MÔ HÌNH BẢO MẬT VÀ ĐẢM BẢO AN TOÀN THÔNG TIN HIỆN ĐẠI

LÊ MẠNH HÙNG, LÊ MỸ TÚ, NGUYỄN THANH TÙNG

Tóm tắt: *Do sự phát triển khoa học công nghệ, đặc biệt trong lĩnh vực Điện tử, Viễn thông, Toán học và Mật mã, Thu tin mã thám...thì thông tin trao đổi trên các kênh thông tin công cộng ngày càng gặp nhiều rủi ro và có nhiều mối đe dọa vì vậy đảm bảo an ninh thông tin là một vấn đề cấp bách và cần thiết. Bài viết tập trung giới thiệu mô hình đảm bảo an ninh thông tin hiện đại và xu hướng phát triển.*

Từ khóa: Bảo mật thông tin, Mật mã, Thuật toán chữ ký số, An toàn thông tin

MÔ HÌNH BẢO MẬT VÀ ĐẢM BẢO AN TOÀN THÔNG TIN HIỆN ĐẠI

Mô hình đảm bảo an ninh thông tin hiện đại được mô tả theo quan điểm về khoa học và công nghệ bao gồm từ 6 thành phần:

- **Thuật toán mật mã:** đảm bảo an ninh thông tin dựa trên kỹ thuật mật mã, hàm tóm lược, thuật toán chữ ký số...
- **Các biện pháp kỹ thuật không dựa vào kỹ thuật mật mã:** có nghĩa là các phương pháp đảm bảo an ninh thông tin không dựa trên kỹ thuật mật mã, ví dụ: Hàm thời gian (Time Variant Parametrs), Kỹ thuật sinh trắc học (như phân tích vân bàn tay, mặt người, giọng nói...),
- **Giao thức an toàn**, thực hiện dịch vụ an toàn đã chọn, các giao thức có thể sử dụng thuật toán mật mã hoặc các biện pháp kỹ thuật không mật mã, ví dụ các giao thức xác thực hoặc các giao thức chia sẻ bí mật...
- **Các Hệ thống an toàn**, mở rộng ứng dụng hoặc sử dụng bằng phần cứng thực hiện các dịch vụ đã chọn để bảo vệ thông tin. Trường hợp đặc biệt ứng dụng các giao thức an toàn đã chọn, ví dụ các hệ thống thực hiện mạng riêng ảo (giao thức xác thực, bảo mật và toàn vẹn), trong một vài trường hợp Hệ thống an toàn chỉ sử dụng các biện pháp kỹ thuật không mật mã để bảo vệ thông tin như: bức tường lửa (firewall), lọc gói tin dựa vào danh sách điều khiển truy cập. Ẩn mã (steganografia) là một phương tiện hiệu quả che giấu thông tin, dữ liệu...
- **Tổ chức điều hành an toàn thông tin**, có nghĩa là quản lý an ninh hệ thống thông tin bắt đầu từ đánh giá rủi ro, thiết kế an toàn, thông qua thực hiện và khai thác.
- **Pháp luật**, có nghĩa là các vấn đề lập pháp có tác động đến an toàn thông tin (bao gồm cả chất lượng).

Sau đây chúng ta sẽ xem xét kỹ xu hướng phát triển của từng lĩnh vực đã đề cập ở trên:

A. Thuật toán mật mã:

Sự phát triển mạnh mẽ của các thuật toán mật mã trên thế giới được thúc đẩy và đặc trưng bởi hai xu hướng trái ngược nhau. Xu hướng thứ nhất là thúc đẩy sự phát triển mạnh mẽ, phân tầng của Kỹ thuật mã thám nhờ sử dụng Hệ thống tính toán phân tán; Thứ hai là xu hướng tác động tiêu cực đến mã thám vì thuật toán ngày càng đáp ứng được nhu cầu và thực hiện tốt các kỹ thuật mã mật hoàn hảo.

