HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
CƠ SỞ TP. HỒ CHÍ MINH

BÀI GIẢNG

BẢO MẬT HỆ THỐNG THÔNG TIN

DÀNH CHO HỆ ĐÀO TẠO TỪ XA

Biên soạn: Lê Phúc

Tháng 7/2007

MỞ ĐẦU

Tài liệu này được xây dựng với mục đích giúp sinh viên hệ đào tạo từ xa nghiên cứu các vấn đề về bảo mật hệ thống thông tin. Bảo mật hệ thống thông tin là tập các kỹ thuật, dịch vụ, cơ chế và ứng dụng phụ trợ giúp triển khai các hệ thống thông tin với độ an toàn cao nhất, mà cụ thể là để bảo vệ ba đặc trưng cơ bản của một hệ thống an toàn là *tính Bí mật*, *tính Toàn vẹn* và *tính Khả dụng* của thông tin.

Tính bảo mật của hệ thống là vấn đề được cân nhắc ngay khi thiết kế hệ thống và được thực hiện xuyên suốt trong quá trình thi công, vận hành và bảo dưỡng hệ thống. Trong thời điểm mà việc kết nối vào mạng Internet, nơi chứa rất nhiều nguy cơ tấn công tiềm ẩn, đã trở thành một nhu cầu sống còn của các hệ thống thông tin thì vấn đề bảo mật càng cần phải được quan tâm và đầu tư đúng mức.

Tài liệu này nhắm đến đối tượng sinh viên là những người vừa học vừa làm, do đó các vấn đề bảo mật thực tế trên mạng được quan tâm nhiều hơn là các cơ sở lý thuyết. Các chuyên đề về mật mã cũng được trình bày đơn giản theo cách nhìn của người sử dụng, không quá chuyên sâu về cơ sở toán học, do đó, nếu có nhu cầu tìm hiểu sâu hơn hoặc chứng minh các thuật toán, sinh viên cần phải đọc thêm các tài liệu về lý thuyết số.

Nội dung tài liệu được chia thành 3 chương:

-Chương 1:*Tổng quan về bảo mật hệ thống thông tin*, trình bày các vấn đề chung về bảo mật và an toàn hệ thống, các nguy cơ và các phương thức tấn công vào hệ thống thông tin, các ứng dụng bảo vệ hệ thống thông tin đang được sử dụng như Firewall và IDS…

-Chương 2: *Mật mã và xác thực thông tin*, trình bày các cơ chế mật mã và xác thực nhằm đảm bảo tính Bí mật và Toàn vẹn của thông tin. Phần này mô tả nguyên lý của các thuật toán mật mã thông dụng, hàm băm, chữ ký số và các vấn đề quản lý khoá.

-Chương 3: *Các ứng dụng bảo mật trong hệ thống thông tin*, trình bày các ứng dụng thực tế như các giao thức xác thực, bảo mật trong kết nối mạng với IPSec, bảo mật trong ứng dụng Internet với SSL và SET.

Cuối mỗi chương đều có phần tóm tắt, các câu hỏi trắc nghiệm và bài tập, giúp sinh viên hệ thống hoá lại kiến thức đã học. Đặc biệt, các bài tập thực hành và lập trình sẽ giúp sinh viên nắm rõ hơn phần lý thuyết, nên cố gắng thực hiện các bài tập này một cách chu đáo.

Hy vọng tài liệu này sẽ ít nhiều giúp ích cho việc nghiên cứu chuyên đề an toàn hệ thống thông tin của các bạn sinh viên.

Tháng 7/2007.

Tác giả.

CHƯƠNG I
TỔNG QUAN VỀ BẢO MẬT HỆ THỐNG THÔNG TIN

Giới thiệu:

Chương này giúp học viên nắm được các khái niệm thường dùng trong bảo mật và an toàn hệ thống, nguyên tắc xây dựng một hệ thống thông tin bảo mật, nhận diện và phân tích các nguy cơ và rủi ro đối với hệ thống thông tin, từ đó có kế hoạch nâng cấp và bảo vệ hệ thống.

Nội dung chương này gồm các phần như sau:

-Các đặc trưng của một hệ thống bảo mật.

-Nguy cơ và rủi ro đối với hệ thống thông tin.

-Các khái niệm dùng trong bảo mật hệ thống

-Chiến lược bảo mật hệ thống AAA.

-Một số hình thức xâm nhập hệ thống.

-Kỹ thuật ngăn chặn và phát hiện xâm nhập.

I.1 TỔNG QUAN

Vấn đề bảo đảm an toàn cho các hệ thống thông tin là một trong những vấn đề quan trọng cần cân nhắc trong suốt quá trình thiết kế, thi công, vận hành và bảo dưỡng hệ thống thông tin.

Cũng như tất cả các hoạt động khác trong đời sống xã hội, từ khi con người có nhu cầu lưu trữ và xử lý thông tin, đặc biệt là từ khi thông tin được xem như một bộ phận của tư liệu sản xuất, thì nhu cầu bảo vệ thông tin càng trở nên bức thiết. Bảo vệ thông tin là bảo vệ *tính bí mật* của thông tin và *tính toàn vẹn* của thông tin. Một số loại thông tin chỉ còn ý nghĩa khi chúng được giữ kín hoặc giới hạn trong một số các đối tượng nào đó, ví dụ như thông tin về chiến lược quân sự chẳng hạn. Đây là tính bí mật của thông tin. Hơn nữa, thông tin không phải luôn được con người ghi nhớ do sự hữu hạn của bộ óc, nên cần phải có thiết bị để lưu trữ thông tin. Nếu thiết bị lưu trữ hoạt động không an toàn, thông tin lưu trữ trên đó bị mất đi hoặc sai lệch toàn bộ hay một phần, khi đó tính toàn vẹn của thông tin không còn được bảo đảm.

Khi máy tính được sử dụng để xử lý thông tin, hiệu quả xử lý thông tin được nâng cao lên, khối lượng thông tin được xử lý càng ngày càng lớn lên, và kéo theo nó, tầm quan trọng của thông tin trong đời sống xã hội cũng tăng lên. Nếu như trước đây, việc bảo vệ thông tin chỉ chú trọng vào vấn đề dùng các cơ chế và phương tiện vật lý để bảo vệ thông tin theo đúng nghĩa đen của từ này, thì càng về sau, vấn đề bảo vệ thông tin đã trở nên đa dạng hơn và phức tạp hơn. Có thể kể ra hai điều thay đổi lớn sau đây đối với vấn đề bảo vệ thông tin:

1-Sự ứng dụng của máy tính trong việc xử lý thông tin làm thay đổi dạng lưu trữ của thông tin và phương thức xử lý thông tin. Cần thiết phải xây dựng các cơ chế bảo vệ thông tin theo đặc thù hoạt động của máy tính. Từ đây xuất hiện yêu cầu bảo vệ sự an toàn hoạt động của máy tính ***(Computer Security)*** tồn tại song song với yêu cầu bảo vệ sự an toàn của thông tin ***(Information Security)***.

2-Sự phát triển mạnh mẽ của mạng máy tính và các hệ thống phân tán làm thay đổi phạm vi tổ chức xử lý thông tin. Thông tin được trao đổi giữa các thiết bị xử lý thông qua một khoảng cách vật lý rất lớn, gần như không giới hạn, làm xuất hiện thêm nhiều nguy cơ hơn đối với sự an toàn của thông tin. Từ đó xuất hiện yêu cầu bảo vệ sự an toàn của hệ thống mạng ***(Network***

Security), gồm các cơ chế và kỹ thuật phù hợp với việc bảo vệ sự an toàn của thông tin khi chúng được trao đổi giữa các thiết bị trên mạng.

Cùng với việc nhận diện hai điều thay đổi lớn đối với vấn đề bảo đảm an toàn thông tin, hiện nay, khái niệm bảo đảm thông tin ***(Information Assurance)*** được đề xuất như một giải pháp toàn diện hơn cho bảo mật thông tin. Theo đó, vấn đề an toàn của thông tin không còn chỉ giới hạn trong việc đảm bảo tính bí mật và tính toàn vẹn của thông tin, phạm vi bảo vệ không còn giới hạn trong các hệ thống máy tính làm chức năng xử lý thông tin nữa, mà diễn ra trong tất cả các hệ thống tự động (automated systems). Yêu cầu bảo vệ không còn chỉ tập trung ở vấn đề an toàn động ***(Security)*** nữa mà bao gồm cả vấn đề an toàn tĩnh ***(Safety)*** và vấn đề tin cậy của hệ thống ***(Reliability).***

Trong phạm vi tài liệu này, vấn đề Bảo mật hệ thống thông tin (Information System Security) là vấn đề trọng tâm nhất. Toàn bộ tài liệu sẽ tập trung vào việc mô tả, phân tích các cơ chế và kỹ thuật nhằm cung cấp sự bảo mật cho các hệ thống thông tin. Một hệ thống thông tin, theo cách hiểu ngầm định trong tài liệu này, là hệ thống xử lý thông tin bằng công cụ máy tính, được tổ chức tập trung hoặc phân tán. Do vậy, nội dung của tài liệu sẽ vừa đề cập đến vấn đề bảo mật máy tính (Computer Security) và bảo mật mạng (Network Security). Tuy vậy, các kỹ thuật bảo mật mạng chỉ được đề cập một cách giản lược, dành phần cho một tài liệu khác thuộc chuyên ngành Mạng máy tính và truyền thông, đó là tài liệu Bảo mật mạng.

