ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TT&TT

NGUYỄN TIẾN DŨNG

AN TOÀN VÀ BẢO MẬT DỮ LIỆU BẰNG MÃ HOÁ ỨNG DỤNG TRONG HỆ THỐNG TRAO ĐỔI VĂN BẢN ĐIỆN TỬ

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên, 2014

MỞ ĐẦU

Ngày nay, sự phát triển mạnh mẽ của Công nghệ Thông tin, Internet, các dịch vụ phong phú của nó đã tạo ra và cung cấp cho con người những công cụ, phương tiện hết sức thuận tiện để trao đổi, tổ chức, tìm kiếm và cung cấp thông tin. Tuy nhiên, cũng như trong các phương thức truyền thống, việc trao đổi, cung cấp thông tin điện tử (văn bản điện tử) trong nhiều công việc, nhiều lĩnh vực đòi hỏi tính an toàn, tính bảo mật của thông tin là hết sức quan trọng trong việc trao đổi thông tin. Khi nhu cầu trao đổi thông tin, dữ liệu ngày càng lớn và đa dạng thì các tiến bộ về Điện tử-Viễn thông, Công nghệ Thông tin không ngừng được phát triển, các ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin, dữ liệu cần được đổi mới vì lo ngại nguy cơ mất an toàn, an ninh thông tin đang là một trong những nguyên nhân chính khiến cho nhiều cơ quan, đơn vị chưa triển khai rộng việc trao đổi văn bản điện tử và sử dụng thư điện tử. Vậy đòi hỏi chúng ta phải nghiên cứu không ngừng các vấn đề an toàn và bảo mật thông tin, dữ liệu để bảo đảm cho các hệ thống thông tin hoạt động an toàn, hiệu quả. Sự phát triển của công nghệ mã hóa đã nghiên cứu và đưa ra nhiều mô hình kỹ thuật cho phép áp dụng xây dựng các ứng dụng và đòi hỏi tính an toàn, tính bảo mật thông tin, dữ liệu cao. Hiện nay các văn bản như Chỉ thị số 34/2008/CT-TTg về tăng cường sử dụng hệ thống thư điện tử trong hoạt động của các cơ quan Nhà nước và Chỉ thị số 15/CT-TTg của Thủ tướng Chính phủ về tăng cường sử dụng văn bản điện tử trong hoạt động của các cơ quan Nhà nước.

Tại Hội nghị trực tuyến Tổng kết 05 năm triển khai thực hiện Chỉ thị số 34/2008/CT-TTg và 01 năm thực hiện Chị thị số 15/CT-TTg của Thủ tướng

Chính phủ do Bộ Thông tin và Truyền thông tổ chức ngày 24/9/2013, nhiều Bộ, ngành, địa phương cùng chung mối lo ngại về việc mất an toàn, an ninh thông tin, dữ liệu khi triển khai ứng dụng thư điện tử và trao đổi văn bản điện tử. Tuy nhiên, công tác đảm bảo an toàn, bảo mật dữ liệu còn nhiều khó khăn, các hệ thống an toàn, bảo mật và an ninh thông tin, dữ liệu chủ yếu được cài đặt riêng lẻ, chưa được triển khai đồng bộ, khả năng phòng chống virus, bảo mật chưa cao.

Để đảm bảo an toàn và bảo mật dữ liệu, thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra, các lỗ hổng về an toàn, bảo mật mà chưa được phát hiện ra đối với thông tin, dữ liệu được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng, việc xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu độ thiệt hại. Vấn đề đảm bảo An toàn và bảo mật dữ liệu trong hệ thống trao đổi văn bản điện tử là vấn đề nóng hổi, cần quan tân hàng đầu trong hoạt động thực tiễn của quá trình trao đổi văn bản điện tử giữa các cá nhân, các tổ chức, các cơ quan Nhà nước vv… Xuất phát từ thực tiễn đó, với mong muốn tìm hiểu sâu và vận dụng những kiến thức đã học về An toàn và bảo mật thông tin để ứng dụng và giải quyết một số vấn đề thực tiễn, lo lắng của các cơ quan, đơn vị trên địa bàn tỉnh Ninh Bình và đặc biệt là Sở Thông tin và Truyền thông tỉnh Ninh Bình, tôi chọn đề tài: "**An toàn và bảo mật dữ liệu bằng mã hóa ứng dụng trong hệ thống trao đổi văn bản điện tử"** làm đề tài luận văn của mình.

CHƯƠNG I: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT DỮ LIỆU. MÃ HOÁ VÀ CHỮ KÝ SỐ TRONG AN TOÀN VÀ BẢO MẬT THÔNG TIN

1.1 Nội dung của an toàn và bảo mật dữ liệu

Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về Điện tử - Viễn thông và Công nghệ Thông tin không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an tàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể đươc quy tụ vào ba nhóm sau:

- Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
- Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
- Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

Ba nhóm trên có thể được ứng dụng riêng lẻ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: Tính kín đáo riêng tư của thông tin.

- Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.

- Tính trách nhiệm: Đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xẩy ra đối với thông tin dự liệu được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng. Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được các giải pháp để giảm thiểu thiệt hại.

Có hai loại hành vi xâm phạm thông tin dữ liệu đó là: Vi phạm chủ động và vi phạm thụ động. Vi phạm thụ động chỉ nhằm mục đích cuối cùng là nắm bắt được thông tin (đánh cắp thông tin). Việc làm đó có khi không biết được nội dung cụ thể nhưng có thể dò ra được người gửi, người nhận nhờ thông tin điều khiển giao thức chứa trong phần đầu các gói tin. Kẻ xâm nhập có thể kiểm tra được số lượng, độ dài và tần số trao đổi. Vì vậy vi phạm thụ động không làm sai lệch hoặc huỷ hoại nội dung thông tin dữ liệu được trao đổi. Vi phạm thụ đông thường khó phát hiện nhưng có thể có những biện phát ngăn chặn hiệu quả. Vi phạm chủ động là dạng vi phạm có thể làm thay đổi nội dung, xoá bỏ, làm trễ, xắp xếp lại thứ tự hoặc làm lặp lại gói tin tại thời điểm đó hoặc sau một thời gian. Vi phạm chủ động có thể thêm vào một số thông tin ngoại lai để làm sai lệch nội dung thông tin trao đổi. Vi phạm chủ động dễ phát hiện nhưng để ngăn chặn hiệu quả thì khó khăn hơn nhiều.

Một thực tế là không có một biện pháp bảo vệ an toàn thông tin dữ liệu nào là an toàn tuyệt đối. Một hệ thống dù được bảo vệ chắc chắn đến đâu cũng không thể đảm bảo an toàn tuyệt đối.

1.2 Các loại tấn công trên hệ thống

Trong những năm gần đây, với sự phát triển mạnh mẽ của Công nghệ Thông tin, truyền thông cùng với nhiều ngành công nghệ cao khác đã và đang làm biến đổi sâu sắc đời sống kinh tế, chính trị, văn hoá, xã hội của đất nước. Việc ứng dụng các công nghệ mới và nâng cao công tác bảo mật cho hệ thống mạng nhằm nâng cao năng xuất làm việc để đạt được những chỉ tiêu đề ra là hết sức quan trọng, hiện nay các loại tội phạm về an ninh mạng có xu hướng gia tăng và tinh vi hơn thì việc bảo mật, an toàn cho hệ thống thông tin là rất cần thiết. Trong thực tế có trất nhiều loại, tấn công hệ thống như:

- Social Engineering (xã hội): Loại tấn công này với hai mục đích chính là đùa cợt và trục lợi. Kỹ thuật này phụ thuộc nhiều vào sơ hở của nhân viên, hacker có thể gọi điện thoại hoặc gửi e-mail giả danh người quản trị hệ thống từ đó lấy mật khẩu của nhân viên và tiến hành tấn công hệ thống. Cách tấn công này rất khó ngăn chặn. Cách duy nhất để ngăn chặn nó là giáo dục khả năng nhận thức của nhân viên về cách đề phòng.

