL; các thiết bị nhân như /dev/random hay /dev/urandom.
- An toàn mạng (có rất nhiều vấn đề): trình packet sniffer; file /etc/services; trình tcp_wrappers; trình inetd; an toàn NFS (network file system); ...

Chương 2 „Login và xác thực người dùng“ đã mô tả chi tiết về quá trình đăng nhập (từ khi dấu nhắc login cho tới khi xác thực xong và hệ thống đưa ra dấu nhắc shell), phương pháp xác thực người dùng cũng như cách quản lý người dùng trên hệ thống Linux:

- Trình bày lưu đồ của việc đăng nhập bằng trình getty và login
- Quản lý tài khoản và mật khẩu với file /etc/passwd và /etc/group. Hàm crypt() được sử dụng để mã mật khẩu (có dùng DES hay MD5 ở trong với tham số salt. Mật khẩu shadow là một cách tăng cường an ninh an toàn. Trong Linux có hỗ trợ công cụ Cracklib và Cracklib_dict để đánh giá độ mạnh của mật khẩu và nhắc nhở người dùng.
- PAM (Pluggable Authentication Modules) là các thư viện chia sẻ (shared libraries), cho phép người quản trị hệ thống lựa chọn cách xác thực người dùng. Nói cách khác, ta không phải biên dịch lại các ứng dụng sử dụng PAM (PAM-aware), và vẫn có thể chuyển đổi cách xác thực khác nhau. Linux PAM có 4 kiểu tác vụ (quản lý) độc lập là: quản lý xác thực (authentication), quản lý tài khoản (account), quản lý phiên (session), và quản lý mật khẩu (password). Tổ hợp các lược đồ quản lý và cách đối xử với một ứng dụng được thiết lập bởi các đề mục trong file cấu hình của Linux PAM. Cú pháp của các file cấu hình này đã được mô tả trong báo cáo (đó là file /etc/pam.conf hoặc một số file trong thư mục /etc/pam.d/). Trong báo cáo có nêu ra đến 33 modules khả dụng, đó là: pam_cracklib; pam_deny; pam_limits; pam_nologin;... Với mỗi module, trong báo cáo có đề cập đến các thông tin như: mô tả chức năng; cách dùng; thành phần xác thực; ....Cuối cùng có liệt kê các gói và thư viện mà PAM yêu cầu, đó là: ld-linux.so.2, libcrypt.so.1, ...

Phần II „An ninh của hệ điều hành Sun Solaris“

Chương 1 „Giới thiệu và đánh giá khả năng an toàn của Solaris“ đã trình bày về 4 mức bảo vệ trong Solaris:

(1) Điều khiển đăng nhập: xác nhận mật khẩu dùng file che; định thời gian có liệu lực, hạn chế số giờ truy nhập; không cho phép mật khẩu cũ; mật khẩu phải đủ dài; cấm sau nhiều lần bị từ chối; tự động khoá màn hình và ra khỏi mạng; bảo vệ truy nhập từ xa; chú ý đặc biệt đến root/su.

(2) Điều khiển truy nhập tài nguyên hệ thống: thiết lập và kiểm tra thực trạng an toàn; bảo vệ file; kiểm toán;

(3) Các dịch vụ phân tán an toàn và những nền tảng phát triển: có các dịch vụ xác thực, bí mật và toàn vẹn; PAM; GSS-API (General Security Services Application Programming Interface); có dịch vụ cấp phép ; các tiện ích an toàn từ xa (rcp, rsh, rlogin)

(4) Điều khiển truy nhập tới mạng vật lý: đề phòng từ bên trong và bên ngoài với Solstice Firewall-1 và Solstice Sunscreen.

Chương 2 „Quản lý hệ thống an toàn“ bao gồm 4 vấn đề:

(1) Cho phép truy nhập tới hệ thống máy tính: Duy trì an toàn cổng vật lý; Duy trì điều khiển đăng nhập; Hạn chế truy nhập tới dữ liệu trong các file; Duy trì điều khiển mạng; Kiểm soát việc sử dụng hệ thống; Đặt biến đường dẫn một cách đúng đắn; An toàn các file; Theo dõi việc đăng nhập của siêu người dùng (root); Cài đặt firewall; Sử dụng công cụ tăng cường an toàn tự động

(2) An toàn file: Các lệnh quản lý file; Mã hoá file; Các danh sách điều khiển truy nhập ACL.

(3) An toàn hệ thống: Những hạn chế đăng ký truy nhập; Các cách đăng nhập đặc biệt; Quản lý thông tin mật khẩu (file NIS, NIS+, /etc/passwd, /etc/shadow); Sử dụng Shell hạn chế; Theo dõi đăng nhập của superuser.

(4) An toàn mạng: Các hệ thống firewall; Xác thực và cấp phép; Chia xẻ các file; Hạn chế truy nhập của superuser; Sử dụng các cổng bí mật; Sử dụng ASET.

Chương 3 „Các tác vụ an toàn file“ đã mở đầu bằng việc trình bày về các tính năng an toàn file: các lớp người dùng; các quyền đối với file; các quyền đối với thư mục; các quyền đặc biệt; umask mặc định. Sau đó đã mô tả chi tiết các thao tác để: hiển thị thông tin về file; thay đổi quyền sở hữu file; thay đổi các quyền đối với file; kiểm soát các quyền đặc biệt; sử dụng các danh sách điều khiển truy nhập (ACL).

Chương 4 „Các tác vụ an toàn hệ thống“ đã chỉ dẫn từng bước để: hiển thị trạng thái đăng nhập của người dùng; hiển thị những người dùng không có mật khẩu; vô hiệu hoá tạm thời đăng nhập của người dùng; lưu lại những cuộc đăng nhập thất bại; tạo một mật khẩu quay số; vô hiệu hoá tạm thời các cuộc đăng nhập bằng quay số; hạn chế Superuser (root) đăng nhập tới thiết bị điều khiển; giám sát những người sử dụng lệnh su; hiển thị những lần thử truy nhập tới thiệt bị điều khiển của Superuser (root).

Chương 5 „Sử dụng các dịch vụ xác thực“ gồm các nội dung sau:

- RPC an toàn là cách thức xác thực xác nhận cả máy chủ và người dùng. RPC an toàn dùng xác thực hoặc Diffie-Hellman hoặc Kerberos. Cả hai cơ chế xác thực này dùng mã DES. Môi trường NFS dùng RPC an toàn và được hiểu như NFS an toàn. Cả hai kiểu xác thực Diffie-Hellman và Kerberos version 4 đều được hỗ trợ.
- Đối với xác thực Diffie-Hellman thì khoá công khai và bí mật được lưu trong CSDL NIS hoặc NIS+. Sau đây là các giao dịch trong một phiên clien-server có sử dụng AUTH_DH: sinh cặp khoá (bằng lệnh newkey hoặc nisaddcred); thực

hiện lệnh keylogin; sinh khoá giao tiếp; liên lạc lần đầu với server; giải mã khoá giao tiếp; lưu thông tin trên server; gửi trả nhãn xác minh cho client; client xác thực server.

- Kerberos tiến hành xác thực mật khẩu đăng nhập của người dùng. Người dùng đưa vào lệnh kinit để thu được thẻ đã phê chuẩn thời gian của phiên (hoặc 8 giờ, là thời gian phiên mặc định) từ server xác thực Kerberos. Khi người dùng logout, thẻ có thể bị huỷ (dùng lệnh kdestroy).
- PAM cung cấp cách thức để "tải vào" các dịch vụ xác thực và đảm bảo trợ giúp nhiều dịch vụ xác thực. PAM cho phép bạn "cắm thêm" công nghệ xác thực mới mà không cần thay đổi các dịch vụ hệ thống tiếp nhận như login, ftp, telnet và .....
  - Những lợi ích của việc dùng PAM: linh hoạt, dễ dùng, ...
  - 4 kiểu của PAM: xác thực; tài khoản; phiên; mật khẩu
  - PAM cung cấp một phương pháp xác thực người dùng nhiều dịch vụ bằng *stacking*. Phương pháp stacking có thể đòi hỏi một người dùng nhớ một vài mật khẩu. Với tính năng *ánh xạ mật khẩu*, mật khẩu chính được dùng để giải mã các mật khẩu khác, nên người dùng không cần nhớ hay đưa vào nhiều mật khẩu
  - Phần mềm PAM gồm có: thư viện PAM (/usr/bib/libpam); các modules; file cấu hình pam.conf
  - Các modules PAM: pam_unix; dial_auth;...
  - Thao tác với PAM gồm có: lập sơ đồ; cấm truy nhập trái phép từ xa bằng PAM; bổ sung PAM module; kích hoạt thông báo lỗi của PAM; ....

Chương 6 "Sử dụng công cụ tăng cường an toàn tự động" mô tả cách dùng công cụ tăng cường an toàn tự động (ASET- Automated Security Enhancement Tool) để giám sát hoặc hạn chế truy nhập tới các file hệ thống và các thư mục.

- ASET có 3 mức an toàn: an toàn thấp, an toàn trung bình và an toàn cao. Các file cơ bản của ASET: tune.low, tune.med, tune.high, uid_aliases, các file Checklist và file mô trường asetenv.
- ASET có cả thảy 7 tác vụ: Kiểm chứng các quyền đối với các file hệ thống; kiểm soát các file hệ thống; kiểm soát người dùng/nhóm; kiểm soát các file cấu hình hệ thống; kiểm tra môi trường; kiểm tra eeprom; thiết lập firewall. Thư mục /usr/aset/reports/latest chứa các báo cáo gần nhất cho từng tác vụ (tune.rpt, cklist.rpt, usrgrp.rpt,....).
- Cấu hình ASET bao gồm: thay đổi file môi trường asetenv; chọn các tác vụ để chạy (TASK); lập kế hoạch thực hiện(PERIODIC_SCHEDULE); đặc tả file bí danh (UID_ALIASES); kiểm tra mở rộng đối với NIS+ (YPCHECK); biến đổi các file điều chỉnh (tune.low, tune.med, tune. High); khôi phục các file hệ thống do ASET biến đổi
- Bạn cũng có thể dùng ASET trong môi trường phân tán NFS. Với tư cách người giám quản mạng, bạn có trách nhiệm cài đặt, chạy và quản lý các tác vụ quản trị đối với tất cả client của bạn.
- Các biến môi trường của ASET bao gồm: ASETDIR, ASETSECLEVEL , ...
- Có 2 cách chạy ASET: trực tuyến hoặc định kỳ
- ASET hỗ trợ việc sửa chữa các sự cố.

Phần III „An ninh của các hệ điều hành họ Microsoft Windows"

Chương 1 „Tổng quan" đã nhắc lại mô hình lập mạng trong môi trường Windows.

Mạng được hình thành gồm có hai phần chính: chủ (server) điều hành và cung cấp các dịch vụ, khách (client) nhận dịch vụ và chịu sự điều hành. Về cơ bản có hai mô hình lập mạng trong môi trường Windows: mô hình nhóm làm việc (workgroup model) và mô hình miền (domain model). Sau đó đã đánh giá khái quát về an ninh an toàn của hai môi trường là Windows9x vàWindowsNT. Đối với WinNT đã giới thiệu: cấu trúc hệ thống; khả năng bảo vệ nhờ thiết kế hướng đối tượng; các hệ con bảo mật của WinNT (bao gồm Local Security Authority; Logon Process; Security Account Manager; Security Reference Monitor; Directory database; Discretionary Access Controls)

Chương 2 „Đăng nhập, sử dụng dịch vụ“ đã đề cập đến vấn đề hết sức kinh điển, đó là mật khẩu. Cần phân biệt mật khẩu Windows 9x với mật khẩu WinNT. Mật khẩu WinNT có dùng DES làm hàm một chiều, còn Win2000 ngầm định sử dụng giao thức thẩm định quyền Kerberos v5. Có thể dùng các thiết bị bảo mật bên thứ ba (ví dụ như thẻ khoá) để cải thiện hệ bảo mật cho người sử dụng quay số vượt trên mức bảo mật sẵn có của các dịch vụ Windows NT RAS.

Chương 3 “Phân quyền đối với thư mục, tệp” đã trình bày về các hệ thống file có trong họ Windows, bao gồm: FAT, NTFS, CDFS, HPFS. Phân quyền đối với thư mục và tệp thực chất là bảo mật các tài nguyên mạng thông qua permission chia sẻ. Có 4 loại giấy phép, đó là: No access; Read; Change và Full Control.

Chương 4 „NTFS“ đã trình bày các tính năng của NTFS, đó là: hỗ trợ tên tệp dài; hỗ trợ nén tệp,.. Đối với tệp NTFS có 4 loại quyền: No Access, Read, Change và Full Conttrol. Đối với thư mục NTFS có 8 loại quyền: No Access, List, Read, Add, Add&Read, Change, Full Control, Special File Access. Cần chú ý phân biệt permission của cá nhân và của nhóm, permission cục bộ và trên mạng, permission chia sẻ và NTFS. Win2000 còn hỗ trợ mã hoá tệp với EFS.

1.7 Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network hacker, Virut máy tính. Chủ trì nhóm nghiên cứu: TS. Đặng Vũ Sơn

Báo cáo gồm có 3 phần. Phần I „Khả năng an toàn của các hệ điều hành mạng“ gồm có 3 mục và Phụ lục. Phần II „Network hacker“ có 5 mục và Phụ lục. Phần III „Virút máy tính“ có 5 mục và Phụ lục.

Phần I „Khả năng an toàn của các hệ điều hành mạng“ .

Mục 1 „Tổng quan về hệ điều hành“ :

- Hệ điều hành là gì? Hệ điều hành là một chương trình quản lý tài nguyên (bộ xử lý, bộ nhớ, I/O, thiết bị lưu trữ và các thiết bị khác, đa thành phần (tạo ra nhiều bản copy) và chuyển đổi (làm cho dễ sử dụng hơn) các tài nguyên phần cứng. Hệ điều hành cũng là chương trình quản lý máy tính ảo mà cung cấp các máy tính ảo với các tiến trình (processes) chạy trên đó.
- Phân loại hệ điều hành: đơn/đa chương trình; phân chia thời gian/thời gian thực; tập trung/phân tán.
- Lịch sử phát triển của hệ điều hành
- Căn cứ vào 6 yêu cầu chuẩn tắc đánh gia hệ thống máy tính tin cậy, Bộ Quốc phòng Mỹ đưa ra 4 cấp đánh giá: D, C (có C1 và C2), B (có B1, B2 và B3), A (có A và A1).

Mục 2 „Cơ chế an toàn của hệ điều hành“ trình bày 3 vấn đề an toàn chung đối với các tất cả các hệ điều hành mạng:

- An toàn truy nhập mạng: bao gồm Xác định tính chân thực của người dùng; Xác định trạm làm việc mà người dùng được phép truy nhập vào mạng từ đó;Xác định người lạ mặt; Ngày mãn hạn của khoản mục người dùng;... Đặc biệt, đã bình luận về cách kiểm tra mật khẩu của WinNT, Novell Netware và Unix
- An toàn hệ thống: Các thao tác đối với tài khoản (tạo/xóa người dùng/nhóm, ...); Các thao tác đối với thiết bị (tắt máy, dùng máy in, backup dữ liệu,...)
- An toàn file và thư mục: quyền truy nhập cục bộ; quyền truy nhập từ xa. Có phân tích kỹ đối với Win2000.

Mục 3 „Các lỗ hổng an toàn“ đã nêu ra :

- Đối với hệ điều hành Windows nêu ra một số lỗi gây ra do Internet Information Services; Dịch vụ dữ liệu từ xa (Remote Data Services); SQL Server; NETBIOS; Anonymous Logon; LAN Manager Authentication; General Windows Authentication; IE; Remote Registry Access; Windows Scripting Host
- Đối với hệ điều hành Unix nêu ra một số lỗi gây ra bởi Remote Procedure Calls; Apache Web Server; Secure Shell; SNMP; FTP; R-sevices Trust Relationship; Line Printer Daemon; Sendmail; BIND/DNS; General Unix Authentication
- Các lỗ hổng có thể đến từ: (1) hệ điều hành và các ứng dụng; (2) do người sử dụng; (3) do người lập trình. Trong tài liệu có nêu chi tiết nhiều trường hợp cụ thể thuộc 3 kiểu trên.
- Một số hệ điều hành có lỗ hổng về mật mã (ví dụ như FTP daemon của Unix)

Phụ lục có giới thiệu Nessus là một phần mềm giám sát an ninh mạng. Đã giới thiệu cách cài đặt, cấu hình, chạy khai thác chương trình kèm theo file nhật ký kết quả chạy trình.

Phần II „Network hacker“

Mục 1 „Hacker là ai“ đã phân ra black hat và white hat, hacher thường dân, hacker chính trị, hacker là người trong cuộc và hacker là tội phạm có tổ chức.

Mục 2 „Hacker hack như thế nào“ đã nêu ra qui trình 9 bước để hack, đó là: FootPrinting, Scanning, Enumeration, Gaining Access, Escalating Priviliges, Pilfering, Covering Tracks, Creating „Back Doors“, Denial of Services. Hacker hoạt động hiểu quả là do: cấu hình sai máy chủ, lỗi trong các ứng dụng, nhà cung cấp thiếu trách nhiệm, thiếu người có trình độ.

Mục 3 „Những lỗi của hệ điều hành mà hacker có thể khai thác“ đã liệt kê ra: lỗi tràn bộ đệm, gói IP bị chặn bắt và bị phân tích (bằng Sniffer chẳng hạn), mật khẩu yếu, ... Cuối mục có đưa ra một ví dụ thực hiện tấn công hệ thống Unix: thu thập thông tin về mục tiêu; khai thác FTP, TFTP bug; khai thác các dịch vụ khác như RPC, NIS; khai thác Sendmail; crack unix password file; khai thác lỗ hổng WU-FTP Server.

Mục 4 „Mật mã và các vấn đề liên quan đến hacker“ đặt ra câu hỏi là: có thể sử dụng mật mã để chống hacker hay không? Mật mã có thể dùng vào 2 việc: bảo vệ mật khẩu và mã dữ liệu được lưu trữ.

Mục 5 „Phòng chống hacker“ đã nêu ra 3 nguyên nhân khiến người ta quan tâm tới việc bảo vệ thông tin trên Internet, đó là: bảo vệ dữ liệu, bảo vệ tài nguyên mạng,

bảo vệ danh tiếng của cơ quan. Đã nêu ra một hướng dẫn bảo mật cho hệ thống gồm 6 bước: (1) thành lập bộ phận chuyên trách về vấn đề bảo mật; (2) thu thập thông tin; (3) thẩm định tính rủi ro của hệ thống; (4)xây dựng giải pháp (dùng firewall, IDS, VPN, sinh trắc học, smart card,...); (5) thực hiện và giáo dục; (6) tiếp tục kiểm tra, phân tích và thực hiện.

Phụ lục giới thiệu phần mềm giám sát an ninh mạng SNORT. Đây là một Network IDS. Nó có các chế độ làm việc sau: Sniffer mode, Packet Logger mode, Network Intrusion Detection Mode. SNORT sử dụng một ngôn ngữ đơn giản và dễ hiểu để mô tả các rule, gồm có từ khoá Include, các Variables, từ khoá Config với các directives. Một rule gồm có rule header và rule options. Rule header lại gồm có rule actions (có thể là alert, log, pass, activate và dynamic), protocol (TCP, UDP, ICMP), IP address, cổng dịch vụ và toán tử định hướng. Phần cuối có nêu kết quả thực nghiệm khảo sát mạng bằng SNORT.

Phần III „Virut máy tính“

Mục 1 „Tổng quan về virus máy tính“ đã dành phần đầu để trả lời câu hỏi „virus máy tính là gì“. Tiếp theo là phân loại virus: theo đối tượng lây nhiễm (B-virus và F-virus), theo phương pháp lây nhiễm, theo mực độ phá hoại, theo họ virus. Virus cũng có tên gọi khác là trojan horse hay worm.

Mục 2 „B-virus“ đã nêu cơ chế lây lan của B-virus. B-virus có thể chia ra Single B-Virus và Doublr B-Virus. Một B-virus gồm có phần install và phần thân (gồm 4 phần nhỏ là phần lây lan, phần phá hoại, phần dữ liệu và phần Boot record). Các đặc tính của một B-virus gồm có: tính tồn tại duy nhất (trên đĩa/trong vùng nhớ); tính thường trú; tính lây lan; tính phá hoại (định thời/ngẫu nhiên và liên tục); tính gây nhiễm và nguỵ trang; tính tương thích. Phần cuối mục có phân tích kỹ thuật các đặc tính trên, ngoài ra còn có: kỹ thuật định vị chương trình; kỹ thuật đa hình; kỹ thuật biến hình; kỹ thuật chống mô phỏng; kỹ thuật chống theo dõi; kỹ thuật đường hầm-cửa hậu; kỹ thuật anti-tunnel.

Mục 3 „F-virus“ đã xét đến 2 môi trường là DOS và Win32. Đối với các virus trên DOS đã đề cập đến: phương pháp lây lan; phân loại thành 2 loại (Transient File Virus và Resident File Virus); Cấu trúc của TF-virus gồm 3 phần: lây lan, phá hoại, buffer. Cấu trúc của RF-virus gồm 4 phần: install, lây, phá, buffer. Cũng như B-virus, một F-virus có các yêu cầu: tính tồn tại duy nhất (trong vùng nhớ, trên file), tính lây lan (định vị trên file, tìm file đối tượng), tính phá hoại (với TF-virus, với RF-virus), tính thường trú (trước khi trả quyền điều khiển, sau khi đoạt lại quyền điều khiển), tính kế thừa. Sau đó, báo cáo có phân tích kỹ thuật đối với các đặc tính vừa nêu cùng với kỹ thuật gây nhiễu và nguỵ trang, kỹ thuật lấy ngắt. Đối với F-virus trên Win32 đã phân tích về các rings của môi trường hoạt động Windows và các kỹ thuật như: lây nhiễm, kiểm tra sự tồn tại, sử dụng Structured Exception Handling, định vị, công nghệ thường trú, tìm kiếm file đối tượng, tạo áo giáp, nguỵ trang, chống mô phỏng.

Mục 4 „Phân tích kỹ thuật virus trên mạng“ đã đề cập tới mạng LAN và Internet. Một số câu hỏi đã được bàn luận là: thế nào là trojan? Bị nhiễm trojan như thế nào? Trojan nguy hiểm như thế nào? Trojan hoạt động như thế nào? Trojan có những loại gì? Dùng chương trình nào để chống lại?

Mục 5 „Mật mã và virus“ đề cập đến một chủ đề khó, liệu có thể dùng mật mã để phát hiện và phòng chống virus hay không? Đối với B-virus thì mật mã không phòng chống được, còn đối với F-virus thì có thể phòng chống bằng cách đổi tên file. Có thể dùng chữ ký số để phát hiện file bị virus. Cách thức phòng chống virut được ghép vào cuối mục này (nếu đưa thành mục riêng thì hay hơn)

Phụ lục là một danh sách các loại virus tiêu biểu cùng với mô tả của chúng: Nimda, Code Red, Chernobyl,...

2. Nhóm thứ hai: Các sản phẩm bảo mật gói IP trên các môi trường Linux, Solaris và Windows

2.1 Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux. Chủ trì nhóm nghiên cứu: TS. Trần Duy Lai

Báo cáo gồm 2 phần. Phần I có tên là „Lập trình mạng trong Linux“ có 2 chương. Chương 1 là „Mạng IP trong Linux“ và chương 2 là „Lập trình mạng trong Linux“. Phần II „Các sản phẩm bảo mật gói IP“ có 4 mục. Ba mục A, B và C trình bày về 3 phần mềm TRANSCRIPT, IP-CRYPTO và DL-CRYPTO. Mỗi mục A, B và C đều có 2 chương, chương đầu giới thiệu về giải pháp và chương thứ hai giới thiệu về sản phẩm phần mềm. Riêng mục thứ tư là mục D có 2 chương trình bày về giải pháp mật mã bao gồm : mã dữ liệu bằng mã khối và trao đổi khoá tự động.

Phần I „Lập trình mạng trong Linux“

Chương 1 „Mạng IP trong Linux“ đã đề cập đến các nội dung sau:

- Chồng giao thức (protocol stack) là một phần trong kernel code, nó gồm có SOCKET layer, INET layer, TCP/UDP layer, IP layer, Network device layer.
- Cấu trúc của socket buffer gồm: sk, stamp, dev, h,.... Các lệnh làm việc với sk_buff bao gồm: skb_dequeue(), skb_queue_head(), ...
- File /proc/net/route chứa Forwarding Information Base.
- Trình bày tổng quát về quá trình khởi tạo mạng khi hệ điều hành khởi động, cách sử dụng trình ifconfig và route để thiết lập kết nối mạng, các thủ tục có liên quan(devinet_ipctl(), ifconfig_main(), INET_rprint(),....)
- Trình bày về quá trình kết nối (connection): cấu trúc của socket; socket và định tuyến; quá trình kết nối gồm gethostbyname(), socket(), connect(), close().
- Các bước để gửi dữ liệu gồm: ghi dữ liệu vào socket; tạo một gói UDP/TCP; bọc gói trong IP; truyền một gói.
- Các bước để nhận dữ liệu: đọc dữ liệu từ socket; nhận một gói; chạy „bottom half“; huỷ bọc gói trong IP; chấp nhận gói UDP/TCP; đọc từ socket phần 2
- Các bước của IP Forwarding: nhận một gói; chạy „bottom half“; kiểm tra gói trong IP; chuyển gói trong IP; truyền một gói
- Internet Routing Protocol: Neighbor Table; Forwarding Information Base và Routing Cache; các cấu trúc fn_zone (network zone), fib_node (network node information), fib_info (network protocol information), rtable (routing table entry), dst_entry (destination cache), neighbor (neighbor link)

Chương 2 „Lập trình mạng trong Linux“ : Hệ điều hành Linux áp dụng chuẩn công nghiệp Berkeley socket API, socket này có nguồn gốc trong sự phát triển BSD Unix (4.2/4.3/4.4 BSD). Trong chương này đã xem xét cách để quản lý bộ nhớ và bộ đệm

đã được cài đặt trong tầng mạng và trong các trình điều khiển thiết bị của nhân Linux.

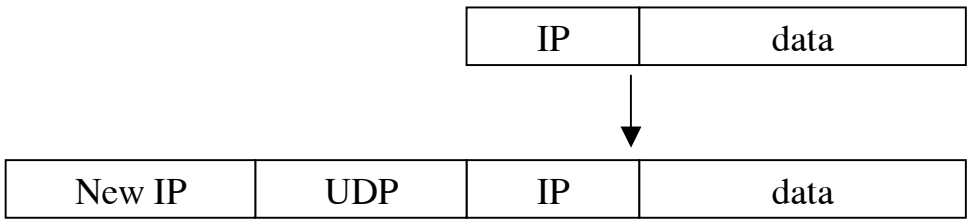
- Trình bày chi tiết về sk_buffs, đây là một danh sách liên kết 2 chiều.
- Các thủ tục hỗ trợ mức cao hơn là sock_queue_rcv_skb() và sock_alloc_send_skb()
- Thiết bị mạng: đặt tên cho thiết bị; đăng ký một thiết bị; các hàm dev_queue_xmit() và netif_rx(); cấu trúc của thiết bị gồm có tên, các tham số giao diện bus (địa chỉ và ngắt), các biến tầng giao thức, các biến tầng liên kết, các cờ; hàng đợi. Các hàm (methods) của thiết bị mạng gồm: setup; truyền (dev→hard_start_xmit()); Frame Headers (dev→hard_header); nhận (dev_alloc_skb()). Ngoài ra, còn trình bày về Activation, Shutdown, Configuration và Statistics của thiết bị mạng.
- Trong chương này cũng có đề cập đến IP-multicasting và các thủ tục hỗ trợ Ethernet là eth_header(), eth_rebuild_header(), eth_type_trans(), eth_copy_and_sum()

Nghiên cứu kỹ, nắm chắc cách xử lý gói tin mạng trong Linux *là nhân tố quyết định* để có thể thực hiện thành công các giải pháp can thiệp mật mã nhằm bảo mật gói tin được truyền trên mạng.

Phần II „Các sản phẩm bảo mật gói IP“

A. Phần mềm TRANSCRYPT

Chương 1 „Giải pháp Transcrypt“ : Transcrypt dựa trên phần mềm CIPE (Crypto IP Encapsulation). Các công việc đã được làm là: khai thác làm chủ hoạt động của hệ thống và thay đổi phần mật mã (bao gồm thuật toán mã dữ liệu và toàn bộ phần trao đổi khoá). Transcrypt “bao bọc” các gói tin IP (đã được mã hoá) bởi các gói tin UDP và gửi chúng bằng kỹ thuật UDP thông thường. Đây là sự khác biệt với việc bao bọc IP trong IP. Trong báo cáo đã trình bày về việc mã hoá gói tin và trình trao đổi khoá Kex.



Chương 2 „Phần mềm Transcrypt“ đã trình bày về mã nguồn của Transcrypt, cách biên dịch và cài đặt, cách thiết lập cấu hình và cách chạy chương trình (gồm các bước nạp module và chạy chương trình daemon transcryptd. Trong báo cáo cũng trình bày các tuỳ chọn để cấu hình phần mềm. Transcrypt hỗ trợ nạp khoá bằng 2 cách: kết nối bằng khoá bí mật trao đổi trước hoặc trao đổi khoá phiên tự động bằng trình Kex.