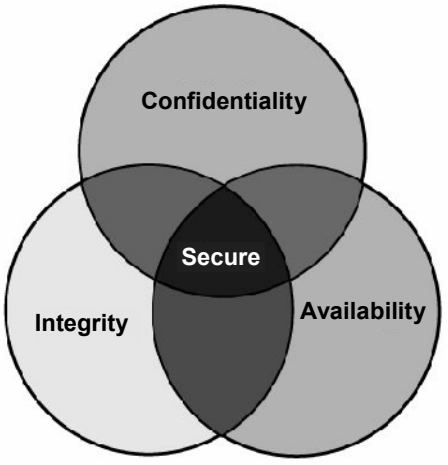
I.2 CÁC ĐẶC TRƯNG CỦA MỘT HỆ THỐNG THÔNG TIN BẢO MẬT

Một hệ thống thông tin bảo mật (Secure Information System) là một hệ thống mà thông tin được xử lý trên nó phải đảm bảo được 3 đặc trưng sau đây:

-Tính bí mật của thông tin ***(Confidentiality)***

-Tính toàn vẹn của thông tin ***(Integrity)***

-Tính khả dụng của thông tin ***(Availability).***



Hình 1.1: *Mô hình CIA*

Ba đặc trưng này được liên kết lại và xem như là mô hình tiêu chuẩn của các hệ thống thông tin bảo mật, hay nói cách khác, đây là 3 thành phần cốt yếu của một hệ thống thông tin Bảo mật. Mô hình này được sử dụng rộng rãi trong nhiều ngữ cảnh và nhiều tài liệu khác nhau, và

được gọi tắt là mô hình ***CIA*** (chú ý phân biệt với thuật ngữ CIA với ý nghĩa Confidentiality, Itegrity, Authentication trong một số tài liệu khác).

Phần sau đây sẽ trình bày chi tiết về từng đặc trưng này.

I.2.1 Tính bí mật:

Một số loại thông tin chỉ có giá trị đối với một đối tượng xác định khi chúng không phổ biến cho các đối tượng khác. *Tính bí mật của thông tin là tính giới hạn về đối tượng được quyền truy xuất đến thông tin*. Đối tượng truy xuất có thể là con người, là máy tính hoặc phần mềm, kể cả phần mềm phá hoại như virus, worm, spyware, …

Tuỳ theo tính chất của thông tin mà mức độ bí mật của chúng có khác nhau. Ví dụ: các thông tin về chính trị và quân sự luôn được xem là các thông tin nhạy cảm nhất đối với các quốc gia và được xử lý ở mức bảo mật cao nhất. Các thông tin khác như thông tin về hoạt động và chiến lược kinh doanh của doanh nghiệp, thông tin cá nhân, đặc biệt của những người nổi tiếng, thông tin cấu hình hệ thống của các mạng cung cấp dịch vụ, v.v… đều có nhu cầu được giữ bí mật ở từng mức độ.

Để đảm bảo tính bí mật của thông tin, ngoài các cơ chế và phương tiện vật lý như nhà xưởng, thiết bị lưu trữ, dịch vụ bảo vệ, … thì kỹ thuật mật mã hoá (Cryptography) được xem là công cụ bảo mật thông tin hữu hiệu nhất trong môi trường máy tính. Các kỹ thuật mật mã hoá sẽ được trình bày cụ thể ở chương II. Ngoài ra, kỹ thuật quản lý truy xuất (Access Control) cũng được thiết lập để bảo đảm chỉ có những đối tượng được cho phép mới có thể truy xuất thông tin. Access control sẽ được trình bày ở phần 3 của chương này.

Sự bí mật của thông tin phải được xem xét dưới dạng 2 yếu tố tách rời: sự *tồn tại của thông tin* và *nội dung của thông tin đó*.

Đôi khi, tiết lộ sự tồn tại của thông tin có ý nghĩa cao hơn tiết lộ nội dung của nó. Ví dụ: chiến lược kinh doanh bí mật mang tính sống còn của một công ty đã bị tiết lộ cho một công ty đối thủ khác. Việc nhận thức được rằng có điều đó tồn tại sẽ quan trọng hơn nhiều so với việc biết cụ thể về nội dung thông tin, chẳng hạn như ai đã tiết lộ, tiết lộ cho đối thủ nào và tiết lộ những thông tin gì,…

Cũng vì lý do này, trong một số hệ thống xác thực người dùng (user authentication) ví dụ như đăng nhập vào hệ điều hành Netware hay đăng nhập vào hộp thư điện tử hoặc các dịch vụ khác trên mạng, khi người sử dụng cung cấp một tên người dùng (user-name) sai, thay vì thông báo rằng user-name này không tồn tại, thì một số hệ thống sẽ thông báo rằng mật khẩu (password) sai, một số hệ thống khác chỉ thông báo chung chung là "Invalid user name/password" (người dùng hoặc mật khẩu không hợp lệ). Dụng ý đằng sau câu thông báo không rõ ràng này là việc từ chối xác nhận việc tồn tại hay không tồn tại một user-name như thế trong hệ thống. Điều này làm tăng sự khó khăn cho những người muốn đăng nhập vào hệ thống một cách bất hợp pháp bằng cách thử ngẫu nhiên.

I.2.2 Tính toàn vẹn:

Đặc trưng này đảm bảo sự tồn tại nguyên vẹn của thông tin, loại trừ mọi sự thay đổi thông tin có chủ đích hoặc hư hỏng, mất mát thông tin do sự cố thiết bị hoặc phần mềm. Tính toàn vẹn được xét trên 2 khía cạnh:

-Tính nguyên vẹn của nội dung thông tin.

-Tính xác thực của nguồn gốc của thông tin.

Nói một cách khác, tính toàn vẹn của thông tin phải được đánh giá trên hai mặt: *toàn vẹn về nội dung* và *toàn vẹn về nguồn gốc*.

Ví dụ: một ngân hàng nhận được lệnh thanh toán của một người tự xưng là chủ tài khoản với đầy đủ những thông tin cần thiết. Nội dung thông tin được bảo toàn vì ngân hàng đã nhận được một cách chính xác yêu cầu của khách hàng (đúng như người xưng là chủ tài khoản gởi đi). Tuy nhiên, nếu lệnh thanh toán này không phải cho chính chủ tài khoản đưa ra mà do một người nào khác nhờ biết được thông tin bí mật về tài khoản đã mạo danh chủ tài khoản để đưa ra, ta nói nguồn gốc của thông tin đã không được bảo toàn.

Một ví dụ khác, một tờ báo đưa tin về một sự kiện vừa xảy ra tại một cơ quan quan trọng của chính phủ, có ghi chú rằng nguồn tin từ người phát ngôn của cơ quan đó. Tuy nhiên, nếu tin đó thật sự không phải do người phát ngôn công bố mà được lấy từ một kênh thông tin khác, không xét đến việc nội dung thông tin có đúng hay không, ta nói rằng nguồn gốc thông tin đã không được bảo toàn.

Sự tòan vẹn về nguồn gốc thông tin trong một số ngữ cảnh có ý nghĩa tương đương với sự đảm bảo tính không thể chối cãi (non-repudiation) của hệ thống thông tin.

Các cơ chế đảm bảo sự toàn vẹn của thông tin được chia thành 2 loại: các cơ chế ngăn chặn ***(Prevention mechanisms)*** và các cơ chế phát hiện ***(Detection mechanisms)***.

Cơ chế ngăn chặn có chức năng ngăn cản các hành vi trái phép làm thay đổi nội dung và nguồn gốc của thông tin. Các hành vi này bao gồm 2 nhóm: hành vi cố gắng *thay đổi thông tin khi không được phép truy xuất đến thông tin* và hành vi *thay đổi thông tin theo cách khác với cách đã được cho phép*.

Ví dụ: một người ngoài công ty cố gắng truy xuất đến cơ sở dữ liệu kế toán của một công ty và thay đổi dữ liệu trong đó. Đây là hành vi thuộc nhóm thứ nhất. Trường hợp một nhân viên kế toán được trao quyền quản lý cơ sở dữ liệu kế toán của công ty, và đã dùng quyền truy xuất của mình để thay đổi thông tin nhằm biển thủ ngân quỹ, đây là hành vi thuộc nhóm thứ hai.

Nhóm các cơ chế phát hiện chỉ thực hiện chức năng giám sát và thông báo khi có các thay đổi diễn ra trên thông tin bằng cách phân tích các sự kiện diễn ra trên hệ thống mà không thực hiện chức năng ngăn chặn các hành vi truy xuất trái phép đến thông tin.

Nếu như tính bí mật của thông tin chỉ quan tâm đến việc thông tin có bị tiết lộ hay không, thì tính toàn vẹn của thông tin vừa quan tâm tới tính chính xác của thông tin và cả mức độ tin cậy của thông tin. Các yếu tố như nguồn gốc thông tin, cách thức bảo vệ thông tin trong quá khứ cũng như trong hiện tại đều là những yếu tố quyết định độ tin cậy của thông tin và do đó ảnh hưởng đến tính toàn vẹn của thông tin. Nói chung, việc đánh giá tính toàn vẹn của một hệ thống thông tin là một công việc phức tạp.

I.2.3 Tính khả dụng:

Tính khả dụng của thông tin là tính sẵn sàng của thông tin cho các nhu cầu truy xuất hợp lệ.