- Impersonation (mạo danh): Là ăn cắp quyền truy cập của người sử dụng có thẩm quyền. Có nhiều cách kẻ tấn công như một hacker có thể mạo danh một người dùng hợp pháp. Ví dụ, hacker có thể nghe lén một phiên telnet sử dụng các công cụ nghe lén như Tcpdump hoặc Nitsniff. Dĩ nhiên sau khi lấy được Password, hacker có thể đăng nhập hệ thống như là người dùng hợp pháp.

- Exploits (khai thác lỗ hổng): Là hình thức tấn công này liên quan đến việc khai thác lỗi hổng trong phần mềm hoặc hệ điều hành. Do gấp rút hoàn thành để đáp ứng nhu cầu của thị trường, các phần mềm thường chưa được kiểm tra lỗi kỹ ngay cả trong dự án phần mềm lớn như hệ điều hành lỗi này cũng rất phổ biến. Các hacker thường xuyên quét các host trong mạng để tìm các lỗi này và tiến hành thâm nhập.

- Data Attacks (tấn công dữ liệu): Lập trình Script đã mang lại sự linh động cho sự phát triển của Web và bên cạnh đó cũng mang lại sự nguy hiểm cho các hệ thống do các đoạn mã độc. Những script hiện hành có thể chạy trên cả server (thường xuyên) và client. Bằng cách đó, các script có thể gửi mã độc vào hệ thống như trojan, worm, virus…

- Infrastructure Weaknesses (Điểm yếu cơ sở hạ tầng): Một số điểm yếu lớn nhất của cơ sở hạ tầng mạng được tìm thấy trong các giao thức truyền thông. Đa số hacker nhờ kiến thức về cơ sở hạ tầng sẵn có đã tận dụng những lỗ hổng và sử dụng chúng như là nơi tập trung để tấn công. Có nhiều lỗ hổng của các giao thức truyền thông và đã có bản vá những lỗi này tuy nhiên do sự mất cảnh giác không cập nhật bản vá kịp thời của những người quản trị hệ thống mà các hacker có thể tận dụng những lỗ hổng này để tấn công. Dĩ nhiên hacker sẽ phải liên tục quét hệ thống để tìm những lỗ hổng chưa được vá lỗi.

- Denial of Service (tấn công Từ chối dịch vụ): Đây là kỹ thuật tấn công rất được ưa chuộng của hacker. Loại tấn công này chủ yếu tập trung lưu lượng để làm ngưng trệ các dịch vụ của hệ thống mạng. Hệ thống được chọn sẽ bị tấn công dồn dập bằng các gói tin với các địa chỉ IP giả mạo. Để thực hiện được điều này hacker phải nắm quyền kiểm soát một số lượng lớn các host trên mạng (thực tế các host này không hề biết mình đã bị nắm quyền kiểm soát bởi hacker)

từ đó tập trung yêu cầu đến dịch vụ của hệ thống đích cho đến khi dịch vụ bị ngưng trệ hoàn toàn.

- Active Wiretap: Trong kiểu tấn công này, dữ liệu sẽ bị chặn lại trong quá trình truyền. Khi bị chặn lại có hai hành động chủ yếu đối với dữ liệu: một là gói tin sẽ bị thay đổi địa chỉ IP nguồn hoặc đích hoặc số thứ tự của gói tin, hai là dữ liệu không bị thay đổi nhưng sẽ bị sao chép để sử dụng cho những mục đích khác.