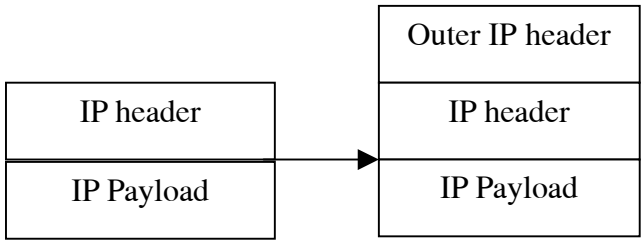
B. Phần mềm IP-CRYPTO

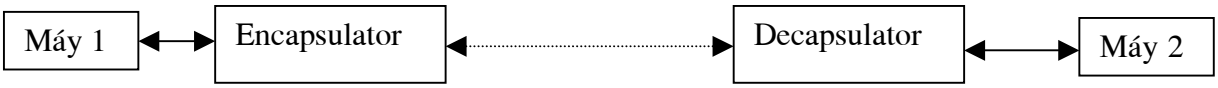
Phần mềm IP-CRYPTO phỏng theo FreeS/WAN nhưng chỉ hỗ trợ một mode tunnel

với những thuật toán mật mã được thay thế (mã dữ liệu và trao đổi khoá).

Chương 1 „Giải pháp bảo mật của IP-CRYPTO“ đã đề cập đến:

- Kỹ thuật tạo card mạng ảo và cách gửi gói tin qua card mạng ảo
- Cách nhận gói tin mạng trong nhân Linux
- Chế độ đường hầm (tunnel mode), Encapsulating Security Payload Packet Format (với các trường Connetion Identifier Index, Sequence Number,...)
- Phân tích chương trình nguồn của quá trình gửi và nhận gói tin trong IP-Crypto





Chương 2 „Phần mềm IP-Crypto“ đã trình bày về mã nguồn và bộ cài đặt của IP-Crypto; cách biên dịch và cài đặt nó; cách thiết lập cấu hình (gồm có cấu hình mạng, trao đổi khoá thủ công, trao đổi khoá tự động, sử dụng trình keyingd); mô hình chạy thử nghiệm.

C. Phần mềm DL-CRYPTOR

Chương 1 „Bảo mật ở tầng DataLink“ trình bày về giải pháp can thiệp mật mã. Cấu trúc gói tin MAC (Medium Access Control) với các phần Preamble, Header và CRC được trình bày. Trong nhân linux việc gửi và nhận gói tin mạng được chứa trong cấu trúc chứa gói tin struct sk_buff. Mọi xử lý ở các tầng khác nhau đều xử lý trên cấu trúc này. Ta thấy trong nhân linux việc gửi và nhận gói tin ở tầng data link được thực hiện nhờ hai hàm là dev_queue_xmit() trong trường hợp gửi gói tin đi và net_bh() trong trường hợp nhận gói tin. Hàm dev_queue_xmit() sẽ chuyển dữ liệu vào hàng đợi cho giao diện vật lý gửi gói tin đi. Mặt khác hàm net_bh() sẽ lấy gói tin do giao diện vật lý nhận được đưa vào bộ đệm hàng đợi để chuyển lên cho các giao thức ở trên xử lý. Vì vậy chúng ta thấy để can thiệp mật mã vào tầng data link thì giải pháp can thiệp vào hai hàm này là phương pháp tối ưu nhất. *Khi gói tin được truyền đi, hàm dev_queue_xmit() sẽ thực hiện việc mã hoá và sang bên nhận hàm net_bh() sẽ thực hiện việc giải mã*. Như vậy, đối với các giao thức mạng ở tầng cao hơn (ví dụ, giao thức tầng mạng IP) ở hai máy là trong suốt.

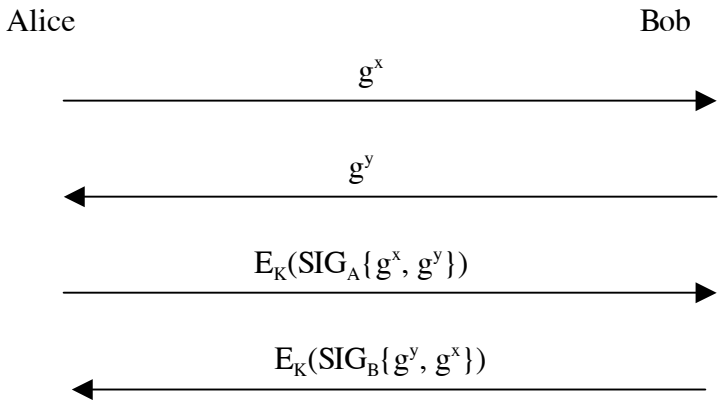
Chương 2 „Phần mềm DL-Cryptor“ đã trình bày về mã nguồn của DL-Cryptor, cách biên dịch và cài đặt, cách thiết lập cấu hình và 2 chế độ làm việc của DL-Cryptor (trao đổi khoá thủ công và tự động).

D. Giải pháp mật mã

Chương 1 „Mã dữ liệu bằng mã khối“ đã trình bày về 2 chế độ làm việc của mã khối

được dùng đến trong khi mã gói IP là OFB (Output Feedback Mode) và CBC(Cipher Block Chaining Mode).

Chương 2 „Trao đổi khoá tự động“ đã trình bày về giao thức trao đổi khoá STS (Station-To-Station), nó có ưu điểm là chống lại được tấn công người đứng giữa. Giao thức STS đã được cải tiến để trở thành giao thức STS đối xứng như sau:



Trong chương này đã trình bày về việc lập trình giao thức STS đối xứng để được trình trao đổi khoá Kex, cách sử dụng trình Kex và đặc biệt là việc dùng trình trao đổi khoá đi kèm với 3 phần mềm bảo mật là Transcrypt, IP-Crypto và DL-Cryptor.

2.2 Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris. Chủ trì nhóm nghiên cứu: TS. Đặng Vũ Sơn

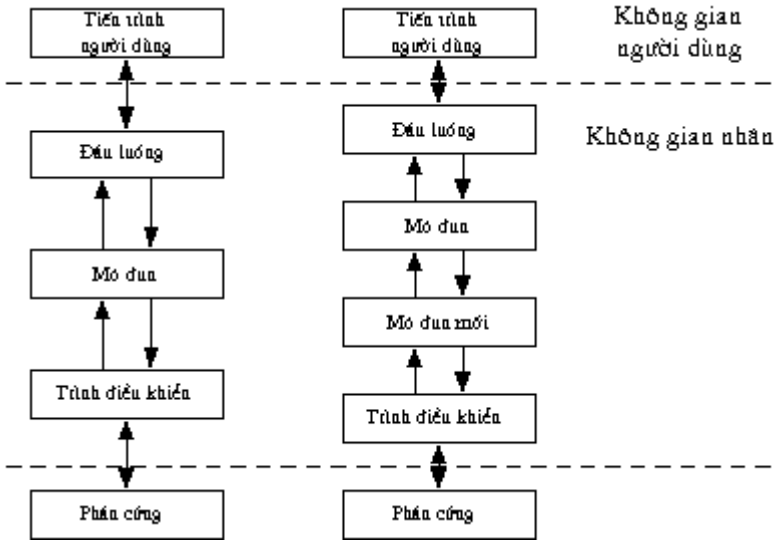
Đây là một giải pháp bảo mật đã được nghiên cứu trong Ban Cơ yếu. Do đầu tư của đề tài KC.01.01, kết quả này đã được hoàn thiện, đặc biệt là nội dung của chương 4 đã được thực hiện thêm. Tuy vậy, về mặt tài liệu thì báo cáo vẫn được viết thành 4 chương, trong đó 3 chương đầu nhằm giới thiệu cách tiếp cận dùng công nghệ lập trình STREAMS để can thiệp mật mã vào Solaris.

Chương 1 „Khái quát chung về giải pháp bảo vệ gói IP bằng kỹ thuật mật mã“ thực sự là một bài tổng quan về công nghệ IPSEC. Nhóm nghiên cứu đã phân tích khả năng bảo vệ thông tin khi can thiệp mật mã vào mỗi tầng của giao thức TCP/IP, đánh giá ưu nhược điểm của giải pháp can thiệp mật mã vào tầng IP. Phân tích cơ chế truyền dữ liệu của giao thức TCP/IP, các dịch vụ bảo vệ gói IP bằng kỹ thuật mật mã. Từ đó đưa ra mô hình chức năng của hệ thống bảo vệ gói IP bằng kỹ thuật mật mã.

Chương 2 „Cơ chế quản lý dữ liệu của giao thức TCP/IP trên Solaris“ thực chất là trình bày về *giải pháp, cách tiếp cận, phương pháp nghiên cứu* :

- STREAMS là phần bổ xung mới đây tới kiến trúc của nhân (kernel) UNIX.. STREAMS được thiết kế để giải quyết một vài hạn chế của mô hình SOCKET, đặc biệt trong lĩnh vực mạng và truyền thông. Cốt lõi của mô hình STREAMS là nó được cài đặt giống như chồng giao thức. Một chồng STREAMS hay còn gọi là một *luồng* (stream) bao gồm một trình điều khiển luồng ở đáy (STREAMS driver) để điều khiển giao diện với phần cứng, không có hoặc có một số mô đun (STREAMS module) tương ứng các mức giao thức khác nhau và một đầu luồng (stream head) điều khiển giao diện giữa luồng và tiến trình người dùng (user process).

- Các thành phần của luồng gồm: các hàng đợi (queue); các thông báo (message); các module; các trình điều khiển (driver).
- Các thao tác trên luồng gồm: open, read, write, close, ioctl, getmsg, getpmsg, putmsg, putpmsg, poll, pipe
- Việc xây dựng luồng gồm có: mở một file thiết bị STREAMS; thêm và huỷ các module; đóng một luồng.
- Các trình xử lý luồng gồm có: put và service
- Các thông báo là phương tiện truyền thông trong luồng. Các thông báo thông thường: M_BREAK, M_CTL, M_DATA,... Tất cả các thông báo được tạo bởi một hoặc nhiều khối thông báo. Một khối thông báo là một danh sách liên kết của các bộ ba (triples), mỗi bộ bao gồm hai cấu trúc (một khối thông báo (msgb) và một khối dữ liệu (datab) và một vùng nhớ đệm. Trong báo cáo đã đề cập đến: việc gửi và nhận thông báo; cấu trúc hàng đợi; việc xử lý các thông báo; giao diện dịch vụ và một số cấu trúc dữ liệu được dùng trong luồng (Streamtab, queue, qint, module_info, msgb, datab)
- Trong STREAMS các trình điều khiển được mở (opened) và các mô đun được chèn vào (pushed). Có ba kiểu của trình điều khiển thiết bị:Trình điều khiển phần cứng (Hardware Driver); Trình điều khiển ảo (Pseudo Driver); Trình điều khiển đa luồng (Multiplexer Driver). Trong báo cáo đi sâu vào việc xây dựng đa luồng STREAMS TCP/IP.



Mô hình STREAMS

Chương 3 „Giải pháp bảo vệ dữ liệu trong nhân hệ điều hành Solaris“ đã trình bày giải pháp bắt gói IP để thực hiện việc mã hoá trong mô hình STREAMS TCP/IP là xây dựng và chèn tầng lọc gói IPF thêm vào. Cơ chế mã hoá là: Gói IP được sinh ra bởi các ứng dụng trên mạng Lan được truyền theo cáp mạng đến giao diện elx1 của “nút mã hoá” của mạng LAN và được chứa trong hàng đợi đọc của giao diện elx1. Tiếp đó gói IP lần lượt được chuyển lên hàng đợi đọc của tầng IPF và hàng đợi đọc của tầng IP. Tại đây địa chỉ đích của gói IP được sử dụng để hệ thống quyết định đường đi tiếp theo nhờ vào các lệnh route. Gói IP được chuyển sang hàng đợi viết của tầng IP, sau đó được chuyển xuống hàng đợi viết của tầng IPF. Tại hàng đợi viết của tầng IPF, phân đoạn TCP (TCP segment) được mã hoá và được chuyển tiếp xuống hàng đợi viết của giao diện elx0 và được chuyển theo lên mạng để đi tiếp. Để tiết kiệm về mặt thiết bị, chúng ta nên tích hợp nút mã hoá với Router lọc gói.

Chương 4 „Khảo sát khả năng chống lại các phần mềm hacker và tốc độ truyền dữ liệu của hệ thống bảo vệ gói IP trên Solaris“ đã khảo sát khả năng ngăn chặn của một số phần mềm hacker của bộ phần mềm IPSEC_SUN, đó là: Sniffit V.0.3.5, IPSCAN, Packetboy, ICMP_Bomber. Hơn thế nữa, những khả năng này của bộ phần

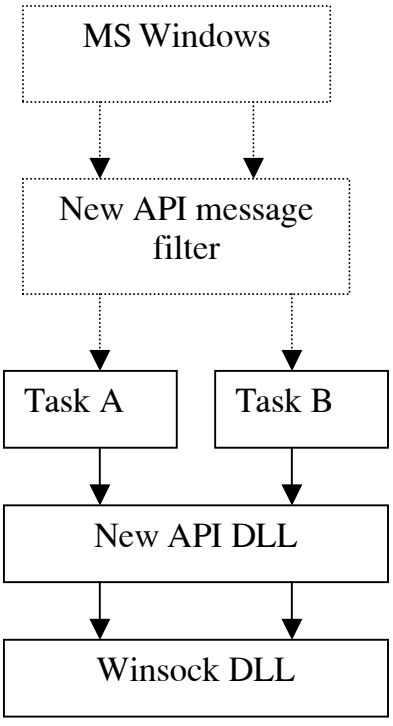
mềm IPSEC_SUN còn được so sánh với bộ phần mềm IPSEC trên Linux là FreeS/WAN. Bên cạnh đó, nhóm nghiên cứu cũng khảo sát ảnh hưởng của bộ phần mềm IPSEC_SUN đối với thời gian truyền dữ liệu của dịch vụ FTP và so sánh với FreeS/WAN.

2.3 Quyển 4C: Phần mềm bảo mật trên môi trường Windows. Chủ trì nhóm nghiên cứu: TS Nguyễn Nam Hải

Trong điều kiện của nước ta là một nước phụ thuộc hoàn toàn vào công nghệ nhập ngoại thì vấn đề an toàn cũng cần phải được nghiên cứu sao cho phù hợp với hoàn cảnh của chúng ta. Làm thế nào vừa tận dụng được sức mạnh của các hệ thống phần mềm thương mại hiện nay nhưng vẫn kiểm soát được mức độ an toàn của thông tin trên mạng là một trong những vấn đề đáng được quan tâm.

Nội dung nghiên cứu phần này nhằm mục đích nghiên cứu xây dựng giải pháp bảo vệ thông tin trên các mạng máy tính được xây dựng trên nền tảng mô hình mạng Winsock. Mô hình mạng Winsock là một mô hình mạng được phát triển mạnh mẽ sử dụng rộng rãi ngày nay. Do vậy định hướng nghiên cứu vào mô hình này là cần thiết và có ý nghĩa thực tiễn.

Giải pháp và kỹ thuật được sử dụng: Toàn bộ dòng thông tin trên mạng trong các Platform Windows đều chuyển qua Winsock. Vấn đề đặt ra là làm thế nào để có thể khống chế được dòng thông tin này để phục vụ cho các mục tiêu riêng biệt. Can thiệp trực tiếp vào các Modul trong Winsock là một việc làm khó có thể thực hiện được bởi đối với những người phát triển ứng dụng thì Winsock chỉ như một chiếc hộp đen. Chúng ta chỉ có thể biết được giao diện với Winsock mà thôi. Vậy cách tiếp cận là như thế nào. Chúng tôi tiếp cận theo kiểu xây dựng một API mới trên Windows Socket API. Dòng thông tin trước khi chuyển qua Winsock sẽ qua một tầng mới do ta xây dựng và ở tầng này chúng ta có thể khống chế được dòng thông tin mạng.



Khi xây dựng một tầng mới trên tầng Winsock có nhiều kỹ thuật phải giải quyết. Một trong những kỹ thuật cần phải quan tâm đó là xử lý các message được gửi từ Winsock cho ứng dụng. Nếu không chặn được dòng message này thì không thể điều khiển được quá trình truyền thông giữa ứng dụng tại client và phần ứng dụng tại server. Chẳng hạn khi ta chèn thêm một packet vào dòng packet của ứng dụng. Nếu ta không xử lý được các message gửi từ Winsock cho ứng dụng thì hầu như chắc chắn connection giữa client và server sẽ bị huỷ bỏ và quá trình trao đổi thông tin giữa client và server sẽ bị huỷ giữa chừng. Kỹ thuật được chọn xử lý ở đây là sử dụng kỹ thuật subclass. Mục tiêu chính của nó là chặn toàn bộ các message gửi từ Winsock cho ứng dụng, xử lý những message cần thiết và trả lại những message của ứng dụng cho ứng dụng xử lý.

Chương I „Mô hình Winsock“ đã dành phần đầu để trình bày về 3 thành tố của mô hình mạng Winsock,

đó là: (1) Winsock application: cung cấp những chức năng của các tầng 5, 6, 7 trong mô hình OSI. Nó là một chương trình ứng dụng cùng với giao diện người dùng, nó cũng có thể là một thư viện động DLL trung gian cùng với API mức cao hơn và các ứng dụng của nó. Trong mô hình Winsock ta xem một ứng dụng bất kỳ mà truy nhập Winsock DLL như là một ứng dụng của Winsock; (2) Network system: cung cấp các chức năng của các tầng 1, 2, 3, 4 trong mô hình OSI; (3) Winsock API: nằm giữa 2 tầng trên, cung cấp truy nhập tới cả network system và các ứng dụng của Winsock sử dụng các dịch vụ của hệ thống để gửi và nhận thông tin. Một liên kết giữa Client và Server trong mô hình Winsock gồm 5 thành phần: Giao thức, địa chỉ IP của Client, số hiệu cổng của Client, địa chỉ IP của Server, số hiệu cổng của Server. Socket có trạng thái, trạng thái hiện thời của socket xác định các phép toán mạng nào sẽ được tiếp tục, các phép toán nào sẽ bị treo lại và những phép toán mạng nào sẽ bị huỷ. Có hai kiểu socket: Datagram Socket và Stream socket. Mỗi kiểu socket có những trạng thái và những phép chuyển khác nhau.

Chương II „Xây dựng socket an toàn“ mô tả cấu trúc của Secure Socket, cách thức làm việc và lợi ích đối với môi trường truyền thông từ xa. Nhóm nghiên cứu phát triển giao diện tại tầng giao vận cho truyền thông TCP/IP được gọi là Secure Socket để phục vụ cho mục tiêu nén và mã hoá dữ liệu truyền qua Internet và các mạng PSTN.Secure Socket được cài đặt tại các trạm, Server và trong FireWall để đảm bảo an toàn và truyền thông tốc độ cao giữa trạm và các máy trạm. Secure Socket cung cấp giao diện lập trình ứng dụng Winsock chuẩn cho các ứng dụng TCP/IP chẳng hạn như Web Browser, telnet, ftp mà không bất kỳ sự thay đổi nào đối với các trình ứng dụng và TCP/IP. Các yêu cầu được đặt ra khi thiết kế là: khả năng thích nghi; trong suốt; có khả năng mở rộng; dễ cài đặt và hiệu quả. Secure socket bao gồm thư viện liên kết động tầng giao vận. Nó được đặt giữa các chương trình ứng dụng và TCP/IP, các trình tiện dụng tương tác với người dùng. Tại các PC client thì Winsock là giao diện lập trình ứng dụng chuẩn cho TCP/IP. Chúng ta có thể thực hiện nén, mã hoá và xác thực dữ liệu mà không cần thay đổi phần mềm ứng dụng hoặc TCP/IP.

- Có một vài cách để chặn các lệnh của Winsock : Thay thế các địa chỉ hàm; Thay đổi thông tin liên kết; Đổi tên thư viện Winsock. Nhóm đề tài đã chọn cách thứ 3 để thực hiện.
- Khi sử dụng các hàm của Winsock, có hai dạng thao tác: Dạng đồng bộ và dạng dị bộ. Nhóm nghiên cứu đã chọn thao tác kiểu dị bộ, sử dụng hàm Winsock WSAAsynselect (hàm này được dùng để đăng ký hàm của Windows) để nhận thông báo và thay đổi Mode về dị bộ. Secure Socket chặn WSAAsynselect và thay thế tham số “Windows handle” của nó bằng “Windows handle” của Secure socket. Sau đó phát lại lệnh tới Winsock.Dll. Hàm send() ở dạng dị bộ hàm cần chặn và xử lý.

Trong chương III có mô tả lại thuật toán mã khối IDEA được dùng để mã dữ liệu. Phần phụ lục trình bày trình bầy những modul cơ bản phục vụ cho thử nghiệm tư tưởng thiết kế đã trình bầy trong phần trước. Chương trình thử nghiệm gồm các phần cơ bản sau: Các mô đun thuộc socket được thiết kế lại; Các mô đun phục vụ cho mã hoá nội dung các gói dữ liệu; Các mô đun phục vụ cho việc xác thực nội dung các gói dữ liệu; Các mô đun phục vụ cho việc tạo khoá phiên. Những kỹ thuật mật mã trình bầy trong phần này chỉ nhằm mục đích khẳng định những ý tưởng thiết kế trong phần trước là hoàn toàn khả thi. Các giao thức hội thoại giữa client và server được thiết kế để nhằm khẳng định nhóm nghiên cứu có thể chủ động thực hiện hội thoại giữa Client và Server theo bất kỳ giao thức an toàn nào.

3. Nhóm thứ ba: Cung cấp và sử dụng chứng chỉ số

3.1 Quyển 6A: Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung. Chủ trì nhóm nghiên cứu: TS. Trần Duy Lai

Trên nền của phần mềm có mã nguồn mở OpenCA, chúng tôi đã xây dựng một hệ thống cấp chứng chỉ với mô hình đơn giản: trung tâm sinh cặp khoá và chỉ có RootCA. Để phục vụ cho quy mô nhỏ, có thể chúng ta không cần đến cả máy RA (và cả máy RAO nữa cũng không cần đến).

Chương 1 „Cài đặt thiết lập cấu hình cho máy CA“ đã dành phần đầu để giới thiệu về PKI, CA, RA, X.509 v 3 certificate, certification paths, revocation. Sau đó đi vào trình bày cách vận hành máy CA:

- Để cài đặt máy CA cần có RedHat Linux 7.2, Perl version 5.6.0 và Apache version 1.3.12. Trong báo cáo đã mô tả chi tiết các bước cấu hình cho Apache Server, cho MySSL và MyCA. Các thư mục và tệp có liên quan đã được mô tả kèm theo chức năng. Menu chính gồm 4 mục: Initiazation, Process Cert Request, Certificates và CRL. Các chức năng trong mỗi mục cũng đã được liệt kê.
- Tiếp theo, báo cáo mô tả việc Khởi tạo cho CA gồm có 3 bước là: (1) Initialize local Perl Database; (2) Generate RootCA Key pair and Self sign Certificate; (3) Export Root CA Certificate and Empty CRL to LDAP.

Chương 2 „LDAP và Public Database trong hệ thống MyCA“ dành cho việc lưu trữ chứng chỉ số còn hiệu lực hay đã bị huỷ bỏ sao cho việc khai thác sử dụng được tiện lợi. Người ta thường dùng LDAP Server để làm việc này, mặc dù về mặt nguyên tắc có thể dùng một database server bất kỳ.

- Trước hết, việc cài đặt và cấu hình LDAP Server được trình bày. Trên nền của LDAP Server, một database được khởi tạo, đó chính là Public Database. Trong tài liệu có mô tả chức năng của các thư mục và tệp có liên quan đến Public Database. Trên trang giao diện chính của Public Database các chức năng được phân làm 3 nhóm, đó là: Download CA Certificates Chain From LDAP, Download Certifcates from LDAP và Update CRLs.
- Trong tài liệu đã mô tả chi tiết các thao tác sau: Tải chứng chỉ của CA từ Public Database Server (có phân biệt cho người dùng sử dụng Windows hay Linux); Tải chứng chỉ của người khác từ Public Database Server (phân biệt người sử dụng dùng Windows hay Linux); Cập nhật CRLs (phân biệt cho trình duyệt Netscape, cho Apache Server, cho IE hay IIS.

Chương 3 „Qui trình phát hành chứng chỉ số“ mô tả 6 bước công việc sau: (1) Nhập thông tin về người được cấp; (2) Ký yêu cầu cấp chứng chỉ; (3) Chuyển đổi định dạng của chứng chỉ; (4) Cấp chứng chỉ cho người dùng; (5) Cập nhật chứng chỉ vừa phát hành lên LDAP server; (6) In nội dung chứng chỉ.

Chương 4 „Quy trình huỷ bỏ chứng chỉ số“ mô tả bước công việc sau: (1) Huỷ bỏ một chứng chỉ bởi người quản trị; (2) Phát hành CRL và cập nhật lên LDAP; (3) Tải CRL từ máy LDAP về máy phục vụ; (4) In chứng nhận huỷ bỏ chứng chỉ cho người sử dụng.

3.2 Quyển 7A: Một hệ chữ ký số có sử dụng RSA. Chủ trì nhóm nghiên cứu: TS. Trần Duy Lai

Đối với nhiều loại dữ liệu thì tính xác thực đôi khi lại cần hơn tính bảo mật. Mật mã khoá công khai đã giải quyết được bài toán xác thực bằng hệ chữ ký số (với sự trợ giúp của hàm băm). Có nhiều thuật toán chữ ký số, nhưng RSA là một thuật toán quen thuộc và nó có trong chuẩn của nhiều nước, nhiều tổ chức quốc tế. Thế nhưng dùng đúng thuật toán chữ ký số RSA không phải là một việc dễ. Bên cạnh việc lựa chọn tham số sao cho an toàn, chúng ta còn phải chú ý tới cách chuẩn bị dữ liệu để ký, chứ không phải cứ việc „luỹ thừa với số mũ là khoá bí mật“ là xong. Trong việc chọn tham số an toàn thì không chỉ có p và q, mà còn có cả e và d nữa. Có một điều cần chú ý là tiêu chuẩn an toàn đối với RSA mã khác với RSA ký.

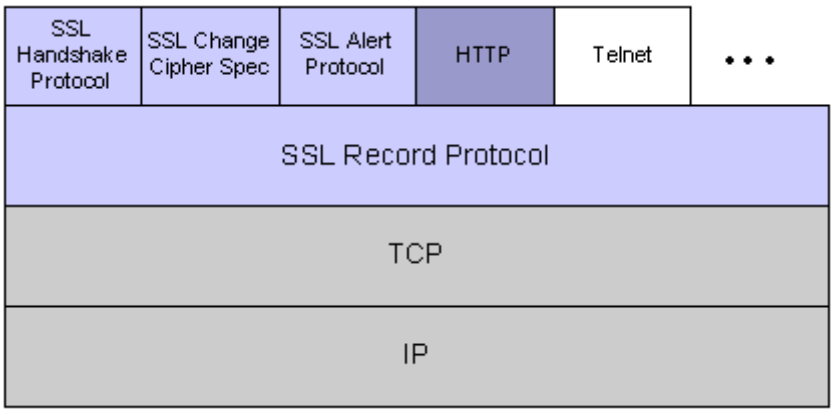
Chương I „Chữ ký số dựa trên mật mã hiện đại“ đề cập tới một số cái mang tính lý thuyết, đó là: Định nghĩa và tính chất của phép ký/phép kiểm tra; Chữ ký số từ hệ mã có thể đảo ngược; Lược đồ chữ ký số cùng với appendix; Lược đồ ký khôi phục thông báo; Điểm qua các kiểu tấn công trên lược đồ ký; Hàm băm (để ký được nhanh).

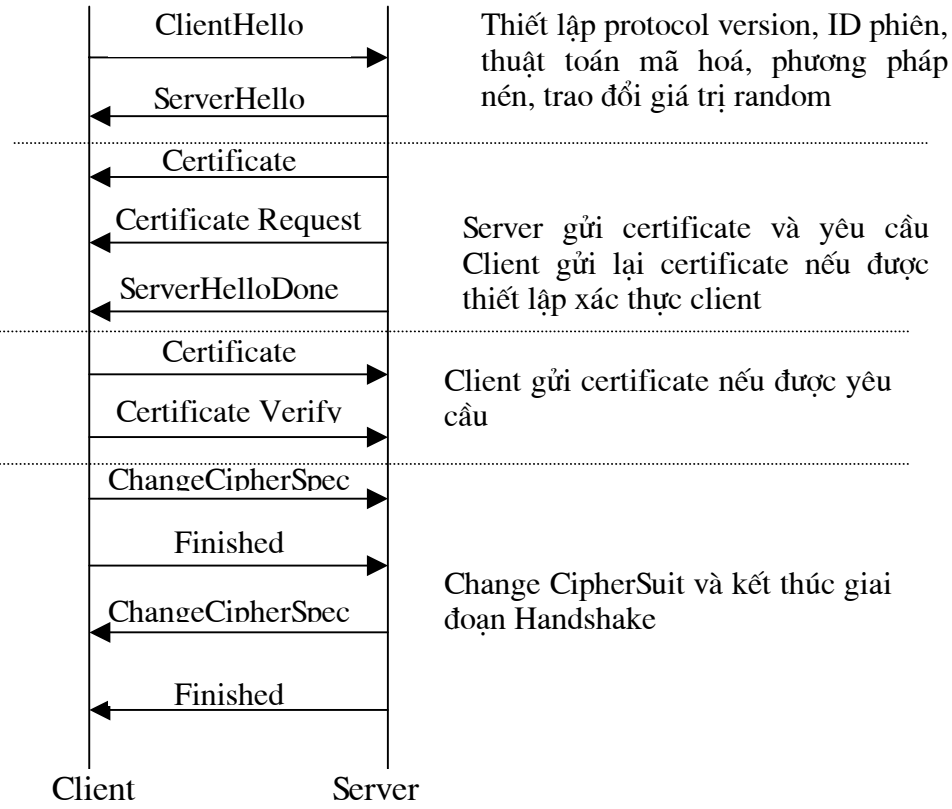
Chương II „Lược đồ chữ ký số RSA“ đã điểm qua các tấn công đối với chữ ký RSA: phân tích số nguyên; tính chất nhân của RSA; bài toán reblocking; ....Trong tài liệu có trình bày 2 định dạng chuẩn, đó là ISO/IEC 9796 và PKCS#1, trong đó PKCS#1 (của hãng RSA) được chọn để lập trình. Trong tài liệu trình bày thuật toán ký theo PKCS#1 phiên bản 1.5, đây chưa phải là chuẩn ký dùng RSA tốt nhất. Chuẩn ký tốt nhất dùng RSA là RSA-PSS trong PKCS#1 phiên bản 2.1.

