ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Võ Đại Trung

MỘT SỐ VẤN ĐỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ PHỤC VỤ CÔNG TÁC HÀNH CHÍNH

Ngành: Công nghệ thông tin
Mã số: 1.01.10

LUẬN VĂN THẠC SỸ

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS TRỊNH NHẬT TIẾN.

HÀ NỘI - 2007

LỜI CẢM ƠN

Tôi xin gửi lời cám ơn chân thành đến các thầy cô, bạn bè, đồng nghiệp và nhà trường đã tạo điều kiện giúp đỡ tôi trong quá trình học tập vừa qua. Đặc biệt tôi xin gửi lời cám ơn thầy giáo PGS, TS Trịnh Nhật Tiến, người đã hướng dẫn tôi hoàn thành luận văn này.

Do thời gian có hạn, khả năng còn hạn chế, do vậy luận văn không tránh khỏi những sai sót. Tác giả xin ghi nhận và cám ơn tất cả các ý kiến đóng góp của các thầy cô và các bạn.

MỤC LỤC

GIẢI THÍCH MỘT SỐ THUẬT NGỮ VÀ TỪ VIẾT TẮT

Từ viết tắt	Viết đầy đủ	Giải thích
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ.
ATTT	An toàn thông tin	An toàn thông tin
CA	Certification Authority	Làm nhiệm vụ quản lý cấp phát và thu hồi chứng chỉ số
CGI	Common Gateway Interface	Là một phương pháp cho phép giao tiếp giữa server và chương trình nhờ các định dạng đặc tả thông tin.
CNTT	Công nghệ thông tin	Công nghệ thông tin
CQHC	Cơ quan Hành chính	Cơ quan Hành chính
CQNN	Cơ quan nhà nước	Cơ quan nhà nước
CSDL	Cơ sở dữ liệu	Cơ sở dữ liệu
DHCP	Dynamic Host Configuration Protocol	Hệ thống giao thức cấu hình IP động
DLL	Dynamic Link Library	Thư viện liên kết động.
DNSSEC	DNS Security	Là một cơ chế bảo mật mới bằng cách cho phép các Website kiểm tra các tên miền của họ và chịu trách nhiệm đối với các địa chỉ IP theo các chữ ký điện tử và thuật toán mã hoá công khai.
EE	End Entity	Người sử dụng cuối (có thể là một thiết bị phần cứng nào đó hay một module phần mềm ví dụ như ActiveX, Java Applet)
Firewall	Tường lửa	Là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại truy cập trái phép nhằm bảo vệ nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của thông tin không mong muốn.

FTP	File Transfer Protocol	Giao thức truyền file qua mạng
G2B	Goverment to Business	Chính phủ với Doanh nghiệp
G2E	Goverment to Employee	Chính phủ với Công chức
G2G	Goverment to Government	Chính phủ với Chính phủ
G4C	Goverment for Citizen	Chính phủ với Công dân
GDĐT	Giao dịch điện tử	Giao dịch điện tử
HTTP	Hypertext Transfer Protocol	Giao thức truyền siêu văn bản.
HTTPS	Hypertext Transfer Protocol Secure	Giao thức truyền siêu văn bản qua một kết nối an toàn. Khác với HTTP, nó mặc định cổng TCP và bổ sung thêm tầng mã hoá/ xác thực giữa HTTP và TCP.
IMAP	Internet Mesaging Access Protocol	Giao thức truy cập truyền thông điệp trên Internet
JSP	JavaServer Pages	Là một công nghệ Java cho phép các nhà phát triển tạo nội dung HTML, XML hay một số định dạng khác của trang web. Công nghệ này cho phép nhúng mã Java và một số hành động xử lý đã được định trước (pre-defined actions) vào trong nội dung tĩnh của trang web.
LDAP	Lightweight Directory Access Protocol	Giao thức truy nhập dịch vụ thư mục theo chuẩn X.500. Thông thường CA sử dụng dịch vụ thư mục để lưu trữ dữ liệu chứng chỉ số.
LRA	Local Registration Authority	Là một thành phần tuỳ chọn của một PKI, nó duy trì định danh của người dùng từ các CA có thể phát hành các chứng chỉ số.
MAC	Message	Mã xác thực thông điệp

