BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. NGUYỄN ĐÌNH VINH, TS. TRẦN ĐỨC SỰ, KS. VŨ THỊ VÂN

GIÁO TRÌNH

CƠ SỞ AN TOÀN THÔNG TIN

HÀ NỘI, 2013

BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

TS. NGUYỄN ĐÌNH VINH, TS. TRẦN ĐỨC SỰ, KS. VŨ THỊ VÂN

GIÁO TRÌNH

CƠ SỞ AN TOÀN THÔNG TIN

HÀ NỘI, 2013

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

AC	Hệ thống tự động hoá
AES	Advanced Encryption Standard – Chuẩn mã hóa tiên tiến
ATTT	An toàn thông tin
BLP	Bell – Lapadula
BVTT	Bảo vệ thông tin
CA	Certification Authority – Cơ quan cấp chứng chỉ
CBT	Các thiết bị tính toán
CC	Common Criteria – Tiêu chí chung
CNTT	Công nghệ thông tin
CRL	Certificate revocation list – Danh sách thu hồi chứng chỉ
CSAT	Chính sách an toàn
CSAT – D	Chính sách an toàn lựa chọn
CSAT – M	Chính sách an toàn bắt buộc
CSDL	Cơ sở dữ liệu
DAC	Discretionary Access Control – Điều khiển truy cập tùy chọn
DDoS	Distributed Denial of Service – Từ chối dịch vụ phân tán
DES	Data Encryption Standard – Chuẩn mã hóa dữ liệu
DMZ	Demilitarized Zone – Khu vực phi quân sự
DNS	Domain Name System – Hệ thống phân giải tên miền
DoS	Denial of Service – Từ chối dịch vụ
DRDoS	Distributed Reflection DoS – Từ chối dịch vụ theo phương pháp phản xạ
ĐTAT	Đối tượng an toàn
HAT	Hệ an toàn
HRU	Harison – Ruzzo - Ullman
HSBV	Hồ sơ bảo vệ
HTTT – VT	Hệ thống Thông tin – Viễn thông
IDPS	Intrusion detection and prevention system – Hệ thống ngăn chặn và phát hiện xâm nhập

IDS	Intrusion detection system – Hệ thống phát hiện xâm nhập
IPS	Intrusion prevention system – Hệ thống ngăn chặn xâm nhập
ISMS	Information Security Management System – Hệ thống quản lý an toàn thông tin
ISO/IEC	The International Organization for Standardization and the International Electrotechnical Commission – Tổ chức tiêu chuẩn hóa quốc tế và Ủy ban kỹ thuật điện quốc tế
ISP	Internet Service Provider – Nhà cung cấp dịch vụ Internet
KCZ	Tổ hợp các thiết bị bảo vệ
MAC	Mandatory Access Control – Điều khiển truy cập bắt buộc
MD5	Message-Digest algorithm 5
MHAT	Mô hình an toàn
MHAT – D	Mô hình an toàn lựa chọn
MHAT – M	Mô hình an toàn bắt buộc
MK	Mật khẩu
MT	Máy tính
MTĐT	Máy tính điện tử
NAT	Network Address Translation – Chuyển đổi địa chỉ mạng
ND	Nhận dạng
NIST	National Institute of Standart and Technology – Viện Tiêu chuẩn và Kỹ thuật Quốc gia
NRU	No Read Up – Không đọc lên
NWD	No Write Down – Không ghi xuống
OSI	Open Systems Interconnection – Kết nối các hệ thống mở
PGP	Pretty Good Privacy
PIN	Personal Identification Number – Số định danh cá nhân
PKI	Public Key Infastructure – Cơ sở hạ tầng khóa công khai
RAT	Remote Administration Tool – Công cụ quản trị từ xa
SSL	Secure Sockets Layer
SSO	Single Sign On – Đăng nhập một lần
TBBV	Thiết bị bảo vệ

TCTP	Tiếp cận trái phép
TLS	Transport Layer Security
TT	Thông tin
TT – VT	Thông tin – Viễn thông
VPN	Virtual private network – Mạng riêng ảo
XT	Xác thực
YCCN	Yêu cầu chức năng
YCĐB	Yêu cầu đảm bảo

DANH MỤC BẢNG

DANH MỤC HÌNH VẼ

LỜI NÓI ĐẦU

Vấn đề an toàn thông tin (ATTT) đã được hình thành từ những năm 70 của thế kỷ trước (TK 20). Nó đã tiến được những bước dài cơ bản. Mặc dù vậy, trong khuôn khổ của bản thân vấn đề vẫn còn rất nhiều bài toàn chưa có lời giải. An toàn thông tin là vấn đề gắn liền với công nghệ thông tin (CNTT); mà CNTT ngày càng phát triển nhanh và là một trong những yếu tố quan trọng thúc đẩy nền kinh tế trí thức hình thành và phát triển với những xu thế toàn cầu hoá đầy thời cơ và thách thức với loài người. Vì thế ngày nay, vấn đề ATTT vẫn là vấn đề được ưu tiên ở cả góc độ quốc gia và quốc tế.

Thông tin và ATTT là yếu tố quan trọng hàng đầu của an ninh quốc gia. Mặc dù những năm gần đây, những cơ sở pháp lý đầu tiên trong lĩnh vực bảo đảm ATTT đã được xây dựng (Luật Cơ yếu, Chỉ thị của Bộ Chính trị về công tác Cơ yếu, các nghị định dưới Luật Cơ yếu, các bộ luật về giao dịch điện tử, về thương mại điện tử…), nhưng đây chưa phải là giải pháp toàn bộ và hoàn chỉnh. Đó mới chỉ là những nền móng đầu tiên. Sự phân tích hiện trạng vấn đề ATTT hiện nay đưa tới kết luận về tính cấp thiết phải có một tiếp cận đồng bộ hệ thống trong việc giải quyết những nhiệm vụ của sự nghiệp bảo đảm ATTT. Một trong những nhiệm vụ quan trọng đó là vấn đề con người – chúng ta thiếu hàng vạn cán bộ làm CNTT, trong đó có các kỹ sư ATTT.

Việc mở chuyên ngành đào tạo kỹ sư ATTT tại Học viện Kỹ thuật Mật mã (Ban cơ yếu Chính phủ) là để nhằm từng bước thực hiện nhiệm vụ lâu dài nói trên. Giáo trình cơ sở an toàn thông tin có thể coi là nhập môn của chuyên ngành ATTT này.

Đây là môn học quan trọng của chuyên ngành ATTT, nó cung cấp những khái niệm, những kiến thức cơ bản có tác dụng định hướng và gợi mở cho sinh viên đi vào học tập và nghiên cứu toàn bộ các môn học khác về ATTT sau này. Chính vì vậy, chúng tôi muốn giới thiệu một cái nhìn tổng thể vừa bao quát đầy đủ các vấn đề cơ bản của chuyên ngành, lại vừa thể hiện được mức độ phát triển của từng vấn đề cũng như thành tựu mới nhất với một độ sâu nhất định (nhất là các vấn đề về công nghệ an toàn). Đây là nhiệm vụ hết sức khó khăn (và nhiều khi nhóm tác giả cảm thấy là quá sức mình), chúng tôi đã cố gắng tới mức cao nhất để giải quyết nó, còn thành công đến đâu thì xin chờ thực tiễn trả lời.

Giáo trình gồm 5 chương:

Chương 1: Tổng quan về an toàn thông tin. Chương này giúp sinh viên nắm bắt được những kiến thức cơ bản về lý thuyết thông tin, an toàn thông tin, các tính chất đảm bảo an toàn thông tin.

Chương 2: Các hiểm họa gây mất an toàn thông tin. Chương này cung cấp cho sinh viên những kiến thức cơ bản về hiểm họa gây mất an toàn thông tin, các loại hiểm họa, một số hiểm họa gây mất an toàn thông tin và một số kiểu tấn công phổ biến.

Chương 3: Các phương pháp đảm bảo an toàn thông tin. Chương này đề cập đến mô hình bảo vệ thông tin theo chiều sâu, các nguyên lý và các phương pháp cơ bản để đảm bảo an toàn thông tin.

Chương 4: Chính sách và mô hình an toàn thông tin. Chương này cung cấp những kiến thức cơ bản về chính sách và các mô hình an toàn thông tin phổ biến.

Chương 5: Các tiêu chí đánh giá và chuẩn an toàn thông tin. Chương này sẽ giới thiệu cho sinh viên về các tiêu chí đánh giá phổ biến và bộ chuẩn an toàn thông tin ISO 27x.

Mỗi chương của học phần đều bao gồm phần câu hỏi để sinh viên củng cố kiến thức được truyền đạt trên lớp.

Giáo trình được viết và hiệu chỉnh lần đầu tiên, chắc chắn còn rất nhiều khiếm khuyết về nội dung cũng như phương pháp thể hiện, chúng tôi rất mong nhận được những ý kiến đóng góp của các đồng nghiệp, các bạn đọc và sinh viên xa gần để hoàn chỉnh tiếp trong quá trình thực hiện.