Ví dụ: các thông tin về quản lý nhân sự của một công ty được lưu trên máy tính, được bảo vệ một cách chắc chắn bằng nhiều cơ chế đảm bảo thông tin không bị tiết lộ hay thay đổi. Tuy nhiên, khi người quản lý cần những thông tin này thì lại không truy xuất được vì lỗi hệ thống. Khi đó, thông tin hoàn toàn không sử dụng được và ta nói tính khả dụng của thông tin không được đảm bảo.

Tính khả dụng là một yêu cầu rất quan trọng của hệ thống, bởi vì một hệ thống tồn tại nhưng không sẵn sàng cho sử dụng thì cũng giống như không tồn tại một hệ thống thông tin nào. Một hệ thống khả dụng là một hệ thống làm việc trôi chảy và hiệu quả, có khả năng phục hồi nhanh chóng nếu có sự cố xảy ra.

Trong thực tế, tính khả dụng được xem là nền tảng của một hệ thống bảo mật, bởi vì khi hệ thống không sẵn sàng thì việc đảm bảo 2 đặc trưng còn lại (bí mật và toàn vẹn) sẽ trở nên vô nghĩa.

Hiện nay, các hình thức tấn công từ chối dịch vụ DoS (Denial of Service) và DDoS (Distributed Denial of Service) được đánh giá là các nguy cơ lớn nhất đối với sự an toàn của các hệ thống thông tin, gây ra những thiệt hại lớn và đặc biệt là chưa có giải pháp ngăn chặn hữu hiệu. Các hình thức tấn công này đều nhắm vào tính khả dụng của hệ thống.

Một số hướng nghiên cứu đang đưa ra các mô hình mới cho việc mô tả các hệ thống an toàn. Theo đó, mô hình CIA không mô tả được đầy đủ các yêu cầu an toàn của hệ thống mà cần phải định nghĩa lại một mô hình khác với các đặc tính của thông tin cần được đảm bảo như:

-Tính khả dụng (Availability)

-Tính tiện ích (Utility)

-Tính toàn vẹn (Integrity)

-Tính xác thực (Authenticity)

-Tính bảo mật (Confidentiality)

-Tính sở hữu (Possession)

I.3 CÁC NGUY CƠ VÀ RỦI RO ĐỐI VỚI HỆ THỐNG THÔNG TIN

I.3.1 Nguy cơ:

Nguy cơ (threat) là những sự kiện có khả năng ảnh hưởng đến an toàn của hệ thống.

Ví dụ: tấn công từ chối dịch vụ (DoS và DDoS) là một nguy cơ đối với hệ thống các máy chủ cung cấp dịch vụ trên mạng.

Khi nói đến nguy cơ, nghĩa là sự kiện đó chưa xảy ra, nhưng *có khả năng xảy ra và có khả năng gây hại cho hệ thống*. Có những sự kiện có khả năng gây hại, nhưng không có khả năng xảy ra đối với hệ thống thì không được xem là nguy cơ.

Ví dụ: tấn công của sâu Nimda (năm 2001) có khả năng gây tê liệt toàn bộ hệ thống mạng nội bộ. Tuy nhiên, sâu Nimda chỉ khai thác được lỗi bảo mật của phần mềm IIS (Internet Information Service) trên Windows (NT và 2000) và do đó chỉ có khả năng xảy ra trên mạng có máy cài đặt hệ điều hành Windows. Nếu một mạng máy tính chỉ gồm toàn các máy cài hệ điều hành Unix hoặc Linux thì sâu Nimda hoàn toàn không có khả năng tồn tại, và do vậy, sâu Nimda không phải là một nguy cơ trong trường hợp này.

Có thể chia các nguy cơ thành 4 nhóm sau đây:

-Tiết lộ thông tin / truy xuất thông tin trái phép

-Phát thông tin sai / chấp nhận thông tin sai

-Phá hoại / ngăn chặn hoạt động của hệ thống

-Chiếm quyền điều khiển từng phần hoặc toàn bộ hệ thống

Đây là cách phân chia rất khái quát. Mỗi nhóm sẽ bao gồm nhiều nguy cơ khác nhau.

- Nghe lén, hay đọc lén (gọi chung là *snooping*) là một trong những phương thức *truy xuất thông tin trái phép*. Các hành vi thuộc phương thức này có thể đơn giản như việc nghe lén một cuộc đàm thoại, mở một tập tin trên máy của người khác, hoặc phức tạp hơn như xen vào một kết nối mạng *(wire-tapping)* để ăn cắp dữ liệu, hoặc cài các chương trình ghi bàn phím (*key-logger)* để ghi lại những thông tin quan trọng được nhập từ bàn phím.
- Nhóm nguy cơ *phát thông tin sai / chấp nhận thông tin sai* bao gồm những hành vi tương tự như nhóm ở trên nhưng mang tính chủ động, tức là có thay đổi thông tin gốc. Nếu thông tin bị thay đổi là thông tin điều khiển hệ thống thì mức độ thiệt hại sẽ nghiêm trọng hơn nhiều bởi vì khi đó, hành vi này không chỉ gây ra sai dữ liệu mà còn có thể làm thay đổi các chính sách an toàn của hệ thống hoặc ngăn chặn hoạt động bình thường của hệ thống.

  Trong thực tế, hình thức tấn công xen giữa *Man-in-the-middle* (MITM) là một dạng của phương thức phát thông tin sai / chấp nhận thông tin sai. Hoạt động của hình thức tấn công này là xen vào một kết nối mạng, đọc lén thông tin và thay đổi thông tin đó trước khi gởi đến cho nơi nhận.

  Giả danh *(spoofing)* cũng là một dạng hành vi thuộc nhóm nguy cơ phát thông tin sai / chấp nhận thông tin sai. Hành vi này thực hiện việc trao đổi thông tin với một đối tác bằng cách giả danh một thực thể khác.

  Phủ nhận hành vi *(repudiation)* cũng là một phương thức gây sai lệch thông tin. Bằng phương thức này, một thực thể thực hiện hành vi phát ra thông tin, nhưng sau đó lại chối bỏ hành vi này, tức không công nhận nguồn gốc của thông tin, và do đó vi phạm yêu cầu về tính toàn vẹn của thông tin.

  Ví dụ: một người chủ tài khoản yêu cầu ngân hàng thanh toán từ tài khoản của mình. Mọi thông tin đều chính xác và ngân hàng đã thực hiện lệnh. Tuy nhiên sau đó người chủ tài khoản lại phủ nhận việc mình đã đưa ra lệnh thanh toán. Khi đó, thông tin đã bị sai lệch do nguồn gốc của thông tin không còn xác định.
- Nhóm nguy cơ thứ 3 bao gồm các hành vi có mục đích *ngăn chặn hoạt động bình thường của hệ thống* bằng cách làm chậm hoặc gián đoạn dịch vụ của hệ thống. Tấn công từ chối dịch vụ hoặc virus là những nguy cơ thuộc nhóm này.
- *Chiếm quyền điều khiển hệ thống* gây ra nhiều mức độ thiệt hại khác nhau, từ việc lấy cắp và thay đổi dữ liệu trên hệ thống, đến việc thay đổi các chính sách bảo mật và vô hiệu hoá các cơ chế bảo mật đã được thiết lập.

  Ví dụ điển hình cho nhóm nguy cơ này là các phương thức tấn công nhằm chiếm quyền root trên các máy tính chạy Unix hoặc Linux bằng cách khai thác các lỗi phần mềm hoặc lỗi cấu hình hệ thống. Tấn công tràn bộ đệm *(buffer overflow)* là cách thường dùng nhất để chiếm quyền root trên các hệ thống Linux vốn được xây dựng trên nền tảng của ngôn ngữ lập trình C.

I.3.2 Rủi ro và quản lý rủi ro:

Rủi ro (risk) là xác suất xảy ra thiệt hại đối với hệ thống.

Rủi ro bao gồm 2 yếu tố: Khả năng xảy ra rủi ro và thiệt hại do rủi ro gây ra. Có những rủi ro có khả năng xảy ra rất cao nhưng mức độ thiệt hại thì thấp và ngược lại.

Ví dụ: rủi ro mất thông tin trên hệ thống không có cơ chế bảo vệ tập tin, chẳng hạn như Windows 98. Windows 98 không có cơ chế xác thực người sử dụng nên bất cứ ai cũng có thể sử dụng máy với quyền cao nhất. Nếu trên đó chỉ có chứa các tập tin văn bản không có tính bí mật thì việc mất một tập tin thì thiệt hại gây ra chỉ là mất công sức đánh máy văn bản đó. Đây là dạng rủi ro có *xác suất xảy ra cao nhưng thiệt hại thấp*.

Một ví dụ khác: trên máy chủ cung cấp dịch vụ có một phần mềm có lỗi tràn bộ đệm, và nếu khai thác được lỗi này thì kẻ tấn công có thể chiếm được quyền điều khiển toàn bộ hệ thống. Tuy nhiên, đây là phần mềm không phổ biến và để khai thác được lỗi này, kẻ tấn công phải có những kỹ năng cao cấp. Rủi ro hệ thống bị chiếm quyền điều khiển được đánh giá là có *khả năng xảy ra thấp, nhưng nếu có xảy ra, thì thiệt hại sẽ rất cao*.