Chương III „ Module thực hiện ký và kiểm tra chữ ký số sử dụng chứng chỉ số“ trình bày một số công nghệ có liên quan tới việc tạo ra chữ ký theo chuẩn. Có một số PKCS (Public Key Cryptography Standard) được đề cập đến, đầu tiên là PKCS#1, sau đó là PKCS#7 (Cryptographic Message Syntax Standard), PKCS#8 (Private-Key Information Syntax Standard). Trong chương này module thực hiện việc ký và kiêm tra một tệp dữ liệu có sử dụng chứng chỉ số (khoá được lấy ra từ chứng chỉ số). Các tệp header và thư viện cần thiết là: libcrypto.a, sign.o, sign.h, verify.o và verify.h.

3.3 Quyển 8A: Dùng chứng chỉ số với các dịch vụ Web và Mail. Chủ trì nhóm nghiên cứu: PGS. TS. Lê Mỹ Tú

Chương 1 „Giao thức Secure Socket Layer“ cần thiết bởi vì đây chính là giải pháp để bảo mật giao dịch giữa Web Server và Web Client. SSL v3 gồm có SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Specification và SSL Alert Protocol.





Đối với Application data, SSL Record Protocol thực hiện 3 việc: phân mảnh dữ liệu (frame); (2) nén dữ liệu (3) mã hoá và tạo MAC rồi chuyển xuống tầng TCP. Các tham số mật mã liên quan đến một phiên liên lạc được thực hiện thông qua SSLv3 Handshake Protocol. Khi SSL client và SSL server bắt đầu một phiên liên lạc chúng cần thống nhất về phiên bản của giao thức sẽ được dùng, lựa chọn thuật toán mã hoá cho phiên liên lạc, có thể có hoặc không việc xác thực lẫn nhau, và sử dụng thuật toán mã hoá khoá công khai để sinh khoá chung cho phiên liên lạc đó. Trong báo cáo đã trình bày cụ thể quá trình thực hiện SSLv3 Handshake qua các bước giữa client/server như sau: Client Hello; Server Hello; Certificate; Certificate Request; ServerHelloDone; Certificate; Certificate Verify; ChangeCipherSpec; Finished; ChangeCipherSpec; Finished. Các dữ liệu được trao đổi gồm có: Hello Messages; Server Cerificate; Server Key Exchange Message; Certificate Request; Server Hello Done; Client Certificate; Client Key Exchange Message; Certificate Verify và Finished. Ở cuối chương có trình bày cách tính khoá cho phiên liên lạc.

Chương 2 „Sử dụng chứng chỉ số với dịch vụ Web“ đã trình bày các thao tác sau:

- Cài đặt chứng chỉ cho trình duyệt Web: xét hai trường hợp là IE và Netscape. Đối với IE, trước khi Cài đặt chứng chỉ cần phải Cài đặt tiện ích trợ giúp.
- Cập nhật CTL và CRL từ Public Database Server
- Cài đặt và thiết lập cấu hình cho phần mềm E-shop có sử dụng chứng chỉ trên Apache Server
- Sử dụng lệnh https để truy nhập tới E-shop bằng IE hoặc Netscape: nếu cả hai chứng chỉ còn hiệu lực thì kết nối sẽ thành công, ngược lại, nếu một trong hai chứng chỉ đã hết hiệu lực thì kết nối sẽ không thành công.

Chương 3 „Sử dụng chứng chỉ số với dịch vụ Mail“ đã trình bày cách đưa chứng chỉ số vào trình thư tín Outlook Express, cách dùng chứng chỉ số để mã hoá và xác thực

thư, cách cập nhật các CRL. Chú ý rằng đối với Outlook Express, chúng ta chỉ có thể dùng những thuật toán mã dữ liệu có sẵn như DES.

3.4 Quyển 8B: Bảo mật dịch vụ Web thông qua Proxy Server. Chủ trì nhóm nghiên cứu: ThS. Đặng Hoà

Chương 1 „SQUID Proxy Server“ :

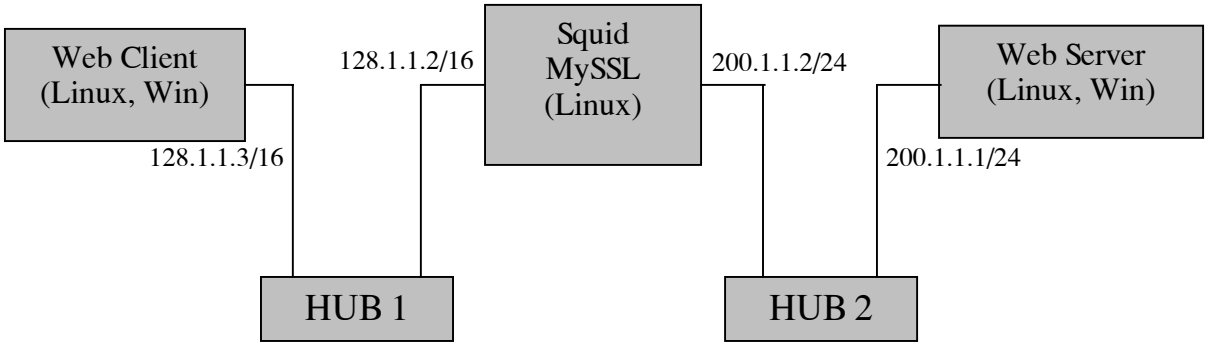
- Squid là ***proxy caching server*** có mã nguồn mở cho các máy khách sử dụng web, hỗ trợ các đối tượng dữ liệu của các giao thức FTP, gopher và HTTP. Squid được sử dụng ở 2 chế độ: chế độ tăng tốc http (httpd-accelerator) để tăng khả năng cung cấp của Web server, và chế độ proxy-caching server mà ta thường sử dụng.
- Các thuật ngữ được sử dụng với Squid gồm có: Internet Object; Internet Object Caching; Cache Hierarchy; parent cache; sibling cache; Internet Cache Protocol; Hyper Text Caching Protocol; Squid cache resolution algorithm.
- Tệp cấu hình squid.conf khá phức tạp. Trong tệp này có 7 thẻ liên quan đến mạng; có 9 thẻ liên quan đến cây lưu trữ; có 12 thẻ liên quan đến cache size; có 15 thẻ liên quan tới thư mục lưu trữ và tệp log; có 18 thẻ liên quan đến các chương trình bên ngoài; có 14 thẻ để điều chỉnh cache; có 10 thẻ liên quan đến giới hạn thời gian kết nối; có 7 thẻ dành cho điều khiển truy nhập; có 6 thẻ liên quan tới quản trị hệ thống; có 4 thẻ dành cho việc đăng ký cache server; có 5 thẻ để tăng tốc Web; có 41 thẻ để giới hạn băng tần và ngoài ra còn một số tuỳ chọn khác nữa.
- Chúng ta quan tâm tới những lựa chọn hỗ trợ SSL, đó là https_port và ssl_unclean_shutdown.

Chương 2 „Tích hợp mật mã cho Proxy“ đã trình bày về MySSL. Một cách tóm tắt, MySSL nhận được từ OpenSSL sau khi thực hiện các công việc sau: Loại bỏ những phần mã nguồn không sử dụng đến; Loại bỏ giao thức SSL v2; Loại bỏ các thuật toán mã có sẵn, thay vào đó là thuật toán Mã khối của Ngành CY; Loại bỏ các thuật toán băm trừ MD5 và SHA-1; Loại bỏ các thuật toán ký, trừ RSA; Loại bỏ chương trình sinh số nguyên tố xác suất, thay vào đó là thuật toán sinh tham số RSA an toàn. Trong tài liệu có mô tả cấu trúc file và thư mục của MySSL và phân tích những đoạn chương trình nguồn quan trọng có liên quan đến: thuật toán mã khối (các tệp mk1_core.c, mk1_cbc.c, ...); thuật toán mã và ký RSA; thuật toán băm MD5 và SHA-1; thư viện HMAC. Cuối chương có trình bày cách biên dịch và cài đặt MySSL cũng như cách biên dịch và cài đặt SQUID có hỗ trợ dịch vụ mật mã từ MySSL.

Chương 3 „Trình duyệt MyBrowser và tích hợp mật mã cho trình duyệt MyBrowser“ gồm các nội dung sau:

- Giới thiệu Mozzila 1.0 cùng các công nghệ chính được sử dụng trong đó là XPCOM, XPToolkit với XUL (XML-based User Interface Language) và XBL (eXtensible Binding Language)
- NSS là bộ chương trình nguồn cung cấp một thư viện độc lập thực hiện các dịch vụ bảo mật phục vụ cho việc phát triển các ứng dụng cross-platform. Khi xây dựng một ứng dụng sử dụng NSS, ứng dụng đó có thể được cung cấp các giao thức SSL v1, SSL v2, TLS, các chuẩn mật mã khoá công khai PKCS#5, PKCS#7, PKCS#11, PKCS#12, S/MIME, chứng chỉ số theo chuẩn X.509 v3 và rất nhiều các chuẩn mật mã khác.
- Trình duyệt MyBrowser nhận được từ Mozzila 1.0 bằng cách tối thiểu hoá và tích hợp mật mã. Trong tài liệu có trình bày cách biên dịch ra MyBrowser.

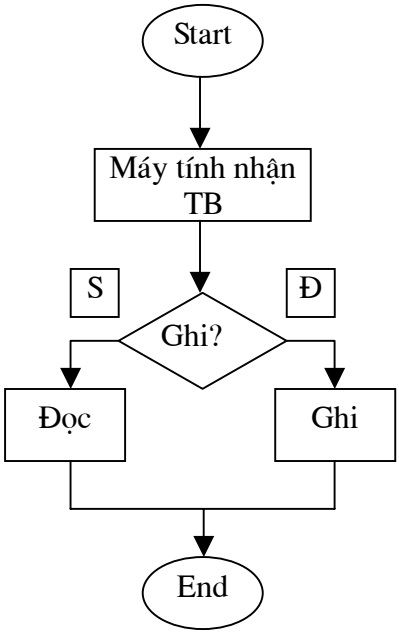
Chương 4 „Bảo mật dịch vụ web thông qua Proxy“ gồm các thông tin sau:
- Cài đặt và cấu hình Web Server: có thể dùng Apache Web Server hoặc IIS.
- Thiết lập cấu hình cho Proxy Server
- Cài đặt trình duyệt MyBrowser và cài đặt chứng chỉ số cho MyBrowser
- Mô hình thử nghiệm như sau:



- Các thao tác được thử nghiệm: truy nhập trang web; ghi trang web vào hệ thống và tải tệp.

3.5 Quyển 9A: Một số thiết bị được sử dụng để ghi khoá. Chủ trì nhóm nghiên cứu: TS. Nguyễn Hồng Quang

Chương 1 „Sử dụng iKey 1000 lưu chứng chỉ số và khoá bí mật“ đã giới thiệu thiết bị iKey của hãng Rainbow Technologies. Trong tài liệu đã giới thiệu chi tiết các thao tác cần làm khi cài đặt phần mềm đi kèm với thiết bị lên máy tính. Tiếp theo đó đã trình bày các bước nhằm dùng iKey để lưu chứng chỉ số và khoá bí mật, đó là: khởi tạo định dạng cho iKey; thiết lập tên cho iKey; khởi tạo (hay đặt lại) vùng lưu chứng chỉ số; thay đổi mật khẩu; lưu chứng chỉ số. Sau đó là cách đăng ký chứng chỉ số với các ứng dụng như IE và Outlook Express.



Chương 2 „Thiết kế một loại thiết bị nghiệp vụ“ đã trình bày việc thiết kế, xây dựng một loại thiết bị nghiệp vụ có giao diện USB. Sơ đồ khối tổng quát của thiết bị gồm có 3 khối: khối giao diện, khối vi xử lý và khối nhớ. Khối giao diện sử dụng linh kiện IC USB FT245 BM của hãng FTDI. Khối vi xử lý sử dụng linh kiện AT89C2051 của hãng Atmel. Khối nhớ sử dụng linh kiện AT24C64 của hãng Atmel. Quá trình làm việc của thiết bị được mô tả như sau: Khi cắm thiết bị vào trong máy tính, máy tính sẽ có nguồn cho thiết bị và thiết bị sẽ hoạt động, trao đổi với máy tính để máy tính nhận biết thiết bị là một thiết bị USB chuẩn, sau đó thiết bị sẽ đợi để xác định quá trình tiếp theo là đọc hay ghi và thực hiện theo chức năng đó cho đến kết thúc. Quá trình làm việc này được mô tả như lưu đồ đi kèm. Trong báo cáo có trình bày lưu đồ của thuật toán đọc/ghi dữ

liệu.

4. Nhóm thứ tư: Đảm bảo toán học

4.1 ***Quyển 3A: Sinh tham số an toàn cho hệ mật RSA.*** Chủ trì nhóm nghiên cứu: TS. Lều Đức Tân

Mật mã khoá công khai cần có số nguyên tố lớn, nhưng chỉ „lớn“ không thì chưa đủ. Không phải số nguyên tố nào cũng dùng cho mật mã khoá công khai được một cách nói chung và cho một hệ mật cụ thể nào đó nói riêng (ví dụ như RSA hay Elgamal).

Chương I „Hệ tiêu chuẩn cho hệ mật RSA“ đã đề cập đến 4 tiêu chuẩn cho số nguyên tố dùng cho RSA của chuẩn X9.31 (đây là một chuẩn của các tổ chức tài chính Mỹ). Trên cơ sở 4 tiêu chuẩn đó, cùng với việc xét các tấn công phân tích số bằng phương pháp sàng trường số, tấn công phân tích số dựa vào đường cong elliptic, phương pháp phân tích số p±1 của Williams, tấn công kiểu giải hệ phương trình và phân tích số dựa vào gcd(p±1, q±1), nhóm nghiên cứu đã đưa ra hệ tiêu chuẩn của mình với những ngưỡng cụ thể. Độ an toàn của bài toán phân tích số phụ thuộc vào sự phát triển của công nghệ tính toán, nếu lấy luật Moore làm cơ sở (sau 18 tháng công suất tính toán tăng gấp đôi với cùng giá thành) thì nhóm các tác giả đã đưa ra một hệ dự kiến gồm 5 tiêu chuẩn cho các tham số p và q dùng cho hệ mật RSA dùng vào thời điểm năm 2003 với thời gian an toàn là y năm, đó là:

- Số modulo N phải có độ lớn cỡ n bít với n thoả mãn bất đẳng thức $4.91 n^{\frac{1}{3}} (\ln n + \ln \ln 2)^{\frac{2}{3}} \geq E$ với E được tính theo công thức : $E = 56 + \frac{Y + y - 2003}{1.5}$
- Các số nguyên tố p và đều xấp xỉ $\sqrt{N}$
- gcd(p-1, q-1) phải có ước nguyên tố lớn không dưới E bit
- max{gcd(p±1, q±1)} không quá $\frac{n - 2E}{4}$ bit
- λ(p±1) phải có ước nguyên tố lớn không dưới 2E bit.

Chương II „Xây dựng phần mềm sinh số nguyên tố dùng cho hệ mật RSA“ đã bắt đầu bằng các định lý Pocklington và Lucas, trên cơ sở đó các hàm PocklingtonPrimeTest, LucasPrimeTest và LucasPocklingtonPrimeTest (dùng PocklingtonPrimeTest và LucasPrimeTest) được xây dựng. Tiếp đó, thuật toán sinh số nguyên tố bằng phương pháp tăng dần độ dài được trình bày (sử dụng LucasPocklingtonPrimeTest), về mặt lý thuyết có đánh giá số lần dãn trung bình và mật độ số nguyên tố sinh được theo cách này. Số nguyên tố thoả mãn các điều kiện 2 và 5 trong số 5 điều kiện trên được gọi là số RSA-mạnh. Thuật toán StrongPrimeGenerator (theo kiểu của Gordon) đã được xây dựng để sinh số RSA-mạnh (thuật toán này có dùng đến hàm PrimeP-1Generator(k), hàm này sinh ra số nguyên tố với p-1 có ước nguyên tố k bit, hàm PrimeP-1Generator có dùng đến PocklingtonPrimeTest). Lực lượng các số RSA-mạnh được sinh theo thuật toán StrongPrimeGenerator đã được đánh giá về mặt lý thuyết. Cuối cùng, các cặp số nguyên tố p và q thoả mãn các điều kiện 3 và 4 trong số 5 điều kiện đã được kể ở trên được gọi là cặp số nguyên tố có quan hệ mạnh. Hàm RSA-Generator đã được thiết kế để sinh ra những số như vậy, hàm này có gọi đến hàm PrimeP-1Generator và hàm GordonGenerator. Đến lượt mình, hàm GordonGenerator lại được xây dựng trên cơ sở hàm LucasPocklingtonPrimeTest và thuật toán CRT.

4.2 ***Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal.*** Chủ trì nhóm nghiên cứu: TS. Lều Đức Tân

Trong chương I, với tiêu đề "Vai trò của số nguyên tố mạnh dạng p=2q+1 trong mật mã", giải quyết vấn đề số nguyên tố mạnh dùng ở đâu và cụ thể hơn là điểm ra 3 ứng dụng chủ yếu trong mật mã đó là *bài toán bảo mật tin* dùng hệ mật Elgamal, *bài toán xác thực tin* theo sơ đồ chữ ký Elgamal và *bài toán thoả thuận khoá* theo sơ đồ Diffie-Hellman. Đặc điểm chung của các loại hình trên là tính an toàn của chúng đều được coi là tương đương với tính khó giải của bài toán logarit trên trường GF(p), chính vì thế phần 2 của chương đi vào trình bày các thuật toán giải bài toàn này với mục đích không gì khác là dẫn ra được câu trả lời là "Để đảm bảo tính an toàn cho các loại hình trên thì tham số nguyên tố được sử dụng phải là những số lớn cỡ trên 500 bit và có dạng p=2q+1 với q nguyên tố".

Chương II, "Sinh số nguyên tố bằng phương pháp tăng dần độ dài", trình bày một phương pháp sinh số nguyên tố hoàn toàn dựa vào định lý Pocklington. Mặc dù rằng trên góc độ thời gian tính thì các thuật toán kiểm tra tính nguyên tố dựa vào định lý Pocklington chỉ có nghĩa đối với các lớp số nguyên nhỏ thế nhưng thuật toán của chúng tôi đưa ra dùng để sinh các số nguyên tố lớn không theo phương thức sinh truyền thống là "Lấy ngẫu nhiên một số nguyên – Kiểm tra tính nguyên tố của nó, cho đến khi tìm được số nguyên tố" mà theo cách "Sinh các số nguyên tố nhỏ dùng chúng làm cơ sở để sinh các số nguyên tố lớn hơn cho đến khi được số nguyên tố có độ dài mong muốn". Về mặt lý thuyết thì bất cứ một số nguyên tố nào cũng có thể được sinh từ phương pháp của chúng tôi tất nhiên với khả năng không như nhau. Quan trọng hơn cả trong việc đưa ra thuật toán này là nó có thể sinh các số nguyên tố dùng trong hệ mật Elgamal một cách rất hiệu quả.

Chương III, "Chương trình sinh số nguyên tố cho hệ mật Elgamal", đi vào giải quyết vấn đề xây dựng cơ sở lý thuyết của thuật toán và hiện thực hoá bằng một chương trình sinh số nguyên tố mạnh trên một lớp số nguyên cụ thể:

- Phần 1 của chương này giới thiệu về lớp $\mathbf{L}_p(k)$ với đầy đủ việc đánh giá về lực lượng số nguyên tố trong lớp và thuật toán sinh các số nguyên tố trong đó, với sự lựa chọn p =2, bằng cách dựa vào định lý Pepin và quan trọng là ở Chú ý 3.3 chúng tôi đã chỉ ra được một thuật toán cực nhanh để sinh các số nguyên tố Pepin (các số nguyên tố dạng $q_1=r2^k+1$ với r lẻ và có độ dài bit không quá k) và sau đó là với p là số có độ dài cỡ một nửa độ dài số nguyên tố cần sinh chúng ta đã có được một kiểu sinh rất nhanh các nhân nguyên tố q có dạng $q=Rq_1+1$ với R chẵn và $R\leq q_1$ (những số nguyên dạng trên được kiểm tra nhanh tính nguyên tố bằng định lý Pocklington và chúng tôi gọi những số nguyên tố này là những số Pocklington) với độ dài đủ lớn (từ 500 đến 1500 bit). Đây chính là lớp số mà chúng tôi quyết định lựa chọn để xây dựng phần mềm tìm các số nguyên tố lớn trên đó.
- Phần 2, "Việc sinh các số nguyên tố mạnh và gần mạnh", ngoài việc thống nhất bằng cách đưa ra định nghĩa cho khái niệm gần mạnh trong phần này đã đưa ra một kết quả cực kỳ đơn giản nhưng rất hiệu quả để khẳng định tính mạnh của một số nguyên tố đó là Định lý 3.5. Theo kết quả trên thì với q là số nguyên tố lẻ, để chứng tỏ p=2q+1 nguyên tố (tức là số nguyên tố mạnh) ta chỉ cần kiểm tra đẳng thức $2^{2q}=1 \pmod p$ và 3 không phải là ước của p. Như vậy cùng với phần 1,

đến đây chúng ta đã có được đầy đủ cơ sở lý thuyết cho một thuật toán nhanh dùng để sinh các số nguyên tố mạnh.

- Phần 3, "Tính toán trên các số lớn", nhằm hiện thực hoá được thuật toán đã chỉ ra ở 2 phần trên bằng một chương trình phần mềm sinh số nguyên tố mạnh. Việc tính toán trên các số lớn là một việc làm rất quen thuộc cho nên chúng tôi không trình bày tỷ mỷ mọi thủ tục và hàm tính toán số học nói chung mà chủ yếu đi vào phân tích những cải tiến nhỏ mà chúng tôi đã thực hiện khi lập trình trong đó ba phép toán được đề cập đến là phép nhân, phép chia và phép luỹ thừa các số lớn. Bằng việc thực hiện phép luỹ thừa theo phương pháp xét số mũ với cơ số thay đổi và tính sẵn 32 luỹ thừa từ x^{32} đến x^{63} (mod N) mỗi khi cần tính x^y (mod N), chương trình sinh số nguyên tố mạnh của nhóm đề tài đã có được sự cải thiện đáng kể về tốc độ sinh bởi vì phép lỹu thừa là phép toán chủ yếu trong thuật toán sinh và cũng là phép toán chiếm nhiều thời gian nhất.

Phụ lục "Một số kết quả thử nghiệm", nhằm giới thiệu một số kết quả thử nghiệm của phần mềm đã viết để sinh các tham số cho hệ mật Elgamal bao gồm các nội dung:

- Một số kết quả thống kê thu được về thời gian sinh trung bình cùng mật độ trung bình của số nguyên tố mạnh và gần mạnh theo một số độ dài cụ thể như 512, 1024 và 1500 bit.
- Ví dụ về toàn bộ các số nguyên tố Pepin dạng $q_1=r2^{16}+1$ với r lẻ và $q_1<2^{32}$, số lượng các số nguyên tố Pocklington dạng $q=Rq_1+1$ với R chẵn và $q<2^{32}$ và toàn bộ các số nguyên tố Sophie trong các số nêu trên (việc tìm các số trên được thực hiện bằng phương pháp sàng Erathostenes).

Đánh giá chung: Vấn đề được đặt ra nhằm xây dựng được một phần mềm nhằm sinh ra các tham số phục vụ cho một lớp các hệ mật khoá công khai hiện đang được sử dụng ngày càng phổ biến trong lĩnh vực bảo mật và an toàn thông tin. Cũng như mọi sản phẩm khoa học khác, yêu cầu tối thiểu và tiên quyết đối với phần mềm (với tư cách là một máy sinh các số nguyên tố) đó là những số nguyên tố được nó sinh ra dùng ở đâu (hệ mật nào), chỉ tiêu chất lượng của chúng ra sao (chủ yếu là chỉ tiêu liên quan đến độ mật của hệ mật) và sau cùng là hiệu quả của chương trình (tính chấp nhận được về thời gian sinh). Cụ thể hoá những vấn đề trên, trong đề cương của đề tài chúng tôi đã đăng ký là *xây dựng phần mềm* sinh các số nguyên tố dạng $p=2q+1$ với q cũng nguyên tố trong một lớp số cụ thể nào đó.

4.3 ***Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả.***

Chủ trì nhóm nghiên cứu: TS. Trần Văn Trường

Chương 1 „Mở đầu về mã khối“ giới thiệu chung về mô hình toán học của hệ mã khối khoá bí mật. Độ an toàn của hệ mã khối trước Giả thuyết nổi tiếng của *Kerckhoff:* Thám mã đối phương là được biết toàn bộ chi tiết của quá trình mã hóa và giải mã chỉ trừ giá trị khóa bí mật. Từ đó dẫn tới một số dạng tấn công thám mã chung nhất đối với mã khối, đồng thời cũng đặt ra ngay một số yêu cầu tối thiểu đối với một hệ mã khối an toàn là phải có cỡ khối và cỡ khoá đủ lớn. Để đảm bảo tính hiệu quả một hệ mã khối cần phải có cấu trúc đều, đối xứng mã/dịch và các thành phần của nó cũng phải dễ dàng trong quá trình cứng hoá hay chương trình hoá mức cao. Chương này cũng đã giới thiệu một số cấu trúc mã khối cơ bản như cấu trúc đối xứng thuận nghịch Feistel, cấu trúc truy hồi Matsui, cấu trúc cộng-nhân Massey...và

một số thuật toán mã khối cụ thể để minh hoạ như thuật toán GOST của Liên bang Nga, thuật toán IDEA.

Chương 2 „Thám mã khối“ :Một số những công việc quan trọng khởi đầu cho quá trình thiết kế xây dựng mã khối là cần thiết nghiên cứu những phương pháp thám mã khối điển hình, từ đó rút ra những đặc trưng an toàn cơ bản của một hệ mã khối. Chương này tập trung nghiên cứu lý thuyết về các phương pháp thám mã khối cơ bản như thám mã vi sai, thám mã vi sai bậc cao, thám mã tuyến tính và các dạng đặc biệt của thám mã tuyến tính, thám mã nội suy, thám mã khoá quan hệ.. chủ yếu áp dụng trên chuẩn mã dữ liệu DES. Về mặt lý thuyết chúng tôi chỉ nêu những nguyên tắc thám mã cơ bản đối với mã khối (dựa trên chuẩn mã dữ liệu DES) mà không trình bày chi tiết thuật toán (vì có thể tìm thấy trong nhiều tài liệu khác). Phần thực hành, chúng tôi tập trung nghiên cứu khai thác phương pháp thám mã phi tuyến dựa trên ý tưởng thám mã tuyến tính để xây dựng thuật toán thám hệ DES rút gọn 8-vòng nhằm tìm đủ 56 bít khoá của chúng. Các vấn đề được trình bày là:

- Thám mã vi sai được phát minh từ năm 1991 bởi các nhà mật mã Biham và Shamir. Đây là tấn công đầu tiên phá chuẩn mã dữ liệu DES của Mỹ với độ phức tạp tấn công nhỏ hơn độ phức tạp của phương pháp vét cạn khoá. Ý tưởng cơ bản của phương pháp này là thám mã vi sai xoay quanh việc so sánh kết quả của phép XOR giữa hai bản rõ với kết quả của phép XOR giữa hai bản mã tương ứng. Với giả thiết rằng các bản rõ được lấy ngẫu nhiên đều trên không gian các đầu vào có thể, hãy thử xem phân bố của các kết quả phép XOR đầu ra có tuân theo phân bố ngẫu nhiên đều hay không. Nếu bảng phân bố là không đều, thì thám mã có thể lợi dụng để xây dựng phương pháp tấn công lên hệ mật bằng kiểu tấn công bản rõ chọn lọc. Đối với chuẩn mã dữ liệu DES, xuất phát từ thành phần phi tuyến duy nhất và cũng khó tuyến tính hoá nhất là các hộp thế các tác giả đã tìm ra được điểm yếu và từ đó đã thác triển ra thành các đặc trưng vi sai với xác xuất đủ lớn để có thể sử dụng để tấn công tìm khoá tại vòng cuối cùng. Độ phức tạp của tấn công do Biham và Shamir đề xuất trên DES vào cỡ 2^{47} sơ với phương pháp duyệt khoá là 2^{56} như đã nói ở trên.
- Thám mã tuyến tính được phát minh bởi Mitsuru Matsui năm 1993 đã tấn công tìm đủ 56 bít khoá của DES với độ phức tạp 2^{43} nhỏ hơn phương pháp thám vi sai. Nguyên lý chung của phương pháp thám mã tuyến tính đối với hệ DES là do hệ DES đã công khai toàn bộ các phép biến đổi trong nó, trong đó chỉ có các hộp nén mới là các phép biến đổi phi tuyến. Cái bí mật còn lại duy nhất khi sử dụng DES đó là khoá K được sử dụng cụ thể. Nếu tất cả các phép biến đổi của DES đều là tuyến tính, thì với ẩn số là khoá K cho trước cố định, bằng công cụ mô phỏng trên máy tính và sử dụng các cặp bản rõ-mã tương ứng ta có thể thiết lập được hệ thống phương trình tuyến tính để tìm lại được các bít khoá K đó trong thời gian đa thức. Tuy nhiên, các hộp nén (thành phần quan trọng nhất của hệ DES) là các phép biến đổi phi tuyến được chọn lựa cẩn thận, nên muốn thám DES thì phải tấn công vào chính thành trì này. Mục đích của phương pháp thám mã tuyến tính trên DES là tìm một biểu diễn xấp xỉ tuyến tính cho hệ này để có thể phá chúng nhanh hơn phương pháp tấn công vét kiệt. Và tất nhiên, những nhược điểm của các hộp nén sẽ lại được tiếp tục khai thác cho mục đích này. Qua khảo sát cụ thể 8 hộp nén của DES, Matsui đã xây dựng được các xấp xỉ tuyến tính trên toàn hệ mã với xác suất đúng có độ lệch klhá xa so với 1/2. Từ đó đã hình thành nên tấn công tuyến tính với các hệ mã khối nói chung. Sau đó để tăng cường thêm tính hiệu qảu của phương pháp này, nhiều bài báo đã đề xuất thêm các dạng tấn công dùng xấp xỉ nhiều lần, xấp xỉ phi tuyến...Chúng tôi đã thực

hành một phương pháp tấn công phi tuyến với DES 8-vòng, bằng chương trình máy tính cụ thể, chúng tôi đã tìm đủ được 56 bít khoá trên một máy tính 933 MHz với thời gian trung bình mất cỡ 1 ngày. Chương trình thám mã DES 8-vòng đã được liệt kê trong Phụ lục A.