	Authentication Code	
MITM	Man-in-the-middle attack	Tấn công trung chuyển. Kẻ tấn công giả mạo người nhận và nhận gói tin trước khi chủ nhân thật nhận được nó.
NNTP	Network News Transfer Protocol	Giao thức ứng dụng của Internet, được sử dụng chủ yếu trong việc đọc và post các tin bài dạng Usenet qua mạng. Người đọc và người post tin bài cùng truy nhập vào máy chủ hosting, đọc các bài báo này một cách trực tiếp từ một ổ đĩa cục bộ.
PGP	Pretty Good Privacy	Là một ứng dụng được dùng rất phổ biến, cho phép mã hóa dữ liệu.
PKC	Public Key Certificate	Là chữ ký số lên khoá công khai của người dùng. Thông thường gọi tắt là chứng chỉ số.
PKCS	Public Key Certificate Standards	Các chuẩn chứng chỉ khoá công khai
PKI	Public Key Infrastructure	Cơ sở hạ tầng về mật mã khoá công khai
QLHCNN	Quản lý hành chính nhà nước	Quản lý hành chính nhà nước
RA	Registration Authority	Làm nhiệm vụ trung gian giữa người sử dụng và CA. RA nhận ra các yêu cầu của người sử dụng, kiểm tra và chuyển yêu cầu lên cho CA, đồng thời nhận kết quả từ CA về và chuyển giao lại cho người sử dụng.
RFC	Request for Comments	Là tập hợp những tài liệu nói về chuẩn, nghi thức cho Internet.
S/MIME	Security/ Multipurpose Internet Mail Extensions	Cung cấp các dịch vụ bảo mật thông điệp cho các ứng dụng truyền thông điệp điện tử.
SMTP	Simple Mail Transfer Protocol	Giao thức dùng để gửi Mail từ Mail Client đến Mail Server.
SSL	Secure Sockets Layer	SSL là giao thức đa mục đích để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước nhằm mã hoá toàn bộ thông tin gửi/ nhận.

TCP	Transmission Control Protocol	Là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự. TCP còn phân biệt giữa dữ liệu của nhiều ứng dụng (chẳng hạn, dịch vụ Web và dịch vụ thư điện tử) đồng thời chạy trên cùng một máy chủ.
Telnet	Teletype Network	Giao thức mạng được dùng trên các kết nối với Internet hoặc các kết nối tại mạng máy tính cục bộ LAN. Mục đích của giao thức TELNET là cung cấp một phương tiện truyền thông chung chung, có tính lưỡng truyền, dùng độ rộng 8 bit, định hướng byte.
TLS	Transport Layer Security	Là một giao thức đảm bảo sự bí mật giữa các ứng dụng giao dịch điện tử với những người dùng của nó khi máy khách và máy chủ giao dịch với nhau, nó đảm bảo rằng không có một thành phần thứ 3 nào có thể nghe lén và sửa đổi thông điệp. TLS là một cải tiến của SSL.
UDP	User Datagram Protocol	Giao thức vận chuyển không kết nối. Dùng UDP, chương trình trên mạng máy tính có thể gởi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian.
VA	Validation Authority	Là một giải pháp phần mềm hoàn chỉnh có khả năng bảo mật, mở rộng và xác nhận chứng chỉ số hợp lệ đối với việc mở rộng hệ thống.
VPN	Vitual Private Network	Là một mạng riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các địa điểm hoặc người sử dụng từ xa với một LAN ở trụ sở trung tâm. Thay vì dùng kết nối phức tạp như đường dây thuê bao số, VPN tạo ra các liên kết ảo được truyền qua Internet giữa mạng riêng của một tổ chức với địa điểm hoặc người dùng ở xa.

MỞ ĐẦU

Ngày nay khi mà nhu cầu giao dịch trực tuyến ngày một tăng cao thì mối đe dọa và hậu quả tiềm ẩn đối với thông tin trong giao dịch điện tử (GDĐT) lại trở nên rất lớn. Nguy cơ rủi ro đối với thông tin trong GDĐT được thể hiện hoặc tiềm ẩn trên nhiều khía cạnh khác nhau, như: người sử dụng, kiến trúc hệ thống công nghệ thông tin, chính sách bảo mật thông tin, các công cụ quản lý và kiểm tra, quy trình phản ứng, ...

Một trong những nguy cơ tiềm tàng nguy hiểm nhất đối với mạng máy tính mở là đạo tặc tin học, xuất hiện từ phía bọn tội phạm và giới tình báo. Nguy hiểm bởi nó xuất phát từ phía những kẻ có chuyên môn cao và sử dụng kỹ thuật tinh vi (như đoán mật khẩu, khai thác các điểm yếu của hệ thống và các chương trình hệ thống, giả mạo địa chỉ IP, đón lõng các trạm đầu cuối, cài rệp điện tử, virus máy tính phá hoại CSDL, sửa nội dung thông tin theo ý đồ đen tối của chúng, thậm chí nếu cần còn có thể làm tắc nghẽn kênh truyền,...), không những đối với từng cơ quan, doanh nghiệp mà còn đối với cả Chính phủ và ảnh hưởng tác hại của nó không chỉ riêng trong lĩnh vực kinh tế mà cả đối với lĩnh vực chính trị, an ninh quốc phòng.

Để giải quyết vấn đề này, cần nghiên cứu xây dựng các hệ thống đảm bảo an toàn thông tin cho các hệ thống giao dịch điện tử trên cơ sở quy định hiện hành của pháp luật Việt Nam.

Song song với sự ra đời rất sớm của các giải pháp và công nghệ bảo đảm an toàn thông tin nói chung và bảo đảm an toàn truyền tin trên mạng máy tính nói riêng, lý thuyết độ phức tạp tính toán, lý thuyết mật mã và an toàn thông tin đã không ngừng được nghiên cứu phát triển và ngày một trở nên phong phú, hoàn thiện. Đây là cơ sở khoa học quan trọng và không thể thiếu trong việc giải quyết các bài toán về bảo đảm an toàn thông tin trong giao dịch điện tử.

Đảm bảo an toàn thông tin trong giao dịch điện tử nói chung và giao dịch điện tử phục vụ công tác quản lý hành chính Nhà nước nói riêng là một vấn đề có tính quyết định đến thành công và hiệu quả của việc triển khai các hệ thống ứng dụng CNTT trong các cơ quan nhà nước. Do vậy việc nghiên cứu đề xuất xây dựng các mô hình hệ thống đảm bảo an toàn thông tin trong giao dịch điện tử là việc làm cấp bách hiện nay. Cần phải xây dựng được các hệ thống đảm bảo an toàn thông tin trong giao dịch điện tử thì khi đó việc triển khai xây dựng các ứng dụng giao dịch điện tử mới thực sự hiệu quả và tiến tới xây dựng thành công Chính quyền điện tử/ Chính phủ điện tử theo đúng nghĩa của nó.

Luận văn đề cập đến thực trạng về đảm bảo an toàn thông tin trong giao dịch điện tử của các cơ quan Nhà nước hiện nay, nghiên cứu lý thuyết, công nghệ đảm bảo an toàn thông tin và hành lang pháp lý trong giao dịch điện tử, từ đó đề xuất xây dựng mô hình đảm bảo an toàn thông tin trong giao dịch điện tử của các cơ quan nhà nước và hệ thống ứng dụng mô phỏng.

Luận văn gồm 4 chương và 1 phụ lục:

Chương 1: Các khái niệm cơ bản về lý thuyết mật mã và an toàn thông tin.

Trong chương này đưa ra các khái niệm toán học cơ bản, định nghĩa và hệ thống lại các vấn đề lý thuyết cơ sở đảm bảo an toàn thông tin trong giao dịch điện tử như: hệ mật mã, chữ ký điện tử, chứng chỉ số.

Chương 2: Cơ sở hạ tầng đảm bảo ATTT trong GDĐT.

Nêu các vấn đề đảm bảo ATTT trong GDĐT, vai trò của cơ sở hạ tầng về mật mã khoá công khai trong hệ thống GDĐT. Trình bày khái niệm, các thành phần kỹ thuật cơ bản, các công cụ, phương tiện và các giao thức của nó.

Chương 3: Xây dựng mô hình đảm bảo ATTT trong GDĐT phục vụ công tác Hành chính Nhà nước.

Nêu lên các loại hình giao dịch điện tử của cơ quan Nhà nước được quy định hiện hành, đánh giá thực trạng về giao dịch điện tử trong các cơ quan Hành chính Nhà nước hiện nay, đề xuất xây dựng mô hình hệ thống đảm bảo an toàn thông tin phục vụ giao dịch điện tử của cơ quan Hành chính Nhà nước đảm bảo các quy chuẩn kỹ thuật và quy định của luật pháp Việt Nam.

Chương 4: Xây dựng hệ thống thử nghiệm, mô phỏng các hoạt động giao dịch điện tử cơ bản trong cơ quan Hành chính.

Phụ lục: Một số quy định của Nhà nước đảm bảo cho việc xây dựng và triển khai các hệ thống giao dịch điện tử: Nêu vắn tắt cơ sở pháp lý phục vụ xây dựng và triển khai các hệ thống giao dịch điện tử tại Việt Nam (Luật giao dịch điện tử; Nghị định về chữ ký số và chứng thư số và một số quy định khác trong công tác Quản lý Hành chính Nhà nước có liên quan).

TÀI LIỆU THAM KHẢO

1. *"Luật Giao dịch điện tử"* được Quốc hội thông qua ngày 29/11/2005, luật có hiệu lực từ ngày 01/03/2006.
2. *"Luật Công nghệ thông tin"*, có hiệu lực từ ngày 01/01/2007.
3. *Quyết định 181/2003/QĐ-TTg* của Thủ tướng Chính phủ về việc ban hành quy chế thực hiện cơ chế "một cửa" tại cơ quan hành chính ở địa phương.
4. *Nghị định 110/2004/NĐ-CP của Chính phủ về công tác Văn thư.*
5. *Pháp lệnh Bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH10* ngày 28/12/2000 của Uỷ ban Thường vụ Quốc hội.
6. *Nghị định số 33/2002/NĐ-CP* ngày 28/03/2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh Bảo vệ bí mật Nhà nước.
7. *Nghị định 26/2007/NĐ-CP*, ban hành ngày 15/02/2007 quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số.
8. Phan Đình Diệu (2006), *"Lý thuyết mật mã và An toàn thông tin"*, Nhà xuất bản Đại học Quốc gia Hà Nội.
9. Trịnh Nhật Tiến (12-2005), *Báo cáo khoa học đề tài "Nghiên cứu xây dựng Cơ sở hạ tầng về mật mã khóa công khai bảo đảm an toàn truyền tin trên mạng máy tính Thành phố Hà Nội"*.
10. Nguyễn Ngọc Tuấn, Hồng Phúc (2005), *"Công nghệ bảo mật"*, Nhà xuất bản thống kê.
11. Nguyễn Nam Hải, Đào Thị Hồng Vân, Phạm Ngọc Thúy (2004), *"Chứng thực trong thương mại điện tử"*, Nhà xuất bản Khoa học và Kỹ thuật.
12. D.Stinson (1995), *"Cryptography: Theory and Practice"*, CRC Press.
13. B.Schneider (1995), *"Applied Cryptography"*, 2th edition, Wiley.
14. Lê Hồng Hà, Tổng thư ký Hội Tin học - Viễn thông Hà Nội, thành viên Ban soạn thảo Luật CNTT. *"An toàn thông tin trong giao dịch điện tử"*.
15. *Nghị định 64/2007/NĐ-CP*, ban hành ngày 10/04/2007 về việc ứng dụng CNTT trong hoạt động của cơ quan nhà nước.
16. D. Rechard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu–Jen Chang (2001), *"Introduction to Public Key Technology and the Federal PKI Infrastructure"*. NIST.
17. An RSA Data Security White Paper. *"Understanding Public Key Infrastructure"*. RSA Data Security Inc.
18. *"Daily official gazette free of charge", "Electronic sale by credit card of any official Spanish publication"*. The Official State Gazette (BOE) Ministry of the Presidency (http://www.boe.es).

19. Website http://www.rsa.com; http://selab.edu.ms; http://www.openca.org.