Cần chú ý phân biệt giữa nguy cơ và rủi ro. ***Nguy cơ*** *là những hành vi, những sự kiện hoặc đối tượng có khả năng gây hại cho hệ thống.* ***Rủi ro*** *là những thiệt hại có khả năng xảy ra đối với hệ thống*.

Ví dụ: Tấn công từ chối dịch vụ là một nguy cơ (threat). Đây là một sự kiện có khả năng xảy ra đối với bất kỳ hệ thống cung cấp dịch vụ nào. Thiệt hại do tấn công này gây ra là hệ thống bị gián đoạn hoạt động, đây mới là rủi ro (risk). Tuy nhiên, không phải bất kỳ tấn công từ chối dịch vụ nào xảy ra cũng đều làm cho hệ thống ngưng hoạt động, và hơn nữa, tấn công từ chối dịch vụ không phải là nguồn gốc duy nhất gây ra gián đoạn hệ thống; những nguy cơ khác như lỗi hệ thống (do vận hành sai), lỗi phần mềm (do lập trình), lỗi phần cứng (hư hỏng thiết bị, mất điện, …) cũng đều có khả năng dẫn đến gián đoạn hệ thống.

Một ví dụ khác, xét trường hợp lưu trữ tập tin trên một máy tính chạy hệ điều hành Windows 98 đã nói ở trên. Nguy cơ đối với hệ thống là *các hành vi sửa hoặc xoá tập tin trên máy người khác*. Những người hay sử dụng máy tính của người khác cũng được xem là nguy cơ đối với hệ thống. Rủi ro đối với hệ thống trong trường hợp này là việc *tập tin bị mất hoặc bị sửa*.

Trong thực tế, việc đề ra chính sách bảo mật cho một hệ thống thông tin phải đảm bảo được sự cân bằng giữa lợi ích của việc bảo đảm an toàn hệ thống và chi phí thiết kế, cài đặt và vận hành các cơ chế bảo vệ chính sách đó.

Công việc quản lý rủi ro trên một hệ thống là quy trình cần thiết để nhận diện tất cả những rủi ro đối với hệ thống, những nguy cơ có thể dẫn đến rủi ro và phân tích lợi ích / chi phí của giải pháp ngăn chặn rủi ro. Quy trình phân tích rủi ro bao gồm các bước:

-Nhận dạng các rủi ro đối với hệ thống

-Chọn lựa và thực hiện các giải pháp để giảm bớt rủi ro.

-Theo dõi và đánh giá thiệt hại của những rủi ro đã xảy ra, làm cơ sở cho việc điều chỉnh lại hai bước đầu.

I.3.3 Vấn đề con người trong bảo mật hệ thống:

Con người luôn là trung tâm của tất cả các hệ thống bảo mật, bởi vì tất cả các cơ chế, các kỹ thuật được áp dụng để bảo đảm an toàn hệ thống đều có thể dễ dàng bị vô hiệu hoá bởi con người trong chính hệ thống đó.

Ví dụ: hệ thống xác thực người sử dụng yêu cầu mỗi người trong hệ thống khi muốn thao tác trên hệ thống đều phải cung cấp tên người dùng và mật khẩu. Tuy nhiên, nếu người được cấp mật khẩu không bảo quản kỹ thông tin này, hoặc thậm chí đem tiết lộ cho người khác biết, thì khả năng xảy ra các vi phạm đối với chính sách an toàn là rất cao vì hệ thống xác thực đã bị vô hiệu hoá.

Những người có chủ ý muốn phá vỡ chính sách bảo mật của hệ thống được gọi chung là những người xâm nhập *(intruder* hoặc *attacker)* và theo cách nghĩ thông thường thì đây phải là những người bên ngoài hệ thống.

Tuy nhiên, thực tế đã chứng minh được rằng chính những người bên trong hệ thống, những người có điều kiện tiếp cận với hệ thống lại là những người có khả năng tấn công hệ thống cao nhất. Đó có thể là một nhân viên đang bất mãn và muốn phá hoại, hoặc chỉ là một người thích khám phá và chứng tỏ mình. Các tấn công gây ra bởi các đối tượng này thường khó phát hiện và gây thiệt hại nhiều hơn các tấn công từ bên ngoài.

Những người không được huấn luyện về an toàn hệ thống cũng là nơi tiềm ẩn các nguy cơ do những hành vi vô ý của họ như thao tác sai, bỏ qua các khâu kiểm tra an toàn, không tuân thủ chính sách bảo mật thông tin như lưu tập tin bên ngoài thư mục an toàn, ghi mật khẩu lên bàn làm việc, …

I.4 NGUYÊN TẮC XÂY DỰNG MỘT HỆ THỐNG BẢO MẬT

I.4.1 Chính sách và cơ chế:

Hai khái niệm quan trọng thường được đề cập khi xây dựng một hệ thống bảo mật:

-Chính sách bảo mật ***(Security policy)***

-Cơ chế bảo mật ***(Security mechanism)***

Chính sách bảo mật là hệ thống các quy định nhằm đảm bảo sự an toàn của hệ thống.

Cơ chế bảo mật là hệ thống các phương pháp, công cụ, thủ tục, …dùng để thực thi các quy định của chính sách bảo mật.

Chính sách bảo mật có thể được biểu diễn bằng ngôn ngữ tự nhiên hoặc ngôn ngữ toán học.

Ví dụ: trong một hệ thống, để bảo đảm an toàn cho một tài nguyên (resource) cụ thể, chính sách an toàn quy định rằng *chỉ có người dùng nào thuộc nhóm quản trị hệ thống (Administrators) mới có quyền truy xuất, còn những người dùng khác thì không*. Đây là cách biểu diễn bằng ngôn ngữ tự nhiên.

Có thể biểu diễn quy định này bằng ngôn ngữ toán học như sau:

Gọi: U là tập hợp các người dùng trong hệ thống.

A là tập hợp các người dùng thuộc nhóm quản trị.

O là tập hợp các đối tượng (tài nguyên) trong hệ thống

Thao tác Access(u, o) cho giá trị TRUE nếu người dùng u có quyền truy xuất đến đối tượng o, ngược lại, cho giá trị FALSE.

Quy định p trong chính sách an toàn được phát biểu như sau:

$$\forall u \in U, \ \forall o \in O: Access(u, o) = TRUE \Leftrightarrow u \in A$$

Ma trận cũng thường được dùng để biểu diễn một chính sách bảo mật.

Ví dụ: một hệ thống với các tập người dùng $U = \{u_1, u_2, u_3, u_4\}$ và tập đối tượng $O = \{o_1, o_2, o_3, o_4\}$. Các thao tác mà một người dùng u có thể thực hiện được trên một đối tượng o bao gồm đọc (r), ghi (w) và thực thi (x). Quy định về khả năng truy xuất của từng người dùng đến từng đối tượng trong hệ thống được biểu diễn bằng ma trận như sau:

	u_1	u_2	U_3	u_4
o_1	x	x	R	
o_2	x	r	R	
o_3	w		R	
o_4	w		R	

Quan sát ma trận, ta biết rằng người dùng u_3 được quyền đọc trên tất cả các đối tượng từ o_1 đến o_4, trong khi đó người dùng u_4 thì không có quyền truy xuất đến bất kỳ đối tượng nào.

Cơ chế bảo mật thông thường là các *biện pháp kỹ thuật*.

Ví dụ: xây dựng bức tường lửa (firewall), xác thực người dùng, dùng cơ chế bảo vệ tập tin của hệ thống quản lý tập tin NTFS để phân quyền truy xuất đối với từng tập tin / thư mục trên đĩa cứng, dùng kỹ thuật mật mã hoá để che giấu thông tin, v.v…

Tuy nhiên, đôi khi cơ chế chỉ là những *thủ tục (procedure)* mà khi thực hiện nó thì chính sách được bảo toàn.

Ví dụ: phòng thực hành máy tính của trường đại học quy định: sinh viên không được sao chép bài tập của sinh viên khác đã được lưu trên máy chủ. Đây là một quy định của chính sách bảo mật. Để thực hiện quy định này, các cơ chế được áp dụng bao gồm: tạo thư mục riêng trên máy chủ cho từng sinh viên, phân quyền truy xuất cho từng sinh viên đến các thư mục này và yêu cầu sinh viên phải lưu bài tập trong thư mục riêng, mỗi khi rời khỏi máy tính phải thực hiện thao tác logout khỏi hệ thống.

Trong cơ chế này, các biện pháp như tạo thư mục riêng, gán quyền truy xuất, … là các biện pháp kỹ thuật. Biện pháp yêu cầu sinh viên thóat khỏi hệ thống (logout) khi rời khỏi máy là một biện pháp thủ tục. Nếu sinh viên ra về mà không thóat ra khỏi hệ thống, một sinh viên khác có thể sử dụng phiên làm việc đang mở của sinh viên này để sao chép bài tập. Khi đó, rõ ràng chính sách bảo mật đã bị vi phạm.

Cho trước một chính sách bảo mật, cơ chế bảo mật phải đảm bảo thực hiện được 3 yêu cầu sau đây:

-Ngăn chặn các nguy cơ gây ra vi phạm chính sách

-Phát hiện các hành vi vi phạm chính sách

-Khắc phục hậu quả của rủi ro khi có vi phạm xảy ra.

Thông thường, việc xây dựng một hệ thống bảo mật phải dựa trên 2 giả thiết sau đây:

1-Chính sách bảo mật phân chia một cách rõ ràng các trạng thái của hệ thống thành 2 nhóm: an toàn và không an toàn.