Hà Nội, tháng 08 năm 2013

Các tác giả.

CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN

1.1. THÔNG TIN

Trong lịch sử tồn tại và phát triển của mình, con người thường xuyên cần đến thông tin. Ngày nay, với sự bùng nổ thông tin, thông tin càng trở thành một trong những nhu cầu sống còn của con người và khái niệm "thông tin" đang trở thành khái niệm cơ bản, chung của nhiều ngành khoa học.

1.1.1. Các khái niệm cơ bản

Thông tin (Information) là một khái niệm trừu tượng mô tả các yếu tố đem lại hiểu biết, nhận thức cho con người cũng như các sinh vật khác. Thông tin tồn tại khách quan, có thể được tạo ra, truyền đi, lưu trữ, chọn lọc. Thông tin cũng có thể bị sai lệch, méo mó do nhiều nguyên nhân khác nhau: bị xuyên tạc, cắt xén… Những yếu tố gây sự sai lệch thông tin gọi là các yếu tố nhiễu.

Trên quan điểm ATTT, TT là tập hợp các cứ liệu (các tin tức) về thế giới bao quanh chúng ta (các sự kiện, các cá nhân, các hiện tượng, các quá trình, các nhân tố và các mối liên hệ giữa chúng), được thể hiện trong dạng thức phù hợp cho việc truyền đi bởi những người này và tiếp nhận bởi những người kia và được sử dụng với mục đích thu nhận kiến thức (các tri thức) và đưa ra những quyết định.

Dữ liệu (data) là các sự kiện không có cấu trúc, không có ý nghĩa rõ ràng, cho đến khi chúng được tổ chức theo một tiến trình tính toán nào đó. Như vậy, thông tin là dữ liệu đã được xử lý xong, mang ý nghĩa rõ ràng.

Ngày nay TT được hình thành, tồn tại và vận động trong các hệ thống thông tin – viễn thông (TT – VT). Chúng ta cần định nghĩa rõ về khái niệm hệ thống TT – VT.

Hệ thống TT – VT: tập hợp các thiết bị kỹ thuật và bảo đảm phần mềm, liên hệ với nhau bằng các kênh truyền và nhận TT. Từ các yếu tố ngăn cách nhau về vị trí địa lý, chúng liên kết chặt chẽ với nhau thành một thể thống nhất nhằm mục đích bảo đảm chu trình công nghệ xử lý TT (tìm kiếm, lưu trữ, bảo vệ, xử lý, hiệu đính) và cung cấp cho người dùng kết quả của sự xử lý này ở dạng đòi hỏi. Tóm lại, hệ thống TT – VT bao gồm các mạng máy tính, các bảo đảm toán học (các phần mềm) và hệ thống liên lạc.

1.1.2. Các tính chất của thông tin

Như vậy, ta thấy TT - đó là các tri thức trong ý nghĩa rộng nhất của từ này. Vì rằng TT phản ánh các thuộc tính của các đối tượng vật chất và mối quan hệ giữa chúng, nên theo các khái niệm cơ bản của triết học, TT có thể coi là đối tượng của nhận thức.

Suy cho cùng, bảo đảm TT là cơ sở cho bất kỳ hoạt động nào của con người. TT trở thành một trong những phương tiện cơ bản để giải quyết các vấn đề và các nhiệm vụ của một quốc gia, của các đảng chính trị và các nhà lãnh đạo của các cơ cấu thương mại khác nhau và của các cá nhân con người.

Ngày nay, kinh tế thế giới phát triển ở mức độ cao, khoa học công nghệ đã đưa tới sự ra đời của nền kinh tế tri thức. Lượng TT tích luỹ được về mọi khía cạnh của cuộc sống xã hội hiện đại đã là khổng lồ. Các TT mới được sáng tạo ra với tốc độ ngày càng cao. Nhưng mặt khác, để thu nhận TT bằng con đường tiến hành những nghiên cứu, khảo sát riêng (của cá nhân hoặc của tập thể) ngày càng trở nên đắt giá, tốn kém và khó khăn. Cho nên việc thu lượm TT bằng con đường rẻ hơn nhưng bất hợp pháp (tức là ăn cắp TT) ngày càng trở nên thường xuyên và mở rộng.

Trong bối cảnh nói trên, ngày càng tăng tính cấp thiết của nhiệm vụ bảo vệ TT (BVTT) trong tất cả các lĩnh vực hoạt động của con người: trong phục vụ các cơ quan Nhà nước (lãnh đạo, chỉ huy, an ninh, quốc phòng, đối ngoại); trong thương mại, kinh doanh; trong hoạt động khoa học công nghệ, trong sản xuất và thậm chí trong đời sống riêng tư của các cá nhân. Sự cạnh tranh thường xuyên giữa các phương pháp ăn cắp TT (và các phương tiện thực hiện chúng) với các phương pháp (phương tiện) bảo vệ thông tin đã dẫn đến sự

xuất hiện trên thị trường rất nhiều chủng loại thiết bị BVTT, và cũng đã xuất hiện vấn đề lựa chọn chúng sao cho tối ưu và sử dụng cho hiệu quả trong những điều kiện cụ thể.

Vì vậy thông tin không những là đối tượng của nhận thức mà nó còn là đối tượng của sự bảo vệ. Chúng ta sẽ xem xét các tính chất của thông tin theo hai phương diện này.

1.1.2.1. Theo khía cạnh thông tin là đối tượng của nhận thức

Khi xem xét ở khía cạnh là đối tượng của nhận thức, thông tin có các tính chất sau:

- TT là phi vật chất trong ý nghĩa rằng không thể đo các thông số của nó, ví dụ như khối lượng, kích thước, năng lượng… bằng các máy móc và các phương pháp vật lý quen thuộc.

- TT được ghi trên một vật mang vật chất, có thể lưu giữ, xử lý, truyền tải theo các kênh liên lạc khác nhau. Môi trường vận động thông tin là môi trường truyền tin, nó bao gồm các kênh liên lạc tự nhiên hoặc nhân tạo như sóng âm, tia sáng, dây dẫn, sóng âm thanh, sóng hình... Kênh liên lạc thường nối các thiết bị của máy móc với nhau hay nối với con người. Con người có hình thức liên lạc tự nhiên và cao cấp là tiếng nói, từ đó nghĩ ra chữ viết. Ngày nay nhiều công cụ phổ biến thông tin đã xuất hiện: bút viết, máy in, điện tín, điện thoại, phát thanh, truyền hình, phim ảnh…

- Bất kỳ đối tượng vật chất nào cũng chứa TT về bản thân nó hoặc về một đối tượng khác. Về nguyên tắc, thì bất kỳ cấu trúc vật chất nào hoặc bất kỳ dòng năng lượng nào cũng có thể mang thông tin. Các vật có thể mang thông tin được gọi là giá mang tin (support). Thông tin luôn mang một ý nghĩa xác định nhưng hình thức thể hiện của thông tin thì rõ ràng mang tính quy ước. Chẳng hạn ký hiệu "V" trong hệ đếm La Mã mang ý nghĩa là 5 đơn vị nhưng trong hệ thống chữ La tinh nó mang nghĩa là chữ cái V. Trong máy tính điện tử, nhóm 8 chữ số 01000001 nếu là số sẽ thể hiện số 65, còn nếu là chữ sẽ là chữ "A".

Không có TT thì cuộc sống không thể tồn tại dưới bất cứ hình thức nào, không thể hoạt động được bất kỳ hệ thống TT nào do con người và tự nhiên

tạo ra. Không có TT, các hệ thống sinh học và các hệ thống nhân tạo chỉ còn là một đống các nguyên tố hoá học. Các thí nghiệm cách ly các cơ quan cảm giác của con người, ngăn cản sự trao đổi TT của con người với môi trường xung quanh, đã chứng tỏ rằng sự đói TT gây ra những hậu quả huỷ diệt không kém gì đói khát vật chất.

1.1.2.2. Theo khía cạnh thông tin là đối tượng của sự bảo vệ

Chúng ta hãy điểm qua các tính chất của TT như là đối tượng của sự bảo vệ.

- Đối tượng cần bảo vệ là các vật mang TT

Thông tin đến được với con người là vì nó được chứa đựng trong các vật thể mang TT. Ví dụ, một bản tin chiến sự ta nhận được nhờ đọc báo (TT thể hiện qua chữ viết và được in trên vật mang là giấy) hoặc nhờ nghe đài (TT thể hiện qua tiếng nói âm thanh – sóng âm là vật mang). Vì bằng các thiết bị vật chất chỉ có thể bảo vệ được các đối tượng vật chất, nên đối tượng cần bảo vệ là các vật mang TT (vật chất).