Xem xét về thiết kế cấu trúc của thuật toán mật mã, đã có sự thay đổi cơ bản trong cấu trúc của hệ mật mới nhất - Rijndael, sau đó là thuật toán DES (Data Encryption Standard). Đến nay trong hệ mật đối xứng về nguyên tắc vẫn sử dụng lược đồ Feistel. Cạnh tranh với DES, hệ mật AES (Advanced Encryption Standard) công bố nhiều thuật toán mới mà hoạt động của chúng dựa trên lược đồ Feistel. Hiện nay Hệ mật khóa công khai đang đóng một

vai trò nổi trội. Đặc biệt Hệ mật khóa công khai sử dụng công cụ toán học phát triển như Hệ mật dựa trên đường cong eliptic. Thuật toán Rijndael là thuật toán dựa trên hệ mật mã đối xứng, trong đó độ dài khóa 128, 192, 256, 512...bit. Độ dài khóa nêu trên cần đảm bảo được độ an toàn trong vài thập kỷ tiếp theo. Tương tự Thuật toán DES sử dụng khóa hiệu quả 128 bit, Thuật toán 3DES 256 bit. Viện tiêu chuẩn và công nghệ quốc gia (NIST) Mỹ đã cập nhật thuật toán hàm tóm lược SHA (Secure Hash Algorythm) với đề nghị thuật toán mới với ký hiệu SHA-256, SHA-384, SHA-512, với các độ dài tóm lược tạo nên bởi thuật toán này...Trong lĩnh vực chữ ký số cho đến nay thuật toán DSA (Digital Signature Algorithm) với độ dài 256 bit vẫn xem là an toàn.

B. Các biện pháp kỹ thuật không dựa vào kỹ thuật mật mã:

Trong các biện pháp kỹ thuật không dựa vào kỹ thuật mật mã cần phải nhấn mạnh vào xu hướng sử dụng các biện pháp kỹ thuật sinh trắc học. Kỹ thuật sinh trắc học dùng để xác thực người dùng, mà nguồn thông tin xác thực có thể là vân tay, khuôn mặt, chữ viết (bao gồm cả chữ ký), đặc trưng giọng nói...Đã thúc đẩy nhiều công trình nghiên cứu nhằm đưa ra các công thức toán học mô tả các đặc trưng sinh trắc mà kết quả tạo nên được các Hệ thống xác thực hiệu quả hơn với độ chính xác cao (mức sai số chỉ là phần nhỏ sau dấu phẩy của phần trăm). Nguồn sinh trắc đặc trưng xác thực thường có một vài chục đến một vài trăm đại lượng đưa vào phân tích. Ví dụ Hệ thống nhận dạng dựa trên hình bàn tay có thể dựa trên khoảng 100 đại lượng đặc trưng như: độ rộng, độ dày của bàn tay, độ dài độ dày của ngón tay....

Càng ngày người ta càng sử dụng biện pháp xác thực lai ghép, trong đó ngoài các phương pháp xác thực thông thường (nhận dạng vân tay, nhận dạng khuôn mặt...), người ta còn chú ý đến vị trí hiện tại của người được nhận dạng dựa vào máy thu cá nhân của người đó trong Hệ thống định vị GPS (Global Positioning System). Người ta dự đoán rằng việc sử dụng hàng loạt kỹ thuật sinh trắc không những cho phép tương tác ngày càng tốt hơn giữa người dùng và hệ thống thông tin mà còn xóa bỏ rào cản liên quan đến việc phải nhớ quá nhiều bộ mã: PIN, mật khẩu,...hoặc chìa khóa khi về nhà hoặc lên xe ô tô...