2-Cơ chế bảo mật có khả năng ngăn chặn hệ thống tiến vào các trạng thái không an toàn.

Chỉ cần một trong hai giả thiết này không đảm bảo thì hệ thống sẽ không an toàn. Từng cơ chế riêng lẻ được thiết kế để bảo vệ một hoặc một số các quy định trong chính sách. Tập hợp tất cả các cơ chế triển khai trên hệ thống phải đảm bảo thực thi tất cả các quy định trong chính sách.

Hai nguy cơ có thể xảy ra khi thiết kế hệ thống bảo mật do không đảm bảo 2 giả thiết ở trên:

1-Chính sách không liệt kê được tất cả các trạng thái không an toàn của hệ thống, hay nói cách khác, chính sách không mô tả được một hệ thống bảo mật thật sự.

2-Cơ chế không thực hiện được tất cả các quy định trong chính sách, có thể do giới hạn về kỹ thuật, ràng buộc về chi phí, …

Dựa trên những nhận thức này, có thể đánh giá mức độ an toàn của một cơ chế như sau:

Gọi P là tập hợp tất cả các trạng thái của hệ thống, Q là tập hợp các trạng thái an toàn theo định nghĩa của chính sách bảo mật, giả sử cơ chế đang áp dụng có khả năng giới hạn các trạng thái của hệ thống trong tập R. Ta có các định nghĩa như sau:

-Nếu $R \subseteq Q$: cơ chế được đánh giá là *an toàn (secure mechanism).*

-Nếu $R = Q$: cơ chế được đánh giá là *chính xác (precise mechanism).*

-Nếu tồn tại trạng thái $r \in R$ sao cho $r \notin Q$: cơ chế được đánh giá là *lỏng lẻo (broad mechanism).*

I.4.2 Các mục tiêu của bảo mật hệ thống:

Một hệ thống bảo mật, như trình bày ở phần 2 của chương này, là hệ thống thoả mãn 3 yêu cầu cơ bản là tính bí mật, tính toàn vẹn và tính khả dụng, gọi tắt là CIA.

Để thực hiện mô hình CIA, người quản trị hệ thống cần định nghĩa các trạng thái an toàn của hệ thống thông qua chính sách bảo mật, sau đó thiết lập các cơ chế bảo mật để bảo vệ chính sách đó.

Một hệ thống lý tưởng là hệ thống:

-Có chính sách xác định một cách chính xác và đầy đủ các trạng thái an toàn của hệ thống;

-Có cơ chế thực thi đầy đủ và hiệu quả các quy định trong chính sách.

Tuy nhiên trong thực tế, rất khó xây dựng những hệ thống như vậy do có những hạn chế về kỹ thuật, về con người hoặc do chi phí thiết lập cơ chế cao hơn lợi ích mà hệ thống an toàn đem lại. Do vậy, khi xây dựng một hệ thống bảo mật, thì ***mục tiêu*** đặt ra cho cơ chế được áp dụng phải bao gồm 3 phần như sau:

Ngăn chặn (prevention): mục tiêu thiết kế là ngăn chặn các vi phạm đối với chính sách. Có nhiều sự kiện, hành vi dẫn đến vi phạm chính sách. Có những sự kiện đã được nhận diện là nguy cơ của hệ thống nhưng có những sự kiện chưa được ghi nhận là nguy cơ. Hành vi vi phạm có thể đơn giản như việc để lộ mật khẩu, quên thóat khỏi hệ thống khi rời khỏi máy tính, … hoặc có những hành vi phức tạp và có chủ đích như cố gắng tấn công vào hệ thống từ bên ngoài.

Các cơ chế *an toàn (secure mechanism)* hoặc *cơ chế chính xác (precise mechanism)* theo định nghĩa ở trên là các cơ chế được thiết kế với mục tiêu *ngăn chặn*.

Tuy nhiên, khi việc xây dựng các cơ chế an toàn hoặc chính xác là không khả thi thì cần phải quan tâm đến 2 mục tiêu sau đây khi thiết lập các cơ chế bảo mật:

Phát hiện (detection): mục tiêu thiết kế tập trung vào các sự kiện vi phạm chính sách đã và đang xảy ra trên hệ thống.

Thực hiện các cơ chế phát hiện nói chung rất phức tạp, phải dựa trên nhiều kỹ thuật và nhiều nguồn thông tin khác nhau. Về cơ bản, các cơ chế phát hiện xâm nhập chủ yếu dựa vào việc theo dõi và phân tích các thông tin trong nhật ký hệ thống *(system log)* và dữ liệu đang lưu thông trên mạng *(network traffic)* để tìm ra các dấu hiệu của vi phạm. Các dấu hiệu vi phạm này (gọi là *signature*) thường phải được nhận diện trước và mô tả trong một cơ sở dữ liệu của hệ thống (gọi là *signature database*).

Ví dụ: khi máy tính bị nhiễm virus. Đa số các trường hợp người sử dụng phát hiện ra virus khi nó đã thực hiện phá hoại trên máy tính. Tuy nhiên có nhiều virus vẫn đang ở dạng tiềm ẩn chứ

chưa thi hành, khi đó dùng chương trình quét virus sẽ có thể phát hiện ra. Để chương trình quét virus làm việc có hiệu quả thì cần thiết phải cập nhật thường xuyên danh sách virus. *Quá trình cập nhật là quá trình đưa thêm các mô tả về dấu hiệu nhận biết các loại virus mới vào cơ sở dữ liệu (virus database hoặc virus list).*

Phục hồi (recovery): mục tiêu thiết kế bao gồm các cơ chế nhằm chặn đứng các vi phạm đang diễn ra *(response)* hoặc khắc phục hậu quả của vi phạm một cách nhanh chóng nhất với mức độ thiệt hại thấp nhất *(recovery)*.

Tùy theo mức độ nghiêm trọng của sự cố mà có các cơ chế phục hồi khác nhau. Có những sự cố đơn giản và việc phục hồi có thể hoàn toàn được thực hiện tự động mà không cần sự can thiệp của con người, ngược lại có những sự cố phức tạp và nghiêm trọng yêu cầu phải áp dụng những biện pháp bổ sung để phục hồi.

Một phần quan trọng trong các cơ chế phục hồi là việc nhận diện sơ hở của hệ thống và điều chỉnh những sơ hở đó. Nguồn gốc của sơ hở có thể do chính sách an toàn chưa chặt chẽ hoặc do lỗi kỹ thuật của cơ chế.

I.5 CHIẾN LƯỢC BẢO MẬT HỆ THỐNG AAA

AAA (Access control, Authentication, Auditing) được xem là bước tiếp cận cơ bản nhất và là chiến lược nền tảng nhất để thực thi các chính sách bảo mật trên một hệ thống được mô tả theo mô hình CIA.

Cơ sở của chiến lược này như sau:

1-Quyền truy xuất đến tất cả các tài nguyên trong hệ thống được xác định một cách tường minh và gán cho các đối tượng xác định trong hệ thống.

2-Mỗi khi một đối tượng muốn vào hệ thống để truy xuất các tài nguyên, nó phải được xác thực bởi hệ thống để chắc chắn rằng đây là một đối tượng có quyền truy xuất.

3-Sau khi đã được xác thực, tất cả các thao tác của đối đượng đều phải được theo dõi để đảm bảo đối tượng không thực hiện quán quyền hạn của mình.

Cần phân biệt với AAA trong ngữ cảnh quản lý *mạng truy nhập* với ý nghĩa Authentication, Authorization, Accounting – là dịch vụ trên các máy chủ truy nhập từ xa *(remote access server)* để thực hiện quản lý truy nhập mạng của người sử dụng, theo dõi lưu lượng sử dụng và tính cước truy nhập. AAA trong trường hợp này thường triển khai cùng với các dịch vụ như RADIUS, TACACS+, …

AAA gồm 3 lĩnh vực tách rời nhưng hoạt động song song với nhau nhằm tạo ra các cơ chế bảo vệ sự an toàn của hệ thống. Phần sau đây trình bày chi tiết về 3 lĩnh vực của AAA.

I.5.1 Điều khiển truy xuất:

Điều khiển truy xuất (Access control) được định nghĩa là *một quy trình được thực hiện bởi một thiết bị phần cứng hay một module phần mềm, có tác dụng chấp thuận hay từ chối một sự truy xuất cụ thể đến một tài nguyên cụ thể.*

Điều khiển truy xuất được thực hiện tại nhiều vị trí khác nhau của hệ thống, chẳng hạn như tại thiết bị truy nhập mạng (như remote access server-RAS hoặc wireless access point - WAP), tại hệ thống quản lý tập tin của một hệ điều hành ví dụ NTFS trên Windows hoặc trên các hệ thống Active Directory Service trong Netware 4.x hay Windows 2000 server,…

Trong thực tế, điều khiển truy xuất được thực hiện theo 3 mô hình sau đây:

-Mô hình điều khiển truy xuất bắt buộc (Mandatory Access Control_MAC): là mô hình *điều khiển truy xuất được áp dụng bắt buộc* đối với toàn hệ thống. Trong môi trường máy tính, cơ chế điều khiển truy xuất bắt buộc được tích hợp sẵn trong hệ điều hành, và có tác dụng đối với tất cả các tài nguyên và đối tượng trong hệ thống, người sử dụng không thể thay đổi được.