- Nếu ta coi mỗi bit đầu ra của hệ mã khối là một hàm Boolean trên các bít đầu vào, thì với giả thiết bậc đại số của các hàm boolean này đủ nhỏ, ta có thể hình thành nên một tấn công vi sai bậc cao (tương tự như đạo hàm bậc cao của một đa thức bậc thấp sẽ nhanh chóng biến thành hằng số với xác suất 1).
- Mặt khác nếu xem toàn bộ đầu ra của hệ mã khối như là hàm của toàn bộ đầu vào tương ứng, và với giả thiết rằng hàm véc tơ Boolean đó có thể biểu diễn xấp xỉ bởi một đa thức bậc thấp với số các số hạng có hệ số khác không đủ nhỏ trên $GF(2)^n$ thì có thể dùng phương pháp nội suy Lagrange để lập lại được hàm này, và từ đó có hình thành nên kiểu tấn công nội suy. Ngoài ra, lược đồ khoá của hệ mã khối có những mối quan hệ nhất định giữa các khoá con vòng cũng sẽ dẫn đến kiểu tấn công khoá quan hệ, tấn công kiểu trượt khối...
- Phần cuối của chương xuất phát từ các kiểu tấn công trên đã đưa ra yêu cầu cơ bản của một hệ mã khối an toàn, hiệu quả:
    - Hệ mã phải có độ dài khối rõ, khối khoá đủ lớn (không gian rõ và khoá lớn) để tránh tấn công vét kiệt trên không gian rõ cũng như không gian khoá (thường độ dài cỡ khối lớn hơn hoặc bằng 128);
    - Hệ mã phải có độ đo vi sai và độ đo độ lệch tuyến tính tối thiểu để tránh được hai kiểu tấn công nguy hiểm nhất là tấn công vi sai và tấn công tuyến tính theo các nguyên lý như đã trình bày trên;
    - Các hộp thế, các phép biến đổi phi tuyến cần phải có bậc đại số cao tránh tấn công nội suy, tấn công vi sai bậc cao.
    - Tầng tuyến tính trong các hàm vòng cần phải được lựa chọn cẩn thận để khi phối hợp với tầng phi tuyến phải tạo ra hệ mã có tính khuyếch tán tốt theo các nguyên lý của chương 1, để tránh các tấn công địa phương trên các khối mã nhỏ.
    - Các phép biến đổi đầu vào đầu ra của một hệ mã khối cũng không được quá đơn giản (như DES) mà cần phải là tầng che dấu, ngăn cản việc thiết lập các vi sai hay các mảng đánh dấu tuyến tính các vòng đầu cuối đã biết trước đối với thám mã.
    - Lược đồ tạo khoá cần phải tránh được các lớp khoá yếu, và nói chung nên dùng kiểu khoá phiên độc lập (nếu có thể được). Đặc biệt lược đồ khoá không tồn tại những quan hệ khoá đơn giản do tính đều, hay cân xứng trong lược đồ gây nên, nhưng lại phải đảm bảo các khoá là tốt như nhau để tránh các kiểu tấn công khoá quan hệ, tấn công trượt khối dựa trên tính giống nhau trong các phân đoạn tạo khoá con (không phụ thuộc số vòng của hệ mã).

Chương 3 „Khảo sát hệ mã khối an toàn theo các đặc trưng độ đo giải tích“. Như chúng ta đã biết mô hình chung phổ biến của một hệ mã khối gồm hai phần: phần ngẫu nhiên hoá dữ liệu và phần lược đồ tạo khoá cho hệ mã. Phần ngẫu nhiên hoá dữ liệu gồm các cấu trúc cơ bản đã giới thiệu trong chương 1, có thể thấy nó thường chứa ba lớp: các hộp thế (lớp trong cùng), hàm vòng (lớp giữa) và cấu trúc mã-dịch (lớp ngoài cùng). Phần lược đồ khoá cũng sẽ được giới thiệu ở cuối chương, nó có thể gồm lược đồ on-line (tính cùng quá trình mã-dịch), hay off-line (tính trước quá trình mã-dịch), hoặc là lược đồ khoá độc lập với phần ngẫu nhiên hoá dữ liệu hay phụ thuộc phần ngẫu nhiên hoá dữ liệu. Để cho hệ mã là an toàn chống được các tấn

công đã nêu, cần phải thiết kế xây dựng các hộp thế, hàm vòng và nghiên cứu lựa chọn cấu trúc mã-dịch sao cho hạn chế tối đa các tấn công phân tích mã hoặc vô hiệu hoá các phương pháp thám mã cụ thể. Đồng thời lược đồ khoá phải tránh được các quan hệ khoá đơn giản hoặc tránh các sự tương tự giữa các công đoạn tạo khoá...Muốn vậy chúng ta phải xây dựng và theo dõi được sự ảnh hưởng lẫn nhau giữa các độ đo an toàn của các thành phần cấu tạo nên hệ mã. Vì thế, nội dung chính của Chương 3 sẽ gồm các nghiên cứu khảo sát và xây dựng các thành phần cơ bản của hệ mã khối là:Nghiên cứu về các hộp thế của mã khối; Nghiên cứu về các dạng hàm vòng an toàn; Nghiên cứu độ an toàn thực tế của cấu trúc mã-dịch kiểu Feistel; Nghiên cứu về các lược đồ tạo khoá của mã khối. Kết quả cụ thể của chương là đã giới thiệu được các độ đo an toàn cơ bản liên quan đến hộp thế, hàm vòng, đã trình bày các dạng thiết kế hộp thế như là hàm véc tơ Boolean có các tính chất đều, bậc đại số cao, độ phi tuyến cao, độ đo vi sai nhỏ đều và độ đô độ lệch tuyến tính đủ nhỏ...Cấu trúc ngoài cùng ở đây được lựa chọn trình bày là dạng Feistel đã được các nhà mật mã thế giới chỉ ra có độ đo an toàn về cả lý thuyết và thực tế. Đó là những cơ sở cần thiết để thiết kế xây dựng cho thuật toán mã khối cụ thể.

Chương 4 „Khảo sát mã khối theo nhóm sinh của các hàm mã hoá“. Việc tìm các tính yếu của một hệ mã khối căn cứ vào những đặc tính cụ thể của nhóm sinh của các hàm mã hoá của hệ mã để trên cơ sở đó hình thành nên những tiêu chuẩn khi thiết kế xây dựng các hệ mã khối an toàn là một hướng đi được một số tác giả như Kennth G. Paterson, Ralph Wernsdorf, Sarval Patel, Zulfikar Ramran và Ganapathy...quan tâm và cũng đã đưa ra được những kết quả có ý nghĩa. Trong chương này chúng tôi bắt chước theo những ý tưởng của các tác giả nêu trên, trong đó có trình bày lại kết quả theo chúng tôi cho là có ý nghĩa nhất về mặt mật mã đó là khái niệm nguyên thuỷ của nhóm các phép thế của tác giả Kennth G. Paterson rồi lấy đó làm trong tâm phát triển. Công lao chủ yếu của chúng tôi đưa ra trong bài này là đưa ra các kết quả liên quan đến khái niệm t-phát tán và t-phát tán mạnh cùng với ý nghĩa mật mã của chúng. Qua các kết quả đã đưa ra cũng toát lên một vấn đề rất thực tế đó là mọi tính yếu về nhóm các phép thế có ảnh hưởng đến tính an toàn của hệ mật thì việc loại bỏ chúng chỉ là cần thiết vì rất dễ khắc phục các khuyết tật hình thức trên nhóm sinh (chỉ bằng cách bổ xung vào tập các hàm mã hoá cùng lắm là 2 hàm đơn giản) trong khi bản chất mật mà chỉ phụ thuộc vào chính tập các hàm mã hoá. Cũng có thể nói rằng tính phát tán và tính nguyên thuỷ của hệ mã khối liên quan chặt chẽ với khái niệm khuyếch tán (diffusion) như Shannon đã đề cập liên quan tới các hệ mã tích.

Chương 5 „Khảo sát các đặc trưng của mã khối theo quan điểm xích Markov“. Các hệ mã khối hiện tại đều thuộc dạng thuật toán mã hoá tiến hành lặp đi lặp lại một hàm (thường được gọi là hàm vòng). Hai phương pháp tấn công rất nổi tiếng đối với loại mã khối này là tấn công vi sai và tấn công tuyến tính như đã nói trong chương 2. Hiệu quả của hai phương pháp này được thể hiện trên các phương diện sau đây: tập các cặp rõ, và các cặp mã tương ứng (trong tấn công vi sai), tập các cặp rõ/ mã tương ứng (trong tấn công tuyến tính) có độ lớn là bao nhiêu thì xác suất thành công của người mã thám đủ cao? Khi có tập này rồi thì thời gian tiến hành có thực tế hay không? Khả năng thực tế trong việc thu thập tập hợp này? Đối với người lập mã, các câu hỏi thường được đặt ra như sau: Hàm vòng phải được thiết kế như thế nào để các công thức ở trên đúng với xác suất bé? Số vòng lặp tối thiểu phải là bao nhiêu để khiến cho lực lượng cần thiết của tập rõ/mã làm nản lòng các nhà mã thám? Việc nghiên cứu mã khối trên quan điểm xích Markov đã giúp các nhà mật mã trả lời các

câu hỏi đó trên những điểm lớn, khái quát. Cụ thể trong chương đã giới thiệu các xich Markov để thám vi sai và thám tuyến tính đối với hệ mã khối thoả mãn các tính chất nào đó. Khái niệm mật mã Markov và các nhóm luân phiên trong khi khảo sát độ an toàn của hàm mã khối cũng liên quan chặt chẽ với nhau. Cụ thể với các hệ mã DES và IDEA ta có khẳng định, nếu giả thiết tương đương ngẫu nhiên đúng cho phần mật mã tương ứng, thì DES và IDEA(32) là an toàn chống lại thám vi sai sau đủ nhiều vòng đối với tất cả các mật mã Markov này. Những kết quả này còn đúng cho tất cả các mật mã lặp r vòng, nếu các hàm một vòng là tương tự DES sinh ra nhóm luân phiên. Kết luận rút ra của chương này là:

- Khi nghiên cứu mã khối dưới góc độ mật mã Markov, người ta đã tìm cách chứng minh mật mã này có xích Markov tương ứng là bất khả quy và không có chu kỳ. Nếu làm được điều này thì có thể khẳng định mật mã là an toàn trước tấn công vi sai và tấn công tuyến tính khi số vòng lặp đủ lớn.
- Đã có hai cách để chứng minh xích Markov là bất khả quy và không có chu kỳ. Một là dùng lý thuyết đồ thị ngẫu nhiên, và phương pháp thứ hai là sử dụng tính chất của nhóm luân phiên. Phương pháp thứ hai là khó song kết quả của nó là tất định.
- Nhìn chung ta vẫn chưa đưa ra được "số vòng đủ lớn" là bao nhiêu?
- Giả thiết tương đương ngẫu nhiên không phải luôn luôn đúng vì vậy để chứng minh một mã khối là an toàn trên quan điểm xích Markov cũng còn rất nhiều việc phải làm.

Chương 6: Xây dựng thuật toán mã khối MK_KC-01-01. Trong chương này chúng tôi thiết kế một thuật toán mã khối cụ thể đảm bảo các thông số an toàn, hiệu quả phục vụ cho đề tài:

- Trước hết, phần ngẫu nhiên hoá dữ liệu được xây dựng theo cấu trúc 3 lớp: trong, giữa và ngoài cùng. Lớp ngoài cùng chúng tôi chọn cấu trúc Feistel có thể đánh giá được các độ đo an toàn trước các tấn công mạnh nhất hiện nay. Lớp giữa là có cấu trúc kiểu mạng thay thế hoán vị 2-SPN (có 2 tầng phi tuyến được xen giữa bởi 1 tầng tuyến tính) như đã nêu trong chương 3. Lớp trong cùng là các hộp thế phi tuyến. Các hộp thế này được lựa chọn từ 2 hộp thế S1 và S2 đã được khảo sát trong chương 3 có các độ đo an toàn tốt tránh các kiểu tấn công đã khảo sát. Ngoài ra các phép hoán vị, phép dịch vòng được lựa chọn cẩn thận sao cho hệ mã có tính khuyếch tán ngẫu nhiên đều. Các phép biến đổi đầu vào và đầu ra đều lấy là phép XOR với khoá tương ứng.
- Phần lược đồ khoá, dùng để ngẫu nhiên một mầm khoá có độ dài 128-bit thành các khoá con đủ cho các vòng lặp và các phép biến đổi đầu vào và đầu ra. Phần lược đồ khoá cũng đã chú ý để tránh tấn công kiểu trượt khối, đồng thời sử dụng tối đa các hộp thế phi tuyến của phần ngẫu nhiên hoá dữ liệu.
- Mô hình mã, giải mã; các tham số cụ thể trong mô hình và lược đồ tạo khoá đã được trình bày trong chương. Các thông số an toàn lý thuyết và thực nghiệm đã chỉ ra rằng hệ mã khối MK_KC-01-01 đáp ứng được các yêu cầu an toàn và hiệu quả.

4.4 Phụ lục: Một số nghiên cứu về hàm băm và giao thức mật mã

Mở đầu Phụ lục là kết quả „Nghiên cứu thám mã MD4“. Trên cơ sở kết quả của Dobbertin đã công bố năm 1997, một thành viên tham gia đề tài đã tính lại các xác suất thành công, căn chỉnh lại một số công thức cho được chính xác, lập trình thực

hiện thuật toán tìm va chạm đối với MD4, đồng thời thực hành chạy trên máy Dell Power Edge 450 Mhz.

Trong phụ lục còn có trình bày lại 2 bài báo của các tác giả nước ngoài là „Va chạm vi sai của SHA-0“ và „Phân tích SHA-1 trong chế độ mã hoá“. Lý do 2 bài báo này được lựa chọn là vì: SHA-1 được phát triển trên cơ sở những cái tương tự trước đó là MD2, MD4, MD5, SHA-0 và SHA-1. Do SHA-0 có va chạm, cho nên nó đã được sửa thành SHA-1. Bài báo phân tích SHA-1 trong chế độ mã hoá đã cho thấy nó là một thuật toán mã hoá SHACAL dựa trên SHA-1 là một thuật toán tốt. Còn xét SHA-1 như một hàm băm thì sao? ít ra nó cũng đứng vững được 9 năm, cho tới đầu tháng 2 năm 2005, thì có 3 nhà mật mã học người Trung quốc đã tìm được thuật toán phá nó với thời gian nhanh hơn vét cạn, rất tiếc bài báo đầy đủ về thuật toán này chưa được công bố. Kết quả đột phá này được giới thiệu qua bài viết „Cập nhật thông tin về hàm SHA-1“.

Như tác giả Bruce Schneier viết ngày 18 tháng 2 năm 2005 sau sự kiện SHA-1 bị tấn công: „Các hàm băm là thành tố mật mã được hiểu biết ít, các kỹ thuật băm được phát triển ít hơn so với các kỹ thuật mã hoá“. Cho nên nhóm đề tài cũng chưa có được những nghiên cứu sâu sắc, bởi vì có nhiều kỹ thuật chưa được nhuần nhuyễn. Trong phụ lục cũng có trình bày lại 4 bài báo theo 3 hướng nghiên cứu về thiết kế các hàm băm, đó là: Phương pháp thiết kế các hàm băm dựa trên mã khối, Nguyên tắc thiết kế hàm băm , Hàm băm nhanh an toàn dựa trên mã sửa sai và Độ mật của hàm băm lặp dựa trên mã khối.

Cuối phụ lục là một nghiên cứu tổng quan về giao thức mật mã và trình bày một bài báo về giao thức STS. Đây là giao thức dựa trên giao thức Diffie-Hellman chuẩn nhưng được cải biên để chống lại tấn công người đứng giữa. Giao thức này đã được nhóm đề tài sử dụng để lập trình thực hiện giao thức trao đổi khoá phục vụ các phần mềm mã gói IP trên môi trường Linux.

5. Một số nội dung khác

5.1 Về tính sáng tạo, tính mới của các kết quả nghiên cứu thuộc Đề tài

Khi đăng ký thực hiện đề tài KC.01.01, đội ngũ những người nghiên cứu của Học viện Kỹ thuật Mật mã nói riêng và Ban Cơ yếu Chính phủ nói chung cũng đã có quan tâm tới bài toán bảo mật thông tin trên các mạng dùng giao thức IP nói riêng (và giao thức mạng nói chung), tới vấn đề đảm bảo tính chân thực của khoá công khai đi kèm với tính danh của người dùng nói chung (sao cho Public Key Of User A đúng là của A), nhưng có thể nói là chưa ở state-of-the-art. Các sản phẩm bảo mật thư tín điện tử nói riêng và các giải pháp bảo mật ở tầng ứng dụng nói chung đã được quan tâm tới từ rất sớm, còn các giải pháp bảo mật ở tầng IP thì mới đạt được những kết quả bước đầu. Vấn đề chứng chỉ số cũng vậy, chúng tôi chưa quan tâm tới những chuẩn của PKI như khuôn dạng chứng chỉ X.509, cách huỷ bỏ chứng chỉ,...

- Trên cơ sở sản phẩm phần mềm IP-Crypto v 1.0, Học viện KTMM đã tiếp tục nâng cấp hoàn thiện để có những ứng dụng thực tế.
- Trên cơ sở phần mềm cấp chứng chỉ số với mô hình sinh khoá tập trung, Ban CYCP cũng đã có đầu tư để cho ra sản phẩm với mô hình người dùng tự sinh cặp khoá bí mật/công khai (rồi gửi khoá công khai cho trung tâm ký). So với mô hình sinh khoá tập trung thì mô hình này phức tạp hơn.

- Trên cơ sở phát triển giải pháp can thiệp mật mã ở tầng DataLink trong môi trường Linux, bên cạnh sản phẩm DL-Cryptor của đề tài KC.01.01, một họ phần mềm bảo mật gói IP mới với giải pháp can thiệp mật mã vào tầng cầu (Bridge) đã ra đời. Phần mềm này có ưu điểm là mã được cả những gói tin IP-multicast (dùng cho Video Conferencing).
- Những cán bộ tham gia thực hiện đề tài KC.01.01 cũng đã nghiên cứu giải pháp can thiệp mật mã để bảo vệ gói IP ở tầng vật lý (can thiệp vào trình điều khiển card mạng). Bằng cách này có thể mở rộng ra việc bảo mật các môi trường truyền thông khác với Ethernet (như E1).

5.2 Về phương pháp nghiên cứu, báo cáo khoa học

- Trong quá trình nghiên cứu, chúng tôi đã *dựa vào hệ điều hành Linux nói riêng đi sâu khai thác các phần mềm có mã nguồn mở nói chung*. Mã nguồn mở là một điều kiện tốt để làm việc tích hợp mật mã. Trên cơ sở khai thác Linux, chúng tôi đã tạo ra sản phẩm bảo mật với giải pháp can thiệp mật mã ở tầng IP và DataLink. Bằng cách đi sâu vào tầng DataLink, sau này, chúng tôi đã tạo ra một dòng sản phẩm với giải pháp can thiệp mật mã ở tầng cầu, nó cho phép bảo mật các gói IP-multicast được dùng trong các ứng dụng Video Conferencing. Việc can thiệp mật mã ở tầng thấp hơn còn giúp chung tôi bảo mật được dữ liệu trong các môi trường khác với Ethernet (như E1) và không cứ phải dùng giao thức mạng IP. Giải pháp bảo mật dịch vụ Web thông qua SQUID Proxy Server cũng được thực hiện nhờ vào việc tận dụng mã nguồn mở.
- Các báo cáo khoa học đã được viết chi tiết, có các hình vẽ minh hoạ đi kèm giúp cho người đọc dễ nắm bắt được vấn đề (đối với một số phần mềm đó chính là các giao diện).

5.3 Những bài báo, những báo cáo kết quả nghiên cứu của đề tài

- Đề tài đã tham dự ICT IRDA'04 với 5 báo cáo:

Tt	Tên báo cáo	Tác giả
1	Linux Bridge và dùng Linux để bảo mật	KS Nguyễn Cảnh Khoa, TS Trần Duy Lai
2	Giới thiệu một phần mềm cung cấp chứng chỉ số	PGS TS Lê Mỹ Tú, KS Hoàng Văn Thức, KS Đinh Quốc Tiến
3	Một giải pháp bảo mật mạng tại tầng DataLink trong mô hình OSI	ThS Đặng Hoà, KS Nguyễn Quốc Toàn KS Nguyễn Cảnh Khoa
4	Khảo sát mã khối theo nhóm sinh của các hàm mã hoá	TS Lều Đức Tân
5	Một vài cải biên cho thuật toán sinh số nguyên tố theo Định lý Pocklington	TS Trần Duy Lai

- Một số kết quả nghiên cứu của KC.01.01 cũng đã được báo cáo trong Hội nghị khoa học năm 2002 của Học viện KTMM và giới thiệu trong Kỷ yếu các kết quả nghiên cứu của Học viện.

5.4 Về giá trị ứng dụng và triển vọng áp dụng kết quả KHCN

- Phần mềm IP-Crypto v1.0 đã được nâng cấp lên thành IP-Crypto 2.0 để cài đặt vào thiết bị chuyên dụng do Xí nghiệp M2 chế tạo trên nền một máy tính nhúng với hệ điều hành Linux đã được tối thiểu. Phần mềm này hiện nay đã được nâng cấp lên thành IP-Crypto v 3.0 có hỗ trợ chứng chỉ số để bảo mật 4 mạng LAN của Tổng cục An ninh- Bộ Công An.
- Phần mềm cung cấp chứng chỉ số đã được sử dụng thử tại Cục E15-Tổng cục VI- Bộ Công An với dịch vụ thư tín.
- Việc bảo mật dịch vụ WEB với chứng chỉ số cũng đã được dùng thử tại Cục Cơ yếu- BTTM (nhằm mở rộng các dịch vụ có hỗ trợ bảo mật trên trục mạng).

5.5 Về hiệu quả kinh tế và hiệu quả kinh tế xã hội:

- Các phần mềm bảo mật mạng dùng giao thức IP đang được mở rộng diện sử dụng (tại Bộ Công An, trước hết là 13 mạng LAN của Tổng cục An ninh; sau đó là 30 mạng LAN thuộc trung tâm chỉ huy; mạng của Chính phủ theo đề án 112;...)
- Hiện nay, Cục Quản lý Kỹ thuật Nghiệp vụ Mật mã- Ban Cơ yếu Chính phủ đang xây dựng dự án cung cấp chứng chỉ số cho khu vực Nhà nước. Vấn đề triển khai sử dụng chứng chỉ số trong khu vực dân sự cũng đang được nhiều cơ quan quan tâm (nhất là Bộ Bưu chính Viễn thông).

5.6 Đánh giá về kết quả đào tạo và những đóng góp khác của đề tài

- Sau đây là một số luận văn Cao học (chuyên ngành Kỹ thuật Mật mã) có liên quan đến đề tài KC.01.01 đã được hoàn thành:

tt	Tên luận văn	Người thực hiện/Đơn vị	Người hướng dẫn
1	Về một phương pháp bảo mật thư tín điện tử trên mạng Internet	Hoàng Thị Thu Hằng/ HVKTMM	PGS-TS Lê Mỹ Tú
2	Sinh tham số cho hệ mật RSA	Kiều Văn Hùng/ Cục V18-BCA	TS Lều Đức Tân
3	Tích hợp mật mã và kiểm soát hệ thống cho một hệ thư tín điện tử mã nguồn mở	Hoàng Văn Thức/ HVKTMM	TS Trần Duy Lai
4	Nghiên cứu đảm bảo vấn đề chứng thực trong các hoạt động thương mại điện tử	Đào Thị Hồng Vân/ HVKTMM	TS. Nguyễn Nam Hải

- Một số cán bộ trẻ đã tham gia thực hiện đề tài, đã có điều kiện làm việc và trưởng thành như Hoàng Văn Thức (cấp chứng chỉ số để dùng với Mail/Web), Nguyễn Cảnh Khoa (giải pháp bảo mật ở các tầng khác nhau), Trần Hồng Thái (thám mã khối và tìm va chạm của hàm băm), Nguyễn Quốc Toàn (tiếp cận với mật mã đường cong elliptic)

- Qua quá trình làm đề tài, những người làm đề tài cũng có kinh nghiệm hơn trong việc hình thành những đề tài nhánh trong một đề tài lớn.

Kết luận và kiến nghị

Đề tài KC.01.01 đã được thực hiện trong thời gian hơn 3 năm, tất cả các sản phẩm đăng ký đã được hoàn thành. Bốn nhóm sản phẩm (báo cáo khoa học, phần mềm, thiết bị) đã được hình thành, đó là: (1) những nghiên cứu tổng quan, tìm hiểu giải pháp; (2) các phần mềm bảo mật gói IP; (3) cung cấp và sử dụng chứng chỉ số; (4) đảm bảo toán học.

Một số sản phẩm của đề tài đã được Ban Cơ yếu tiếp tục đầu tư phát triển nâng cấp và đã có những ứng dụng thực tế mang lại hiệu quả thực sự và góp phần thúc đẩy quá trình thực hiện nhu cầu bảo mật thông tin trên các mạng của các đề án 112 của Chính phủ (trước hết là tại Bộ Công An). Những kết quả nghiên cứu đã đạt được của đề tài KC.01.01 đã được tiếp tục hoàn thiện để tạo ra những sản phẩm mới, ví dụ như phần mềm mã ở tầng cầu để bảo mật hội nghị truyền hình.

Trong một tương lai gần, thương mại điện tử và chính phủ điện tử sẽ phát triển mạnh ở nước ta. Đó là môi trường thuận lợi để cho những sản phẩm hỗ trợ PKI phát triển. Nhưng nó cũng làm nảy sinh một vấn đề hết sức quan trọng, đó là nhu cầu cần có một bộ chuẩn các thuật toán mật mã để dùng chung cho các sản phẩm đó. Đây là một công việc lớn, hiện đang được các cán bộ nghiên cứu đã thực hiện đề tài KC.01.01 nói riêng và đội ngũ cán bộ nghiên cứu trong Ban Cơ yếu Chính phủ nói riêng tập trung giải quyết.

Lời cảm ơn

Việc thực hiện đề tài KC.01.01 đã giúp cho nhiều sản phẩm quan trọng đối với Ngành Cơ yếu được hình thành nhanh hơn. Điều quan trọng nữa là, với đề tài KC.01.01, những người làm công tác nghiên cứu trong Ngành Cơ yếu đã có điều kiện tiếp cận với nhiệm vụ bảo mật các một loại hình thông tin mới, đó là các thông tin kinh tế xã hội, đáp ứng nhu cầu sử dụng sản phẩm mật mã cho các lĩnh vực không phải là an ninh quốc phòng. Đây là một công việc lớn, bởi vì bên cạnh các thông tin tác nghiệp của các cơ quan Đảng và Nhà nước (như chính phủ điện tử), còn có các thông tin phục vụ phát triển kinh tế của các doanh nghiệp, công ty,... Bên cạnh các giải pháp kỹ thuật, vấn đề này còn phụ thuộc vào các yếu tố khác như chính sách quản lý, các văn bản pháp qui khác,...

Nhóm đề tài xin chân thành cảm ơn Bộ Khoa học Công nghệ, Vụ Khoa học Các ngành Kinh tế Kỹ thuật, Ban Chủ nhiệm chương trình KC.01, GS TS Vũ Đình Cự (Chủ nhiệm chương trình KC.01) đã tạo điều kiện giúp đề tài được tiến hành.

Nhóm đề tài cũng chân thành cảm ơn các đồng chí Lãnh đạo Ban Cơ yếu Chính phủ, Học viện Kỹ thuật Mật mã và các cơ quan như Vụ Khoa học Công nghệ (Ban CYCP), Vụ Kế hoạch Tài chính (Ban CYCP), Phòng Quản lý Nghiên cứu Khoa học và Phòng Kế hoạch Tài chính của Học viện KTMM đã tạo điều kiện thuận lợi và có những đóng góp cho đề tài.