C. Giao thức an toàn

Mặc dù vị trí của dịch vụ bảo vệ an toàn thông tin có thể ở trong mọi lớp mạng. Trong mạng truyền dẫn hữu tuyến không thể hiện rõ nét xu hướng ứng dụng dịch vụ bảo vệ an toàn thông tin cùng với giao thức truyền tin. Trong mạng không dây ở 02 lớp mạng thấp nhất việc ứng dụng bảo mật dữ liệu được thực hiện bằng cơ chế mã mật. Thường sử dụng ở đây hệ mật mã dòng đối xứng giả ngẫu nhiên (Ví dục RC4) với độ dài khóa không dài (ví dụ 64 bit), đôi khi cố ý thấp hơn ví dụ: khoảng 40 bit. Chắc chắn rằng ở mức an toàn này người ta thường kết hợp với một vài phương pháp truyền tin (ví dụ: kỹ thuật nhảy tần FHSS - frequency Hopping Spread Spectrum, DSSS - Direct Sequence Spread Spectrum) nhằm bảo vệ chống thu trộm một cách ngẫu nhiên nhưng không bảo vệ được trước các tấn công nâng cao. Một vài giao thức an toàn phổ biến nhất đối với mạng không dây ví dụ: như WEP (Wired Equivalent Privacy) sử dụng cùng với Chuẩn IEEE 802.11 có chứa lỗi trong cấu trúc nên trong trường hợp đặc biệt kết hợp với mã Cyclic cục bộ kiểu CRC-32 để đảm bảo tính toàn vẹn. Ngoài bảo mật trong mạng không dây người ta còn xác thực các trạm đầu cuối dựa vào hệ mật đối xứng sử dụng khóa chung.

Trong các giao thức phổ biến của mạng truyền dữ liệu như mạng ATM, Frame Relay, MPLS... không xử lý bất kỳ dịch vụ bảo vệ thông tin nào. Đặc biệt giao thức MPLS thường được nhầm lẫn như là mạng an toàn, mặc dù độ an toàn mạng MPLS không sai khác mấy so với các mạng truyền dữ liệu khác. Bởi vì theo những người sáng lập ra các giao thức mạng thì trách nhiệm bảo mật dữ liệu thuộc về người sử dụng.

Trong các lớp mạng trên, dịch vụ bảo mật thông tin thường tùy chọn và là bài toán dành cho lớp mạng sử dụng giao thức TCP/IP. Xu thế bảo mật dữ liệu sử dụng giao thức liên mạng TCP/IP thường chia ra 02 cách.

Cách 1: thay thế giao thức IPv4 bằng giao thức IPv6 hoặc bổ sung giao thức IPv4 bằng giao thức IPsec. Đối với IPsec và IPv6 cơ chế an toàn như sau:

- Tiêu đề xác thực - nhằm đảm bảo tính toàn vẹn và tính xác thực
- Đóng gói IP bí mật - Gói an toàn nhằm đảm bảo tính bí mật tùy thuộc vào thuật toán và chế độ làm việc, cũng như cách thức đảm bảo tính toàn vẹn và xác thực.

Cách thức phân phối khóa mã xác thực được thực hiện dựa vào giao thức IKE - Internet Key Exchange.

Cách thứ 2: Bổ sung vào lớp vận tải giao thức thực hiện đảm bảo tính bí mật, toàn vẹn , xác thực; thường gọi là TLS (Transport Layer Security) mà các phiên bản trước đây thường gọi SSL (Secure Socket Layer). An toàn được thực hiện bởi giao thức TLS thường giới hạn cho các ứng dụng sử dụng giao thức TCP (ví dụ: HPTP, FPT, SMTP, POP3). Với thay đổi đặc biệt với cách gọi đến lớp vận tải giao thức TLS không thay đổi cấu trúc ứng dụng. Điều đó thích ứng với lớp an toàn trong môi trường WAP (WTLS - Wireless Transport Layer Security).

Bảo mật hệ thống đóng vai trò quan trọng. Tính bảo mật thường được thực hiện thông qua tính toàn vẹn và xác thực (ví dụ: Hệ thống thư điện tử an toàn PEM - Privacy Ehancement for Internet Electronic Mail và PGP - Pretty Good Privacy). Đôi khi tính bảo mật đạt được bằng cách ẩn danh. Để thực hiện mục đích này thông thường ứng dụng hệ thống không xác định người lướt internet và hệ thống nhắn tin vô danh.

D. Các hệ thống an toàn

Bức tường lửa (firewall) là Hệ thống được sử dụng rộng rãi để bảo vệ an toàn thông tin trên mạng. Dạng đơn giản nhất của hệ thống này là bộ lọc, nhằm loại bỏ những gói tin đến từ một vị trí cụ thể, cũng như loại bỏ các đơn vị dữ liệu không chính xác. Các bức tường lửa thực hiện dịch vụ kiểm soát truy cập, cũng như trên cơ sở bản ghi (log) được tạo nên cho phép bạn kiểm toán. Bức tường lửa, mặc dù được sử dụng thông dụng nhất trong các mạng sử dụng giao thức TCP/IP, nhưng cũng được tích hợp cho các mạng dữ liệu, chẳng hạn như mạng ATM. Ngoài tầng mạng và tầng vận tải Bức tường lửa có thể hoạt động ở mức giao thức của tầng ứng dụng như là hệ thống trung gian.

Hệ thống quan trọng tiếp theo để bảo vệ an toàn thông tin là ***Hệ thống phát hiện xâm nhập (Instruction Detection System)***. Đây là một hệ thống phát hiện hành vi không tuân thủ với hành vi đúng đã được định dạng trước đó hoặc phát hiện các vi phạm rõ ràng sự bảo đảm an toàn hệ thống. Các Hệ thống phát hiện xâm nhập có thể trao đổi lẫn nhau thông tin về các cuộc tấn công về dạng các mẫu gian lận, cũng có thể thử phát hiện các hành vi khác nhau hoặc bất thường. Nguồn kiến thức về các biến cố dành cho Hệ thống phát hiện xâm nhập có thể lấy từ các tầng mạng, đặc biệt: tầng mạng, tầng vận tải, tầng ứng dụng và cả trong hệ điều hành máy.

Hệ thống quản lý gian lận (fraud management system): Hệ thống quản lý gian lận (fraud management system) được thiết kế cho các nhà khai thác viễn thông có nhiều yếu tố chung với hệ thống phát hiện xâm nhập. Mục đích của việc triển khai hệ thống như vậy là để giảm gian lận được thực hiện bởi khách hàng hoặc nhân viên không trung thực. Gian lận có thể xảy ra trong hình thức các hóa đơn chưa thanh toán, hoặc các phương pháp miễn phí sử dụng tài nguyên của nhà điều hành. Hệ thống gian lận thường làm việc trên cơ sở thông tin thanh toán, mà thường bị hạn chế về thời gian (sự chậm trễ trong truy cập vào thông tin thanh toán), cũng như hạn chế độ tin cậy của các hệ thống để đảm bảo tính chính xác của hệ thống thanh toán.

Hệ thống quản lý gian lận có thể tận dụng lợi thế của các thông tin hoạt động trực tiếp từ hệ thống cảnh báo. Sử dụng những hệ thống như vậy đòi hỏi phải có thiết bị báo hiệu đắt tiền, lắp đặt chính xác ở những vị trí thích hợp mới đem lại hiệu quả cao.

Một mối đe dọa lớn đối với các mạng truyền dữ liệu là các phần mềm độc hại: Virus, sâu mạng, virus con ngựa thành Tơ roa...thường được phát tán qua thư điện tử ở dạng file đính kèm...Vì vậy xu hướng hiện nay là tích hợp các hệ thống mật mã với các hệ thống phát hiện xâm nhập và phát hiện phần mềm độc hại. Cần phải nhấn mạnh rằng trong các hệ thống mật mã hiện đại thường kết hợp mã mật và nén dữ liệu. Quá trình nén dữ liệu thường được thực hiện trước khi mã mật vì nén dữ liệu đã mã mật thường không hiệu quả.

Bảo vệ thông tin bằng mật mã thường được sử dụng trong mạng riêng ảo VPN (Virtual Private Network). Trong mạng TCP/IP thường sử dụng giao thức IPSec. Trong mạng MPLS-VPN tính bảo mật đạt được nhờ vào giao thức IPSec.

Ngoài ra, ẩn mã (steganografia) là một phương tiện hiệu quả che giấu thông tin, dữ liệu...để bảo vệ quyền tác giả, chống can thiệp khai thác bất hợp pháp, trao đổi thông tin mật. Ẩn mã đơn giản chỉ là một trong nhiều cách bảo đảm tính bí mật của dữ liệu. Thực tế tốt nhất là nên kết hợp ẩn mã với phương pháp bảo mật khác.

E. Tổ chức điều hành an toàn thông tin

Trong cách tổ chức an toàn thông tin nên xem xét hai khía cạnh: điều hành an toàn và an toàn điều hành. Điều hành an toàn xét về mặt kỹ thuật là điều hành các dịch vụ và các cơ chế bảo vệ thông tin. Được thực hiện bằng cách cung cấp thông tin quản lý các dịch vụ và các cơ chế, cũng như việc thu thập và lưu trữ thông tin về các dịch vụ đó và các cơ chế dịch vụ. Xét từ mặt tổ chức an toàn thông tin đó là là quá trình thiết kế, thực hiện, đánh giá và vận hành hệ thống một cách an toàn. Để lựa chọn giải pháp kỹ thuật và tổ chức điều hành an toàn đúng đắn, đòi hỏi phải phân tích các rủi ro như: phân tích mối các đe dọa, các điểm yếu ... Bởi vì điều hành an toàn là một quá trình, không phải là một hành động đơn lẻ, điều hành với các rủi ro cao.

Các đề xuất an toàn cho các hệ thống thông tin thường được thể hiện trong chiến lược an ninh thông tin từng quốc gia. An toàn điều hành là thực hiện chính sách an toàn thông tin trong lĩnh vực quản lý cấu hình hệ thống, hiệu suất, hỏng hóc...đã được tính toán phù hợp yêu cầu đảm bảo an ninh thông tin. Đối với các nhà khai thác viễn thông thì an toàn của hệ thống được xem như một thuộc tính của hệ thống với các đặc tính sau: đảm bảo tính bí mật, tính toàn vẹn, tính sẵn sàng, độ tin cậy...

Ngày nay, không chỉ chữ ký điện tử, mà cơ sở hạ tầng khóa công khai (PKI - Public Key Infrastructure) ngày càng thông dụng cho phép việc tạo ra các dịch vụ sử dụng chứng chỉ khóa công khai.

Vấn đề cơ bản trong cơ sở hạ tầng khóa công khai là chứng chỉ tin cậy. Một chứng thực tiêu biểu gồm các thành phần sau: Khóa công khai; Tên: có thể là tên người, máy chủ hoặc tổ chức; Thời hạn sử dụng; Địa chỉ URL của trung tâm thu hồi chứng thực (để kiểm tra). Tiêu chuẩn chứng thực khóa công khai phổ biến nhất hiện này là X.509 do ITU-T ban hành.

Cho đến nay, phần lớn các giải pháp sử dụng các thuật toán khóa công khai được thiết kế để làm việc thích hợp với cơ sở hạ tầng khóa công khai. Ví dụ: TLS / SSL, S/MI- ME (Secure / Multipurpose Internet Mail Extensions), SET (Secure Electronic Transactions), PEM (Privacy Enhancement for Internet Electronic Mail). Ngoài ra Cơ sở hạ tầng khóa công khai không dây (Wireless PKI) viết tắt (W-PKI) được đầu tư nghiên cứu nhờ đó mở rộng khả năng ứng dụng vào các dịch vụ dựa trên chứng chỉ số dùng cho điện thoại di động.

F. Luật pháp

Sự gia tăng cạnh tranh trong truyền tin và bảo mật thông tin luôn gắn chặt với các mối đe dọa và những tội phạm. Bởi vì các mối đe dọa này ngày càng tăng về số lượng, chất

lượng, quy mô... so với mức độ gây hại của các virus, sâu mạng...trước đây. Vì vậy không có gì đáng ngạc nhiên là chúng ta phải xem xét điều này trên khía cạnh Pháp luật. Ở nhiều nước sự xuất hiện của virus máy tính, hacker... gây ra thiệt hại lớn cho các Cơ quan, doanh nghiệp... vì vậy đòi hỏi phải nhanh chóng xây dựng những điều luật nhằm hạn chế và loại bỏ loại tội phạm trên. Tuy nhiên, thực tế là các tội phạm mạng... bắt đầu có tính chất xuyên biên giới, quốc tế hóa. Nếu như chúng ta sử dụng những hệ thống mã mật hiện đại nhất mà thế giới tội phạm (mafia mức độ thế giới: buôn lậu ma túy, buôn lậu vũ khí, khủng bố...) không thể bẻ khóa được thì vấn đề luật pháp không phải bàn cãi. Nhưng những người dùng lương thiện khai thác hệ thống truyền thông hiện đại khác...sẽ phải đối mặt loại tội phạm này.

Vì vậy đối với mỗi nước phải xây dựng những văn bản luật pháp về bảo vệ bí mật nhà nước, bảo vệ thông tin truyền thông trên mạng...Ở Mỹ ba văn bản cơ bản được ban hành: *Luật về bảo vệ dữ liệu cá nhân, Luật về bảo vệ thông tin mật và Luật về chữ ký điện tử.*

Luật về bảo vệ dữ liệu cá nhân không chỉ bảo vệ dữ liệu liên quan đến một cá nhân, những gì về một người cụ thể có thể được công khai, mà còn kiểm tra sự truy cập khai thác tập dữ liệu của từng cá nhân một cách chặt chẽ.

Luật bảo vệ thông tin mật là một bước tiến rất quan trọng đối với các hệ thống bảo vệ thông tin mật. Pháp luật hiện hành liệt kê rõ ràng những thông tin mật cần bảo vệ và làm rõ trách nhiệm những người được tiếp cận với chúng.

Luật về chữ ký điện tử về cơ bản dựa trên chứng thực chữ ký điện tử. Tương tự như chữ ký truyền thống. Tự chữ ký bằng tay không có giá trị gì cả nếu không được xác thực. ví dụ: ra ngân hàng giao dịch sau khi ký xong cần đưa chứng minh thư ra để xác thực. Tương tự chữ ký điện tử cũng cần được xác thực. Chữ ký truyền thống thường được kiểm tra và xác thực bằng chứng minh nhân dân (hoặc hộ chiếu) tại một địa điểm và thời gian cụ thể, còn xác thực chữ ký điện tử diễn ra trong không gian ảo và gần như không có thời gian cụ thể.

Nước ta, Đảng và Nhà nước hết sức quan tâm chỉ đạo công tác bảo mật thông tin. Nhiều văn bản pháp luật đã được ban hành: *Luật Cơ yếu (số: 05/2011/QH13), Pháp lệnh bảo vệ bí mật nhà nước ((Số 30/2000/PL-UBTVQH10), Luật Giao dịch điện tử ngày 29/11/2005; Nghị định 26/2007/NĐ-CP ngày 15/02/2007* quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số...Đó là những căn cứ pháp lý hết sức quan trọng để triển khai nhiệm vụ bảo mật và an toàn thông tin.

KẾT LUẬN

Bảo đảm bí mật và an toàn thông tin trong lĩnh vực An ninh - Quốc phòng và Kinh tế - Xã hội trong giai đoạn hiện nay là hết sức quan trọng. Để triển khai xây dựng tốt Hệ thống thông tin mật trên theo mô hình đảm bảo an ninh thông tin hiện đại cần phải quan tâm đồng bộ 6 thành phần nói trên. Nói cách khác phải thực hiện đồng bộ cả về Khoa học Mật mã, Kỹ thuật Mật mã và Nghiệp vụ Mật mã và An toàn Thông tin.

TÀI LIỆU THAM KHẢO

[1]. NIST FIPS PUB 191, *"Advenced Encryption Standard (AES)"*. National Institute of Standards and Technology, U. S. Department of Commerce, 2009.

[2]. NIST FIPS PUB 186, *"Digital Signature Standard. National Institute of Standards and Technology"*, U. S. Department of Commerce, 2010.

[3]. NIST FIPS PUB 180-1, *"Secure Hash Standard (SHS). National Institute of Standards and Technology"*, U. S. Department of Commerce, 2013.

[4]. ITU-T X. 509, OSI, *"The Directory – Part 8: Authentication Framework"*, Revision 3

ABSTRACT

MODERN MODEL FOR SECURITY AND SAFETY INFORMATION

Due to the development of science and technology, particularly in the field of Electronics, Telecommunications, Mathematics and Cryptography, The private detective codes ... the exchange of information on the public information channel more risky and there are so many threats to ensure information security is an urgent issue and necessary. The paper focuses introduce modern model for security and safety information and trends

Keywords: Information security, Cryptography, Digital Signature Algorithm, Safety information

Nhận bài ngày 19 tháng 5 năm 2014
Hoàn thiện ngày 05 tháng 6 năm 2014
Chấp nhận đăng ngày 25 tháng 7 năm 2014

Địa chỉ: Học viện Kỹ thuật Mật mã