Ví dụ: trong hệ thống an toàn nhiều cấp *(multilevel security)*, mỗi đối tượng *(subject*) hoặc tài nguyên *(object)* được gán một mức bảo mật xác định. Trong hệ thống này, các đối tượng có mức bảo mật thấp không được đọc thông tin từ các tài nguyên có mức bảo mật cao, ngược lại các đối tượng ở mức bảo mật cao thì không được ghi thông tin vào các tài nguyên có mức bảo mật thấp. Mô hình này đặc biệt hữu dụng trong các hệ thống bảo vệ bí mật quân sự *(mô hình Bell-LaPadula, 1973).*

Những đặc điểm phân biệt của mô hình điều khiển truy xuất bắt buộc:

-Được thiết lập cố định ở mức hệ thống, người sử dụng (bao gồm cả người tạo ra tài nguyên) không thay đổi được.

-Người dùng và tài nguyên trong hệ thống được chia thành nhiều mức bảo mật khác nhau, phản ánh mức độ quan trọng của tài nguyên và người dùng.

-Khi mô hình điều khiển bắt buộc đã được thiết lập, nó có tác dụng đối với tất cả người dùng và tài nguyên trên hệ thống.

-Mô hình điều khiển truy xuất tự do (Discretionary Access Control_DAC): là mô hình điều khiển truy xuất trong đó việc xác lập quyền truy xuất đối với từng tài nguyên cụ thể *do người chủ sở hữu của tài nguyên đó quyết định*. Đây là mô hình được sử dụng phổ biến nhất, xuất hiện trong hầu hết các hệ điều hành máy tính.

Ví dụ: trong hệ thống quản lý tập tin NTFS trên Windows XP, chủ sở hữu của một thư mục có toàn quyền truy xuất đối với thư mục, có quyền cho phép hoặc không cho phép người dùng khác truy xuất đến thư mục, có thể cho phép người dùng khác thay đổi các xác lập về quyền truy xuất đối với thư mục.

Xem và thay đổi quyền truy xuất DAC trên một thư mục trong Windows XP:

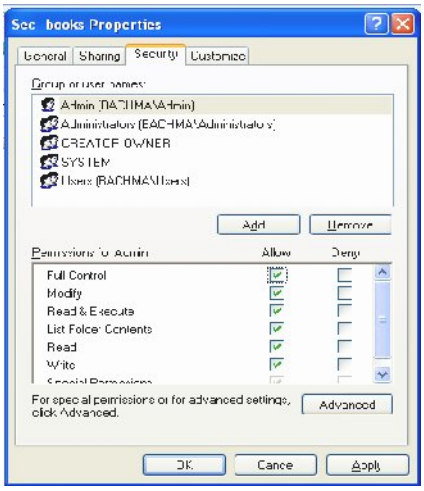
-Khởi động **Windows Explorer** bằng cách click phải vào biểu tượng **My Computer** và chọn **Explorer**.

-Mặc định, Windows XP không thể hiện các thông tin chi tiết về quyền truy xuất đối với thư mục. Muốn thể hiện các thông tin này, vào menu **Tools**, chọn **Folder Options**, click vào tab **View**, trong cửa sổ **Advanced settings**, tìm dòng **Use simple file sharing (Recommended)** ở cuối danh sách và bỏ tuỳ chọn này (uncheck), chọn **OK**.

-Click phải vào một thư mục tuỳ ý trong cửa sổ **Windows Explorer**, chọn **Properties**, click vào tab **Security** (Hình 1.2).

-Cửa sổ **Group or User names** liệt kê các người dùng và nhóm người dùng hiện có trong hệ thống. Cửa sổ **Permissions for …** liệt kê các quyền đã được gán cho nhóm hoặc người dùng tương ứng.

-Thử cho phép hoặc xoá bỏ các quyền mặc định của một người dùng bất kỳ.



Hình 1.2: *Điều khiển truy xuất tự do trong Windows XP*

Đặc điểm phân biệt của mô hình điều khiển truy xuất tự do:

-Không được áp dụng mặc định trên hệ thống

-Người chủ sở hữu của tài nguyên (owner), thường là người tạo ra tài nguyên đó hoặc người được gán quyền sở hữu, có toàn quyền điều khiển việc truy xuất đến tài nguyên.

-Quyền điều khiển truy xuất trên một tài nguyên có thể được chuyển từ đối tượng (user) này sang đối tượng (user) khác.

-Mô hình điều khiển truy xuất theo chức năng (Role Based Access Control_RBAC): đây là mô hình điều khiển truy xuất dựa trên vai trò của từng người dùng trong hệ thống (user' roles).

Ví dụ: một người quản lý tài chính cho công ty (financial manager) thì có quyền truy xuất đến tất cả các dữ liệu liên quan đến tài chính của công ty, được thực hiện các thao tác sửa, xóa, cập nhật trên cơ sở sữ liệu. Trong khi đó, một nhân viên kế toán bình thường thì chỉ được truy xuất đến một bộ phận nào đó của cơ sở dữ liệu tài chính và chỉ được thực hiện các thao tác có giới hạn đối với cơ sở dữ liệu.

Vấn đề quan trọng trong mô hình điều khiển truy xuất theo chức năng là định nghĩa các quyền truy xuất cho từng nhóm đối tượng tùy theo chức năng của các đối tượng đó. Việc này được định nghĩa ở mức hệ thống và áp dụng chung cho tất cả các đối tượng.

Cơ chế quản lý theo nhóm (account group) của Windows NT chính là sự mô phỏng của mô hình RBAC. Trong cơ chế này, người sử dụng được gán làm thành viên của một hoặc nhiều nhóm trong hệ thống, việc phân quyền truy xuất đến các tài nguyên được thực hiện đối với các nhóm chứ không phải đối với từng người dùng, khi đó các người dùng thành viên trong nhóm sẽ nhận được quyền truy xuất tương đương một cách mặc định. Việc thay đổi quyền truy xuất đối với từng người dùng riêng biệt được thực hiện bằng cách chuyển người dùng đó sang nhóm khác có quyền truy xuất thích hợp.

Đặc điểm phân biệt của mô hình điều khiển truy xuất theo chức năng:

-Quyền truy xuất được cấp dựa trên công việc của người dùng trong hệ thống (user's role)

-Linh động hơn mô hình điều khiển truy xuất bắt buộc, người quản trị hệ thống có thể cấu hình lại quyền truy xuất cho từng nhóm chức năng hoặc thay đổi thành viên trong các nhóm.

-Thực hiện đơn giản hơn mô hình điều khiển truy xuất tự do, không cần phải gán quyền truy xuất trực tiếp cho từng người dùng.

Ứng dụng các mô hình điều khiển truy xuất trong thực tế:

Trong thực tế, mô hình điều khiển truy xuất tự do (DAC) được ứng dụng rộng rãi nhất do tính đơn giản của nó đối với người dùng. Tuy nhiên, DAC không đảm bảo được các yêu cầu đặc biệt về an toàn hệ thống. Do vậy, một mô hình thích hợp nhất là phối hợp cả 3 mô hình: mô hình điều khiển truy xuất bắt buộc, mô hình điều khiển truy xuất tự do và mô hình điều khiển truy xuất theo chức năng.

Ngoài mô hình DAC đã được tích hợp trong hầu hết các hệ điều hành; mô hình RBAC đã được ứng dụng trong dịch vụ Active Directory của Netware 4.11 và Windows 2000 trở về sau; mô hình MAC được đưa vào trong các hệ điều hành như Windows Vista (dưới dạng cơ chế Mandatory Integrity Control), SELinux (kể cả Red Hat Enterprise Linux version 4), Trusted Solaris và Apple Computer (MAC OS X version 10.5 Leopard).

I.5.2 Xác thực:

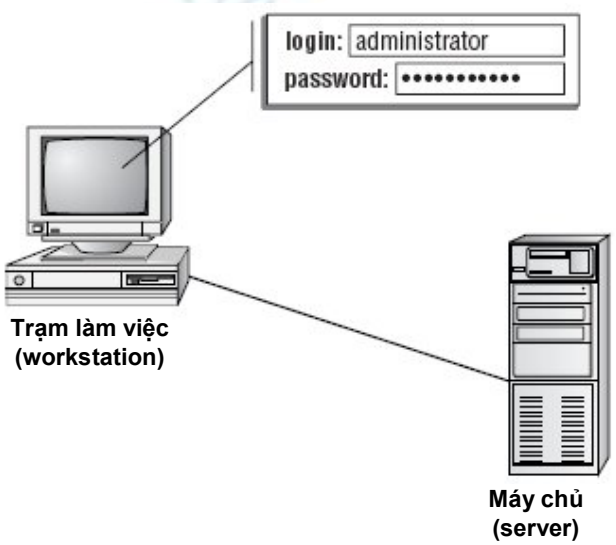
Xác thực (Authentication) là một thủ tục có chức năng xác minh nhận dạng (identity) của một đối tượng trước khi trao quyền truy xuất cho đối tượng này đến một tài nguyên nào đó. Xác thực được thực hiện dựa trên 3 cơ sở:

-What you know (điều mà đối tượng biết), ví dụ mật khẩu.

-What you have (cái mà đối tượng có), ví dụ thẻ thông minh Smartcard.