Người ta phân chia ra vật mang – nguồn tin, vật mang – tải tin và vật mang – thu tin. Ví dụ, một bản vẽ là một nguồn tin, còn tờ giấy mà trên đó có bản vẽ là vật mang tin. Bản chất vật lý của nguồn và vật mang ở đây là một - đó là tờ giấy. Tuy nhiên giữa chúng có sự khác nhau. Tờ giấy khi không có văn bản hoặc hình vẽ trên đó chỉ là tờ giấy trắng và chỉ là nguồn thông tin về các đặc tính vật lý và hóa học của bản thân nó mà thôi. Khi tờ giấy có chứa một TT có ý nghĩa nó sẽ có một tên gọi khác: bản vẽ, bản tin, tài liệu v.v… Bản vẽ các chi tiết hoặc các nút là cấu thành của một tài liệu phức tạp hơn – bản vẽ một chiếc máy, một cơ chế, một tài liệu thiết kế sản phẩm mẫu…

Như vậy theo chức năng, nguồn có thể mang tên gọi khác nhau. Nhưng không phụ thuộc vào tên gọi của các tài liệu, cái cần phải bảo vệ chống lại việc đánh cắp, sao chép, làm thay đổi và phá huỷ thông tin chính là các tờ giấy và chúng có kích thước xác định, trọng lượng rõ ràng, có độ bền cơ học nhất định, có độ bền vững màu sắc hoặc mực in đối với các tác động bên ngoài của môi trường. Các thông số của vật mang tin quyết định các điều kiện và phương pháp lưu giữ thông tin trên đó. Một loại vật mang đặc biệt khác là

các trường (sóng điện từ, sóng âm…). Chúng không có biên giới rõ ràng trong không gian, nhưng các đặc trưng của chúng hoàn toàn đo được. Bản chất của nguồn tin, vật tải tin và vật thu tin có thể như nhau và cũng có thể khác nhau.

Việc truyền TT thực hiện bằng cách di chuyển vật mang TT trong không gian liên quan đến tiêu tốn năng lượng và năng lượng này phụ thuộc độ dài đường đi, các thông số của môi trường và bản chất vật mang.

- Giá trị của TT được đánh giá bởi mức độ có lợi của nó đối với người sử dụng (chủ sở hữu, người có tin, người nhận tin). Ở đây có thể phân chia làm 3 loại TT: có lợi, có hại và trung hoà (vô hại).

+ TT trung hoà không gây ảnh hưởng gì đến trạng thái công việc của người dùng nó.

+ TT có hại là TT mang lại thiệt hại vật chất hoặc tinh thần cho người dùng hoặc người nhận tin đó. Khi một TT có hại được dựng lên một cách chủ ý thì nó còn gọi là TT ngụy trang hay TT hoả mù.

+ TT có lợi mang lại lợi ích nhất định cho người dùng nó.

Lợi ích của TT luôn luôn cụ thể. TT có lợi hay có hại là đối với người dùng cụ thể. Người dùng ở đây hiểu là một cá nhân con người, hoặc một tập thể và thậm chí cả nhân loại. TT cực kỳ có lợi cho một loại người này có thể lại là có hại hoặc không có lợi cho những người khác. Thậm chí, TT quý giá cho toàn bộ nhân loại, ví dụ công nghệ chế tạo các thuốc chữa bệnh hiểm nghèo, nhưng đối với một con người khoẻ mạnh cụ thể lại không đáng quan tâm.

Chính vì vậy, trong BVTT, trước hết người ta xác định phạm vi những người (các công ty, các nhà nước) có nhu cầu đối với TT được bảo vệ. Vì có thể là trong phạm vi đó sẽ xuất hiện các tin tặc (người săn lùng TT được bảo vệ).

Với mục đích bảo vệ thông tin có giá trị (có lợi) chủ sở hữu của TT đó (Nhà nước, tổ chức, cá nhân) định ra trên vật mang TT đó một dấu hiệu quy ước tính giá trị của TT chứa trong đó – Dấu hiệu đó gọi là độ mật của TT.

Độ mật của các TT mà chủ sở hữu là Nhà nước (hoặc các cơ quan Nhà nước) được xác định trên cơ sở "Pháp lệnh bảo vệ bí mật Nhà nước" và Danh mục các bí mật nhà nước của các cơ quan, là thuộc về bí mật quốc gia. Theo nghị định số 33/2002/NĐ-CP ngày 28-3-2002 của Chính phủ, các thông tin mật, thông tin tối mật, thông tin tuyệt mật là các thông tin mà sự đánh cắp hoặc sự phổ biến bất hợp pháp của nó có thể mang lại thiệt hại cho tổ chức, cơ quan Nhà nước, các lĩnh vực kinh tế – xã hội, các tỉnh thành hoặc cả nước.

Để đánh dấu độ mật của các TT thương mại – dịch vụ, kinh tế xã hội người ta dùng nhiều cách phân chia khác nhau, ví dụ: công cộng, hạn chế, độc quyền, hoặc đại chúng, dùng chung, dành riêng…

- Có thể coi TT là một thứ hàng hoá.

TT có lợi, có hại và có thể mua hoặc bán TT. Do vậy TT có giá cả. Cũng như các loại hàng hoá khác, TT có giá cả và giá trị. Giá cả gồm giá trị và lợi nhuận.

Giá trị xác định bởi chi phí mà chủ sở hữu bỏ ra để thu được TT đó bằng cách:

+ Tiến hành các khảo sát, nghiên cứu trong phòng thí nghiệm, trong các trung tâm phân tích, trong các nhóm….

+ Mua TT trên thị trường TT

+ Đạt được TT bằng con đường bất hợp pháp

Lợi nhuận từ TT, do tính đặc thù, có thể có các dạng rất khác nhau, và tiền bạc không phải là hình thức phổ biến nhất. Nói chung, lợi nhuận từ TT có thể thu được bằng các hoạt động sau:

+ Bán TT trên thị trường

+ Vật chất hoá TT trong sản phẩm với các tính chất mới hoặc công nghệ mới mang lại lợi nhuận

+ Sử dụng TT để đưa ra các quyết định hiệu quả hơn: Điều này không hoàn toàn rõ ràng, nhưng lại chính là hình thức phổ biến nhất của lợi nhuận từ TT. Khi tiếp nhận được thông tin, con người thường phải xử lý nó để tạo ra

những thông tin mới, có ích hơn, từ đó có những phản ứng nhất định. Ví dụ trong lĩnh vực quản lý, các thông tin mới là các quyết định quản lý.

- Giá trị của TT thay đổi theo thời gian.

Sự lan truyền của TT và việc sử dụng TT dẫn đến thay đổi giá trị (và giá cả) của nó. Đặc trưng thay đổi giá trị của TT theo thời gian phụ thuộc vào dạng của TT. Với các TT khoa học – kỹ thuật sự phụ thuộc này thường có dạng hình sóng (lúc cao, lúc thấp). Ví dụ, vào đầu thế kỷ 20, các kết quả nghiên cứu về vật lý nguyên tử chỉ mang tính khám phá thuần tuý và chỉ có số ít các nhà bác học quan tâm đến. TT trong lĩnh vực này trở nên cực kỳ giá trị khi đã xuất hiện các khả năng thực tế sử dụng năng lượng nguyên tử. Theo mức độ phổ biến của công nghệ sử dụng năng lượng nói trên, giá trị của TT trong lĩnh vực này lại dần dần giảm sút…

Giá trị phần lớn các dạng TT lan truyền trong xã hội theo thời gian đều giảm dần – TT bị cũ đi. Người ta biểu diễn mức độ cũ đi (mức độ lạc hậu) của TT bằng công thức sau:

$$C_i(\tau) = C_0 \exp(-2{,}3\ \tau / \tau_s)$$

Ở đây: C_i : độ lạc hậu của TT tại thời điểm sử dụng τ

C_0 : giá trị của TT tại thời điểm nó xuất hiện (được tạo ra)

τ : khoảng thời gian từ lúc TT xuất hiện đến thời điểm sử dụng TT

τ_s : độ dài chu kỳ sống (vòng đời) của TT (từ lúc TT xuất hiện đến thời điểm lạc hậu hoàn toàn).

Theo công thức này, sau một vòng đời giá trị của TT giảm xuống còn 0,1 giá trị ban đầu. Phụ thuộc vào chu kỳ sống của TT, đôi khi người ta phân ra thành:

+ TT chiến thuật: đó là TT mà giá trị của chúng giảm đi 10% mỗi ngày (ví dụ TT về tín dụng ngắn hạn, đơn đặt hàng trong vòng 1 tháng).

+ TT chiến lược: đó là TT mà giá trị của nó giảm đi 10% mỗi tháng (ví dụ, TT về các đối tác, về tín dụng dài hạn, về phát triển…)

- Khái niệm lượng thông tin

Lượng TT chứa trong một cuốn sách đối với các độc giả khác nhau sẽ khác nhau. Thậm chí cùng một con người ở các giai đoạn khác nhau của cuộc đời mỗi lần vẫn tìm được trong cuốn sách đó điều gì đó mới hơn cho bản thân. Lượng TT trong đầu một người có thể gián tiếp đánh giá theo việc làm của anh ta vì để có một quyết định đúng đắn cần phải có nhiều TT hơn. Rõ ràng là không thể đánh giá một cách khách quan (không tính tới lợi ích của TT đối với người dùng) lượng TT.

Thông tin có thể tồn tại dưới nhiều dạng khác nhau, xuất phát từ nhiều nguồn khác nhau. Người ta có thể định lượng tin tức bằng cách đo độ bất định của hành vi, trạng thái. Xác suất xuất hiện một tin càng thấp thì độ bất ngờ càng lớn do đó lượng tin càng cao.

Trong lý thuyết TT, để đánh giá lượng TT người ta dùng tiếp cận entrôpi (độ bất định). Theo đó lượng TT được đánh giá bằng độ giảm sự bất định (entrôpi) của người nhận TT trong lựa chọn hoặc chờ đợi sự kiện sau khi nhận được TT. Lượng TT thu được càng lớn, thì xác suất sự kiện càng nhỏ. Cách miêu tả như vậy rất thuận tiện để xác định lượng TT trong một bản tin được truyền theo các kênh liên lạc. Lượng TT trong bản tin gồm N ký hiệu (không tính tới liên hệ giữa các ký hiệu trong bản tin) được tính theo công thức nổi tiếng của Shannon:

$$I = -N\sum_{i=1}^{n} P_i \log_2 P_i$$

Ở đây: P_i : Xác suất xuất hiện ký hiệu i trong bản tin

n: số ký hiệu trong bảng chữ cái.

Từ công thức này suy ra, lượng TT (đo bằng bit, bytes) chỉ phụ thuộc vào số lượng và thống kê của các ký hiệu chứ không phụ thuộc nội dung TT.

Lượng TT xác định theo công thức này, giống nhau khi truyền đi một bản tin vô nghĩa hoặc một bản tin quan trọng sống còn đối với người nhận

TT. Trên quan điểm truyền tin theo các kênh liên lạc thì tiếp cận trên là đúng đắn, vì cái giá bỏ ra để truyền các bản tin như vậy là giống nhau. Còn việc với mục đích gì người gửi tin đi đã chi phí tiền bạc và bản tin này có ích lợi gì cho người nhận – các câu hỏi này không có quan hệ gì đối với liên lạc.

Cũng giống như vậy, trong cuộc nói chuyện qua điện thoại mà người bạn cung cấp cho ta những tin tức đã biết thì lượng TT ta thu được rất nhỏ mặc dù cuộc nói chuyện có thể rất lâu. Khi đó xuất hiện câu hỏi, cái gì đã được truyền đi ở đây. Rõ ràng cái đã được truyền đi chỉ thuần tuý là các tín hiệu điện và tín hiệu âm thanh mà thôi.

Trên thực tế, người ta hay dùng phương pháp đơn giản và thô hơn để đo TT bằng cách tính lượng ký hiệu của bản tin (bằng bit hoặc bytes) hoặc là đo các đặc trưng của vật mang như số trang, số tờ, thời gian truyền tin… mà ý nghĩa của TT và giá trị của nó không được quan tâm.

1.2. KHÁI NIỆM AN TOÀN THÔNG TIN

Theo Luật pháp Hoa Kỳ, An toàn thông tin được định nghĩa là "bảo vệ thông tin và các hệ thống thông tin trước truy cập, sử dụng trái phép, tiết lộ, sự gián đoạn, biến đổi, hoặc hủy diệt". Về bản chất, nó có nghĩa là chúng ta muốn bảo vệ dữ liệu và hệ thống của mình khỏi những người sẽ tìm cách lợi dụng nó.

Theo một ý nghĩa chung, an toàn là bảo vệ tài sản của chúng ta. Điều này có thể có nghĩa là bảo vệ chúng khỏi những kẻ tấn công xâm nhập mạng, thiên tai, điều kiện môi trường bất lợi, mất điện, trộm cắp hoặc phá hoại, hoặc những tình trạng không mong muốn khác. Cuối cùng, chúng ta sẽ cố gắng để đảm bảo bản thân chúng ta có thể chống lại các hình thức tấn công có nhiều khả năng nhất ở mức tốt nhất mà chúng ta có thể cho môi trường của mình.

Khi chúng ta nhìn vào chính xác những gì mà chúng ta cần bảo vệ, chúng ta có thể có một loạt các tài sản tiềm năng. Chúng ta có thể xem xét các tài sản vật lý mà chúng ta có thể muốn đảm bảo an toàn, chẳng hạn như những giá trị cố hữu (vàng thỏi) hoặc những tài sản có giá trị thương mại của chúng ta (phần cứng máy tính). Chúng ta cũng có thể có các tài sản có tính chất siêu trần hơn, chẳng hạn như phần mềm, mã nguồn, hoặc dữ liệu. Trong môi

trường điện toán hiện nay, chúng ta có thể sẽ thấy rằng tài sản logic của chúng ta ít nhất cũng có giá trị bằng, nếu không là lớn hơn tài sản vật chất. Ngoài ra, chúng ta cũng phải bảo vệ những người đang tham gia vào các hoạt động của chúng ta. Con người là tài sản quý giá nhất, bởi vì chúng ta không thể thực hiện công việc mà không có họ. Chúng ta có thể nhân bản các tài sản vật lý và logic và lưu giữ bản sao lưu của chúng ở nơi khác để phòng chống trường hợp thảm họa xảy ra, nhưng nếu không có người có tay nghề để vận hành và duy trì môi trường của chúng ta, chúng ta sẽ nhanh chóng thất bại.

Trong những nỗ lực để bảo vệ tài sản, chúng ta cũng phải xem xét những hậu quả của các giải pháp an toàn được chọn để thực hiện. Có một trích dẫn nổi tiếng nói rằng: "Hệ thống chỉ thực sự an toàn là một hệ thống mà trong đó tắt hết điện, đúc trong một khối bê tông và niêm phong trong một phòng có đường dây chì dò sâu, có vũ trang bảo vệ và thậm chí sau đó tôi vẫn nghi ngờ vào sự an toàn". Mặc dù chúng ta chắc chắn có thể nói rằng một hệ thống ở trạng thái như vậy có thể được coi là an toàn hợp lý, nhưng hệ thống đó chắc chắn không sử dụng hoặc sản xuất được. Khi chúng ta tăng mức độ bảo mật, chúng ta thường làm giảm mức độ năng suất. Với hệ thống được đề cập ở trên, mức độ bảo mật sẽ rất cao, nhưng mức độ năng suất sẽ gần bằng không.

Ngoài ra, khi bảo vệ tài sản, hệ thống, hoặc môi trường, chúng ta cũng phải xem xét mức độ an toàn như thế nào gắn liền với giá trị của tài sản được bảo đảm. Nếu chúng ta sẵn sàng để thích ứng với việc bị giảm hiệu suất, chúng ta có thể áp dụng mức độ bảo mật rất cao cho tất cả tài sản mà chúng ta phải chịu trách nhiệm. Chúng ta có thể xây dựng một cơ sở hàng tỷ đô la được bao quanh bởi hàng rào dây thép gai và được tuần tra bảo vệ vũ trang, cùng với những con chó tấn công dữ dằn, và để tài sản của chúng ta cẩn thận trong một hầm kín bên trong ... Vì thế, tài sản của chúng sẽ không bao giờ bị tổn thương, nhưng đồng thời điều đó sẽ khiến cho tài sản này không có ý nghĩa nhiều. Tuy nhiên, trong một số môi trường, các biện pháp an ninh như vậy có thể không đủ. Trong bất kỳ môi trường nào mà chúng ta dự định thiết lập an toàn mức cao, chúng ta cũng cần phải đưa vào khoản chi phí thay thế tài sản trong trường hợp chúng ta làm mất chúng, và đảm bảo rằng chúng ta thiết lập các mức bảo vệ hợp lý đối với giá trị của chúng. Chi phí an toàn đưa ra không

bao giờ nên vượt xa giá trị của tài sản được bảo vệ. Một câu hỏi đặt ra ở đây là: Vậy khi nào hệ thống của chúng ta an toàn?

Xác định thời điểm chính xác mà chúng ta có thể được coi là an toàn đưa ra một số thách thức. Liệu chúng ta có an toàn nếu hệ thống của chúng ta được vá đúng cách? Hay chúng ta có an toàn nếu sử dụng mật khẩu mạnh? Chúng ta an toàn nếu bị ngắt kết nối hoàn toàn với Internet? Từ một góc độ nào đó, tất cả các câu hỏi có thể được trả lời là "không".