1.3 Yêu cầu an toàn bảo mật của một hệ thông tin

Trong những năm gần đây, vấn đề an toàn bảo mật hệ thống thông tin đang trở thành một vấn đề nóng, đặc biệt với hệ thống thông tin trao đổi văn bản điện tử phục vụ công tác chỉ đạo, điều hành của các cơ quan nhà nước. Có thể nói vấn đề bảo mật và an toàn của hệ thống thông tin mang tính sống còn, do đó cần có các chiến lược an toàn hệ thống:

- Giới hạn quyền hạn tối thiểu (Last Privilege): Đây là chiến lược cơ bản nhất theo nguyên tắc này bất kỳ một đối tượng nào cùng chỉ có những quyền hạn nhất định đối với tài nguyên mạng, khi thâm nhập vào mạng đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.

- Bảo vệ theo chiều sâu (Defence In Depth): Nguyên tắc này nhắc nhở chúng ta không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

- Nút thắt (Choke Point): tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này. Vì vậy phải tổ chức một cơ cấu kiểm soát và điều khiển thông tin đi qua cửa này.

- Điểm nối yếu nhất (Weakest Link): Chiến lược này dựa trên nguyên tắc "một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại một điểm yếu nhất". Kẻ phá hoại thường tìm những chỗ yếu nhất của hệ thống để tấn công, do đó ta cần phải gia cố các yếu điểm của hệ thống, thông thường chúng ta chỉ quan tâm đến kẻ tấn công hơn là kẻ tiếp cận hệ thống, do đó an toàn vật lý được coi là yếu điểm nhất trong hệ thống của chúng ta.

- Tính toàn cục: Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ, nếu có một kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của ai đó và sau đó tấn công hệ thống từ nội bộ bên trong.

- Tính đa dạng bảo vệ: Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

1.4 Khái niệm mật mã, mật mã khóa công khai

Năm 1976, Whitfield Diffie và Martin Hellman công bố một phát kiến mang tên "các phương hướng mới trong mật mã". Công trình đề xuất một dạng mới của hệ thống mật mã, trong đó người gửi và người nhận sử dụng các khoá mã khác nhau nhưng có mối liên hệ với nhau, một trong hai khoá đó được giữ bí mật.

Các thuật toán với mật mã khoá công khai (mật mã bất đối xứng) dựa trên một lớp các bài toán gọi là hàm một chiều. Các hàm này có đặc tính là rất dễ dàng thực hiện theo chiều xuôi nhưng lại rất khó (về khối lượng tính toán) để thực hiện theo chiều ngược lại. Do những đặc tính của hàm một chiều, hầu hết các khoá có thể lại là những khoá yếu và chỉ còn lại một phần nhỏ có thể dùng

để làm khoá. Vì thế, các thuật toán khoá bất đối xứng đòi hỏi độ dài khoá lớn hơn rất nhiều so với các thuật toán khoá đối xứng để đạt được độ an toàn tương đương.

Ngoài ra, việc thực hiện thuật toán khoá bất đối xứng đòi hỏi khối lượng tính toán lớn hơn nhiều lần so với thuật toán khoá đối xứng. Bên cạnh đó, đối với các hệ thống khoá đối xứng, việc tạo ra một khoá ngẫu nhiên để làm khoá phiên chỉ dùng trong một phiên giao dịch là khá dễ dàng. Vì thế, trong thực tế người ta thường kết hợp: Hệ thống mật mã khoá bất đối xứng được dùng để trao đổi khoá phiên còn hệ thống mật mã khoá đối xứng dùng khoá phiên có được để trao đổi các bản tin thực sự.

Trong một hệ mã khoá công khai (mã không đối xứng), khoá mã hoá sử dụng khoá công khai khắc phục điểm yếu của mã hoá khoá đối xứng với những đặc điểm, giải thuật khoá công khai sử dụng 2 khoá khác nhau:

+ Một khoá công khai: Ai cũng có thể biết, dùng để mã hoá thông báo và thẩm tra chữ ký.

+ Một khoá riêng: Chỉ người giữ được biết, dùng để giải mã thông báo và ký chữ ký.

+ Có tính chất bất đối xững.

+ Bên mã hoá không thể giải mã thông báo (nếu dùng để mã hoá thông báo).

+ Bên thẩm tra không thể tạo chữ ký (nếu dùng để ký).