-What you are (đặc trưng của đối tượng): các đặc điểm nhận dạng sinh trắc học như dấu vân tay, võng mạc, …

Trong môi trường máy tính, xác thực được dùng ở nhiều ngữ cảnh khác nhau, ví dụ: xác thực tên đăng nhập và mật khẩu của người sử dụng (hình 1.3) trước khi cho phép người sử dụng thao tác trên hệ thống máy tính (xác thực của hệ điều hành), xác thực tên đăng nhập và mật khẩu trước khi cho phép người dùng kiểm tra hộp thư điện tử (xác thực của Mail server); trong giao dịch ngân hàng, thủ tục xác thực dùng để xác định người đang ra lệnh thanh toán có phải là chủ tài khoản hay không; trong trao đổi thông tin, thủ tục xác thực dùng để xác định chính xác nguồn gốc của thông tin.



Hình 1.3: *Xác thực bằng tên đăng nhập và mật khẩu*

Nhiều kỹ thuật khác nhau được áp dụng để thực thi cơ chế xác thực. Cơ chế *xác thực dùng tên đăng nhập và mật khẩu* là cơ chế truyền thống và vẫn còn được sử dụng rộng rãi hiện nay. Khi việc xác thực được thực hiện thông qua mạng, một số hệ thống thực hiện việc mật mã hoá tên đăng nhập và mật khẩu trước khi truyền đi để tránh bị tiết lộ, nhưng cũng có nhiều hệ thống gởi trực tiếp những thông tin nhạy cảm này trên mạng (ví dụ như các dịch vụ FTP, Telnet, …) gọi là cleartext authentication.

Một số kỹ thuật tiên tiến hơn được dùng trong xác thực như *thẻ thông minh (Smartcard), chứng thực số (digital certificate), các thiết bị nhận dạng sinh trắc học (biometric devices),…*

Để tăng độ tin cậy của cơ chế xác thực, *nhiều kỹ thuật được sử dụng phối hợp nhau* gọi là multi-factor authentication. Ví dụ: xác thực dùng thẻ thông minh kèm với mật khẩu, nghĩa là người sử dụng vừa có thẻ vừa phải biết mật khẩu thì mới đăng nhập được, tránh trường hợp lấy cắp thẻ của người khác để đăng nhập.

Trong thực tế tồn tại hai phương thức xác thực: *xác thực một chiều (one way authentication) và xác thực hai chiều (mutual authentication).*

Phương thức xác thực một chiều chỉ cung cấp cơ chế để một đối tượng (thường là máy chủ) kiểm tra nhận dạng của đối tượng kia (người dùng) mà không cung cấp cơ chế kiểm tra ngược lại (tức không cho phép người dùng kiểm tra nhận dạng của máy chủ). Xét trường hợp một người sử dụng đăng nhập vào một hộp thư điện tử ở xa thông qua dịch vụ web (web mail). Người sử dụng dĩ nhiên phải cung cấp tên đăng nhập và mật khẩu đúng thì mới được phép truy xuất hộp thư. Để đánh cắp mật khẩu của người dùng, kẻ tấn công có thể xây dựng một trang web hòan tòan giống với giao diện của máy chủ cung cấp dịch vụ thư điện tử (mail server) và đánh lừa người sử dụng kết nối đến trang web này. Do không có cơ chế xác thực máy chủ, người sử dụng không thể nhận biết đây là một máy chủ giả mạo nên yên tâm cung cấp tên đăng nhập và mật khẩu.

Phương thức kiểm tra hai chiều cho phép hai đối tượng tham gia giao tác xác thực lẫn nhau, do đó tính chính xác của quá trình xác thực được đảm bảo. Giao thức bảo mật SSL (Secure Sockets Layer) dùng trong dịch vụ web (được trình bày ở chương III) cung cấp cơ chế xác thực hai chiều dùng chứng thực số.

Có nhiều giải thuật xác thực khác nhau. Giải thuật đơn giản nhất chỉ cần so sánh tên đăng nhập và mật khẩu mà người sử dụng cung cấp với tên đăng nhập và mật khẩu đã được lưu trong hệ thống, nếu giống nhau nghĩa là thủ tục xác thực thành công (PAP). Giải thuật phức tạp hơn như CHAP thì thực hiện việc mật mã hóa thông tin trên một giá trị ngẫu nhiên nào đó do máy chủ đưa ra (gọi là challenge) để tránh trường hợp mật khẩu bị đọc lén trên mạng và các hình thức tấn công phát lại (replay attack). Một giải thuật phức tạp khác là Kerberos thực hiện thủ tục xác thực theo một quá trình phức tạp gồm nhiều bước nhằm đảm bảo hạn chế tất cả các nguy cơ gây nên xác thực sai. Các giải thuật xác thực được trình bày cho tiết ở phần I của chương III.

I.5.3 Kiểm tra:

Kiểm tra (Auditing) là cơ chế *theo dõi hoạt động* của hệ thống, *ghi nhận các hành vi* diễn ra trên hệ thống và *liên kết các hành vi này với các tác nhân gây ra hành vi*.

Ví dụ: cài đặt cơ chế kiểm tra cho một thư mục trong hệ thống tập tin NTFS sẽ cho phép người quản trị theo dõi các hoạt động diễn ra trên thư mục như: thao tác nào đã được thực hiện, ngày giờ thực hiện, người sử dụng nào thực hiện, …

Các mục tiêu của kiểm tra:

-Cung cấp các thông tin cần thiết cho việc phục hồi hệ thống khi có sự cố

-Đánh giá mức độ an toàn của hệ thống để có kế hoạch nâng cấp kịp thời

-Cung cấp các thông tin làm chứng cứ cho việc phát hiện các hành vi truy xuất trái phép trên hệ thống.

Trong một hệ thống tin cậy (reliable system) thì việc kiểm tra cũng là một yêu cầu quan trọng bởi vì nó đảm bảo rằng các hành vi của bất kỳ người dùng nào trong hệ thống (kể cả những người dùng hợp hệ đã được xác thực – authenticated user) cũng đều được theo dõi để chắc chắn rằng những hành vi đó diễn ra đúng theo các chính sách an toàn đã được định nghĩa trên hệ thống.

Nguyên tắc chung khi xây dựng các hệ thống an tòan là chia nhỏ các thủ tục thành nhiều công đoạn được thực hiện bởi nhiều tác nhân khác nhau, và do đó việc thực hiện hoàn chỉnh một thủ tục yêu cầu phải có sự tham gia của nhiều tác nhân. Đây là cơ sở để thực thi các cơ chế kiểm tra.

Ví dụ: công việc giữ kho hàng và công việc quản lý sổ sách phải được thực hiện bởi hai nhân viên khác nhau để tránh trường hợp một nhân viên vừa có thể lấy hàng ra ngoài vừa có thể thay đổi thông tin trong sổ quản lý. Nguyên tắc này được áp dụng triệt để trong cơ chế kiểm tra trên hệ thống nhằm phân biệt rõ ràng giữa chức năng kiểm tra với các hoạt động được kiểm tra. Thông thường, một đối tượng được kiểm tra sẽ không có quyền thay đổi các thông tin mà cơ chế kiểm tra ghi lại.

Các thành phần của hệ thống kiểm tra:

-Logger: Ghi lại thông tin giám sát trên hệ thống

-Analyzer: Phân tích kết quả kiểm tra

-Notifier: Cảnh báo về tính an toàn của hệ thống dựa trên kết quả phân tích.

Song song với cơ chế *kiểm tra thường trực* trên hệ thống (auditing), việc *kiểm tra hệ thống định kỳ (system scanning)* có chức năng kiểm tra và phát hiện các sơ hở kỹ thuật ảnh hưởng đến sự an toàn của hệ thống. Các chức năng có thể thực hiện bởi các chương trình kiểm tra hệ thống trên máy tính thường gặp:

-Kiểm tra việc tuân thủ chính sách an toàn về mật khẩu (password policy), ví dụ: người dùng có đổi mật khẩu thường xuyên không, độ dài mật khẩu, độ phức tạp của mật khẩu, …

-Đánh giá khả năng xâm nhập hệ thống từ bên ngoài.

-Kiểm tra phản ứng của hệ thống đối với các dấu hiệu có thể dẫn đến tấn công từ chối dịch vụ hoặc sự cố hệ thống (system crash).