Ngay cả khi hệ thống của chúng ta được vá đúng cách, sẽ luôn có những cuộc tấn công mới làm cho hệ thống của chúng ta dễ bị tổn thương. Khi các mật khẩu mạnh mẽ được sử dụng, sẽ có những con đường khác mà một kẻ tấn công có thể khai thác. Khi chúng ta ngắt kết nối với Internet, hệ thống của chúng ta có thể bị truy cập vật lý hoặc bị đánh cắp. Tóm lại, rất khó để xác định khi nào hệ thống của chúng ta thật sự an toàn. Tuy nhiên, chúng ta có thể đi qua lần lượt các câu hỏi xung quanh.

Không thể đảm bảo an toàn 100%, nhưng ta có thể giảm bớt các rủi ro không mong muốn dưới tác động từ mọi phía của các lĩnh vực hoạt động kinh tế xã hội. Khi các tổ chức, đơn vị tiến hành đánh giá những rủi ro và cân nhắc kỹ những biện pháp đối phó về ATTT, họ luôn luôn đi đến kết luận: những giải pháp công nghệ (kỹ thuật) đơn lẻ không thể cung cấp đủ sự an toàn. Những sản phẩm Anti-virus, Firewalls và các công cụ khác không thể cung cấp sự an toàn cần thiết cho hầu hết các tổ chức. ATTT là một mắt xích liên kết hai yếu tố: yếu tố công nghệ và yếu tố con người.

1. Yếu tố công nghệ: bao gồm những sản phẩm như Firewall, phần mềm phòng chống virus, giải pháp mật mã, sản phẩm mạng, hệ điều hành và những ứng dụng như: trình duyệt Internet và phần mềm nhận Thư điện tử từ máy trạm.

2. Yếu tố con người: Là những người sử dụng máy tính, những người làm việc với thông tin và sử dụng máy tính trong công việc của mình.

Hai yếu tố trên được liên kết lại thông qua các chính sách về ATTT. Chúng ta sẽ thảo luận sâu hơn trong các phần sau.

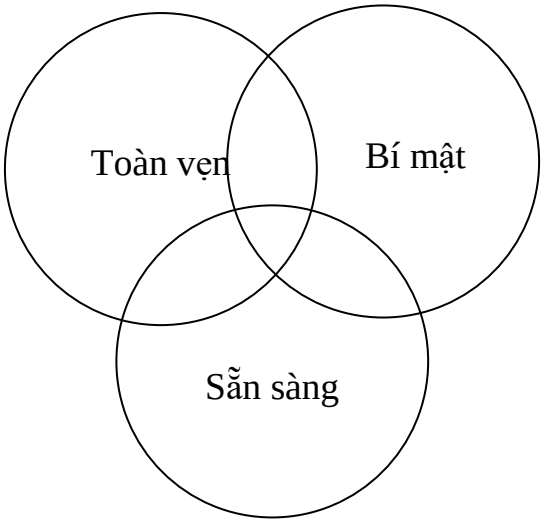
Xác định khi nào hệ thống không an toàn là một nhiệm vụ dễ dàng hơn nhiều, và chúng ta có thể nhanh chóng liệt kê một số yếu tố sẽ đưa hệ thống của chúng ta vào tình trạng này:

- Không vá hệ thống
- Sử dụng mật khẩu yếu như "password" hoặc "1234"
- Tải các chương trình từ Internet
- Mở file đính kèm thư điện tử từ người gửi lạ
- Sử dụng các mạng không dây mà không mã hóa

Chúng ta có thể tiếp tục tạo một danh sách như vậy trong một khoảng thời gian. Một khi chúng ta có thể chỉ ra các khu vực trong một môi trường có thể làm cho hệ thống không an toàn, chúng ta có thể thực hiện các bước để giảm thiểu những vấn đề này. Vấn đề này cũng giống như cắt một nửa cái gì đó lặp đi lặp lại ta sẽ luôn có một phần nhỏ còn lại để cắt một lần nữa. Mặc dù chúng ta có thể không bao giờ có được một trạng thái mà chúng ta có thể gọi là "an toàn", chúng ta có thể thực hiện các bước đi đúng hướng để đạt được trạng thái gần “an toàn”.

1.3. TAM GIÁC AN TOÀN THÔNG TIN

Ba trong số các khái niệm chính trong lĩnh vực an toàn thông tin đó là tính bí mật, tính toàn vẹn và tính sẵn sàng, thường được gọi là bộ ba tính bí mật, tính toàn vẹn và tính sẵn sàng (CIA) hay tam giác an toàn thông tin, như trong hình 1.1 dưới đây.



Hình 1.1 Bộ ba CIA

Thuật ngữ thường dùng cho tính bí mật, tính toàn vẹn và tính sẵn sàng là CIA. Trong một số tài liệu, phần lớn là các tài liệu của ISC2 chúng ta có thể thấy chúng được sắp xếp lại một chút như CAI. Không có ngụ ý nào trong việc thay đổi thứ tự này nhưng nó có thể gây nhầm lẫn cho những người chưa từng biết trước về điều đó. Chúng ta cũng có thể thấy được các khái niệm CIA đôi khi có thể còn được hiểu là: lộ tin, thay đổi và từ chối (DAD – Disclosure, alteration and Denial).

1.3.1. Tính bí mật

Tính bí mật (Confidentiality) là một khái niệm tương tự nhưng không giống với tính riêng tư (Privacy). Tính bí mật là một phần cần thiết cho tính riêng tư và đề cập tới khả năng của chúng ta để bảo vệ thông tin của mình trước những người không được phép xem nó. Tính bí mật là một khái niệm mà chúng ta có thể thực hiện ở nhiều cấp độ khác nhau của một quá trình. Tính bí mật đảm bảo thông tin chỉ cung cấp cho những người có thẩm quyền.

Ví dụ, chúng ta có thể xem xét trường hợp một người rút tiền từ máy ATM, người này sẽ tìm cách duy trì tính bí mật của số nhận dạng cá nhân (PIN), cái mà cho phép anh ta kết hợp với thẻ ATM của mình có thể rút tiền từ máy ATM. Ngoài ra, người sở hữu thẻ ATM cũng hi vọng duy trì được tính bí mật của số tài khoản, số dư và bất kỳ thông tin nào khác cần thiết để

giao dịch với ngân hàng mà từ đó có thể rút được tiền. Ngân hàng sẽ duy trì tính bí mật cho các giao dịch với máy ATM và cân bằng số dư tài khoản sau khi tiền được rút. Nếu tại bất kỳ một điểm nào mà tính bí mật của giao dịch bị tổn thương, có thể sẽ đem lại một hậu quả xấu cho các cá nhân.

Tính bí mật có thể bị tổn thương bởi việc đánh mất máy tính có chứa dữ liệu, một người nào đó nhìn qua vai khi chúng ta nhập mật khẩu, một tài liệu đính kèm trên thư điện tử gửi tới sai địa chỉ người nhận, một kẻ tấn công xuyên thủng hệ thống của chúng ta, hay những vấn đề tương tự như thế.

1.3.2. Tính toàn vẹn

Tính toàn vẹn đề cập đến khả năng ngăn các dữ liệu của chúng ta không bị thay đổi một cách trái phép hoặc thay đổi không như ý muốn. Điều này có nghĩa là sự thay đổi trái phép hoặc việc xóa dữ liệu hay các phần dữ liệu của chúng ta, hoặc nó có thể có nghĩa là có sự ủy quyền nhưng không mong muốn làm thay đổi hay xóa dữ liệu của chúng ta. Để duy trì tính toàn vẹn chúng ta không chỉ cần có các phương tiện ngăn chặn những thay đổi dữ liệu một cách trái phép mà còn cần có khả năng để khôi phục các thay đổi đã được thay đổi có thẩm quyền.

Chúng ta có thể thấy một ví dụ hay về cơ chế cho phép chúng ta kiểm soát tính toàn vẹn trong các hệ thống tập tin của nhiều hệ điều hành hiện đại như Windows và Linux. Đối với mục đích ngăn chặn các thay đổi trái phép, các hệ thống này thường thực hiện việc hạn chế các quyền truy cập mà một người dùng chưa được xác thực có thể thực hiện đối với tập tin nhất định. Ngoài ra một số hệ thống và nhiều ứng dụng tương tự như thế có thể cho phép chúng ta khôi phục lại các thay đổi nếu cần thiết, chẳng hạn như cơ sở dữ liệu.

Tính toàn vẹn đặc biệt quan trọng khi chúng ta đang nói rằng dữ liệu cung cấp nền tảng cho các quyết định khác. Nếu kẻ tấn công đã làm thay đổi các dữ liệu có chứa các kết quả của các xét nghiệm y tế, chúng ta có thể thấy việc điều trị sai phương pháp có khả năng dẫn đến cái chết của bệnh nhân.

1.3.3. Tính sẵn sàng

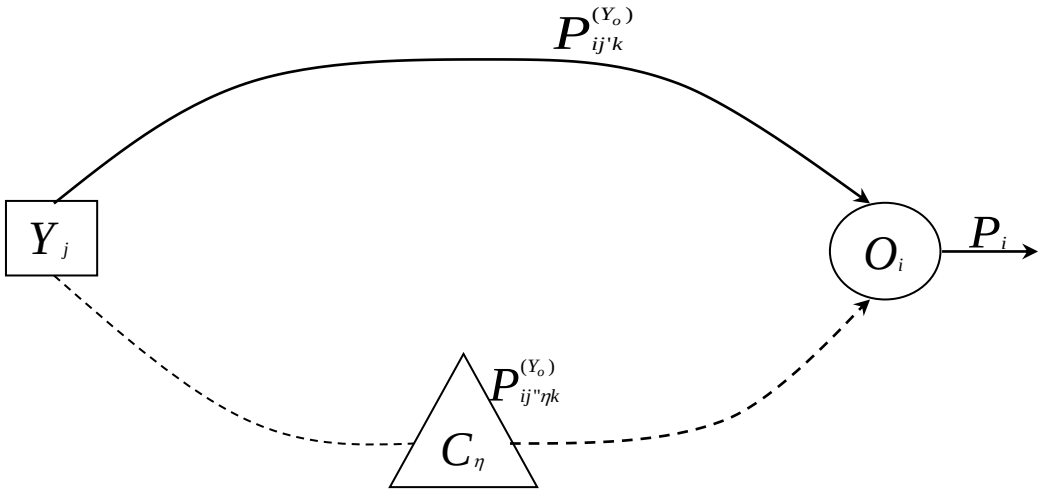
Thành phần cuối cùng trong bộ ba CIA là tính sẵn sàng. Tính sẵn sàng đề cập tới khả năng truy cập dữ liệu khi chúng ta cần tới. Khả năng đáp ứng của thông tin là điều rất quan trọng, điều này thể hiện tính sẵn sàng phục vụ của các dịch vụ. Khả năng đáp ứng của hệ thống chịu ảnh hưởng bởi khá nhiều thành phần: có thể là phần cứng, phần mềm hay hệ thống sao lưu. Khả năng đáp ứng của hệ thống cần được tính đến dựa trên số người truy cập và mức độ quan trọng của dữ liệu. Mất tính sẵn sàng là sự phá vỡ ở bất kỳ vị trí nào trong hệ thống của chúng ta mà làm cản trở việc truy cập của chúng ta vào dữ liệu của mình. Các vấn đề như thế có thể dẫn đến sự tổn thất về điện năng, các vấn đề về hệ điều hành hoặc ứng dụng, các tấn công mạng, sự tổn thương của hệ thống hoặc các vấn đề khác. Khi các vấn đề như thế do một yếu tố bên ngoài gây ra, chẳng hạn như một kẻ tấn công thì chúng thường được gọi là một cuộc tấn công từ chối dịch vụ (DoS).

1.4. MÔ HÌNH TỔNG QUÁT CỦA QUÁ TRÌNH BẢO VỆ THÔNG TIN

Vai trò cơ bản của mô hình tổng quát là chỉ ra các điều kiện cho việc đánh giá khách quan trạng thái chung của hệ thống trên quan điểm độ đo mức bảo vệ TT trong hệ thống (HT). Ở đây các khái niệm như độ mạo hiểm, độ bảo vệ, độ tổn thương của TT có thể coi như đồng nhất. Sự cần thiết của các đánh giá như vậy thường xuất hiện khi phân tích các tình huống chung để đưa ra các quyết định có tính chất chiến lược trong tổ chức BVTT.

Giả sử chúng ta có một hệ thống TT – VT nơi TT đang được xử lý trong các thành phần (ta sẽ gọi là các đối tượng) của nó. hệ thống gồm nhiều đối tượng O_i như vậy. Trong quá trình xử lý TT (mà ta quan tâm), hệ thống có thể ở trong các trạng thái k khác nhau (khái niệm trạng thái của hệ thống như vậy chúng ta sẽ định nghĩa sau). Rõ ràng là toàn bộ hệ thống và các đối tượng O_i luôn luôn chịu tác động liên tục của các hiểm họa về ATTT. Ta ký hiệu các hiểm họa này là Y_j. Giả sử tiếp, trong hệ thống của chúng ta đã có cài đặt một số thiết bị bảo vệ C_η nào đó để chống lại các hiểm họa nhất định đã biết. Ta ký hiệu tập hợp tất cả các hiểm họa còn lại (trừ các hiểm họa đã có thiết bị

bảo vệ chống lại) là Y_0. Khi đó mô hình tổng quát nhất có thể chỉ ra như sơ đồ sau:



Hình 1.2 Mô hình tổng quát BVTT

Trong đó:

- O_i là các đối tượng trong hệ thống cần bảo vệ
- Việc xử lý TT tại O_i chịu tác động liên tục của các hiểm họa ATTT Y_i (trong mọi trạng thái của O_i).
- P_i là xác suất bảo vệ thông tin đang xử lý tại đối tượng O_i (tức độ bảo vệ thông tin tại O_i)
- C_η là các thiết bị bảo vệ chống lại các hiểm họa nhất định đã biết
- $P_{ij'k}^{(Y_o)}$ là xác suất bảo vệ thông tin tại O_i ở trạng thái k của nó (chế độ làm việc của O_i), chống lại tất cả các hiểm họa mà trong hệ thống không có các thiết bị bảo vệ tương ứng (tập hợp các hiểm họa còn lại Y_0), ở đây j' nhận các giá trị số thứ tự của các hiểm họa mà không có thiết bị chống lại

$P_{ij''\eta k}^{(Y_o)}$ là xác suất bảo vệ thông tin như trên chống lại các hiểm họa mà trong hệ thống có cài đặt các thiết bị bảo vệ. Ở đây j" nhận các giá trị số thứ tự các hiểm họa mà hệ thống có các thiết bị chống lại, η nhận giá trị số thứ tự các thiết bị bảo vệ được cài đặt trong hệ thống.

Đặc tính và mức độ tác động của mỗi loại hiểm họa coi là độc lập với nhau.

Hệ thống được coi là không đầy đủ trong ý nghĩa là có tính tới chỉ một số thiết bị bảo vệ chống lại một vài hiểm họa nhất định, còn nhiều hiểm họa không có thiết bị tương ứng chống lại.

Để tính toán đầy đủ thì phải tính tới tương tác giữa các hiểm họa với nhau, cũng như tương tác giữa các thiết bị bảo vệ với nhau, và cả tương tác giữa các thiết bị bảo vệ với các hiểm họa nữa.

Chúng ta có thể viết:

$$P_i = 1 - \prod_{\forall k} (1 - P_{i,k}) \alpha_k$$

ở đây:

P_{ik} là xác suất bảo vệ TT tại O_i ở trạng thái *k*.

α_k là trọng số của trạng thái *k* của hệ thống trong khoảng thời gian đánh giá. Nếu ΔT là khoảng thời gian đánh giá và Δt_k là phần thời gian mà hệ thống xử lý rơi vào trạng thái *k* thì có thể viết:

$$\alpha_k = \frac{\Delta t_k}{\Delta T}$$

Vì hệ thống là không đầy đủ nên có thể viết:

$$P_{ik} = P'_{ik} P''_{ik}$$

ở đây:

P'_{ik} xác suất bảo vệ TT tại O_i ở trạng thái *k* của nó (chế độ làm việc của O_i), chống lại tất cả các hiểm họa mà trong hệ thống không có các thiết bị bảo vệ tương ứng (tập hợp các hiểm họa còn lại Y_o).

P''_{ik} xác suất bảo vệ TT như trên chống lại các hiểm họa mà trong hệ thống có cài đặt các thiết bị bảo vệ.

Có thể viết:

$$P'_{ik} = 1 - \prod_{\forall j'} (1 - P_{ij'k}^{(Y_o)})$$

ở đây *j'* nhận các giá trị số thứ tự các hiểm họa mà không có thiết bị chống lại; còn:

$$P''_{ik} = 1 - \prod_{\forall \eta} \prod_{\forall j''} (1 - P^{(Y_o)}_{ij''\eta k})$$

ở đây, *j''* nhận các giá trị số thứ tự các hiểm họa mà trong hệ thống có các thiết bị chống lại.

η nhận giá trị số thứ tự các thiết bị bảo vệ được cài đặt trong hệ thống.

Xác suất P bảo vệ TT tại một nhóm các đối tượng xử lý của hệ thống sẽ là:

$$P = \prod_{\forall i} P_i$$

Trong bài toán cần phải tính tới các yếu tố thời gian. Các công thức tính độ bảo vệ nêu ở trên chỉ đúng trong một khoảng thời gian không lớn δt. Nếu khoảng thời gian ΔT mà trong đó ta đánh giá độ bảo vệ của hệ thống lớn hơn nhiều so với δt thì ta có:

$$P(\Delta T) = \prod_{z=1}^{\bar{z}} P_z(\delta t)$$

Ở đây $\bar{Z} = [\frac{\Delta T}{\delta t}]$ - phần nguyên, còn $P_z(\delta t)$ - là độ bảo vệ TT ở khoảng thời gian thứ z với độ dài δt.

Mô hình tổng quát này khá đơn giản. Để xác định độ bảo vệ TT chỉ cần biết các đặc trưng thống kê tác động của các hiểm họa khác nhau đối với TT và hiệu quả hoạt động của các thiết bị bảo vệ đã có. Để có được các đặc trưng đó là rất khó, nhưng không phải là không giải quyết được. Cần chỉ ra rằng, mô hình đã bỏ qua một số tương tác quan trọng như đã nói ở trên.

1.5. MỘT SỐ CÔNG VIỆC TRONG LĨNH VỰC AN TOÀN THÔNG TIN

Ở Việt Nam, hầu hết đều nghĩ rằng làm an toàn thông tin nghĩa là đảm bảo an toàn hệ thống mạng (network/system security), trong khi thực tế đây

chỉ là một trong số rất nhiều công việc trong ngành. Vì thế ở đây sẽ giới thiệu bốn nhóm công việc chính trong ngành.

*** An toàn sản phẩm (product security)**

Công việc chính của nhóm này là làm việc với các đội phát triển sản phẩm để đảm bảo sản phẩm làm ra an toàn cho người dùng và an toàn cho hệ thống của công ty, cụ thể là:

- Kiểm định mã nguồn và thiết kế của sản phẩm
- Phát triển các giải pháp kỹ thuật và quy trình phát triển phần mềm an toàn để phát hiện và ngăn chặn những kỹ thuật tấn công đã biết
- Đào tạo nhân lực để nâng cao nhận thức về an toàn thông tin cũng như kỹ năng viết mã an toàn
- Nghiên cứu các hướng tấn công mới có thể ảnh hưởng hệ thống sản phẩm và dịch vụ của công ty

Tóm gọn lại thì nhóm này chuyên tìm lỗ hổng và kỹ thuật tấn công mới.

*** An toàn vận hành (operations security)**

Công việc chính của nhóm này là đảm bảo sự an toàn cho toàn bộ hệ thống thông tin của doanh nghiệp, với ba nhiệm vụ chính:

- Ngăn chặn: đưa ra các chính sách, quy định, hướng dẫn về an toàn vận hành; kiện toàn toàn bộ hệ thống thông tin, từ các vành đai cho đến máy tính của người dùng cuối; cấp và thu hồi quyền truy cập hệ thống; quét tìm lỗ hổng trong hệ thống, theo dõi thông tin lỗ hổng mới và làm việc với các bên liên quan để vá lỗi…
- Theo dõi và phát hiện: giám sát an ninh mạng.
- Xử lý: phản hồi (incident response) và điều tra số (digital forensics) khi xảy ra sự cố an toàn thông tin, từ tài khoản của nhân viên bị đánh cắp, rò rỉ thông tin sản phẩm mới cho đến tấn công từ chối dịch vụ.

*** Phát triển công cụ (applied security)**

Công việc chính của nhóm này là phát triển và cung cấp các công cụ, dịch vụ và thư viện phần mềm có liên quan đến an toàn thông tin cho các nhóm phát triển sản phẩm sử dụng lại.

Nhóm này bao gồm các kỹ sư nhiều năm kinh nghiệm và có kiến thức vững chắc về an toàn thông tin, viết mã an toàn và mật mã học. Họ phát triển

các thư viện và dịch vụ dùng chung như phân tích mã tĩnh – phân tích mã động, hộp cát (sandboxing), xác thực, ủy quyền, mã hóa và quản lý khóa…

Đây là dạng công việc dành cho những ai đang viết phần mềm chuyên nghiệp và muốn chuyển qua làm về an toàn thông tin. Đây cũng là công việc của những người thích làm an toàn sản phẩm nhưng muốn tập trung vào việc xây dựng sản phẩm hơn là tìm lỗ hổng.

Rõ ràng loại công việc này chỉ xuất hiện ở các công ty phần mềm lớn. Ở các công ty phần mềm nhỏ hơn thì các kỹ sư phần mềm thường phải tự cáng đáng công việc này mà ít có sự hỗ trợ từ nguồn nào khác.

*** Tìm diệt mã độc và các nguy cơ khác (threat analysis)**

Công việc chính của nhóm này là phân tích, truy tìm nguồn gốc và tiêu diệt tận gốc mã độc và các tấn công có chủ đích. Mã độc ở đây có thể là virút, sâu máy tính, hay mã khai thác các lỗ hổng đã biết hoặc chưa được biết đến mà phần mềm diệt virút thông thường chưa phát hiện được. Các loại mã độc này thường được sử dụng trong các tấn công có chủ đích vào doanh nghiệp.

Ngoài ra còn nhiều nhóm công việc khác trong ngành an toàn thông tin.

1.6. CÂU HỎI

1. Cho bản tin sau: “Tạp chí cộng sản là cơ quan lý luận và chính trị của Trung ương Đảng cộng sản Việt nam, đưa tin về thành công tốt đẹp của Đại hội X”. Hãy tính lượng thông tin chứa trong bản tin đó (theo công thức của C.Shannon).

2. Sự khác nhau giữa bảo mật (Secrecy hoặc Privacy) và an toàn (Security); an toàn và bí mật (Confidentiality); bí mật và toàn vẹn (Integrity)?

3. Thông tin có những tính chất gì?

4. Tại sao trong mô hình tổng quát của quá trình bảo vệ thông tin lại có công thức sau:

$$P_{ik} = P'_{ik} * P''_{ik}$$

Hãy giải thích ý nghĩa của từng ký hiệu trong công thức trên?

5. Khi nào thì văn bản có lượng thông tin nhiều nhất (theo công thức C.Shannon)?

CHƯƠNG 2. CÁC HIỂM HỌA GÂY MẤT AN TOÀN THÔNG TIN

2.1. CÁC KHÁI NIỆM CƠ BẢN

Để có thể nói cụ thể hơn về các tấn công, chúng ta cần phải giới thiệu một số thuật ngữ mới. Khi chúng ta xem xét một cuộc tấn công cụ thể ảnh hưởng đến chúng ta, chúng ta có thể nói về nó với các hiểm họa, các lỗ hổng và các rủi ro liên quan mà có thể đi kèm với chúng.

Hiểm họa là bất kể cái gì đó có khả năng gây hại cho chúng ta. Các hiểm họa có xu hướng được cụ thể đối với môi trường nhất định, đặc biệt là trong an toàn thông tin. Ví dụ mặc dù một loại virus có thể là vấn đề trên hệ điều hành Windows, virus này sẽ không có bất kỳ tác dụng trên hệ điều hành Linux..

Hiểm họa ATTT của hệ thống TT – VT là những khả năng tác động lên TT được xử lý trong hệ thống và dẫn tới sự biến dạng, huỷ diệt, sao chép, sự ngăn chặn tiếp cận tới TT; là khả năng tác động tới các thành phần của hệ thống dẫn tới sự mất mát, sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang TT, các thiết bị tương tác với vật mang hoặc các thiết bị điều khiển chúng.

Lỗ hổng là điểm yếu mà có thể được sử dụng để gây hại cho chúng ta. Về bản chất chúng là những lỗ hổng có thể bị khai thác bởi các hiểm họa để làm hại chúng ta. Một lỗ hổng có thể là một hệ điều hành hoặc một ứng dụng cụ thể mà chúng ta đang chạy, ở một vị trí vật lý nơi có văn phòng của chúng ta, một trung tâm dữ liệu được phân bố vượt quá khả năng của hệ thống điều hòa không khí, thiếu máy phát điện dự phòng hoặc các yếu tố khác.

Rủi ro là khả năng một cái gì đó xấu sẽ xảy ra. Để một rủi ro xảy ra trong một môi trường cụ thể thì cần phải có cả một hiểm họa và một lỗ hổng mà hiểm họa cụ thể có thể khai thác. Ví dụ nếu chúng ta có một cấu trúc được làm từ gỗ và chúng ta đặt nó trên lửa, chúng ta có cả hiểm họa (lửa) và một tổn thương phù hợp với nó (cấu trúc gỗ). Trong trường hợp này chúng ta chắc chắn có một rủi ro (bị cháy).

Tương tự như vậy nếu chúng ta có cùng hiểm họa là lửa, nhưng cấu trúc của chúng ta được làm bằng bê tông, chúng ta không còn có rủi ro thích hợp bởi vì hiểm họa của chúng ta không có lỗ hổng để khai thác. Chúng ta có thể lập luận rằng ngọn lửa đủ nóng có thể làm hỏng bê tông, nhưng điều này là một khả năng rất khó xảy ra.