Tài liệu tham khảo

Quyển 1A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử

1. An Introduction to IPSEC, Bill Stackpole, *Information Security Management Hanbook*, 4th edition, Chapter 14, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause, 2000.
2. Tài liệu kèm theo phần mềm FreeS/WAN (http://www.freeswan.org)
3. Cohen, F., Managing network security- Part 14: 50 ways to defeat your intrusion detection system. *Network Security*, December, 1997, pp.11-14.
4. Crosbie, M. and Spafford, E.H., Defending a computer system using autonomous agents. *Proceedings of 18th National Information System Security Conference*, 1995, pp. 549-558.
5. Garfinkel, S. and Spafford, G., *Practical Unix and Internet Security,* O'Reilly & Associates, Inc., 1996.
6. Garfinkel, S. and Spafford, G., *Web Security & Commerce*, O'Reilly & Associates, Inc., 1997.
7. Herringshaw, C. Detecting attacks on networks. *IEEE Computer,* 1997, Vol, Vol. 30 (12), pp. 16-17.
8. Mukherjee, B., Heberlein, L. T., and Levitt, K.N., Network intrusion detection. *IEEE Network*, 1994, Vol.8 (3), pp.26-41.
9. Power Richard, Issues and Trends: 1999 CSI/FBI computer crime and security survey, *Computer Security Journal*, Vol.XV, No.2, Spring 1999.
10. Schultz, E.E. and Wack, J., Responding to computer security incidents, in M. Krause and H.F. Tipton (Eds.), *Handbook of Information Security*. Boston:Auerbach, 1996, pp.53-68.
11. Van Wyk, K.R., *Threats to DoD Computer Systems*. Paper presented at 23rd Information Integrity Institute Forum

Quyển 1B: Nước Nga và chữ ký điện tử số

1. C.U.Mfhbxtd, D.D. Ujyxfhjd, H.T.Cthjd, *Jcyjds cjdhtvtyyjq rhbgnjuhfabb, Vjcrdf*, Ujhzxfz kbybz-Ntktrjv, 2002, cnh. 96-98.
2. S. Even and O. Goldreich. *Des-like functions can generate the alternating group*. IEEE Transactions on Information Theory, 29(6):863-865, November 1983.
3. National Soviet Bureau of Standards. Information Processing Systems. Cryptographic Protection. Cryptographic Algorithm. *GOST 28147-89*, 1989.
4. J. P. Pierrzyk and Xian-Mo Zhang. *Permutation generators of alternating groups*. In Advances in Cryptology- AUSCRYPT'90, J.Sebery, J. Pieprzyk (Eds), Lecture Notes in Computer Science, Vol.453, pages 237-244. Springer Verlag, 1990.

Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã

1. FIPS 140-1 - *Security Requirements for Cryptographic Modules*., 1994 January 11.
2. Leon Adams., *Choosing the Right Architecture for Real-Time Signal Processing Designs*., White Paper., SPRA879 - November 2002.

3. Christof Paar., *Reconfigurable Hardware in Modern Cryptography*., ECC 2000 October 4-6., Essen, Germany.
4. Hagai Bar-El., *Security Implications of Hardware vs. Software Cryptographic Modules*., Information Security Analyst., October 2002.
5. Cryptology., http://www.cyphernet.org/cyphernomicon/5.html
6. Leon Adams., *Choosing the Right Architecture for Real-Time Signal Processing Designs*., SPRA879 - November 2002
7. Stephen Brown and Jonathan Rose., *Architecture of FPGAs and CPLDs: A Tutorial.,* Department of Electrical and Computer Engineering University of Toronto.
8. Khary Alexander, Ramesh Karri, Igor Minkin, Kaijie Wu, Piyush Mishra, Xuan Li., *Towards 10-100 Gbps Cryptographic Architectures*., IBM Corporation, Poughkeepsie, NY, 12601.
9. AJ Elbirt, C Paar., *Towards an FPGA Architecture Optimized for Public-Key Algorithms.,* Cryptography and Information Security Laboratory, Worcester, MA 01609.
10. Thomas Blum., *Modular Exponentiation on Reconfigurable Hardware*., Thesis., WORCESTER POLYTECHNIC INSTITUTE.
11. M. Shand and J. Vuillemin. *Fast implementations of RSA cryptography*. In Proceedings 11th IEEE Symposium on Computer Arithmetic, pages 252–259, 1993.
12. H.Orup. *Simplifying quotient determination in high-radix modular multiplication*., In Proceedings 12th Symposium on Computer Arithmetic, pages 193–9, 1995.
13. K. Iwamura, T. Matsumoto, and H. Imai. *Montgomery modular-multiplication., method and systolic arrays suitable for modular exponentiation*. Electronics and Communications in Japan, Part 3, 77(3):40–51, March 1994.
14. J.-P. Kaps. *High speed FPGA architectures for the Data Encryption Standard*., Master's thesis, ECE Dept., Worcester Polytechnic Institute, Worcester, USA, May 1998.
15. Ahmed Shihab, Alcahest; and Martin Langhammer, Altera., *Implementing IKE Capabilities in FPGA Designs*., Dec 05, 2003 URL: http://www.commsdesign.com/showArticle.jhtml?article-ID=16600061
16. Alexander Tiountchik, Institute of Mathematics, National Academy of Sciences of Belarus và Elena Trichina, Advanced Computing Research Centre, University of South Australia., *FPGA Implementation of Modular Exponentiation*.
17. Hauck, S. (1998). "*The Roles of FPGAs in Reprogrammable Systems*" Proceedings of the IEEE 86(4): 615-638.
18. Kris Gaj and Pawel Chodowiec., *Hardware performance of the AES finalists - survey and analysis of results*., George Mason University.
19. AJ Elbirt, W Yip, B Chetwynd, C Paar., *An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists*., ECE Department, Worcester Polytechnic Institute.
20. Kris Gaj and Pawel Chodowiec., *Comparison of the hardware performance of the AES candidates using reconfigurable hardware*., George Mason University.

21. Bruce Schneier, John Kelseyy, Doug Whitingz, David Wagnerx, Chris Hall, Niels Ferguson., *Performance Comparison of the AES Submissions.,* January 3, 1999.
22. J. P. Kaps and C. Paar, *Fast DES implementation on FPGAs and its application to a universal key-search machine*, in Fifth Annual Workshop on Selected Areas in Cryptography, vol. LNCS 1556, Springer-Verlag, August 1998.
23. O. Mencer, M. Morf, and M. J. Flynn, *Hardware Software Tri-Design of Encryption for Mobile Communication Units*, in Proceedings of International Conference on Acoustics, Speech, and Signal Processing, vol. 5, (New York, New York, USA).
24. K. H. Leung, K. W. Ma, W. K. Wong và P. H. W. Leong., *FPGA Implementation of a Microcoded Elliptic Curve Cryptographic Processor.,* Department of Computer Science and Engineering, The Chinese University of Hong Kong.
25. *M. Rosner Elliptic Curve Cryptosystems on reconfigurable hardware.,* Master's Thesis Worcester., Polytechnic Institute Worcester USA 1998.
26. G. Orlando and C. Paar., *A super-serial Galois field multiplier for FPGAs and its application to public key algorithms.,* Proceedings of the IEEE Symposium on Field-programmable custom computing machines., trang 232-239., 1999.
27. T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, B. Schott., *Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512*., Electrical and Computer Engineering, George Mason University, 4400 University Drive, University of Southern California - Information Sciences Institute.
28. Thomas Wollinger and Christof Paar., *How Secure Are FPGAs in Cryptographic Applications?*.,
Report 2003/119, http://eprint.iacr.org/, 5. June 2003
29. Ross Anderson Markus Kuhn., *Tamper Resistance - a Cautionary Note*., The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-9.
30. S Blythe, B Fraboni, S Lall, H Ahmed, U deRiu, *Layout Reconstruction of Complex Silicon Chips*, IEEE Journal of Solid-State Circuits v 28 no 2 (Feb 93) pp 138-145.
31. B. Dipert. *Cunning circuits confound crooks.,* http://www.einsite.net/ednmag/contents/images/21df2.pdf.
32. G. Richard., *Digital Signature Technology Aids IP Protection*., EETimes - News, 1998. http://www.eetimes.com/news/98/1000news/digital.html.
33. K.H. Tsoi, K.H. Leung and P.H.W. Leong., *Compact FPGA-based True and Pseudo Random Number Generators.,* Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin, NT Hong Kong.
34. V. Fischer and M. Drutarovsky. *True random number generator embedded in reconfigurable hardware*. Trong Proceedings Cryptographic Hardware and Embedded Systems Workshop (CHES), trang 415-430, 2002.

Quyển 2A: Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau.

1. *Network Layer Security*, Steven F. Blanding, Chapter 8, Information Security

Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause
2. *Transport Layer Security*, Steven F. Blanding, Chapter 9, Information Security Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause
3. *Application- Layer Security Protocols for Network*, Bill Stackpole, Chapter 10, Information Security Management Hanbook, 4th edition, Boca Raton-London-New York-Washington, editors Harold F.Tipton and Micki Krause

Quyển 3A: Sinh tham số an toàn cho hệ mật RSA

1. Lều Đức Tân, Một số thuật toán kiểm tra tính nguyên tố đối với một số lớp số. Luận án phó tiến sỹ khoa học toán lý, Hà nội 1994.
2. Ian Blanke, Gadiel Seroussi & Nigel Smart. Elliptic Curves in Cryptography. Cambridge Universty press 1999.
3. D. M. Gordon, Strong Primes Are Ease to Find, Advances in Cryptology-Proceedings of EUROCRYPT 84 (LNCS 209), 216-223, 1985.
4. Hans Riesel, Prime Number and Computer Methods for Factorization, Progress in Mathematics, 57, 1985.
5. R. L. Rivest and R. D. Silverman, Are Strong Primes Needed for RSA?
6. Robert D. Silverman, Fast Generation of Random, Strong RSA Primes. The Technical Newsletter of RSA Laborastories. Spring 1997.
7. N.M.Stephens, Lenstra's Factorisation Based On Elliptic Curves. Springer-Verlag 1998, pp. 409-416.

Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal

1. Douglas Robert Stinson, Mật mã Lý thuyết và Thực hành. Bản dịch tiếng Việt Hà nội 1995.
2. Lều Đức Tân. Một số thuật toán kiểm tra nhanh tính nguyên tố của các số trên một số lớp số. Luận án phó tiến sĩ Hà nội 1993.
3. Paulo Ribenboim. The Little Book of Big Primes. Springe-Verlag 1991

Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả

1. AES (nhiều tác giả*), Tuyển tập 15 hệ mã khối dự tuyển chuẩn mã tiên tiến (AES)*, Tài liệu từ Internet.
2. E. Biham, *New types of cryptanalytic attacks using related keys*, EUROCRYPT' 93, pp. 398-409.
3. A. Biryukov, D. Wagner, *Slide Attacks*, Fast Software Encryption, 1999, pp. 245-259.
4. A. Biryukov, D. Wagner, *Advanced Slide Attacks*, EUROCRYPT' 2000, pp. 589-606.
5. S. Burton, Jr. Kaliski, M.J.B. Robshaw*, Linear Cryptanalysis using Multiple Approximations,* CRYPTO'94, pp. 26-39.
6. G. Carter, E. Dawson, and L. Nielsen, *Key Schedules of Iterative Block Ciphers,* Tài liệu từ Internet, (10 trang).
7. F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Eurocrypt' 94, pp. 256-365.

8. C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naimi, Y. Zeng, *Comments on Soviet Encryption Algorithm GOST*, EUROCRYPT'94, pp. 433-438.
9. L. J. O'Conner and J. Dj Golic', *A unified markov approach to differential and linear cryptanalysis,* Asiacrypt, November 1994.
10. L. J. O'Conner**,** *Design Product Ciphers Using Markov Chain***,** Selected Area in Cryptography 1994.
11. L. J. O'Conner**,** *Convergence in Differential Distributions*, Crypto'95, pp.13-23.
12. I. I. Ghicman, A.V. Skorokhod, *Nhập môn về lý thuyết các quá trình ngẫu nhiên*, NXB "HAYKA", Maxcova 1977.
13. G. Hornauer, W. Stephan, R.Wernsdorf, *Markov Ciphers and Alternating Groups*, Eurocrypt'93, p.453-460.
14. T. Jacobsen, L.R. Knudsen, *Interpolation Attacks on the Block Cipher*, Fast Software Encryption, 1997, pp 28-40.
15. Y. Kaneko, F. Sano, K. Sakurai, *On Provable Security against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Mutiple Random Functions*, Tài liệu từ Internet, 15 trang.
16. J. Kelsy, B. Schneier, and D. Wagner, *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SEFER, and Triple-DES*, CRYPTO'96, pp 237-251
17. L. R. Knudsen, *Block Ciphers-Analysis, Design and Applications*, July, 1, 1994 (Ph. D Thesis).
18. L. R. Knudsen, *Practically secure Feistel ciphers*, Fast Software Encryption, 1993, pp. 211-221.
19. L.R. Knudsen, *New potentially "weak" keys for DES and LOKI*, EUROCRYPT' 94, pp. 419-424.
20. L. R. Knudsen, M.J.B. Robshaw, *Non-linear Approximations in Linear Cryptanalysis*, EUROCRYPT' 96, pp. 224-236.
21. M. Kwan, J. Pieprzyk, *A General purpose Technique for Locating Key Scheduling Weaknesses in DES-like Cryptosystems*, ASIACRYPT'91, pp. 237-246.
22. X. Lai, *On the Design and Security of Block Ciphers*, Hartung-Gorre Verlag Konstanz, 1995
23. X. Lai, J.L. Massey and S. Murphy, *Markov Ciphers and Differential cryptanalysis,* Eurocrypt' 91, pp.17-38.
24. M. Matsui, *New Block Encryption Algorithm MISTY*, Fast Software Encryption, 1997, FSE'97, pp. 54-68
25. M. Matsui, *New structure of block ciphers with provable security against differential and linear cryptanalysis*, Fast software Encryption, 1996, pp. 21-23.
26. M. Matsui, *Linear Cryptanalysic Method for DES Cipher*, EUROCRYPT' 93, pp. 386-397.
27. M. Matsui, *The First Experimental Cryptanalysic of the Data Encryption Standard*, CRYTO' 94, pp. 1-11.
28. S. Moriai, T. Shimoyama, T. Kaneko, *Interpolation Attacks of the Block Cipher: SNACK*, Fast Software Encryption, 1999, pp. 275-289.
29. K. Nyberg, *Differentially uniform mappings for cryptography*, EUROCRYPT'93, pp. 55-64, 1994.
30. K. Nyberg, *Linear Approximation of Block Ciphers,* Eurocrypt'94, pp.439-444.

31. K. Nyberg, L. R. Knudsen, *Provable security against a differetial cryptanalysis,* Journal of Cryptology, Vol. 8, pp. 27-37, 1995.
32. Savan Patel, Zulfikar Ramzan, and Ganapathy S. Sundaram, *Towards Making Luby-Rackoff Ciphers Optimal and Practical*, Fast Software Encryption, 1999, pp. 171-185.
33. Kenneth G. Paterson, *Imprimitive Permutation Groups and Trapdoor in Iterated Block Ciphers*, Fast Software Encryption, 1999, pp. 201-214.
34. T. Shimoyama, T. Kaneko, *Quadratic Relation of S-box and Its Application to the Limear Attack of Full Round DES*, CRYPTO'98, pp. 200-211.
35. J. Seberry, X. M. Zhang and Y. Zheng, *Relationships Among Nonlinearity Criteria*, EUROCRYPT'94, pp. 76-388, 1995.
36. D. R. Stinson, *Cryptography: Theory and Practice*, 1995 by CRC Press, Inc.
37. Nguyễn Duy Tiến, *Các mô hình xác suất và ứng dụng, Phần I- Xích Markov và ứng dụng,* NXB Đại học Quốc gia Hà Nội, 2000.
38. R.Wernsdorf, *The One-Round Functions of the DES Generate the Alternating Group*, Proc. Eurocrypt' 92, LNCS 658, 1993, pp. 99-112.

Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux

1. Glenn Herrin, Linux IP Networking-A Guide to the Implementation and Modification of the Linux Protocol Stack
2. Alan Cox, Network buffer and memory management

Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris

1. Streams programming Guide. *1995 Sun Microsystems.*
2. Solaris system administrators guide. *Janice Winsor - 1993 - Ziff-Davis Press Emryville, California*
3. Writing unix device drivers. *George pajari - Addison-Wesley Publishing Company, Inc - 1992*
4. TCP/IP Illustrated Volume 1. Volume2 , Volume 3. *Gary R. Wright - W. Richard Stevens, 1995- Addison-Wesley Publishing Company*
5. Network and internetwork security-Principles and practice. *William Stallings, Ph.D.,1995 by Prentice-Hall, Inc*
6. Computer Communications Security - Principles, Standard Protocols and Techniques. *Warwick Ford - PTR Prentice Hall - 1994*
7. Intenet & TCP/IP Network Security, Security Protocols and Applications -*1996 by The McGraw-Hill Companies, Inc*
8. Building Internet Firewalls. *D. Brent chapman and Elizabeth D. Zwicky - O' Reilly & Associates, Inc.*
9. Firewall complete, *1998 - Mc Graw - Hill*
10. UNIX Network programming Volume 1, *Network APIs: Sockets and XTI - W. Richard Stevents, 1998 Prentice - Hall, Inc*
11. Tài liệu chuyên đề về TCP/IP , *Phạm Văn Hải - Học viện KTMM*
12. http://www.freeswan.org/
13. RFC 2409 :The Internet Key Exchange (IKE)
14. RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
15. RFC 1825 : An overview of a security architecture

16. RFC 1826 : IP Authentication Header
17. RFC 1827 : IP Authentication Header
18. Các RFC khác về IPSEC và FreeS/WAN

Quyển 5A: An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux

1. Authentication HOWTO - Peter Hernberg
2. Shadow Password Howto - Michael H. Jackson mhjack@scnet.com
3. Security HOWTO
4. The Linux-PAM System Administrator's Guide, Adrew G. Morgan
5. Practical Unix Security - Simson Garfinkel and Gene Spafford
6. Các trang man getty(); mingetty(); login(); sulogin();
7. Text - Terminal HOWTO - David S. Lawyer dave@lafn.org
8. Solaris System Administration Guide, Chapter 12 -> Chapter 16
9. Software White Paper: Solaris Security, Tài liệu từ Internet

Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network hacker, Virut máy tính

1. William Stallings Ph.D. (1999), *Cryprography and Network security: Principles and Practice - Second edition*, Prentice -Hall, Inc.,USA.
2. VN-GUIDE, *Bảo mật trên mạng – Bí quyết và giải pháp – Tổng hợp và biên dịch*, Nhà xuất bản thống kê.
3. Các trang web: www.tinhat.com/internet_security/security_holes.html, www.tinhat.com/internet_security/improve.html, www.securityfocus.com, www.saintcorporation.com, www.sans.org, www.fbi.gov, www.cs.wright.edu, www.nessus.org, www.nai.com, www.linuxdoc.org/HOWTO/Secure-Programs-HOWTO.html, www.hackecs.com, www.auscert.org.au, www.securityfocus.com, www.l0pht.com, www.w3.org, www.rhino9.com, iss.net, www.insecure.org, www.cert.org, vnEpress.net, www.viethacker.net
4. Trần Thạch Tùng, *Bảo mật và tối ưu trong Red Hat Linux*, NXB Lao động – Xã hội
5. Edward Amoroso, *Fundamentals of Computer Security Technology*
6. E_book: *Hackers Handbook, State of the art Hacking tools and techniques, Vol 1, 2, 3.*
7. William Stallings Ph.D. (1999), Cryprography and Network security: Principles and Practice - Second edition, Prentice -Hall, Inc.,USA.
8. Các trang web: www.netbus.org, www.saintcorporation.com/products/saint_engine.html, www.rootshell.com, www.hackerjokes.de/, www.hackercracker.net/, www.crackerhttp/, www.hackerethic.org/, www.counter-hack.net/, www.inthehack.com/, www.eleganthack.com/, www.hack-net.com/, www.virtualcrack.com/
9. Ngô Anh Vũ, *Virus tin học huyền thoại và thực tế*, NXB Thành Phố Hồ Chí Minh.
10. Nguyễn Thành Cương, Hướng dẫn phòng và diệt virus máy tính , NXB thống kê
11. Nguyễn Viết Linh và Đậu Quang Tuấn, Hướng dẫn phòng chống virus trong tin *học một cách hiệu quả*, NXB trẻ.
12. Các trang web: www.viruslist.com/, www.norman.com, www.esecurityplanet.com, www.antivirusebook.com, www.waronvirus.com, www.hackertrickz.de

BCYCP
HVKTMM

BCYCP
HVKTMM

BAN CƠ YẾU CHÍNH PHỦ

Học viện Kỹ thuật Mật mã

Báo cáo Tóm tắt Tổng kết Khoa học và Kỹ thuật Đề tài:

NGHIÊN CỨU MỘT SỐ VẤN ĐỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN CHO CÁC MẠNG DÙNG GIAO THỨC LIÊN MẠNG MÁY TÍNH IP

TS Đào Văn Giá, TS. Trần Duy Lai

Hà Nội, 1-2005

BAN CƠ YẾU CHÍNH PHỦ
Học viện Kỹ thuật Mật mã

Báo cáo Tóm tắt Tổng kết Khoa học và Kỹ thuật Đề tài:

NGHIÊN CỨU MỘT SỐ VẤN ĐỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN CHO CÁC MẠNG DÙNG GIAO THỨC LIÊN MẠNG MÁY TÍNH IP

TS Đào Văn Giá, TS. Trần Duy Lai

Hà Nội, 1-2005

Tài liệu này được chuẩn bị trên cơ sở kết quả thực hiện
Đề tài cấp Nhà nước, mã số KC.01.01

Danh sách những người thực hiện

Nhóm thứ nhất : Các nghiên cứu tổng quan, tìm hiểu giải pháp

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	PGS TS Hoàng Văn Tảo	Học viện Kỹ thuật Mật mã
2	PGS TS Lê Mỹ Tú	Học viện Kỹ thuật Mật mã
3	TS Nguyễn Hồng Quang	Phân viện NCKTMM- HVKTMM
4	ThS Đặng Hoà	Phòng QLNCKH- HVKTMM
5	TS Nguyễn Nam Hải	Trung tâm Công nghệ Thông tin
6	TS Đặng Vũ Sơn	Vụ Khoa học Công nghệ
7	TS Trần Duy Lai	Phân viện NCKHMM- HVKTMM
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	ThS Nguyễn Ngọc Điệp	Phòng QLNCKH- HVKTMM
2	ThS Nguyễn Đức Tâm	Khoa Tin học- HVKTMM
3	ThS Nguyễn Đăng Lực	Phân viện NCNVMM- HVKTMM
4	ThS Đoàn Ngọc Uyên	Khoa Tin học- HVKTMM
5	ThS Nguyễn Anh Tuấn	Phân viện NCKHMM- HVKTMM
6	KS Lê Khắc Lưu	Phân viện NCKTMM- HVKTMM
7	ThS Đào Hồng Vân	Trung tâm Công nghệ Thông tin
8	KS Nguyễn Cảnh Khoa	Phân viện NCKHMM-HVKTMM
9	KS Nguyễn Công Chiến	Phòng QLNCKH-HVKTMM

Sản phẩm đã đạt được:

- 07 báo cáo khoa học (các quyển 1A, 1B, 1C, 2A, 2B, 5A và 5B)

Nhóm thứ hai: Các phần mềm bảo mật gói IP

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Nguyễn Nam Hải	Trung tâm Công nghệ Thông tin
2	TS Đặng Vũ Sơn	Vụ Khoa học Công nghệ
3	TS Trần Duy Lai	Học viện Kỹ thuật Mật mã
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	KS Nguyễn Cảnh Khoa	Phân viện KHMM- HVKTMM
2	KS Nguyễn Quốc Toàn	Phân viện KHMM- HVKTMM
3	KS Đinh Quốc Tiến	Phân viện KHMM- HVKTMM
4	KS Nguyễn Tiến Dũng	Trung tâm Công nghệ Thông tin
5	KS Nguyễn Thanh Sơn	Khoa Mật mã- HCKTMM
6	KS Nguyễn Như Tuấn	Khoa Mật mã- HVKTMM

Sản phẩm đã đạt được:

- 03 báo cáo khoa học (các quyển 3A, 3B và 3C)
- 05 phần mềm bảo mật gói IP (01 trên Windows; 01 trên Solaris; 03 trên Linux)

Nhóm thứ ba: Cung cấp và sử dụng chứng chỉ số

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Trần Duy Lai	Phân viện NCKHMM-HVKTMM
2	PGS TS Lê Mỹ Tú	Học viện Kỹ thuật Mật mã
3	ThS Đặng Hoà	Phòng QLNCKH-HVKTMM
4	TS Nguyễn Hồng Quang	Phân viện NCKTMM-HVKTMM
B	**Những người tham gia một trong các kết quả nghiên cứu**	
1	ThS Hoàng Văn Thức	Phân viện NCKHMM-HVKTMM
2	KS Phạm Văn Lực	Phân viện NCKHMM-HVKTMM
3	KS Cao Thanh Nam	Phân viện NCKTMM-HVKTMM
4	ThS La Hữu Phúc	Phân viện NCKTMM-HVKTMM
5	ThS Trịnh Minh Sơn	Phân viện NCNVMM-HVKTMM
6	ThS Hoàng Thu Hằng	Phân viện NCNVMM-HVKTMM

Sản phẩm đã đạt được:

- 04 báo cáo khoa học (các quyển 6A, 7A, 8A, 8B và 9A)
- 03 phần mềm (cấp và thu hồi chứng chỉ số, thư viện chữ ký số, bảo mật Web dùng Proxy Server)
- 01 thiết bị phần cứng để ghi khoá có giao diện USB

Nhóm thứ tư: Đảm bảo toán học

A	***Những người chủ trì một trong các kết quả nghiên cứu***	
1	TS Lều Đức Tân	Phân viện NCKHMM-HVKTMM
2	TS Trần Văn Trường	Phân viện NCKHMM-HVKTMM
B	***Những người tham gia một trong các kết quả nghiên cứu***	
1	TS Nguyễn Ngọc Cương	Phân viện NCKHMM-HVKTMM
2	KS Trần Hồng Thái	Phân viện NCKHMM-HVKTMM
3	ThS Trần Quang Kỳ	Phân viện NCKHMM-HVKTMM
4	ThS Phạm Minh Hoà	Phân viện NCKHMM-HVKTMM
5	KS Nguyễn Quốc Toàn	Phân viện NCKHMM-HVKTMM
C	***Cộng tác viên***	
1	TS Nguyễn Lê Anh	Đại học Xây dựng
2	TSKH Phạm Huy Điển	Viện Toán học

Sản phẩm đã đạt được:

- 03 báo cáo khoa học (các quyển 3A, 3B và 3C)
- 02 phần mềm (sinh tham số an toàn cho hệ mật RSA và Elgamal)

Mục lục

Lời mở đầu

Các nội dung mà đề tài đã tiến hành nhằm thực hiện 2 mục tiêu đã được đăng ký trong bản thuyết minh đề tài, đó là:

- Nghiên cứu một số công nghệ, giải pháp nhằm đảm bảo an toàn, an ninh thông tin cho các mạng dùng giao thức IP, từ đó đề xuất mô hình phù hợp đặc điểm sử dụng ở Việt Nam
- Phục vụ việc phát triển thương mại điện tử (TMĐT) của Việt Nam, hướng tới hội nhập khu vực

Sự phát triển của các mạng máy tính nói riêng và mạng Internet nói chung đã làm cho nhu cầu đảm bảo an ninh an toàn thông tin trên mạng ngày càng tăng. Có nhiều công nghệ mạng (ví dụ như Ethernet và Token Ring), có nhiều giao thức mạng (ví dụ như TCP/IP, IPX/SPX và NETBEUI,...), nhưng do sự phát triển vượt trội của giao thức IP so với các giao thức khác trên thế giới, và căn cứ vào đặc điểm công nghệ mạng được triển khai tại Việt Nam, chúng ta thấy rằng để có thể bảo đảm được an ninh an toàn cho hầu hết các dịch vụ mạng thì chỉ cần tập trung vào giải quyết các bài toán đối với giao thức IP. Nếu có giải pháp và sản phẩm bảo mật tốt cho môi trường IP, khi gặp phải các môi trường truyền thông khác chúng ta có thể dùng các thiết bị chuyển đổi (ví dụ như E1-IP) để sử dụng được các giải pháp và sản phẩm đã có.

Việt Nam đang trong quá trình hội nhập khu vực và hội nhập quốc tế. Thương mại điện tử chính là một công cụ đắc lực phục vụ cho quá trình hội nhập ấy. Ở trong nước cũng đang quá trình xây dựng chính phủ điện tử (đề án 112 của Chính phủ về Tin học hoá quản lý hành chính). Để cho thương mại điện tử cũng như chính phủ điện tử phát triển được đều cần có sự hỗ trợ của các công cụ/sản phẩm đảm bảo an ninh bảo mật thông tin trên các mạng truyền thông tin học.