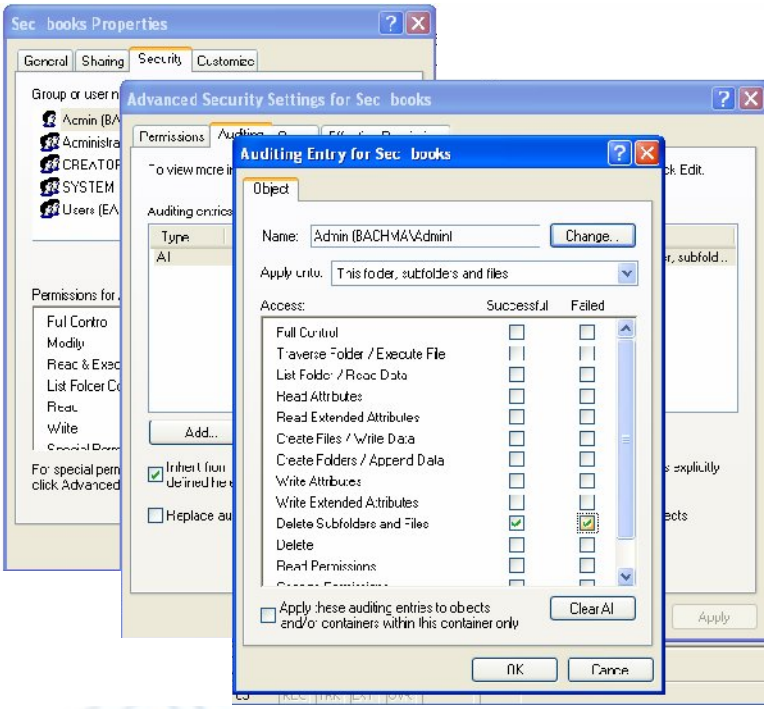
Lưu ý rằng, các công cụ kiểm tra hệ thống cũng đồng thời là các công cụ mà những *kẻ tấn công (attacker)* sử dụng để phát hiện các lỗ hổng bảo mật trên hệ thống, từ đó thực hiện các thao tác tấn công khác. Có nhiều phần mềm quét hệ thống, điển hình như SATAN (System Administrator Tool for Analyzing Network), Nessus, Nmap, …

Cài đặt chức năng Audit của hệ điều hành Windows XP lên một thư mục trên một phân vùng NTFS:

-Mặc định, Windows XP không áp dụng cơ chế kiểm tra, do đó cần phải kích hoạt cơ chế kiểm tra của Windows XP dùng **Local Security Policy** như sau: Vào **Control Panel**, chọn **Administrative Tools**, chọn **Local Security Policy**, trong khung Security Settings ở bên trái cửa sổ, double-click vào mục **Local Policy**, sau đó click vào mục **Audit Policy**. Khi đó, khung bên phải cửa sổ liệt kê các chức năng kiểm tra của Windows XP. Để kích hoạt cơ chế kiểm tra trên thư mục, tìm dòng **Audit object access**, double-click vào dòng này và chọn cả hai mục **Success** và **Failure** trong cửa sổ mới mở. Click OK và đóng tất cả các cửa sổ lại.

-Để áp dụng cơ chế kiểm tra trên một thư mục nào đó: khởi động **Windows explorer**, tìm một thư mục muốn kiểm tra và click phải vào thư mục này, chọn **Properties**, click vào tab **Security**, click vào nút **Advanced**, sau đó click vào tab **Auditing**. Trong cửa sổ **Auditing entries** liệt kê các mục kiểm tra đã cài đặt. Để tạo một mục mới, click vào nút **Add**, chọn tên người dùng hoặc nhóm cần kiểm tra trong cửa sổ **Select User or Group** vừa xuất hiện, click **OK**. Cửa sổ **Aditing Entry** for … xuất hiện, chọn các thao tác muốn kiểm tra, ví dụ **Delete Subfolders and Files** để theo dõi các hành vi xoá tập tin và thư mục con trong mục này. Cần chọn cả hai loại sự kiện là **Successful** và **Failed**. Click **OK** và đóng tất cả các cửa sổ lại.

-Bắt đầu từ đây, tất cả các thao tác xoá các tập tin và thư mục con trong thư mục đã chọn được thực hiện bởi người dùng hoặc nhóm đã chỉ định ở trên đều được theo dõi và ghi lại trong nhật ký hệ thống. Muốn xem các thông tin này thì vào **Control Panel**, chọn **Administrative Tools**, chọn **Event Viewer** và chọn mục **Security**.



Hình 1.4: *Cài đặt Auditing trên thư mục NTFS*

Tóm lại, AAA là phương pháp tiếp cận cơ bản nhất để thực hiện một hệ thống bảo mật theo mô hình CIA. Phương pháp này gồm 3 phần tách rời:

-Thiết lập các cơ chế điều khiển truy xuất cho từng đối tượng (Access control)

-Xác thực các đối tượng trước khi cho phép thao tác trên hệ thống (Authentication)

-Theo dõi các thao tác của đối tượng trên hệ thống (Auditing)

I.6 CÁC HÌNH THỨC XÂM NHẬP HỆ THỐNG

Thuật ngữ ***xâm nhập (intrusion)*** và ***tấn công (attack)*** được sử dụng với ý nghĩa gần giống nhau trong ngữ cảnh bảo mật hệ thống. Xâm nhập mang ý nghĩa phổ quát hơn, chỉ bất kỳ một sự kiện nào có xâm hại đến sự an toàn của hệ thống, một cách chủ động hoặc thụ động. Tấn công thường được dùng để chỉ các hành vi xâm nhập chủ động, được thực hiện bởi con người nhằm vào một hệ thống với mục đích khai thác hoặc phá hoại.

Mục tiêu của xâm nhập là tác động vào 3 thuộc tính CIA của hệ thống.

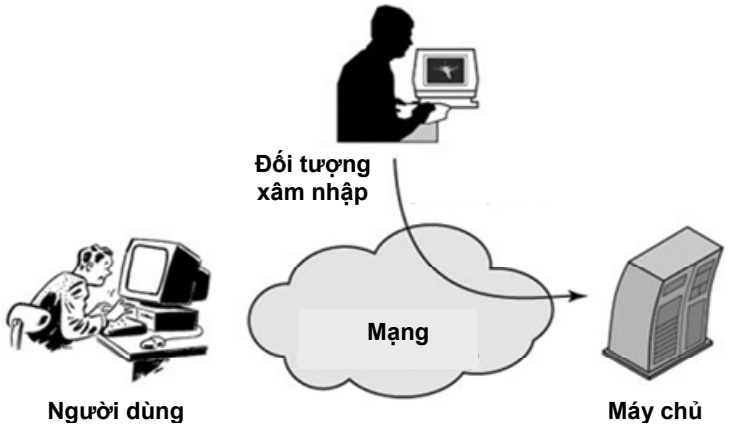
Một cách tổng quát, sự an toàn của một hệ thống thông tin có thể bị xâm phạm bằng những cách sau đây:

-Interruption: làm gián đoạn hoạt động của hệ thống thông tin, ví dụ như phá hoại phần cứng, ngắt kết nối, phá hoại phần mềm, …Hình thức xâm nhập này tác động vào đặc tính Khả dụng của thông tin.

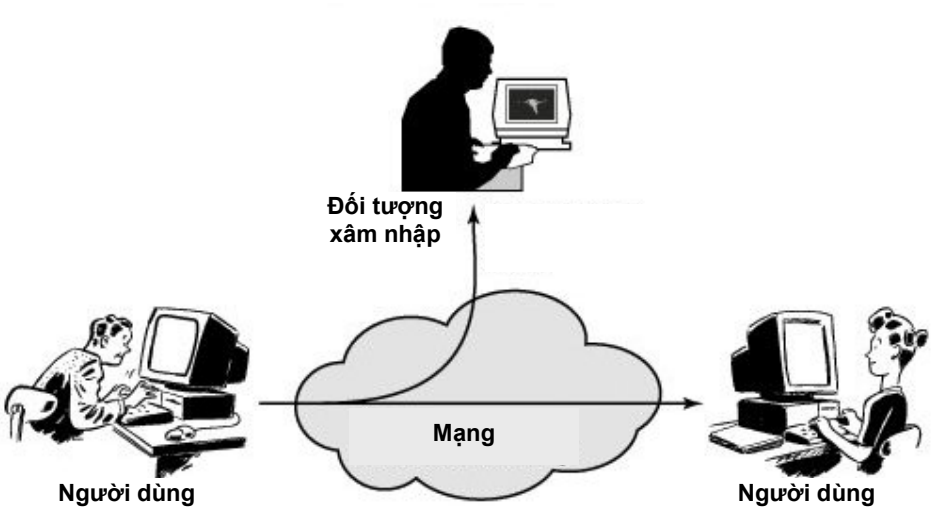
-Interception: truy xuất trái phép vào hệ thống thông tin. Tác nhân của các hành vi xâm nhập kiểu Interception có thể là một người, một phần mềm hay một máy tính làm việc bằng cách quan sát dòng thông tin (monitor) nhưng không làm thay đổi thông tin gốc. Hình thức xâm nhập này tác động vào đặc tính Bí mật của thông tin.

-Modification: truy xuất trái phép vào hệ thống thông tin, đồng thời làm thay đổi nội dung thông tin, ví dụ xâm nhập vào máy tính và làm thay đổi nội dung một tập tin, thay đổi một chương trình làm cho chương trình làm việc sai, thay đổi nội dung một thông báo đang gởi đi trên mạng, v.v… Hình thức xâm nhập này tác động vào tính Toàn vẹn của thông tin.

-Ngoài ra, một hình thức xâm nhập thứ tư là hình thức xâm nhập bằng thông tin giả danh ***(Farbrication)***, ví dụ, giả danh một người nào đó để gởi mail đến một người khác, giả mạo địa chỉ IP của một máy nào đó để kết nối với một máy khác, …Hình thức xâm nhập này làm thay đổi nguồn gốc thông tin, tức cũng là tác động vào đặc tính Toàn vẹn của thông tin.



Hình 1.5*: Xâm nhập kiểu Interruption*



Hình 1.6: *Xâm nhập kiểu Interception*

Trong thực tế, việc xâm nhập hệ thống được thực hiện bởi rất nhiều phương thức, công cụ và kỹ thuật khác nhau, thêm vào đó, việc phát hiện ra các phương thức xâm nhập mới là việc xảy ra rất thường xuyên, nên vấn đề nhận dạng và phân loại các xâm nhập một cách có hệ thống là khó khăn và không chính xác. Có thể phân loại xâm nhập theo các tiêu chí sau đây: