ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN QUỐC HOÀN

NGHIÊN CỨU GIẢI PHÁP AN TOÀN THÔNG TIN BẢO VỆ CỔNG THÔNG TIN ĐIỆN TỬ MỘT CỬA CẤP HUYỆN ỨNG DỤNG CÀI ĐẶT TẠI TỈNH NAM ĐỊNH

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, năm 2012

MỞ ĐẦU

1. Lý do chọn đề tài

Công nghệ thông tin, truyền thông và Internet đang làm thay đổi cơ bản lối sống, cách suy nghĩ, phương thức làm việc của người dân và doanh nghiệp, các giao dịch và trao đổi thông tin trong xã hội.

Hiện nay, việc ứng dụng CNTT trong các giao dịch giữa người dân, doanh nghiệp với cơ quan Nhà nước thông qua việc cung cấp các dịch vụ hành chính công đang chuyển dần từ dạng truyền thống sang môi trường giao dịch điện tử một cửa và qua Internet (mức độ giao dịch qua đường điện tử và qua Internet được chia thành 4 mức từ mức độ một đến mức độ bốn).

Thực tế, tại tỉnh Nam Định khi xây dựng mô hình cổng thông tin điện tử một cửa ở cấp huyện và cài đặt tại UBND các huyện, thành phố mô hình đã đáp ứng được yêu cầu cải cách thủ tục hành chính, giảm bớt sự phiền hà, tiết kiệm nhiều thời gian đỡ tốn kém về kinh phí chi phí cho việc thực hiện giao dịch dịch vụ hành chính giữa người dân, doanh nghiệp với các cơ quan nhà nước.

Khi xây dựng và đưa vào sử dụng cổng thông tin điện tử một cửa cấp huyện ta thấy còn tồn tại hai vấn đề sau:

- Chưa có mô hình cổng thông tin điện tử một cửa chung trong toàn quốc; ở mỗi địa phương tự xây dựng cổng thông tin điện tử một cửa cho riêng mình. Trong một tỉnh, cổng thông tin điện tử một cửa của các huyện, thành phố cũng chưa thống nhất.
- Vấn đề an toàn thông tin còn hạn chế, mặc dù đã có một số giải pháp được áp dụng, tuy nhiên độ tin cậy về bảo đảm an toàn, an ninh thông tin trong cổng thông tin điện tử một cửa chưa cao.

Vì thế, trong khuôn khổ của một luận văn thạc sỹ, tôi chọn đề tài: "**nghiên cứu giải pháp an toàn thông tin bảo vệ cổng thông tin điện tử một cửa cấp huyện ứng dụng cài đặt tại tỉnh Nam Định".**

Vấn đề đảm bảo an toàn, an ninh thông tin cho cổng thông tin điện tử một cửa không phải là một đề tài mới mẻ, đã có rất nhiều những nghiên cứu và các

ứng dụng đã đạt được những kết quả nhất định. Nhưng các nghiên cứu này khi áp dụng vẫn chưa hoàn toàn đáp ứng được yêu cầu thực tế của việc bảo mật và đảm bảo an toàn, an ninh trong các giao dịch điện tử giữa người dân, doanh nghiệp với các cơ quan nhà nước tại cổng thông tin điện tử một cửa cấp huyện đang cài đặt tại Nam Định.

2. Đối tượng và phạm vi nghiên cứu

- Cơ sở lý thuyết các vấn đề an ninh mạng.
- Mô hình giao dịch điện tử một cửa cấp huyện.
- Những giải pháp an toàn thông tin ở một số khâu giao dịch áp dụng cho cổng thông tin một cửa điện tử cấp huyện đang áp dụng thực tế tại tỉnh Nam Định.

3. Hướng nghiên cứu của đề tài

Xây dựng giải pháp bảo vệ an toàn thông tin trong một số khâu giao dịch như:

- Truyền nhận công văn, giấy tờ.
- Xác thực mã giao dịch, bảo vệ và xác thực mã.
- Một số giải pháp phần cứng.

4. Phương pháp nghiên cứu

Luận văn sử dụng phương pháp nghiên cứu lý thuyết, đọc, tìm hiểu, phân tích, đối chiếu, so sánh, tổng hợp viết thành luận văn.

Nghiên cứu thực tế, cài đặt chạy thử nghiệm rút ra kết luận.

5. Ý nghĩa khoa học của đề tài

Đề tài có mục tiêu giải quyết vấn đề cải cách thủ tục hành chính – tiền đề cho phát triển chính quyền điện tử tại địa phương.

Tăng cường tính an toàn và bảo mật thông tin cho cổng thông tin điện tử một cửa cấp huyện. Đảm bảo tính trung thực, chính xác của thông tin giao dịch giữa người dân, doanh nghiệp với các cơ quan nhà nước.

Tăng độ tin cậy của người dân, doanh nghiệp trong các giao dịch với các cơ quan nhà nước.

Để đạt được mục tiêu này cần phải nắm bắt được giải pháp và các biện pháp đảm bảo an toàn, an ninh thông tin cho cổng thông tin điện tử một cửa đồng thời triển khai áp dụng thực tiễn tại ủy ban nhân dân các huyện, thành phố của tỉnh Nam Định, vì vậy đề tài mang đầy đủ ý nghĩa thực tiễn và khoa học.

Chương 1. TỔNG QUAN VỀ AN TOÀN AN NINH TRÊN CỔNG THÔNG TIN ĐIỆN TỬ

1.1. Cơ sở lý thuyết của giải pháp đảm bảo an toàn, an ninh thông tin

1.1.1. An toàn, an ninh thông tin trên mạng

1.1.1.1. Khái niệm về mạng máy tính

Mạng máy tính là một nhóm các máy tính và thiết bị ngoại vi kết nối với nhau thông qua các phương tiện truyền dẫn như cáp xoắn, cáp quang, sóng điện từ, tia hồng ngoại… để chia sẻ dữ liệu cho nhau. Dữ liệu truyền từ máy này sang máy khác đều là các bit nhị phân 0 và 1, sau khi biến đổi thành điện thế hoặc sóng điện từ, sẽ được truyền qua môi trường truyền dẫn.

1.1.1.2. Các hình thức tấn công thông tin trên mạng

a. Tấn công từ chối dịch vụ DOS - MD: Làm cho hệ thống thông tin bị tê liệt không thể phục vụ trong những khoảng thời gian. Đó là dạng tấn công phổ biến và gây thiệt hại nặng nề.

b. Tấn công ở giữa Main in middle - MD: Chặn bắt thông tin ở giữa 2 đối tượng đang trao đổi thông tin sao cho 2 đối tượng không hề hay biết. Đọc nội dung của thông tin, sửa đổi giả mạo rồi lại tiếp tục gửi đi gây tổn thất nặng nề.

c. Tấn công chiếm phiên làm việc TCP/IP Hijacking MD: Lách qua hệ thống và các giao thức bảo mật mà không cần biết mật khẩu sau đó thì đánh cắp thông tin. Sau khi 2 đối tượng thiết lập xong phiên giao dịch (bao gồm nhiều biện pháp xác thực) lúc này hacker mới nhảy vào chiếm lấy phiên làm việc mà không cần phải xác thực vì lúc này phiên làm việc đã được thiết lập.

d.Tấn công giả mạo Reply Attack – Hacker: Thu thập thông tin về đối tượng, sau đó giả mạo các thông số hệ thống của đối tượng rồi vượt qua kiểm soát bảo mật để đánh cắp thông tin.

e.Tấn công giả mạo Spoofing attack MD: Giả mạo một dịch vụ hoặc một địa chỉ, giả mạo thông số hệ thống để đánh cắp thông tin. Như là giả mạo địa chỉ IP giả mạo bảng cam trong switch ARP, giả mạo địa chỉ email gửi, làm 1 trang đăng nhập giả mạo lấy account, giả mạo DNS server, đưa những thông tin lừa đảo và giả mạo người sử dụng để đánh cắp thông tin tín dụng....

f.Tấn công dựa trên yếu tố con người - xã hội Social Engineering: Tấn công dựa vào sở hở của người sử dụng hoặc nhân viên hệ thống hoặc kẻ tấn công thức hiện trà trộn vào hệ thống làm gián điệp để tấn công đánh cắp thông tin đây cũng là một hình thức tấn công thường được sử dụng hoặc hacker lợi dụng rồi dò mật khẩu của hệ thống qua thông tin của nhân viên quản trị như ngày tháng năm sinh, người thân, gia đình…

g.Tấn công lấy trộm mật khẩu bằng cách nghe lén Sniff and Evesdroping: Hacker dùng những công cụ để chặn bắt gói tin sau đó lấy thông tin trong đó có chứa mật khẩu.

h.Tấn công vào mật khẩu: Hacker dùng cách dò xét mật khẩu thử các mật khẩu đơn giản sau đó nếu không được hacker áp dụng cách khác là dùng thư viện để đưa tool vào dò.

1.1.1.3. Các dịch vụ bảo vệ thông tin trên mạng

Chúng ta có thể coi các dịch vụ bảo vệ thông tin như là "bản sao" của các thao tác bảo vệ tài liệu vật lý. Các tài liệu vật lý có các chữ ký và thông tin về ngày tạo ra nó. Chúng được bảo vệ nhằm chống lại việc đọc trộm, giả mạo, phá hủy…Chúng có thể được công chứng, chứng thực, ghi âm, chụp ảnh… Tuy nhiên có các điểm khác nhau giữa tài liệu điện tử và tài liệu giấy:

- Ta có thể phân biệt giữa tài liệu giấy nguyên bản và một tài liệu sao chép. Nhưng tài liệu điện tử chỉ là một dãy các bit nên không thể phân biệt được đâu là tài liệu "nguyên bản" đâu là tài liệu sao chép.

- Mọi sự thay đổi trong tài liệu giấy đều để lại dấu vết như vết xóa, tẩy… Tuy nhiên sự thay đổi tài liệu điện tử hoàn toàn không để lại dấu vết.

Dưới đây là các dịch vụ bảo vệ thông tin trên mạng máy tính:

a. Dịch vụ bí mật (Confidentiality)

Dịch vụ bí mật bảo đảm rằng thông tin trong hệ thống máy tính và thông tin được truyền chỉ được đọc bởi những bên được ủy quyền. Thao tác đọc bao gồm: in, hiển thị,… Nói cách khác, dịch vụ bí mật bảo vệ dữ liệu được truyền chống lại các tấn công bị động nhằm khám phá nội dung thông báo. Thông tin được bảo vệ có thể là tất cả dữ liệu được truyền giữa hai người dùng trong một khoảng thời gian hoặc một thông báo lẻ hay một số trường trong thông báo. Dịch vụ này còn cung cấp khả năng bảo vệ luồng thông tin khỏi bị tấn công phân tích tình huống.

b. Dịch vụ xác thực (Authentication)

Dịch vụ xác thực đảm bảo rằng việc truyền thông là xác thực nghĩa là cả người gửi và người nhận không bị mạo danh. Trong trường hợp có một thông báo đơn như một tín hiệu cảnh báo, tín hiệu chuông, dịch vụ xác thực đảm bảo với bên nhận rằng thông báo đến từ đúng bên nêu danh. Trong trường hợp có một giao dịch đang xảy ra, dịch vụ xác thực đảm bảo rằng hai bên giao dịch là xác thực và không có kẻ nào giả danh làm một trong các bên trao đổi. Nói cách khác, dịch vụ xác thực yêu cầu nguồn gốc của thông báo được nhận dạng đúng với các định danh đúng.

c. Dịch vụ toàn vẹn (Integrity)

Dịch vụ toàn vẹn đòi hỏi rằng các tài nguyên hệ thống máy tính và thông tin được truyền không bị sửa đổi trái phép. Việc sửa đổi bao gồm các thao tác viết, thay đổi, thay đổi trạng thái, xóa thông báo, tạo thông báo, làm trễ hoặc dùng lại các thông báo được truyền. Dịch vụ toàn vẹn có thể áp dụng cho một thông báo, một luồng thông báo hay chỉ một số trường trong thông

báo. Dịch vụ toàn vẹn định hướng kết nối (connection - oriented) áp dụng cho một luồng thông báo và nó bảo đảm rằng các thông báo được nhận có nội dung giống như khi được gửi, không bị nhân bản, chèn, sửa đổi, thay đổi trật tự hay dùng lại kể cả hủy hoại số liệu. Như vậy dịch vụ toàn vẹn định hướng kết nối quan tâm đến cả việc thay đổi thông báo và từ chối dịch vụ. Mặt khác, dịch vụ toàn vẹn phi kết nối chỉ quan tâm đến việc sửa đổi thông báo. Dịch vụ toàn vẹn này thiên về phát hiện hơn là ngăn chặn.

d. Không thể chối bỏ (Nonrepudiation)

Dịch vụ không thể chối bỏ ngăn chặn người gửi hay người nhận chối bỏ thông báo được truyền. Khi thông báo được gửi đi người nhận có thể chứng minh rằng người gửi nêu danh đã gửi nó đi. Khi thông báo nhận được, người gửi có thể chứng minh thông báo đã được nhận bởi người nhận hợp pháp.

e. Kiểm soát truy nhập (Access control)

Kiểm soát truy nhập là khả năng hạn chế và kiểm soát truy nhập đến các hệ thống máy tính và các ứng dụng theo các đường truyền thông. Mỗi thực thể muốn truy nhập đều phải định danh hay xác nhận có quyền truy nhập phù hợp.

f. Sẵn sàng phục vụ (Availability)

Sẵn sàng phục vụ đòi hỏi rằng các tài nguyên hệ thống máy tính luôn sẵn sàng đối với những bên được ủy quyền khi cần thiết. Các tấn công có thể làm mất hoặc giảm khả năng sẵn sàng phục vụ của các chương trình phần mềm và các tài nguyên phần cứng của mạng máy tính. Các phần mềm hoạt động sai chức năng có thể gây hậu quả không lường trước được. Các mối đe dọa chủ yếu tới sự an toàn trong các hệ thống mạng xuất phát từ tính mở của các kênh truyền thông (chúng là các cổng được dùng cho truyền thông hợp pháp giữa các tiến trình như client, server) và hậu quả là làm cho hệ thống bị

tấn công. Chúng ta phải thừa nhận rằng trong mọi kênh truyền thông, tại tất cả các mức của phần cứng và phần mềm của hệ thống đều chịu sự nguy hiểm của các mối đe dọa đó. Biện pháp để ngăn chặn các kiểu tấn công ở trên là:

- Xây dựng các kênh truyền thông an toàn để tránh việc nghe trộm.

- Thiết kế các giao thức xác nhận lẫn nhau giữa máy khách hàng và máy chủ:

+ Các máy chủ phải đảm bảo rằng các máy khách hàng đúng là máy của những người dùng mà chúng đòi hỏi.

+ Các máy khách hàng phải đảm bảo rằng các máy chủ cung cấp các dịch vụ đặc trưng là các máy chủ được ủy quyền cho các dịch vụ đó.

+ Đảm bảo rằng kênh truyền thông là "tươi" nhằm tránh việc dùng lại thông báo.

1.1.2. Bảo mật thông tin

1.1.2.1. Mã hóa tài liệu

a. Hệ mã hóa [7][8]

Một hệ mã hoá gồm 5 thành phần (P, C, K, E, D) thoả mãn các tính chất sau:

P (Plaintext) là tập hợp hữu hạn các bản rõ và được gọi là không gian bản rõ.

C (Ciphertext) là tập hợp hữu hạn các bản mã và được gọi là không gian các bản mã.

K (Key) là tập hợp hữu hạn các khoá hay còn gọi là không gian khóa. Đối với mỗi phần tử k của K được gọi là mốt khóa (Key). Số lượng của không gian khóa phải đủ lớn để không có đủ thời gian thử mọi khóa.

E (Encrytion) là tập hợp các qui tắc mã hoá có thể.

D (Decrytion) là tập hợp các qui tắc giải mã có thể.

Đối với mỗi k ϵ K có một quy tắc mã e_k: P → C và một quy tắc giải mã tương ứng d_k ϵ D. Mỗi e_k: P → C và d_k: C → P là những hàm mà:$d_k(e_k(x)) = x$ với mỗi x ϵ P.

Chúng ta đã biết, thông tin thường được tổ chức dưới dạng bản rõ. Người gửi thực hiện mã hoá bản rõ, kết quả thu được gọi là bản mã. Bản mã này được gửi đi trên một đường truyền tới người nhận, sau khi nhận được bản mã người nhận giải mã nó để thu được bản rõ.

Thuật toán dùng khi sử dụng định nghĩa hệ mã hóa:

$$e_k(C) = P;\ d_k(P) = C$$

Yêu cầu đối với hệ mã hóa:

+ *Độ tin cậy:* Cung cấp bí mật cho các thông tin và dữ liệu được lưu bằng việc sử dụng các kỹ thuật mã hóa.

+ *Tính toàn vẹn:* Cung cấp sự bảo đảm với tất cả các bên rằng thông tin không bị thay đổi từ khi gửi cho tới khi người nhận mở ra.

+ *Không bị chối bỏ*: Người gửi không thể từ chối việc đã gửi thông tin đi.

+ *Tính xác thực:* Người nhận có thể xác minh được nguồn tin mình nhận được là đúng đối tác của mình gửi hay không.

Dựa vào cách truyền khóa có thể phân loại hệ mã hoá thành 2 loại: hệ mã hoá khoá đối xứng (mã hoá khoá bí mật) và hệ mã hoá khoá phi đối xứng (mã hoá khoá công khai).

b. Hệ mã hoá khoá đối xứng[7][8]

Hệ mã hóa khóa đối xứng là hệ mật mã mà từ khóa mã hóa có thể dễ dàng tìm được từ khóa giải mã và ngược lại. Trong một số trường hợp, khóa mã hóa và khóa giải mã là trùng nhau.

Với hệ mật mã khóa đối xứng, người gửi và người nhận phải thỏa thuận một khóa trước khi bản tin được mã hóa và gửi đi, khóa này phải được cất giữ