Các sản phẩm của đề tài (báo cáo khoa học và phần mềm) đã đáp ứng đầy đủ các các nội dung đăng ký trong mục 16 „Yêu cầu khoa học đối với sản phẩm tạo ra“ của bản thuyết minh đề tài, cũng như bảng 2 „Danh mục sản phẩm khoa học công nghệ“ của bản hợp đồng thực hiện đề tài. Báo cáo khoa học của đề tài gồm 18 quyển như sau:

tt	Tên báo cáo
1	**Báo cáo cập nhật các kết quả mới trong lĩnh vực bảo mật mạng và thương mại điện tử:**
	Quyển 1A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử
	Quyển 1B: Nước Nga và chữ ký điện tử số
	Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã
2	**Mô hình bảo mật thông tin cho các mạng máy tính**
	Quyển 2A: Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau
	Quyển 2B: Tổng quan về an toàn Internet
3	**Nghiên cứu đảm bảo toán học**
	Quyển 3A: Sinh tham số an toàn cho hệ mật RSA
	Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal

	Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả
	Phụ lục: Một số nghiên cứu về hàm băm và giao thức mật mã
4	**Hệ thống phần mềm bảo mật mạng**
	Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux
	Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris
	Quyển 4C: Phần mềm bảo mật trên môi trường Windows
5	**An ninh, an toàn của các hệ điều hành mạng**
	Quyển 5A: An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux
	Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network Hacker, Virut máy tính
6	**Hệ thống cung cấp PKI**
	Quyển 6A: Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung
7	**Bộ chương trình cung cấp chữ ký điện tử**
	Quyển 7A: Một hệ chữ ký số có sử dụng RSA
8	**Hệ thống chương trình xác thực trong thương mại điện tử**
	Quyển 8A: Dùng chứng chỉ số với các dịch vụ Web và Mail
	Quyển 8B: Bảo mật dịch vụ Web thông qua Proxy Server
9	**Các sản phẩm nghiệp vụ và qui chế sử dụng**
	Quyển 9A: Một số thiết bị được sử dụng để ghi khoá

Các sản phẩm phần mềm/thiết bị bao gồm:

1	Phần mềm bảo mật gói IP: - Trên môi trường Windows (SECURE SOCKET) - Trên môi trường Linux (TRANSCRYPT, IP-CRYPTOR, DL-CRYPTOR)
2	Phần mềm về chứng chỉ số: - Sinh chứng chỉ số theo mô hình sinh khoá tập trung - Thư viện chữ ký số - Dùng chứng chỉ số để bảo mật dịch vụ Web thông qua Proxy Server
3	Phần mềm đảm bảo toán học: - Phần mềm sinh tham số an toàn cho hệ mật RSA - Phần mềm sinh tham số an toàn cho hệ mật Elgamal
4	Thiết bị nghiệp vụ: - Thiết bị ghi khoá với giao diện USB

TÓM TẮT CÁC NỘI DUNG NGHIÊN CỨU VÀ KẾT QUẢ CHÍNH

1. Nhóm thứ nhất: Nghiên cứu tổng quan, tìm hiểu giải pháp cho các cơ chế đảm bảo an ninh an toàn mạng

1.1 Quyển 1 A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử.

Các nội dung công việc đã được thực hiện là:

- Nghiên cứu về công nghệ IPSEC, đây là một trong các công nghệ tạo nên mạng riêng ảo (VPN), các dịch vụ IPSEC cho phép bạn xây dựng các đường hầm an toàn thông tin qua các mạng không tin cậy (ví dụ như Internet) với cả hai khả năng xác thực và bảo mật. Các vấn đề đã được đi sâu là: các đặc tính của IPSEC; các khái niệm cơ bản như AH, ESP,...; mô hình ứng dụng cùng với ưu nhược điểm của IPSEC
- Nghiên cứu về các hệ thống phát hiện xâm nhập. Vì các bức tường lửa và các chính sách an ninh an toàn là chưa đủ để ngăn chặn mọi tấn công phá hoại, cho nên cần đến hệ phát hiện xâm nhập (IDS - Intrusion Detection System). Các vấn đề sau đã được trình bày: Phát hiện xâm nhập là gì? Các giải pháp phát hiện xâm nhập; Những ưu điểm của IDS ? Những gì cần chú ý khi sử dụng IDS.
- Nghiên cứu tìm hiểu về thương mại điện tử với các nội dung: Các hình thức hoạt động chủ yếu của TMĐT; Tình hình phát triển TMĐT trên thế giới; Tình hình phát triển TMĐT ở Việt Nam; và các vấn đề an toàn trong TMĐT

Quyển 1B: Nước Nga và chữ ký điện tử số.

Ngày 10 tháng 1 năm 2002, tổng thống Nga V. Putin đã ký sắc lệnh liên bang về chữ ký điện tử số. Để đi tới Luật về chữ ký điện tử số, nước Nga đã có một quá trình chuẩn bị kỹ càng từ trước. Liên quan đến vấn đề này, trong báo cáo đã đề cập tới các nội dung sau:

- Bài viết "Những công nghệ hứa hẹn trong lĩnh vực chữ ký điện tử số" đề cập tới dự án chuẩn quốc gia mới của Nga về chữ ký số.
- Bài Chữ ký điện tử hay con đường gian khổ thoát khỏi giấy tờ" đã phân tích so sánh chữ ký số với chữ ký viết tay, khác với chữ ký viết tay, chữ ký số phụ thuộc vào văn bản được ký.
- Vậy nước Nga đã dùng chuẩn chữ ký số nào? Chúng tôi đã mô tả: (1) chuẩn chữ ký số GOST P 34.10-94 ; (2) chuẩn chứ ký số GOST P 34.10-2001; (3) chuẩn hàm băm GOST P.34.11-94; (4) chuẩn mã khối GOST 24187-89 (do chuẩn hàm băm GOST P.34.11-94 có sử dụng thuật toán GOST 24187-89)
- Trong báo cáo chúng tôi đã dịch toàn bộ „*Bộ luật Liên bang về chữ ký điện tử*" gồm 5 chương và 21 điều.
- Trong báo cáo cũng trình bày các thuật toán chuẩn chữ ký số, hàm băm, mã khối của Mỹ và 2 bài báo phân tích so sánh giữa thuật toán mã khối của Nga và thuật toán AES của Mỹ.

1.3 Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã.

Mật mã có thể thực hiện theo cách thủ công hoặc tự động với sự trợ giúp của máy móc. Trong thời đại điện tử, truyền thông và tin học ngày nay *các nguồn tin ngày càng đa dạng*; mọi *thông tin đều được số hóa* với khổng lồ trữ lượng tại chỗ và lưu lượng trên kênh; *đòi hỏi của người dùng ngày càng cao* về độ mật, tốc độ, độ an toàn, tính tiện dụng... Trong tình hình đó, chỉ có một lựa chọn duy nhất là thực hiện mật mã với sự trợ giúp của máy móc. Các nội dung nghiên cứu đã được thực hiện là:

- So sánh thực hiện mật mã bằng phần cứng và phần mềm và trả lời câu hỏi: nên thực hiện mật mã trên cơ sở phần cứng (hardware) hay phần mềm (software)? Đã so sánh về độ an toàn giữa 2 platform (sử dụng chung không gian nhớ RAM; đảm bảo toàn vẹn; thám ngược thiết kế; tấn công phân tích năng lượng; vấn đề lưu trữ khoá dài hạn; phụ thuộc vào độ an toàn của hệ điều hành) và *phân tích các ưu nhược điểm* của hai platform này
- Lựa chọn công nghệ cho cứng hoá mật mã. Với ngành mật mã, ngoài việc chọn công nghệ thích hợp cho *encryption*, cũng quan trọng không kém là công nghệ đó có bảo đảm *security* không. Các công nghệ đã được đưa ra xem xét là: (1) ASIC (2) ASSP (Application-Specific Standard Product); (3) Configurable Processor; (4) DSP (Digital Signal Processor); (5) FPGA (Field Programmable Gate Array); (6) MCU (Microcontroller); (7) RISC/GPP (Reduced Instruction Set Computer/ General Purpose Processor). Tiếp theo đã nghiên cứu về việc dùng FPGA để cứng hoá các loại thuật toán mật mã khác nhau, đó là: (1) sinh khoá dòng; (2) các phép nhân và modulo; (3) mã khối (AES); (4) mật mã elliptic; (5) hàm hash; (6) sinh số ngẫu nhiên.
- Các công việc/ kiến thức cần chuẩn bị để cứng hoá mật mã. Hai nội dung đã được trình bày. Trước hết là những kiến thức cần thiết để thực hiện FPGA bao gồm: kiến thức về toán; kiến thức về kỹ thuật; kiến thức về công nghệ; kiến thức về thị trường vi mạch. Thứ hai là các công cụ cần thiết để thực hiện FPGA bao gồm: công cụ thiết kế (CAD); thiết bị (máy tính, bộ nạp); nhân lực.

1.4 Quyển 2A: Giao thức TCP/IP và các giải pháp bảo mật ở các tầng khác nhau.

Chủ trì nhóm nghiên cứu: ThS. Đặng Hoà

Muốn nghiên cứu giải pháp bảo mật cho giao thức IP thì cần phải hiểu rõ nó. Chính vì vậy mà báo cáo khoa học gồm có 2 phần, phần I „Giao thức mạng TCP/IP“ gồm có 9 chương, phần II „Giải pháp bảo mật“ gồm có 3 chương dành cho 3 tầng: tầng mạng, tầng giao vận và tầng ứng dụng. Chú ý rằng, khái niệm tầng ở 3 chương cuối lại theo mô hình ISO. Các nội dung đã được đề cập đến bao gồm:

- Giới thiệu và khái quát về TCP/IP: nêu ra 4 đặc tính của TCP/IP; nó có các dịch vụ tiêu biểu ở tầng ứng dụng là thư điện tử, chuyển file, truy cập từ xa và www; các dịch vụ ở tầng mạng có thể chia làm 2 loại: dịch vụ không liên kết chuyển gói tin và dịch vụ vận tải dòng dữ liệu tin cậy
- Cấu trúc phân tầng của mô hình TCP/IP: nó có 4 tầng; tầng ứng dụng (Telnet, FTP,...); tầng vận tải (TCP, UDP,...); tầng Internet (IP) (hay còn gọi là tầng mạng); và tầng tiếp cận mạng (Ethernet, ATM,...). Trong tầng tiếp cận mạng cần chú ý việc chuyển đổi giữa địa chỉ IP và địa chỉ vật lý. Trong tầng Internet cần chú ý đến bài toán dẫn đường của gói tin (routing).

- Các địa chỉ Internet: đã trình bày về 5 lớp địa chỉ mạng là A, B, C, D và E. Khái niệm mạng con (subnet) đi kèm với khái niệm địa chỉ mạng và subnet mask. Cách đánh địa chỉ Internet cũng có một số nhược điểm.
- Giao thức ARP để giải quyết bài toán tương ứng địa chỉ Internet với địa chỉ vật lý. Đây là giải pháp giải quyết nhờ tương ứng động, trong mỗi thiết bị mạng sẽ có một cache giải quyết địa chỉ.
- Giao thức Internet chính là dịch vụ chuyển gói tin không liên kết (ở tầng mạng) Đã giới thiệu định dạng của gói tin IP (địa chỉ nguồn, địa chỉ đích, IHL, ...), có đi sâu vào một số trường như kích thước của gói tin, MTU và Fragmentation Offset. Một vài giao thức dẫn đường đã được điểm qua: GGP, EGP, BGP.
- Thảo luận về cơ cấu mà các cổng và các máy sử dụng để trao đổi sự điều khiển hoặc thông báo lỗi. Cơ cấu này được gọi là Giao thức Thông báo điều khiển Internet - Internet Control Message Protocol (ICMP). Giao thức này được coi là một phần của Giao thức Internet, và phải có trong mọi thực hiện của giao thức IP.
- Giao thức gói tin của người sử dụng UDP: định dạng của gói tin UDP, cách bọc gói tin UDP vào gói tin IP. Một cách khái niệm, toàn bộ việc phân cổng và hợp cổng giữa phần mềm UDP và chương trình ứng dụng xảy ra qua cơ chế cổng.
- Giao thức điều khiển truyền tin TCP: nêu lên 5 tính chất của TCP. Phải có một cơ chế giúp cho TCP cung cấp sự tin cậy, đó là xác nhận và truyền lại, đó là các cửa sổ trượt, thiết lập một liên kết TCP. Báo cáo cũng trình bày về khái niệm cổng của TCP, định dạng của đoạn TCP.
- Hệ thống tên vùng: trình bày về các tên vùng quen thuộc như GOV, EDU, COM,..,; tương ứng giữa tên vùng và địa chỉ.
- Đề cập tới An toàn tầng mạng: Network-Layer Security Protocol (NLSP) được công bố trong ISO/IEC 11577. Trong NLSP có hai giao diện: giao diện dịch vụ NLSP và giao diện dịch vụ mạng cơ sở (UN-underlying network).

Mô hình bảy tầng ISO

7	Tầng ứng dụng	PEM, S-HTTP, SET
6	Tầng trình diễn	
5	Tầng phiên	SSL
4	Tầng giao vận	IPSEC
3	Tầng mạng	PPTP, swIPe
2	Tầng liên kết dữ liệu	VPDN, L2F, L2TP
1	Tầng vật lý	Fiber Optics

- Transport Layer Security Protocol (TLSP) được mô tả ở chuẩn ISO/IEC 10736. Nó được đặt hoàn toàn trong tầng giao vận. TLSP được thiết kế để bổ sung vào các giao thức tầng giao vận thông thường mà không phải để thay đổi chúng.
- Các giao thức an toàn tầng ứng dụng của các mạng gồm 3 lĩnh vực: Trao đổi tiền tệ (SET); Gửi thông báo điện tử (PEM, RIPEM, S/MIME, PGP) và Các giao dịch

www (SSL, S-HTTP)

1.5 Quyển 2B: Tổng quan về an toàn Internet.

Internet với chi phí thấp và tồn tại ở mọi nơi đã làm cho các ứng dụng thương mại điện tử trở nên khả thi. Thế nhưng, các rủi ro khi sử dụng Internet có thể gây ra hiện tượng nản chí. Các nội dung đã được nghiên cứu xem xét là:

- An toàn Internet với các vấn đề sau: An toàn mạng với IPSEC; bức tường lửa; Các khía cạnh của An toàn dịch vụ gửi tin; trình bày về 6 ứng dụng có bảo mật là PEM, MIME, S/MIME, PGP, X.400 và MSP ; An toàn web với SSL, S-HTTP và Phần mềm có khả năng tải xuống (Java Applet hay ActiveX); An toàn đối với các ứng dụng thương mại điện tử (EDI, SET,..); đặc biệt có đề cập đến Các thoả thuận của các nhà cung cấp dịch vụ Internet
- Phần nghiên cứu về „Nhu cầu thực tế về bảo mật " đã đề cập tới: Tình hình phát phát triển của CNTT trên thế giới; Tình hình phát triển CNTT trong nước; Mô tả kết quả mạng của Bộ Tài chính (tuy rằng số liệu tương đối cũ). Có thể nói tóm lại, với sự triển khai của các đề án 112 và 47 thì nhu cầu bảo mật các dịch vụ mạng trong nước ta ở thời điểm này là rất lớn.

1.6 Quyển 5A : An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux.

Phần „An toàn của hệ điều hành Linux" đã nghiên cứu về:

- Tổng quan về Linux Security: Phương pháp bảo vệ vật lý; An toàn tài khoản truy nhập; An toàn file và hệ thống file; An toàn mật khẩu; Dùng mật mã; An toàn giao diện đồ hoạ; An toàn nhân và An toàn mạng.
- Đi sâu nghiên cứu vấn đề Login và xác thực người dùng: đã mô tả chi tiết về quá trình đăng nhập (từ khi dấu nhắc login cho tới khi xác thực xong và hệ thống đưa ra dấu nhắc shell), phương pháp xác thực người dùng cũng như cách quản lý người dùng trên hệ thống Linux. Trình bày về một công nghệ là PAM (Pluggable Authentication Modules), đó là các thư viện chia sẻ (shared libraries), cho phép người quản trị hệ thống lựa chọn cách xác thực người dùng. Nói cách khác, ta không phải biên dịch lại các ứng dụng sử dụng PAM (PAM-aware), và vẫn có thể chuyển đổi cách xác thực khác nhau.

Phần „An ninh của hệ điều hành Sun Solaris" đã nghiên cứu về:

- Giới thiệu và đánh giá khả năng an toàn của Solaris với 4 mức bảo vệ: (1) Điều khiển đăng nhập; (2) Điều khiển truy nhập tài nguyên hệ thống (3) Các dịch vụ phân tán an toàn và những nền tảng phát triển; (4) Điều khiển truy nhập tới mạng vật lý
- Quản lý hệ thống an toàn bao gồm 4 vấn đề: (1) Cho phép truy nhập tới hệ thống máy tính; (2) An toàn file; (3)An toàn hệ thống và (4) An toàn mạng
- Các tác vụ an toàn file đã mở đầu bằng việc trình bày về các tính năng an toàn file: các lớp người dùng; các quyền đối với file; các quyền đối với thư mục; các quyền đặc biệt; umask mặc định. Sau đó đã mô tả chi tiết các thao tác để: hiển thị thông tin về file; thay đổi quyền sở hữu file; thay đổi các quyền đối với file; ...

- Các tác vụ an toàn hệ thống: đã chỉ dẫn từng bước để hiển thị trạng thái đăng nhập của người dùng; hiển thị những người dùng không có mật khẩu; vô hiệu hoá tạm thời đăng nhập của người dùng; lưu lại những cuộc đăng nhập thất bại; ...
- RPC an toàn là cách thức xác thực xác nhận cả máy chủ và người dùng. RPC an toàn dùng xác thực hoặc Diffie-Hellman hoặc Kerberos. Cả hai cơ chế xác thực này dùng mã DES. Môi trường NFS dùng RPC an toàn và được hiểu như NFS an toàn. Cả hai kiểu xác thực Diffie-Hellman và Kerberos version 4 đều được hỗ trợ. PAM cung cấp cách thức để "tải vào" các dịch vụ xác thực và đảm bảo trợ giúp nhiều dịch vụ xác thực
- Mô tả cách dùng công cụ tăng cường an toàn tự động (ASET- Automated Security Enhancement Tool) để giám sát hoặc hạn chế truy nhập tới các file hệ thống và các thư mục. ASET có 3 mức an toàn và có cả thảy 7 tác vụ. Có 2 cách chạy ASET: trực tuyến hoặc định kỳ

Phần III „An ninh của các hệ điều hành họ Microsoft Windows“ đã nghiên cứu về:
- Nhắc lại mô hình lập mạng trong môi trường Windows. Mạng được hình thành gồm có hai phần chính và client và server. Có hai mô hình lập mạng : mô hình nhóm làm việc (workgroup model) và mô hình miền (domain model). Sau đó đã đánh giá khái quát về an ninh an toàn của hai môi trường là Windows9x vàWindowsNT.
- Đề cập đến vấn đề hết sức kinh điển, đó là mật khẩu. Cần phân biệt mật khẩu Windows 9x với mật khẩu WinNT. Mật khẩu WinNT có dùng DES làm hàm một chiều, còn Win2000 ngầm định sử dụng giao thức thẩm định quyền Kerberos v5.
- Đối với „Phân quyền đối với thư mục, tệp” đã trình bày về các hệ thống file có trong họ Windows, bao gồm: FAT, NTFS, CDFS, HPFS. Phân quyền đối với thư mục và tệp thực chất là bảo mật các tài nguyên mạng thông qua permission chia sẻ.
- Đã trình bày các tính năng an toàn của NTFS.

1.7 Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network hacker, Virut máy tính. Chủ trì nhóm nghiên cứu: TS. Đặng Vũ Sơn

Phần I „Khả năng an toàn của các hệ điều hành mạng“ đã trình bày về:

- Tổng quan về hệ điều hành : Hệ điều hành là gì? Phân loại hệ điều hành; Lịch sử phát triển của hệ điều hành; 6 yêu cầu chuẩn tắc đánh gia hệ thống máy tính tin cậy và 4 cấp đánh giá.
- Cơ chế an toàn của hệ điều hành gồm có 3 vấn đề an toàn chung đối với các tất cả các hệ điều hành mạng, đó là: An toàn truy nhập mạng; An toàn hệ thống và An toàn file và thư mục
- Trình bày về một số các lỗ hổng an toàn của hệ điều hành Windows, của với hệ điều hành Unix. Các lỗ hổng có thể đến từ: (1) hệ điều hành và các ứng dụng; (2) do người sử dụng; (3) do người lập trình. Một số hệ điều hành có lỗ hổng về mật mã (ví dụ như FTP daemon của Unix)
- Phụ lục có giới thiệu Nessus là một phần mềm giám sát an ninh mạng. Đã giới thiệu cách cài đặt, cấu hình, chạy khai thác chương trình kèm theo file nhật ký kết quả chạy trình.

Phần II „Network hacker“ gồm có:

- Trả lời câu hỏi „Hacker là ai?“ và phân loại hacker.
- Nêu ra qui trình 9 bước để hack. Hacker hoạt động hiểu quả là do: cấu hình sai máy chủ, lỗi trong các ứng dụng, nhà cung cấp thiếu trách nhiệm, thiếu người có trình độ.
- Đã liệt kê ra những lỗi của hệ điều hành mà hacker có thể khai thác. Có đưa ra một ví dụ thực hiện tấn công hệ thống Unix.
- Trả lời câu hỏi là: có thể sử dụng mật mã để chống hacker hay không? Mật mã có thể dùng vào 2 việc: bảo vệ mật khẩu và mã dữ liệu được lưu trữ.
- Đã nêu ra 3 nguyên nhân khiến người ta quan tâm tới việc bảo vệ thông tin trên Internet, đó là: bảo vệ dữ liệu, bảo vệ tài nguyên mạng, bảo vệ danh tiếng của cơ quan. Đã nêu ra một hướng dẫn bảo mật cho hệ thống gồm 6 bước
- Phụ lục giới thiệu phần mềm giám sát an ninh mạng SNORT. Đây là một Network IDS.

Phần III „Virut máy tính“ viết về các vấn đề sau:
- Tổng quan về virus máy tính: trả lời câu hỏi „virus máy tính là gì“ và phân loại virus.
- Đối với B-virus đã trình bày về cơ chế lây lan của nó. B-virus có thể chia ra Single B-Virus và Doublr B-Virus. Đã trình bày về cấu trúc của một B-virus (gồm 4 phần) và các đặc tính của nó (tính tồn tại duy nhất, tính thường trú,...)
- Đối với F-virus đã xét đến 2 môi trường là DOS và Win32. Đối với các virus trên DOS đã đề cập đến: phương pháp lây lan; phân thành 2 loại (Transient File Virus và Resident File Virus); Cấu trúc của TF-virus và RF-virus;Cũng như B-virus, một F-virus có các yêu cầu: tính tồn tại duy nhất, tính lây lan,...
- Đã đề cập tới việc lây nhiễm virus trên mạng LAN và Internet.
- Liệu có thể dùng mật mã để phát hiện và phòng chống virus hay không? Đối với B-virus thì mật mã không phòng chống được, còn đối với F-virus thì có thể phòng chống bằng cách đổi tên file. Có thể dùng chữ ký số để phát hiện file bị virus.
- Phụ lục là một danh sách các loại virus tiêu biểu cùng với mô tả của chúng: Nimda, Code Red, Chernobyl,...

2. Nhóm thứ hai: Các sản phẩm bảo mật gói IP trên các môi trường Linux, Solaris và Windows

2.1 Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux.

Báo cáo gồm 2 phần. Phần I có tên là „Lập trình mạng trong Linux“ có 2 chương. Chương 1 là „Mạng IP trong Linux“ và chương 2 là „Lập trình mạng trong Linux“. Phần II „Các sản phẩm bảo mật gói IP“ có 4 mục. Ba mục A, B và C trình bày về 3 phần mềm TRANSCRIPT, IP-CRYPTO và DL-CRYPTO. Mỗi mục A, B và C đều có 2 chương, chương đầu giới thiệu về giải pháp và chương thứ hai giới thiệu về sản phẩm phần mềm. Riêng mục thứ tư là mục D có 2 chương trình bày về giải pháp mật mã bao gồm : mã dữ liệu bằng mã khối và trao đổi khoá tự động.

Phần I „Lập trình mạng trong Linux“ đã nghiên cứu các vấn đề sau:
- Chồng giao thức (protocol stack) là một phần trong kernel code, nó gồm có

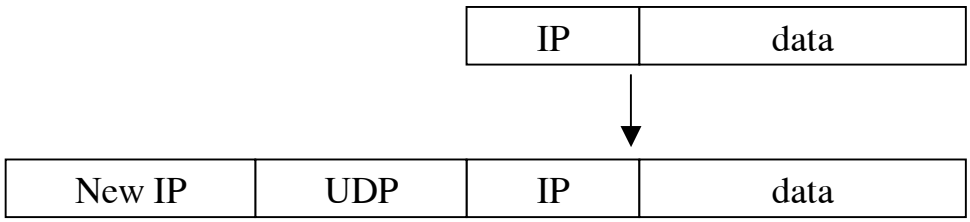
SOCKET layer, INET layer, TCP/UDP layer, IP layer, Network device layer.
- Cấu trúc và các lệnh làm việc với socket buffer. File /proc/net/route chứa Forwarding Information Base.
- Trình bày tổng quát về quá trình khởi tạo mạng khi hệ điều hành khởi động, cách sử dụng trình ifconfig và route để thiết lập kết nối mạng, các thủ tục có liên quan.
- Trình bày về quá trình kết nối, các bước để gửi dữ liệu, các bước để nhận dữ liệu, các bước của IP Forwarding, Internet Routing Protocol.
- Trình bày chi tiết về sk_buffs, Các thủ tục hỗ trợ mức cao hơn.
- Dành một dung lượng lớn để trình bày về thiết bị mạng
- Trong phần này cũng có đề cập đến IP-multicasting và các thủ tục hỗ trợ Ethernet.

Nghiên cứu kỹ, nắm chắc cách xử lý gói tin mạng trong Linux *là nhân tố quyết định* để có thể thực hiện thành công các giải pháp can thiệp mật mã nhằm bảo mật gói tin được truyền trên mạng.

Phần II „Các sản phẩm bảo mật gói IP“

A. Phần mềm TRANSCRYPT

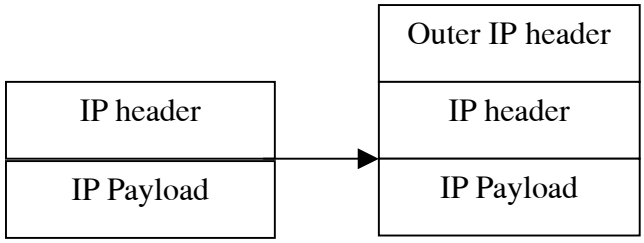
Transcrypt dựa trên phần mềm CIPE (Crypto IP Encapsulation). Các công việc đã được làm là: khai thác làm chủ hoạt động của hệ thống và thay đổi phần mật mã (bao gồm thuật toán mã dữ liệu và toàn bộ phần trao đổi khoá). Transcrypt “bao bọc” các gói tin IP (đã được mã hoá) bởi các gói tin UDP và gửi chúng bằng kỹ thuật UDP thông thường. Đây là sự khác biệt với việc bao bọc IP trong IP. Trong báo cáo đã trình bày về việc mã hoá gói tin và trình trao đổi khoá Kex.

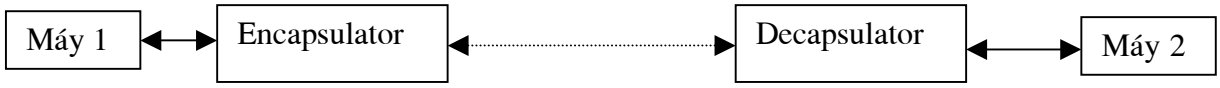


Đã trình bày về mã nguồn của Transcrypt, cách biên dịch và cài đặt, cách thiết lập cấu hình và cách chạy chương trình (gồm các bước nạp module và chạy chương trình daemon transcryptd.

B. Phần mềm IP-CRYPTO

Phần mềm IP-CRYPTO phỏng theo FreeS/WAN nhưng chỉ hỗ trợ một mode tunnel với những thuật toán mật mã được thay thế (mã dữ liệu và trao đổi khoá). Phần trình bày về giải pháp bảo mật của IP-CRYPTO đã đề cập đến: Kỹ thuật tạo card mạng ảo và cách gửi gói tin qua card mạng ảo; Cách nhận gói tin mạng trong nhân Linux; Chế độ đường hầm (tunnel mode), Encapsulating Security Payload Packet Format và Phân tích chương trình nguồn của quá trình gửi và nhận gói tin trong IP-Crypto





Trong báo cáo đã trình bày về mã nguồn và bộ cài đặt của IP-Crypto; cách biên dịch và cài đặt nó; cách thiết lập cấu hình (gồm có cấu hình mạng, trao đổi khoá thủ công, trao đổi khoá tự động, sử dụng trình keyingd); mô hình chạy thử nghiệm.

C. Phần mềm DL-CRYPTOR

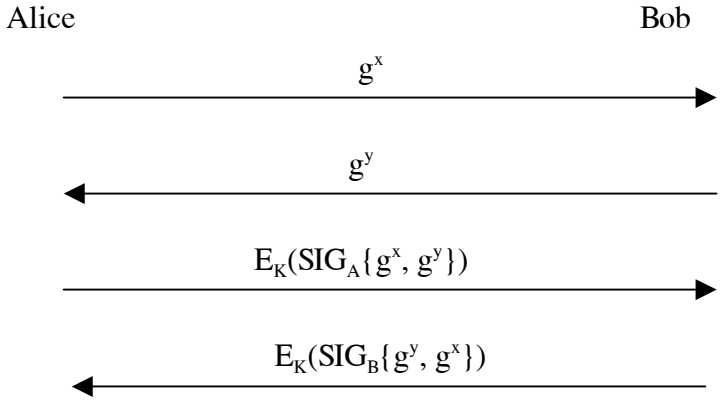
Trình bày về giải pháp can thiệp mật mã. Trong nhân linux việc gửi và nhận gói tin mạng được chứa trong cấu trúc chứa gói tin struct sk_buff. Ta thấy trong nhân linux việc gửi và nhận gói tin ở tầng data link được thực hiện nhờ hai hàm là dev_queue_xmit() trong trường hợp gửi gói tin đi và net_bh() trong trường hợp nhận gói tin. *Khi gói tin được truyền đi, hàm dev_queue_xmit() sẽ thực hiện việc mã hoá và sang bên nhận hàm net_bh() sẽ thực hiện việc giải mã*. Như vậy, đối với các giao thức mạng ở tầng cao hơn (ví dụ, giao thức tầng mạng IP) ở hai máy là trong suốt.

Trong báo cáo đã trình bày về mã nguồn của DL-Cryptor, cách biên dịch và cài đặt, cách thiết lập cấu hình và 2 chế độ làm việc của DL-Cryptor (trao đổi khoá thủ công và tự động).

D. Giải pháp mật mã

Chương 1 „Mã dữ liệu bằng mã khối“ đã trình bày về 2 chế độ làm việc của mã khối được dùng đến trong khi mã gói IP là OFB (Output Feedback Mode) và CBC(Cipher Block Chaining Mode).

Chương 2 „Trao đổi khoá tự động“ đã trình bày về giao thức trao đổi khoá STS (Station-To-Station), nó có ưu điểm là chống lại được tấn công người đứng giữa. Giao thức STS đã được cải tiến để trở thành giao thức STS đối xứng như sau:



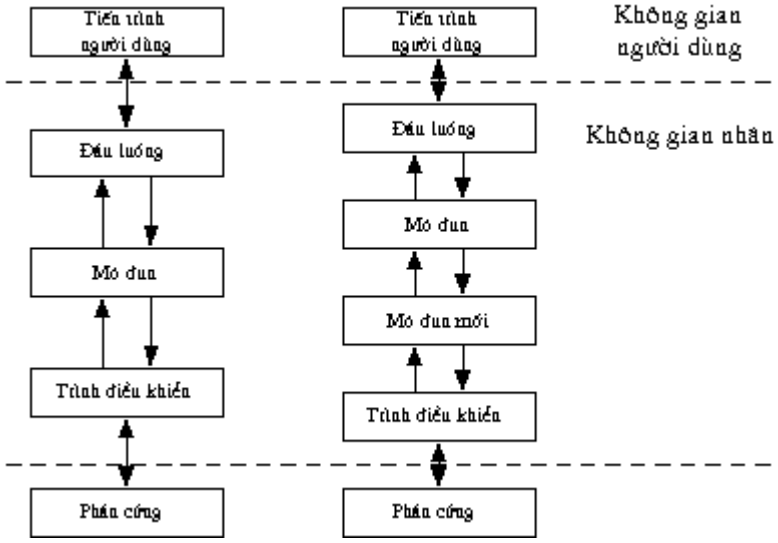
Trong chương này đã trình bày về việc lập trình giao thức STS đối xứng để được trình trao đổi khoá Kex, cách sử dụng trình Kex và đặc biệt là việc dùng trình trao đổi khoá đi kèm với 3 phần mềm bảo mật là Transcrypt, IP-Crypto và DL-Cryptor.

2.2 Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris.

Đây là một giải pháp bảo mật đã được nghiên cứu trong Ban Cơ yếu. Do đầu tư của đề tài KC.01.01, kết quả này đã được hoàn thiện, đặc biệt là nội dung của chương 4 đã được thực hiện thêm. Tuy vậy, về mặt tài liệu thì báo cáo vẫn được viết thành 4 chương, trong đó 3 chương đầu nhằm giới thiệu cách tiếp cận dùng công nghệ lập trình STREAMS để can thiệp mật mã vào Solaris.

Trong báo cáo đã trình bày về *giải pháp, cách tiếp cận, phương pháp nghiên cứu* :

- STREAMS là phần bổ xung mới đây tới kiến trúc của nhân (kernel) UNIX. Cốt lõi của mô hình STREAMS là nó được cài đặt giống như chồng giao thức.
- Các thành phần của luồng gồm: các hàng đợi (queue); các thông báo (message); các module; các trình điều khiển (driver).
- Các thao tác trên luồng gồm: open, read, write, close,...
- Các thông báo là phương tiện truyền thông trong luồng.
- Trong STREAMS các trình điều khiển được mở (opened) và các mô đun được chèn vào (pushed). Có ba kiểu của trình điều khiển thiết bị: Trình điều khiển phần cứng (Hardware Driver); Trình điều khiển ảo (Pseudo Driver); Trình điều khiển đa luồng (Multiplexer Driver). Trong báo cáo đi sâu vào việc xây dựng đa luồng STREAMS TCP/IP.



Mô hình STREAMS

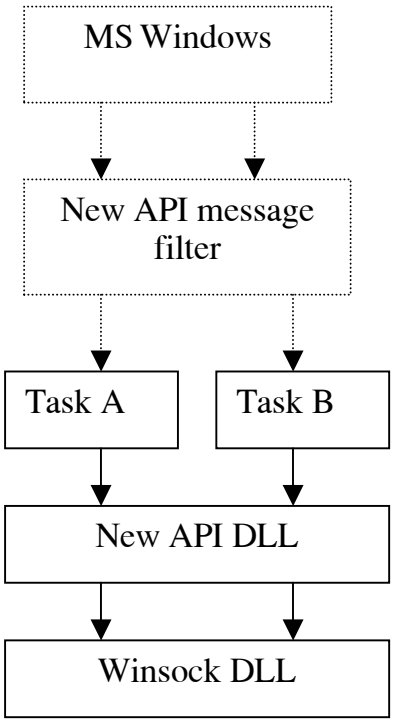
Đã nghiên cứu giải pháp bắt gói IP để thực hiện việc mã hoá trong mô hình STREAMS TCP/IP là xây dựng và chèn tầng lọc gói IPF thêm vào. Để tiết kiệm về mặt thiết bị, chúng ta nên tích hợp nút mã hoá với Router lọc gói.

Về mặt thực hành, nhóm nghiên cứu đã khảo sát khả năng ngăn chặn của một số phần mềm hacker của bộ phần mềm IPSEC_SUN, đó là: Sniffit V.0.3.5, IPSCAN, Packetboy, ICMP_Bomber. Bên cạnh đó, nhóm nghiên cứu cũng khảo sát ảnh hưởng của bộ phần mềm IPSEC_SUN đối với thời gian truyền dữ liệu của dịch vụ FTP và so sánh với FreeS/WAN.

2.3 Quyển 4C: Phần mềm bảo mật trên môi trường Windows.

Trong điều kiện của nước ta là một nước phụ thuộc hoàn toàn vào công nghệ nhập

ngoại thì vấn đề an toàn cũng cần phải được nghiên cứu sao cho phù hợp với hoàn cảnh của chúng ta. Làm thế nào vừa tận dụng được sức mạnh của các hệ thống phần mềm thương mại hiện nay nhưng vẫn kiểm soát được mức độ an toàn của thông tin trên mạng là một trong những vấn đề đáng được quan tâm.



Nội dung nghiên cứu phần này nhằm mục đích nghiên cứu xây dựng giải pháp bảo vệ thông tin trên các mạng máy tính được xây dựng trên nền tảng mô hình mạng Winsock. Mô hình mạng Winsock là một mô hình mạng được phát triển mạnh mẽ sử dụng rộng rãi ngày nay. Do vậy định hướng nghiên cứu vào mô hình này là cần thiết và có ý nghĩa thực tiễn.

Giải pháp và kỹ thuật được sử dụng: Toàn bộ dòng thông tin trên mạng trong các Platform Windows đều chuyển qua Winsock. Vấn đề đặt ra là làm thế nào để có thể khống chế được dòng thông tin này để phục vụ cho các mục tiêu riêng biệt. Can thiệp trực tiếp vào các Modul trong Winsock là một việc làm khó có thể thực hiện được bởi đối với những người phát triển ứng dụng thì Winsock chỉ như một chiếc hộp đen. Chúng ta chỉ có thể biết được giao diện với Winsock mà thôi. Vậy cách tiếp cận là như thế nào. Chúng tôi tiếp cận theo kiểu xây dựng một API mới trên Windows Socket API. Dòng thông tin trước khi chuyển qua Winsock sẽ qua một tầng mới do ta xây dựng và ở tầng này chúng ta có thể khống chế được dòng thông tin mạng. Các chủ đề đã được nghiên cứu là:

- Mô hình Winsock: 3 thành tố của mô hình mạng Winsock, đó là (1) Winsock application; (2) Network system; (3) Winsock API. Một liên kết giữa Client và Server trong mô hình Winsock gồm 5 thành phần: Giao thức, địa chỉ IP của Client, số hiệu cổng của Client, địa chỉ IP của Server, số hiệu cổng của Server. Socket có trạng thái, trạng thái hiện thời của socket xác định các phép toán mạng nào sẽ được tiếp tục, các phép toán nào sẽ bị treo lại và những phép toán mạng nào sẽ bị huỷ. Có hai kiểu socket: Datagram Socket và Stream socket.
- Thiết kế xây dựng socket an toàn: Nhóm nghiên cứu phát triển giao diện tại tầng giao vận cho truyền thông TCP/IP được gọi là Secure Socket để phục vụ cho mục tiêu nén và mã hoá dữ liệu truyền qua Internet và các mạng PSTN. Secure Socket được cài đặt tại các trạm, Server và trong FireWall để đảm bảo an toàn và truyền thông tốc độ cao giữa trạm và các máy trạm. Secure Socket cung cấp giao diện lập trình ứng dụng Winsock chuẩn cho các ứng dụng TCP/IP chẳng hạn như Web Browser, telnet, ftp mà không bất kỳ sự thay đổi nào đối với các trình ứng dụng và TCP/IP. Có một vài cách để chặn các lệnh của Winsock : Thay thế các địa chỉ hàm; Thay đổi thông tin liên kết; Đổi tên thư viện Winsock. Nhóm đề tài đã chọn cách thứ 3 để thực hiện.

3. Nhóm thứ ba: Cung cấp và sử dụng chứng chỉ số

3.1 Quyển 6A: Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung.

Trên nền của phần mềm có mã nguồn mở OpenCA, chúng tôi đã xây dựng một hệ thống cấp chứng chỉ với mô hình đơn giản: trung tâm sinh cặp khoá và chỉ có RootCA. Để phục vụ cho quy mô nhỏ, có thể chúng ta không cần đến cả máy RA. Những nội dung đã được trình bày bao gồm:

- Giới thiệu tổng quan về PKI, về CA, RA, X.509 v 3 certificate, certification paths, revocation; Sau đó đi vào trình bày cách cài đặt và vận hành máy CA.
- LDAP server được dùng cho việc lưu trữ chứng chỉ số còn hiệu lực hay đã bị huỷ bỏ sao cho việc khai thác sử dụng được tiện lợi. Người ta thường dùng LDAP Server để làm việc này, mặc dù về mặt nguyên tắc có thể dùng một database server bất kỳ. Các cài đặt, cấu hình và vận hành máy LDAP Server đã được trình bày.
- Mô tả Qui trình phát hành chứng chỉ số gồm 6 bước công việc sau: (1) Nhập thông tin về người được cấp; (2) Ký yêu cầu cấp chứng chỉ; (3) Chuyển đổi định dạng của chứng chỉ; (4) Cấp chứng chỉ cho người dùng; (5) Cập nhật chứng chỉ vừa phát hành lên LDAP server; (6) In nội dung chứng chỉ.
- Mô tả Quy trình huỷ bỏ chứng chỉ số gồm các bước công việc sau: (1) Huỷ bỏ một chứng chỉ bởi người quản trị; (2) Phát hành CRL và cập nhật lên LDAP; (3) Tải CRL từ máy LDAP về máy phục vụ; (4) In chứng nhận huỷ bỏ chứng chỉ cho người sử dụng.

3.2 Quyển 7A: Một hệ chữ ký số có sử dụng RSA

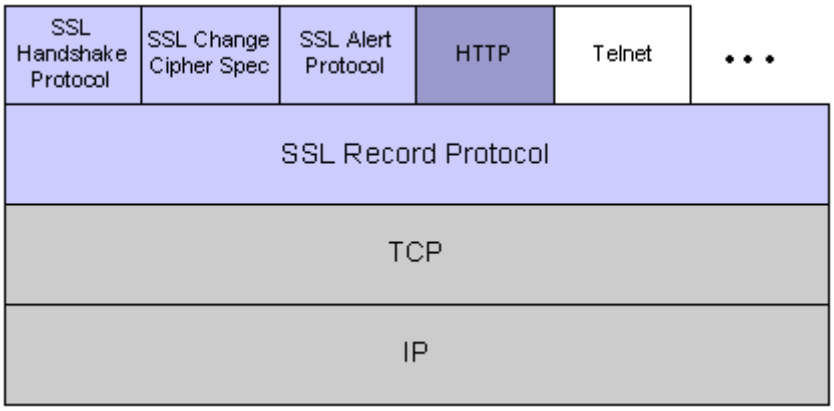
Đối với nhiều loại dữ liệu thì tính xác thực đôi khi lại cần hơn tính bảo mật. Mật mã khoá công khai đã giải quyết được bài toán xác thực bằng hệ chữ ký số (với sự trợ giúp của hàm băm). Có nhiều thuật toán chữ ký số, nhưng RSA là một thuật toán quen thuộc và nó có trong chuẩn của nhiều nước, nhiều tổ chức quốc tế. Thế nhưng dùng đúng thuật toán chữ ký số RSA không phải là một việc dễ. Bên cạnh việc lựa chọn tham số sao cho an toàn, chúng ta còn phải chú ý tới cách chuẩn bị dữ liệu để ký, chứ không phải cứ việc „luỹ thừa với số mũ là khoá bí mật“ là xong. Trong việc chọn tham số an toàn thì không chỉ có p và q, mà còn có cả e và d nữa. Có một điều cần chú ý là tiêu chuẩn an toàn đối với RSA mã khác với RSA ký. Các nội dung dã được nghiên cứu là:

- Chữ ký số dựa trên mật mã hiện đại đã đề cập tới một số cái mang tính lý thuyết, đó là: Chữ ký số từ hệ mã có thể đảo ngược; Lược đồ chữ ký số cùng với appendix; Lược đồ ký khôi phục thông báo; Điểm qua các kiểu tấn công trên lược đồ ký; Hàm băm (để ký được nhanh).
- Lược đồ chữ ký số RSA: đã điểm qua các tấn công đối với chữ ký RSA. Trong tài liệu trình bày thuật toán ký theo PKCS#1 phiên bản 1.5, đây chưa phải là chuẩn ký dùng RSA tốt nhất. Chuẩn ký tốt nhất dùng RSA là RSA-PSS trong PKCS#1 phiên bản 2.1.
- Module thực hiện ký và kiểm tra chữ ký số sử dụng chứng chỉ số: trình bày một số công nghệ có liên quan tới việc tạo ra chữ ký theo chuẩn và module thực hiện việc ký và kiêm tra một tệp dữ liệu có sử dụng chứng chỉ số.

3.3 Quyển 8A: Dùng chứng chỉ số với các dịch vụ Web và Mail.

Các vấn đề được đi sâu nghiên cứu bao gồm:

- Giao thức Secure Socket Layer là cái cần hiểu rõ bởi vì đây chính là giải pháp để bảo mật giao dịch giữa Web Server và Web Client. SSL v3 gồm có SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Specification và SSL Alert Protocol. Đối với Application data, SSL Record Protocol thực hiện 3 việc: phân mảnh dữ liệu (frame); (2) nén dữ liệu (3) mã hoá và tạo MAC rồi chuyển xuống tầng TCP. Các tham số mật mã liên quan đến một phiên liên lạc được thực hiện thông qua SSLv3 Handshake Protocol. Trong báo cáo đã trình bày cụ thể quá trình thực hiện SSLv3 Handshake qua các bước giữa client/server. Ở cuối chương có trình bày cách tính khoá cho phiên liên lạc.

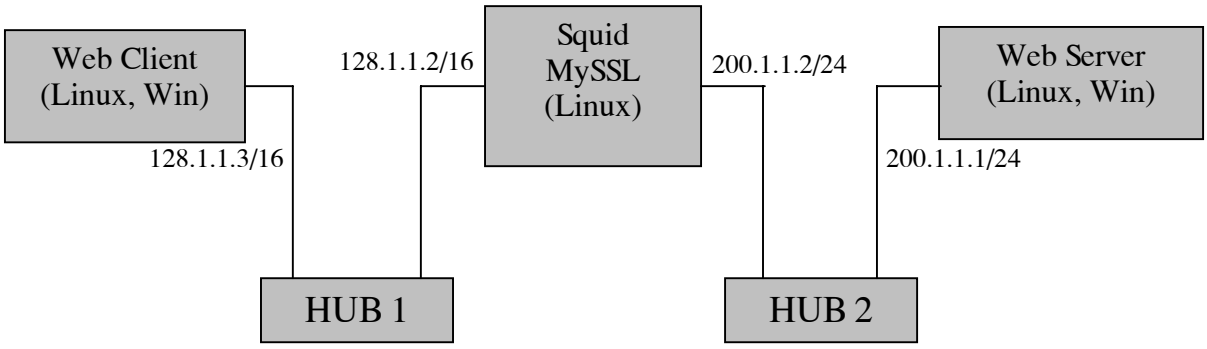


- Đã trình bày các thao tác để sử dụng chứng chỉ số với dịch vụ Web: Cài đặt chứng chỉ cho trình duyệt Web; Cập nhật CTL và CRL từ Public Database Server; Cài đặt và thiết lập cấu hình cho phần mềm E-shop có sử dụng chứng chỉ trên Apache Server; Sử dụng lệnh https để truy nhập tới E-shop bằng IE hoặc Netscape.
- Trình bày cách đưa chứng chỉ số vào trình thư tín Outlook Express, cách dùng chứng chỉ số để mã hoá và xác thực thư, cách cập nhật các CRL.

3.4 Quyển 8B: Bảo mật dịch vụ Web thông qua Proxy Server.

Các nội dung đã được nghiên cứu là:

- SQUID Proxy Server: Tệp cấu hình squid.conf khá phức tạp. Chúng ta quan tâm tới những lựa chọn hỗ trợ SSL, đó là https_port và ssl_unclean_shutdown.
- MySSL nhận được từ OpenSSL sau khi thực hiện các công việc sau: Loại bỏ những phần mã nguồn không sử dụng đến; Loại bỏ giao thức SSL v2; Loại bỏ các thuật toán mã có sẵn, thay vào đó là thuật toán Mã khối của Ngành CY; Loại bỏ các thuật toán băm trừ MD5 và SHA-1; Loại bỏ các thuật toán ký, trừ RSA; Loại bỏ chương trình sinh số nguyên tố xác suất, thay vào đó là thuật toán sinh tham số RSA an toàn.
- Trình duyệt MyBrowser nhận được từ Mozzila 1.0 bằng cách thu gọn, kiểm soát và tích hợp mật mã riêng vào.Trong tài liệu có trình bày cách biên dịch ra MyBrowser.
- Mô hình bảo mật dịch vụ web thông qua Proxy như sau:



3.5 Quyển 9A: Một số thiết bị được sử dụng để ghi khoá.

Các nội dung đã được đề cập đến là:

- Giới thiệu thiết bị iKey của hãng Rainbow Technologies. Đã trình bày các bước nhằm dùng iKey để lưu chứng chỉ số và khoá bí mật, đó là: khởi tạo định dạng cho iKey; thiết lập tên cho iKey; khởi tạo (hay đặt lại) vùng lưu chứng chỉ số; thay đổi mật khẩu; lưu chứng chỉ số. Sau đó là cách đăng ký chứng chỉ số với các ứng dụng như IE và Outlook Express.

- Đã trình bày việc thiết kế, xây dựng một loại thiết bị nghiệp vụ có giao diện USB. Sơ đồ khối tổng quát của thiết bị gồm có 3 khối: khối giao diện, khối vi xử lý và khối nhớ. Khối giao diện sử dụng linh kiện IC USB FT245 BM của hãng FTDI. Khối vi xử lý sử dụng linh kiện AT89C2051 của hãng Atmel. Khối nhớ sử dụng linh kiện AT24C64 của hãng Atmel

4. Nhóm thứ tư: Đảm bảo toán học

4.1 *Quyển 3A: Sinh tham số an toàn cho hệ mật RSA.*

Mật mã khoá công khai cần có số nguyên tố lớn, nhưng chỉ „lớn“ không thì chưa đủ. Không phải số nguyên tố nào cũng dùng cho mật mã khoá công khai được một cách nói chung và cho một hệ mật cụ thể nào đó nói riêng (ví dụ như RSA hay Elgamal).

- Đã đề cập đến 4 tiêu chuẩn cho số nguyên tố dùng cho RSA của chuẩn X9.31 (đây là một chuẩn của các tổ chức tài chính Mỹ). Trên cơ sở 4 tiêu chuẩn đó, cùng với việc xét các tấn công phân tích số bằng phương pháp sàng trường số, tấn công phân tích số dựa vào đường cong elliptic, phương pháp phân tích số $p\pm1$ của Williams, tấn công kiểu giải hệ phương trình và phân tích số dựa vào $\gcd(p\pm1, q\pm1)$, nhóm nghiên cứu đã đưa ra hệ tiêu chuẩn của mình với những ngưỡng cụ thể.
- Xây dựng phần mềm sinh số nguyên tố dùng cho hệ mật RSA bắt đầu bằng các định lý Pocklington và Lucas, trên cơ sở đó các hàm PocklingtonPrimeTest, LucasPrimeTest và LucasPocklingtonPrimeTest được xây dựng. Tiếp đó, thuật toán sinh số nguyên tố bằng phương pháp tăng dần độ dài được trình bày về mặt lý thuyết có đánh giá số lần dãn trung bình và mật độ số nguyên tố sinh được theo cách này. Thuật toán

StrongPrimeGenerator (theo kiểu của Gordon) đã được xây dựng để sinh số RSA-mạnh. Lực lượng các số RSA-mạnh được sinh theo thuật toán StrongPrimeGenerator đã được đánh giá về mặt lý thuyết. Hàm RSA-Generator đã được thiết kế để sinh ra những cặp số nguyên tố cần thiết.

4.2 *Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal.*

Nhóm nghiên cứu đã hoàn thành các công việc sau:

- Giải quyết vấn đề số nguyên tố mạnh dùng ở đâu và cụ thể hơn là điểm ra 3 ứng dụng chủ yếu trong mật mã đó là *bài toán bảo mật tin* dùng hệ mật Elgamal, *bài toán xác thực tin* theo sơ đồ chữ ký Elgamal và *bài toán thoả thuận khoá* theo sơ đồ Diffie-Hellman. Đặc điểm chung của các loại hình trên là tính an toàn của chúng đều được coi là tương đương với tính khó giải của bài toán logarit trên trường GF(p).
- Trình bày một phương pháp sinh số nguyên tố bằng cách tăng dần độ dài hoàn toàn dựa vào định lý Pocklington. Về mặt lý thuyết thì bất cứ một số nguyên tố nào cũng có thể được sinh từ phương pháp của chúng tôi tất nhiên với khả năng không như nhau. Quan trọng hơn cả trong việc đưa ra thuật toán này là nó có thể sinh các số nguyên tố dùng trong hệ mật Elgamal một cách rất hiệu quả.
- Đi vào giải quyết vấn đề xây dựng cơ sở lý thuyết của thuật toán và hiện thực hoá bằng một chương trình sinh số nguyên tố mạnh trên một lớp số nguyên cụ thể: giới thiệu về lớp Lp(k) với đầy đủ việc đánh giá về lực lượng số nguyên tố trong lớp và thuật toán sinh các số nguyên tố trong đó, trên cơ sở đó xây dựng thuật toán sinh các số nguyên tố mạnh và gần mạnh. Trình bay các thủ thuật tính toán trên các số lớn , nhằm hiện thực hoá được thuật toán đã chỉ ra ở trên.
- Phụ lục "Một số kết quả thử nghiệm", nhằm giới thiệu một số kết quả thử nghiệm gồm: Một số kết quả thống kê thu được về thời gian sinh trung bình cùng mật độ trung bình của số nguyên tố mạnh và gần mạnh; Ví dụ về các số nguyên tố Pepin, Sophie.

4.3 Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả.

Chương 1 „Mở đầu về mã khối“ giới thiệu chung về mô hình toán học của hệ mã khối khoá bí mật. Để đảm bảo tính hiệu quả một hệ mã khối cần phải có cấu trúc đều, đối xứng mã/dịch và các thành phần của nó cũng phải dễ dàng trong quá trình cứng hoá hay chương trình hoá mức cao. Chương này cũng đã giới thiệu một số cấu trúc mã khối cơ bản như cấu trúc đối xứng thuận nghịch Feistel, cấu trúc truy hồi Matsui, cấu trúc cộng-nhân Massey...và một số thuật toán mã khối cụ thể để minh hoạ như thuật toán GOST của Liên bang Nga, thuật toán IDEA.

Chương 2 „Thám mã khối“ :Một số những công việc quan trọng khởi đầu cho quá trình thiết kế xây dựng mã khối là cần thiết nghiên cứu những phương pháp thám mã khối điển hình, từ đó rút ra những đặc trưng an toàn cơ bản của một hệ mã khối. Chương này tập trung nghiên cứu lý thuyết về các phương pháp thám mã khối cơ bản như thám mã vi sai, thám mã vi sai bậc cao, thám mã tuyến tính và các dạng đặc biệt của thám mã tuyến tính, thám mã nội suy, thám mã khoá quan hệ.. chủ yếu áp dụng trên chuẩn mã dữ liệu DES. Về mặt lý thuyết chúng tôi chỉ nêu những nguyên tắc thám mã cơ bản đối với mã khối (dựa trên chuẩn mã dữ liệu DES) mà không trình bày chi tiết thuật toán (vì có thể tìm thấy trong nhiều tài liệu khác). Phần thực hành,

chúng tôi tập trung nghiên cứu khai thác phương pháp thám mã phi tuyến dựa trên ý tưởng thám mã tuyến tính để xây dựng thuật toán thám hệ DES rút gọn 8-vòng nhằm tìm đủ 56 bít khoá của chúng.

Chương 3 „Khảo sát hệ mã khối an toàn theo các đặc trưng độ đo giải tích“. Như chúng ta đã biết mô hình chung phổ biến của một hệ mã khối gồm hai phần: phần ngẫu nhiên hoá dữ liệu và phần lược đồ tạo khoá cho hệ mã. Phần ngẫu nhiên hoá dữ liệu gồm các cấu trúc cơ bản đã giới thiệu trong chương 1, có thể thấy nó thường chứa ba lớp: các hộp thế (lớp trong cùng), hàm vòng (lớp giữa) và cấu trúc mã-dịch (lớp ngoài cùng). Phần lược đồ khoá cũng sẽ được giới thiệu ở cuối chương, nó có thể gồm lược đồ on-line (tính cùng quá trình mã-dịch), hay off-line (tính trước quá trình mã-dịch), hoặc là lược đồ khoá độc lập với phần ngẫu nhiên hoá dữ liệu hay phụ thuộc phần ngẫu nhiên hoá dữ liệu. Để cho hệ mã là an toàn chống được các tấn công đã nêu, cần phải thiết kế xây dựng các hộp thế, hàm vòng và nghiên cứu lựa chọn cấu trúc mã-dịch sao cho hạn chế tối đa các tấn công phân tích mã hoặc vô hiệu hoá các phương pháp thám mã cụ thể. Đồng thời lược đồ khoá phải tránh được các quan hệ khoá đơn giản hoặc tránh các sự tương tự giữa các công đoạn tạo khoá...

Chương 4 „Khảo sát mã khối theo nhóm sinh của các hàm mã hoá“. Việc tìm các tính yếu của một hệ mã khối căn cứ vào những đặc tính cụ thể của nhóm sinh của các hàm mã hoá của hệ mã để trên cơ sở đó hình thành nên những tiêu chuẩn khi thiết kế xây dựng các hệ mã khối an toàn. Công lao chủ yếu của chúng tôi đưa ra trong bài này là đưa ra các kết quả liên quan đến khái niệm t-phát tán và t-phát tán mạnh cùng với ý nghĩa mật mã của chúng. Qua các kết quả đã đưa ra cũng toát lên một vấn đề rất thực tế đó là mọi tính yếu về nhóm các phép thế có ảnh hưởng đến tính an toàn của hệ mật thì việc loại bỏ chúng chỉ là cần thiết vì rất dễ khắc phục các khuyết tật hình thức trên nhóm sinh (chỉ bằng cách bổ xung vào tập các hàm mã hoá cùng lắm là 2 hàm đơn giản) trong khi bản chất mật mà chỉ phụ thuộc vào chính tập các hàm mã hoá.

Chương 5 „Khảo sát các đặc trưng của mã khối theo quan điểm xích Markov“. Các hệ mã khối hiện tại đều thuộc dạng thuật toán mã hoá tiến hành lặp đi lặp lại một hàm (thường được gọi là hàm vòng). Hai phương pháp tấn công rất nổi tiếng đối với loại mã khối này là tấn công vi sai và tấn công tuyến tính như đã nói trong chương 2. Hiệu quả của hai phương pháp này được thể hiện trên các phương diện sau đây: tập các cặp rõ, và các cặp mã tương ứng (trong tấn công vi sai), tập các cặp rõ/ mã tương ứng (trong tấn công tuyến tính) có độ lớn là bao nhiêu thì xác suất thành công của người mã thám đủ cao? Khi có tập này rồi thì thời gian tiến hành có thực tế hay không? Khả năng thực tế trong việc thu thập tập hợp này? Đối với người lập mã, các câu hỏi thường được đặt ra như sau: Hàm vòng phải được thiết kế như thế nào để các công thức ở trên đúng với xác suất bé? Số vòng lặp tối thiểu phải là bao nhiêu để khiến cho lực lượng cần thiết của tập rõ/mã làm nản lòng các nhà mã thám? Việc nghiên cứu mã khối trên quan điểm xích Markov đã giúp các nhà mật mã trả lời các câu hỏi đó trên những điểm lớn, khái quát.

Chương 6: Xây dựng thuật toán mã khối MK_KC-01-01. Trong chương này chúng tôi thiết kế một thuật toán mã khối cụ thể đảm bảo các thông số an toàn, hiệu quả phục vụ cho đề tài:

- Trước hết, phần ngẫu nhiên hoá dữ liệu được xây dựng theo cấu trúc 3 lớp: trong, giữa và ngoài cùng. Lớp ngoài cùng chúng tôi chọn cấu trúc Feistel có thể đánh giá được các độ đo an toàn trước các tấn công mạnh nhất hiện nay. Lớp giữa là

có cấu trúc kiểu mạng thay thế hoán vị 2-SPN (có 2 tầng phi tuyến được xen giữa bởi 1 tầng tuyến tính) như đã nêu trong chương 3. Lớp trong cùng là các hộp thế phi tuyến. Các hộp thế này được lựa chọn từ 2 hộp thế S1 và S2 đã được khảo sát trong chương 3 có các độ đo an toàn tốt tránh các kiểu tấn công đã khảo sát. Ngoài ra các phép hoán vị, phép dịch vòng được lựa chọn cẩn thận sao cho hệ mã có tính khuyếch tán ngẫu nhiên đều. Các phép biến đổi đầu vào và đầu ra đều lấy là phép XOR với khoá tương ứng.

- Phần lược đồ khoá, dùng để ngẫu nhiên một mầm khoá có độ dài 128-bit thành các khoá con đủ cho các vòng lặp và các phép biến đổi đầu vào và đầu ra. Phần lược đồ khoá cũng đã chú ý để tránh tấn công kiểu trượt khối, đồng thời sử dụng tối đa các hộp thế phi tuyến của phần ngẫu nhiên hoá dữ liệu.
- Mô hình mã, giải mã; các tham số cụ thể trong mô hình và lược đồ tạo khoá đã được trình bày trong chương. Các thông số an toàn lý thuyết và thực nghiệm đã chỉ ra rằng hệ mã khối MK_KC-01-01 đáp ứng được các yêu cầu an toàn và hiệu quả.

4.4 Phụ lục: Một số nghiên cứu về hàm băm và giao thức mật mã

Mở đầu Phụ lục là kết quả „Nghiên cứu thám mã MD4“. Trên cơ sở kết quả của Dobbertin đã công bố năm 1997, một thành viên tham gia đề tài đã tính lại các xác suất thành công, căn chỉnh lại một số công thức cho được chính xác, lập trình thực hiện thuật toán tìm va chạm đối với MD4, đồng thời thực hành chạy trên máy Dell Power Edge 450 Mhz.

Trong phụ lục còn có trình bày lại 2 bài báo của các tác giả nước ngoài là „Va chạm vi sai của SHA-0“ và „Phân tích SHA-1 trong chế độ mã hoá“. Lý do 2 bài báo này được lựa chọn là vì: SHA-1 được phát triển trên cơ sở những cái tương tự trước đó là MD2, MD4, MD5, SHA-0 và SHA-1. Do SHA-0 có va chạm, cho nên nó đã được sửa thành SHA-1. Bài báo phân tích SHA-1 trong chế độ mã hoá đã cho thấy nó là một thuật toán mã hoá SHACAL dựa trên SHA-1 là một thuật toán tốt. Còn xét SHA-1 như một hàm băm thì sao? ít ra nó cũng đứng vững được 9 năm, cho tới đầu tháng 2 năm 2005, thì có 3 nhà mật mã học người Trung quốc đã tìm được thuật toán phá nó với thời gian nhanh hơn vét cạn, rất tiếc bài báo đầy đủ về thuật toán này chưa được công bố. Kết quả đột phá này được giới thiệu qua bài viết „Cập nhật thông tin về hàm SHA-1“.

Như tác giả Bruce Schneier viết ngày 18 tháng 2 năm 2005 sau sự kiện SHA-1 bị tấn công: „Các hàm băm là thành tố mật mã được hiểu biết ít, các kỹ thuật băm được phát triển ít hơn so với các kỹ thuật mã hoá“. Cho nên nhóm đề tài cũng chưa có được những nghiên cứu sâu sắc, bởi vì có nhiều kỹ thuật chưa được nhuần nhuyễn. Trong phụ lục cũng có trình bày lại 4 bài báo theo 3 hướng nghiên cứu về thiết kế các hàm băm, đó là: Phương pháp thiết kế các hàm băm dựa trên mã khối, Nguyên tắc thiết kế hàm băm , Hàm băm nhanh an toàn dựa trên mã sửa sai và Độ mật của hàm băm lặp dựa trên mã khối.

Cuối phụ lục là một nghiên cứu tổng quan về giao thức mật mã và trình bày một bài báo về giao thức STS. Đây là giao thức dựa trên giao thức Diffie-Hellman chuẩn nhưng được cải biên để chống lại tấn công người đứng giữa. Giao thức này đã được nhóm đề tài sử dụng để lập trình thực hiện giao thức trao đổi khoá phục vụ các phần mềm mã gói IP trên môi trường Linux.

5. Về giá trị ứng dụng và triển vọng áp dụng kết quả KHCN

- Phần mềm IP-Crypto v1.0 đã được nâng cấp lên thành IP-Crypto 2.0 để cài đặt vào thiết bị chuyên dụng do Xí nghiệp M2 chế tạo trên nền một máy tính nhúng với hệ điều hành Linux đã được tối thiểu. Phần mềm này hiện nay đã được nâng cấp lên thành IP-Crypto v 3.0 có hỗ trợ chứng chỉ số để bảo mật 4 mạng LAN của Tổng cục An ninh- Bộ Công An.
- Phần mềm cung cấp chứng chỉ số đã được sử dụng thử tại Cục E15-Tổng cục VI- Bộ Công An với dịch vụ thư tín.
- Việc bảo mật dịch vụ WEB với chứng chỉ số cũng đã được dùng thử tại Cục Cơ yếu- BTTM (nhằm mở rộng các dịch vụ có hỗ trợ bảo mật trên trục mạng).
- Các phần mềm bảo mật mạng dùng giao thức IP đang được mở rộng diện sử dụng (tại Bộ Công An, trước hết là 13 mạng LAN của Tổng cục An ninh; sau đó là 30 mạng LAN thuộc trung tâm chỉ huy; mạng của Chính phủ theo đề án 112;...)
- Hiện nay, Cục Quản lý Kỹ thuật Nghiệp vụ Mật mã- Ban Cơ yếu Chính phủ đang xây dựng dự án cung cấp chứng chỉ số cho khu vực Nhà nước. Vấn đề triển khai sử dụng chứng chỉ số trong khu vực dân sự cũng đang được nhiều cơ quan quan tâm (nhất là Bộ Bưu chính Viễn thông).
- Việc thực hiện đề tài KC.01.01 đã giúp cho nhiều sản phẩm quan trọng đối với Ngành Cơ yếu được hình thành nhanh hơn. Điều quan trọng nữa là, với đề tài KC.01.01, những người làm công tác nghiên cứu trong Ngành Cơ yếu đã có điều kiện tiếp cận với nhiệm vụ bảo mật các một loại hình thông tin mới, đó là các thông tin kinh tế xã hội, đáp ứng nhu cầu sử dụng sản phẩm mật mã cho các lĩnh vực không phải là an ninh quốc phòng. Đây là một công việc lớn, bởi vì bên cạnh các thông tin tác nghiệp của các cơ quan Đảng và Nhà nước (như chính phủ điện tử), còn có các thông tin phục vụ phát triển kinh tế của các doanh nghiệp, công ty,... Bên cạnh các giải pháp kỹ thuật, vấn đề này còn phụ thuộc vào các yếu tố khác như chính sách quản lý, các văn bản pháp qui khác,...

6. Kết luận và kiến nghị

Đề tài KC.01.01 đã được thực hiện trong thời gian hơn 3 năm, tất cả các sản phẩm đăng ký đã được hoàn thành. Bốn nhóm sản phẩm (báo cáo khoa học, phần mềm, thiết bị) đã được hình thành, đó là: (1) những nghiên cứu tổng quan, tìm hiểu giải pháp; (2) các phần mềm bảo mật gói IP; (3) cung cấp và sử dụng chứng chỉ số; (4) đảm bảo toán học.

Một số sản phẩm của đề tài đã được Ban Cơ yếu tiếp tục đầu tư phát triển nâng cấp và đã có những ứng dụng thực tế mang lại hiệu quả thực sự và góp phần thúc đẩy quá trình thực hiện nhu cầu bảo mật thông tin trên các mạng của các đề án 112 của Chính phủ (trước hết là tại Bộ Công An). Những kết quả nghiên cứu đã đạt được của đề tài KC.01.01 đã được tiếp tục hoàn thiện để tạo ra những sản phẩm mới, ví dụ như phần mềm mã ở tầng cầu để bảo mật hội nghị truyền hình.

Trong một tương lai gần, thương mại điện tử và chính phủ điện tử sẽ phát triển mạnh ở nước ta. Đó là môi trường thuận lợi để cho những sản phẩm hỗ trợ PKI phát triển. Nhưng nó cũng làm nảy sinh một vấn đề hết sức quan trọng, đó là nhu cầu cần có một bộ chuẩn các thuật toán mật mã để dùng chung cho các sản phẩm đó. Đây là một công việc lớn, hiện đang được các cán bộ nghiên cứu đã thực hiện đề tài KC.01.01 nói riêng và đội ngũ cán bộ nghiên cứu trong Ban Cơ yếu Chính phủ nói riêng tập trung giải quyết.

7. Tài liệu tham khảo

Quyển 1A: Giới thiệu công nghệ IPSEC, công nghệ phát hiện xâm nhập và thương mại điện tử

1. An Introduction to IPSEC, Bill Stackpole, *Information Security Management Hanbook*, 4th edition, Chapter 14, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause, 2000.
2. Tài liệu kèm theo phần mềm FreeS/WAN (http://www.freeswan.org)
3. Cohen, F., Managing network security- Part 14: 50 ways to defeat your intrusion detection system. *Network Security*, December, 1997, pp.11-14.
4. Crosbie, M. and Spafford, E.H., Defending a computer system using autonomous agents. *Proceedings of 18th National Information System Security Conference*, 1995, pp. 549-558.
5. Garfinkel, S. and Spafford, G., *Practical Unix and Internet Security,* O'Reilly & Associates, Inc., 1996.
6. Garfinkel, S. and Spafford, G., *Web Security & Commerce*, O'Reilly & Associates, Inc., 1997.
7. Herringshaw, C. Detecting attacks on networks. *IEEE Computer,* 1997, Vol, Vol. 30 (12), pp. 16-17.
8. Mukherjee, B., Heberlein, L. T., and Levitt, K.N., Network intrusion detection. *IEEE Network*, 1994, Vol.8 (3), pp.26-41.
9. Power Richard, Issues and Trends: 1999 CSI/FBI computer crime and security survey, *Computer Security Journal*, Vol.XV, No.2, Spring 1999.
10. Schultz, E.E. and Wack, J., Responding to computer security incidents, in M. Krause and H.F. Tipton (Eds.), *Handbook of Information Security*. Boston:Auerbach, 1996, pp.53-68.
11. Van Wyk, K.R., *Threats to DoD Computer Systems*. Paper presented at 23rd Information Integrity Institute Forum

Quyển 1B: Nước Nga và chữ ký điện tử số

1. C.U.Mfhbxtd, D.D. Ujyxfhjd, H.T.Cthjd, *Jcyjds cjdhtvtyyjq rhbgnjuhfabb, Vjcrdf*, Ujhzxfz kbybz-Ntktrjv, 2002, cnh. 96-98.
2. S. Even and O. Goldreich. *Des-like functions can generate the alternating group*. IEEE Transactions on Information Theory, 29(6):863-865, November 1983.
3. National Soviet Bureau of Standards. Information Processing Systems. Cryptographic Protection. Cryptographic Algorithm. *GOST 28147-89*, 1989.
4. J. P. Pierrzyk and Xian-Mo Zhang. *Permutation generators of alternating groups*. In Advances in Cryptology- AUSCRYPT'90, J.Sebery, J. Pieprzyk (Eds), Lecture Notes in Computer Science, Vol.453, pages 237-244. Springer Verlag, 1990.

Quyển 1C: Tìm hiểu khả năng công nghệ để cứng hoá các thuật toán mật mã

1. FIPS 140-1 - *Security Requirements for Cryptographic Modules*., 1994 January 11.
2. Leon Adams., *Choosing the Right Architecture for Real-Time Signal Processing Designs*., White Paper., SPRA879 - November 2002.

3. Christof Paar., *Reconfigurable Hardware in Modern Cryptography*., ECC 2000 October 4-6., Essen, Germany.
4. Hagai Bar-El., *Security Implications of Hardware vs. Software Cryptographic Modules*., Information Security Analyst., October 2002.
5. Cryptology., http://www.cyphernet.org/cyphernomicon/5.html
6. Leon Adams., *Choosing the Right Architecture for Real-Time Signal Processing Designs*., SPRA879 - November 2002
7. Stephen Brown and Jonathan Rose., *Architecture of FPGAs and CPLDs: A Tutorial.,* Department of Electrical and Computer Engineering University of Toronto.
8. Khary Alexander, Ramesh Karri, Igor Minkin, Kaijie Wu, Piyush Mishra, Xuan Li., *Towards 10-100 Gbps Cryptographic Architectures*., IBM Corporation, Poughkeepsie, NY, 12601.
9. AJ Elbirt, C Paar., *Towards an FPGA Architecture Optimized for Public-Key Algorithms.,* Cryptography and Information Security Laboratory, Worcester, MA 01609.
10. Thomas Blum., *Modular Exponentiation on Reconfigurable Hardware*., Thesis., WORCESTER POLYTECHNIC INSTITUTE.
11. M. Shand and J. Vuillemin. *Fast implementations of RSA cryptography*. In Proceedings 11th IEEE Symposium on Computer Arithmetic, pages 252–259, 1993.
12. H.Orup. *Simplifying quotient determination in high-radix modular multiplication*., In Proceedings 12th Symposium on Computer Arithmetic, pages 193–9, 1995.
13. K. Iwamura, T. Matsumoto, and H. Imai. *Montgomery modular-multiplication., method and systolic arrays suitable for modular exponentiation*. Electronics and Communications in Japan, Part 3, 77(3):40–51, March 1994.
14. J.-P. Kaps. *High speed FPGA architectures for the Data Encryption Standard*., Master's thesis, ECE Dept., Worcester Polytechnic Institute, Worcester, USA, May 1998.
15. Ahmed Shihab, Alcahest; and Martin Langhammer, Altera., *Implementing IKE Capabilities in FPGA Designs*., Dec 05, 2003 URL: http://www.commsdesign.com/showArticle.jhtml?article-ID=16600061
16. Alexander Tiountchik, Institute of Mathematics, National Academy of Sciences of Belarus và Elena Trichina, Advanced Computing Research Centre, University of South Australia., *FPGA Implementation of Modular Exponentiation*.
17. Hauck, S. (1998). "*The Roles of FPGAs in Reprogrammable Systems*" Proceedings of the IEEE 86(4): 615-638.
18. Kris Gaj and Pawel Chodowiec., *Hardware performance of the AES finalists - survey and analysis of results*., George Mason University.
19. AJ Elbirt, W Yip, B Chetwynd, C Paar., *An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists*., ECE Department, Worcester Polytechnic Institute.
20. Kris Gaj and Pawel Chodowiec., *Comparison of the hardware performance of the AES candidates using reconfigurable hardware*., George Mason University.

21. Bruce Schneier, John Kelseyy, Doug Whitingz, David Wagnerx, Chris Hall, Niels Ferguson., *Performance Comparison of the AES Submissions.,* January 3, 1999.
22. J. P. Kaps and C. Paar, *Fast DES implementation on FPGAs and its application to a universal key-search machine*, in Fifth Annual Workshop on Selected Areas in Cryptography, vol. LNCS 1556, Springer-Verlag, August 1998.
23. O. Mencer, M. Morf, and M. J. Flynn, *Hardware Software Tri-Design of Encryption for Mobile Communication Units*, in Proceedings of International Conference on Acoustics, Speech, and Signal Processing, vol. 5, (New York, New York, USA).
24. K. H. Leung, K. W. Ma, W. K. Wong và P. H. W. Leong., *FPGA Implementation of a Microcoded Elliptic Curve Cryptographic Processor.,* Department of Computer Science and Engineering, The Chinese University of Hong Kong.
25. *M. Rosner Elliptic Curve Cryptosystems on reconfigurable hardware.,* Master's Thesis Worcester., Polytechnic Institute Worcester USA 1998.
26. G. Orlando and C. Paar., *A super-serial Galois field multiplier for FPGAs and its application to public key algorithms.,* Proceedings of the IEEE Symposium on Field-programmable custom computing machines., trang 232-239., 1999.
27. T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, B. Schott., *Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512*., Electrical and Computer Engineering, George Mason University, 4400 University Drive, University of Southern California - Information Sciences Institute.
28. Thomas Wollinger and Christof Paar., *How Secure Are FPGAs in Cryptographic Applications?*.,
Report 2003/119, http://eprint.iacr.org/, 5. June 2003
29. Ross Anderson Markus Kuhn., *Tamper Resistance - a Cautionary Note*., The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-9.
30. S Blythe, B Fraboni, S Lall, H Ahmed, U deRiu, *Layout Reconstruction of Complex Silicon Chips*, IEEE Journal of Solid-State Circuits v 28 no 2 (Feb 93) pp 138-145.
31. B. Dipert. *Cunning circuits confound crooks.,* http://www.einsite.net/ednmag/contents/images/21df2.pdf.
32. G. Richard., *Digital Signature Technology Aids IP Protection*., EETimes - News, 1998. http://www.eetimes.com/news/98/1000news/digital.html.
33. K.H. Tsoi, K.H. Leung and P.H.W. Leong., *Compact FPGA-based True and Pseudo Random Number Generators.,* Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin, NT Hong Kong.
34. V. Fischer and M. Drutarovsky. *True random number generator embedded in reconfigurable hardware*. Trong Proceedings Cryptographic Hardware and Embedded Systems Workshop (CHES), trang 415-430, 2002.

Quyển 2A: Giao thức TCP/IP và giải pháp bảo mật ở các tầng khác nhau.

1. *Network Layer Security*, Steven F. Blanding, Chapter 8, Information Security

Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause
2. *Transport Layer Security*, Steven F. Blanding, Chapter 9, Information Security Management Hanbook, 4th edition, Boca Raton-London- New York-Washington, editors Harold F.Tipton and Micki Krause
3. *Application- Layer Security Protocols for Network*, Bill Stackpole, Chapter 10, Information Security Management Hanbook, 4th edition, Boca Raton-London-New York-Washington, editors Harold F.Tipton and Micki Krause

Quyển 3A: Sinh tham số an toàn cho hệ mật RSA

1. Lều Đức Tân, Một số thuật toán kiểm tra tính nguyên tố đối với một số lớp số. Luận án phó tiến sỹ khoa học toán lý, Hà nội 1994.
2. Ian Blanke, Gadiel Seroussi & Nigel Smart. Elliptic Curves in Cryptography. Cambridge Universty press 1999.
3. D. M. Gordon, Strong Primes Are Ease to Find, Advances in Cryptology-Proceedings of EUROCRYPT 84 (LNCS 209), 216-223, 1985.
4. Hans Riesel, Prime Number and Computer Methods for Factorization, Progress in Mathematics, 57, 1985.
5. R. L. Rivest and R. D. Silverman, Are Strong Primes Needed for RSA?
6. Robert D. Silverman, Fast Generation of Random, Strong RSA Primes. The Technical Newsletter of RSA Laborastories. Spring 1997.
7. N.M.Stephens, Lenstra's Factorisation Based On Elliptic Curves. Springer-Verlag 1998, pp. 409-416.

Quyển 3B: Sinh tham số an toàn cho hệ mật Elgamal

1. Douglas Robert Stinson, Mật mã Lý thuyết và Thực hành. Bản dịch tiếng Việt Hà nội 1995.
2. Lều Đức Tân. Một số thuật toán kiểm tra nhanh tính nguyên tố của các số trên một số lớp số. Luận án phó tiến sĩ Hà nội 1993.
3. Paulo Ribenboim. The Little Book of Big Primes. Springe-Verlag 1991

Quyển 3C: Nghiên cứu xây dựng thuật toán mã khối an toàn hiệu quả

1. AES (nhiều tác giả*), Tuyển tập 15 hệ mã khối dự tuyển chuẩn mã tiên tiến (AES)*, Tài liệu từ Internet.
2. E. Biham, *New types of cryptanalytic attacks using related keys*, EUROCRYPT' 93, pp. 398-409.
3. A. Biryukov, D. Wagner, *Slide Attacks*, Fast Software Encryption, 1999, pp. 245-259.
4. A. Biryukov, D. Wagner, *Advanced Slide Attacks*, EUROCRYPT' 2000, pp. 589-606.
5. S. Burton, Jr. Kaliski, M.J.B. Robshaw*, Linear Cryptanalysis using Multiple Approximations,* CRYPTO'94, pp. 26-39.
6. G. Carter, E. Dawson, and L. Nielsen, *Key Schedules of Iterative Block Ciphers,* Tài liệu từ Internet, (10 trang).
7. F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Eurocrypt' 94, pp. 256-365.

8. C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naimi, Y. Zeng, *Comments on Soviet Encryption Algorithm GOST*, EUROCRYPT'94, pp. 433-438.
9. L. J. O'Conner and J. Dj Golic', *A unified markov approach to differential and linear cryptanalysis,* Asiacrypt, November 1994.
10. L. J. O'Conner**,** *Design Product Ciphers Using Markov Chain***,** Selected Area in Cryptography 1994.
11. L. J. O'Conner**,** *Convergence in Differential Distributions*, Crypto'95, pp.13-23.
12. I. I. Ghicman, A.V. Skorokhod, *Nhập môn về lý thuyết các quá trình ngẫu nhiên*, NXB "HAYKA", Maxcova 1977.
13. G. Hornauer, W. Stephan, R.Wernsdorf, *Markov Ciphers and Alternating Groups*, Eurocrypt'93, p.453-460.
14. T. Jacobsen, L.R. Knudsen, *Interpolation Attacks on the Block Cipher*, Fast Software Encryption, 1997, pp 28-40.
15. Y. Kaneko, F. Sano, K. Sakurai, *On Provable Security against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Mutiple Random Functions*, Tài liệu từ Internet, 15 trang.
16. J. Kelsy, B. Schneier, and D. Wagner, *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SEFER, and Triple-DES*, CRYPTO'96, pp 237-251
17. L. R. Knudsen, *Block Ciphers-Analysis, Design and Applications*, July, 1, 1994 (Ph. D Thesis).
18. L. R. Knudsen, *Practically secure Feistel ciphers*, Fast Software Encryption, 1993, pp. 211-221.
19. L.R. Knudsen, *New potentially "weak" keys for DES and LOKI*, EUROCRYPT' 94, pp. 419-424.
20. L. R. Knudsen, M.J.B. Robshaw*, Non-linear Approximations in Linear Cryptanalysis*, EUROCRYPT' 96, pp. 224-236.
21. M. Kwan, J. Pieprzyk, *A General purpose Technique for Locating Key Scheduling Weaknesses in DES-like Cryptosystems*, ASIACRYPT'91, pp. 237-246.
22. X. Lai, *On the Design and Security of Block Ciphers*, Hartung-Gorre Verlag Konstanz, 1995
23. X. Lai, J.L. Massey and S. Murphy, *Markov Ciphers and Differential cryptanalysis,* Eurocrypt' 91, pp.17-38.
24. M. Matsui, *New Block Encryption Algorithm MISTY*, Fast Software Encryption, 1997, FSE'97, pp. 54-68
25. M. Matsui, *New structure of block ciphers with provable security against differential and linear cryptanalysis*, Fast software Encryption, 1996, pp. 21-23.
26. M. Matsui, *Linear Cryptanalysic Method for DES Cipher*, EUROCRYPT' 93, pp. 386-397.
27. M. Matsui, *The First Experimental Cryptanalysic of the Data Encryption Standard*, CRYTO' 94, pp. 1-11.
28. S. Moriai, T. Shimoyama, T. Kaneko, *Interpolation Attacks of the Block Cipher: SNACK*, Fast Software Encryption, 1999, pp. 275-289.
29. K. Nyberg, *Differentially uniform mappings for cryptography*, EUROCRYPT'93, pp. 55-64, 1994.
30. K. Nyberg, *Linear Approximation of Block Ciphers,* Eurocrypt'94, pp.439-444.

31. K. Nyberg, L. R. Knudsen, *Provable security against a differetial cryptanalysis,* Journal of Cryptology, Vol. 8, pp. 27-37, 1995.
32. Savan Patel, Zulfikar Ramzan, and Ganapathy S. Sundaram, *Towards Making Luby-Rackoff Ciphers Optimal and Practical*, Fast Software Encryption, 1999, pp. 171-185.
33. Kenneth G. Paterson, *Imprimitive Permutation Groups and Trapdoor in Iterated Block Ciphers*, Fast Software Encryption, 1999, pp. 201-214.
34. T. Shimoyama, T. Kaneko, *Quadratic Relation of S-box and Its Application to the Limear Attack of Full Round DES*, CRYPTO'98, pp. 200-211.
35. J. Seberry, X. M. Zhang and Y. Zheng, *Relationships Among Nonlinearity Criteria*, EUROCRYPT'94, pp. 76-388, 1995.
36. D. R. Stinson, *Cryptography: Theory and Practice*, 1995 by CRC Press, Inc.
37. Nguyễn Duy Tiến, *Các mô hình xác suất và ứng dụng, Phần I- Xích Markov và ứng dụng,* NXB Đại học Quốc gia Hà Nội, 2000.
38. R.Wernsdorf, *The One-Round Functions of the DES Generate the Alternating Group*, Proc. Eurocrypt' 92, LNCS 658, 1993, pp. 99-112.

Quyển 4A: Các phần mềm bảo mật gói IP trên hệ điều hành Linux

1. Glenn Herrin, Linux IP Networking-A Guide to the Implementation and Modification of the Linux Protocol Stack
2. Alan Cox, Network buffer and memory management

Quyển 4B: Hệ thống an toàn trên môi trường mạng Sun Solaris

1. Streams programming Guide. *1995 Sun Microsystems.*
2. Solaris system administrators guide. *Janice Winsor - 1993 - Ziff-Davis Press Emryville, California*
3. Writing unix device drivers. *George pajari - Addison-Wesley Publishing Company, Inc - 1992*
4. TCP/IP Illustrated Volume 1. Volume2 , Volume 3. *Gary R. Wright - W. Richard Stevens, 1995- Addison-Wesley Publishing Company*
5. Network and internetwork security-Principles and practice. *William Stallings, Ph.D.,1995 by Prentice-Hall, Inc*
6. Computer Communications Security - Principles, Standard Protocols and Techniques. *Warwick Ford - PTR Prentice Hall - 1994*
7. Intenet & TCP/IP Network Security, Security Protocols and Applications -*1996 by The McGraw-Hill Companies, Inc*
8. Building Internet Firewalls. *D. Brent chapman and Elizabeth D. Zwicky - O' Reilly & Associates, Inc.*
9. Firewall complete, *1998 - Mc Graw - Hill*
10. UNIX Network programming Volume 1, *Network APIs: Sockets and XTI - W. Richard Stevents, 1998 Prentice - Hall, Inc*
11. Tài liệu chuyên đề về TCP/IP , *Phạm Văn Hải - Học viện KTMM*
12. http://www.freeswan.org/
13. RFC 2409 :The Internet Key Exchange (IKE)
14. RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
15. RFC 1825 : An overview of a security architecture

16. RFC 1826 : IP Authentication Header
17. RFC 1827 : IP Authentication Header
18. Các RFC khác về IPSEC và FreeS/WAN

Quyển 5A: An ninh của các hệ điều hành họ Microsoft Windows, Sun Solaris và Linux

1. Authentication HOWTO - Peter Hernberg
2. Shadow Password Howto - Michael H. Jackson mhjack@scnet.com
3. Security HOWTO
4. The Linux-PAM System Administrator's Guide, Adrew G. Morgan
5. Practical Unix Security - Simson Garfinkel and Gene Spafford
6. Các trang man getty(); mingetty(); login(); sulogin();
7. Text - Terminal HOWTO - David S. Lawyer dave@lafn.org
8. Solaris System Administration Guide, Chapter 12 -> Chapter 16
9. Software White Paper: Solaris Security, Tài liệu từ Internet

Quyển 5B: Cơ chế an toàn của các hệ điều hành mạng, Network hacker, Virut máy tính

1. William Stallings Ph.D. (1999), *Cryprography and Network security: Principles and Practice - Second edition*, Prentice -Hall, Inc.,USA.
2. VN-GUIDE, *Bảo mật trên mạng – Bí quyết và giải pháp – Tổng hợp và biên dịch*, Nhà xuất bản thống kê.
3. Các trang web: www.tinhat.com/internet_security/security_holes.html, www.tinhat.com/internet_security/improve.html, www.securityfocus.com, www.saintcorporation.com, www.sans.org, www.fbi.gov, www.cs.wright.edu, www.nessus.org, www.nai.com, www.linuxdoc.org/HOWTO/Secure-Programs-HOWTO.html, www.hackecs.com, www.auscert.org.au, www.securityfocus.com, www.l0pht.com, www.w3.org, www.rhino9.com, iss.net, www.insecure.org, www.cert.org, vnEpress.net, www.viethacker.net
4. Trần Thạch Tùng, *Bảo mật và tối ưu trong Red Hat Linux*, NXB Lao động – Xã hội
5. Edward Amoroso, *Fundamentals of Computer Security Technology*
6. E_book: *Hackers Handbook, State of the art Hacking tools and techniques, Vol 1, 2, 3.*
7. William Stallings Ph.D. (1999), Cryprography and Network security: Principles and Practice - Second edition, Prentice -Hall, Inc.,USA.
8. Các trang web: www.netbus.org, www.saintcorporation.com/products/saint_engine.html, www.rootshell.com, www.hackerjokes.de/, www.hackercracker.net/, www.crackerhttp/, www.hackerethic.org/, www.counter-hack.net/, www.inthehack.com/, www.eleganthack.com/, www.hack-net.com/, www.virtualcrack.com/
9. Ngô Anh Vũ, *Virus tin học huyền thoại và thực tế*, NXB Thành Phố Hồ Chí Minh.
10. Nguyễn Thành Cương, Hướng dẫn phòng và diệt virus máy tính , NXB thống kê
11. Nguyễn Viết Linh và Đậu Quang Tuấn, Hướng dẫn phòng chống virus trong tin *học một cách hiệu quả*, NXB trẻ.
12. Các trang web: www.viruslist.com/, www.norman.com, www.esecurityplanet.com, www.antivirusebook.com, www.waronvirus.com, www.hackertrickz.de