Chúng ta sẽ thường xuyên nói về rủi ro tiềm năng trong môi trường máy tính, và các rủi ro tiềm năng nhưng không thể xảy ra tấn công. Trong những trường hợp như vậy, chiến lược tốt nhất là dành thời gian để giảm thiểu các cuộc tấn công có khả năng nhất. Nếu chúng ta giấu các tài nguyên đi để cố gắng lập kế hoạch cho tất cả các tấn công có thể, tuy nhiên không phải như thế, chúng ta sẽ làm bản thân mình yếu đi và thiếu sự bảo vệ ở nơi mà chúng ta thực sự cần nó nhất.

2.2. PHÂN LOẠI CÁC HIỂM HỌA GÂY MẤT AN TOÀN THÔNG TIN

Để đưa ra được các yêu cầu ATTT đối với việc bảo vệ HT, trước hết phải tiến hành phân tích hiểm họa của hệ thống. Phải liệt kê được danh mục các hiểm họa; đánh giá được xác suất thực hiện của chúng; cần xác định được mô hình kẻ phá hoại. Đó chính là nội dung cơ bản của phân tích hiểm họa hệ thống. Ngoài việc làm rõ các hiểm họa có thể, cần phải tiến hành phân tích chúng trên cơ sở phân loại theo các dấu hiệu, mà mỗi dấu hiệu sau đó sẽ phản ánh một trong những yêu cầu tổng quát đối với hệ BVTT. Các hiểm họa cùng loại (cùng tương ứng với một dấu hiệu) sẽ cho phép chi tiết hoá yêu cầu tổng quát nói trên đối với mỗi dấu hiệu phân loại.

Sự cần thiết phải phân loại các hiểm họa ATTT đối với một hệ thống là do những điều kiện khách quan sau đây: Kiến trúc của các thiết bị xử lý TT hiện đại, thiết kế về tổ chức, về cấu tạo, về chức năng hoạt động của các trung

tâm máy tính và các mạng; công nghệ và điều kiện xử lý tự động các TT hiện nay ở trong trạng thái mà TT tích luỹ, lưu giữ và xử lý trong đó phải chịu các ảnh hưởng ngẫu nhiên của cực kỳ nhiều các yếu tố, đến mức không thể nào đặt ra được bài toán miêu tả toàn bộ tập hợp các hiểm họa đối với mỗi hệ thống. Cho nên, đối với hệ bảo vệ, người ta thực hiện việc xác định không phải danh mục đầy đủ các hiểm họa, mà chỉ là danh mục các lớp hiểm họa mà thôi.

Phân loại các hiểm họa ATTT của một hệ thống có thể thực hiện theo loạt các dấu hiệu cơ bản sau đây:

- Theo bản chất xuất hiện

- Các hiểm họa tự nhiên: Đó là các hiểm họa do sự tác động lên hệ thống và các thành phần, của các quá trình vật lý khách quan hoặc các hiện tượng thiên tai ngẫu nhiên, không phụ thuộc vào con người.

- Các hiểm họa nhân tạo: Đó là các hiểm họa ATTT đối với hệ thống gây ra bởi hoạt động của con người.

- Theo mức độ định trước

- Hiểm họa của hành động ngẫu nhiên và/hoặc hiểm họa sinh ra do các lỗi hoặc sự bất cẩn của nhân viên.

- Hiểm họa từ các hành động cố ý định trước (kẻ xấu đánh cắp TT).

- Theo nguồn trực tiếp sinh ra

- Nguồn sinh trực tiếp là môi trường tự nhiên: thiên tai, bão tố, phóng xạ….

- Nguồn sinh trực tiếp là con người: cài cắm nội gián, mua chuộc, sao chụp trộm…

- Nguồn sinh là các phần mềm hợp pháp: Khi chạy chương trình làm việc mà gây nên treo máy hoặc gây ra các biến đổi trong cấu trúc dữ liệu.

- Nguồn sinh là các phần mềm bất hợp pháp: như virus, ngựa Troa, bom logic…

- Theo vị trí của nguồn sinh ra

- Nguồn sinh nằm ngoài lãnh thổ kiểm soát nơi đặt hệ thống như: thu trộm các bức xạ thấp như điện từ âm thanh từ các thiết bị và đường dây hoặc thu và khuếch đại các bức xạ tích cực từ các thiết bị phụ trợ không trực tiếp tham gia quá trình xử lý TT (đường điện thoại, đường điện nuôi, lò sưởi…).

- Nguồn sinh nằm ngay trong lãnh thổ kiểm soát (toà nhà đặt máy) như: ăn cắp rác thải công nghệ (giấy viết, giấy nháp có chứa TT), các thiết bị nghe trộm, cháy nổ…

- Nguồn sinh có tiếp cận tới thiết bị đầu cuối.

- Nguồn sinh đặt ngay trong hệ thống: ví dụ, thiết kế cài đặt các thiết bị, các chương trình lấy cắp, phá hoại… Sử dụng không đúng các tài nguyên.

- Theo mức độ phụ thuộc vào hoạt động của hệ thống TT – VT

- Không phụ thuộc vào hoạt động của HT: ví dụ công phá mật mã bảo vệ, ăn cắp các vật mang tin (đĩa từ, bộ nhớ, băng từ…).

- Chỉ xuất hiện trong quá trình tự động xử lý TT: như hoàn thành và phát tán các chương trình vi rút…

- Theo mức độ tác động lên hệ thống

- Hiểm họa thụ động không làm thay đổi gì về cấu trúc và nội dung HT: ví dụ sao chụp các dữ liệu mật.

- Hiểm họa tích cực gây ra những thay đổi nhất định trong cấu trúc và nội dung của HT: ví dụ các bẫy, các vi rút, ngựa Troa, bọ, rệp… làm biến dạng TT…

- Theo các giai đoạn tiếp cận của người dùng hoặc các chương trình tới các tài nguyên HT

- Thể hiện khi thực hiện tiếp cận tài nguyên HT: ví dụ tiếp cận trái phép tới hệ thống.

- Thể hiện sau khi được phép tiếp cận tới HT: ví dụ sử dụng trái phép hoặc sai tài nguyên HT…

- Theo phương pháp tiếp cận tới các tài nguyên HT

- Sử dụng con đường chuẩn thông thường tiếp cận tài nguyên: ví dụ lợi dụng mật khẩu, giả danh người dùng…

- Sử dụng các phương tiện ngầm (không chuẩn): qua mặt các thiết bị kiểm soát, chọc thủng hệ điều hành HT….

- Theo nơi cư trú hiện tại của TT được lưu giữ và xử lý trong HT

- Tiếp cận TT tại các bộ nhớ ngoài (sao chép trộm từ ổ đĩa cứng).

- Tiếp cận TT tại vùng nhớ hoạt động (ROM, RAM): ví dụ đọc TT từ vùng nhớ dành cho hệ điều hành hoặc thiết bị bảo vệ…

- Tiếp cận TT đang trao đổi hay truyền trên các đường liên lạc: ví dụ trích đường liên lạc để biến đổi TT, ăn trộm danh tính người dùng để mạo nhận, đánh lừa xác thực, chiếm đoạt TT đường truyền…

- Tiếp cận TT phản xạ từ thiết bị đầu cuối, hoặc trên máy in: ví dụ ghi các TT phản xạ vào một camera mật…

2.3. MỘT SỐ HIỂM HỌA GÂY MẤT AN TOÀN THÔNG TIN PHỔ BIẾN

Từ những kẻ tấn công bỏ nhiều thời gian và công sức tìm cách để ăn cắp bí mật của công ty đến những nhân viên tận tâm vô tình chạm phím delete, có rất nhiều kẻ thù đối với an toàn thông tin. Do có nhiều loại hiểm họa khác nhau nên rất khó khăn trong việc cố gắng thiết lập và duy trì an toàn thông tin. Các tấn công đến từ nhiều nguồn khác nhau, do đó nó giống như việc cố gắng để chống lại một cuộc chiến tranh trên nhiều mặt trận. Các chính sách tốt có thể giúp chống lại các hiểm họa nội bộ, tường lửa và hệ thống phát hiện xâm nhập có thể giúp chống lại các hiểm họa bên ngoài. Tuy nhiên, chỉ cần một lỗi của một thành phần nào đó có thể dẫn đến một thất bại tổng thể trong việc đảm bảo an toàn thông tin. Điều này có nghĩa rằng ngay cả khi chúng ta chỉ bảo vệ thông tin của mình khỏi các hiểm họa bên ngoài nhưng những người dùng cuối vẫn có thể tạo ra các lỗ hổng bảo mật thông tin. Thống kê gần đây cho thấy phần lớn các thỏa hiệp thành công vẫn là từ người trong cuộc. Trong thực tế, Viện bảo mật máy tính (Computer Security Institute - CSI) tại San Francisco ước tính từ 60 – 80% sự lạm dụng trên mạng xuất phát từ bên trong doanh nghiệp.

Ngoài nhiều nguồn của các cuộc tấn công an toàn thông tin, cũng có nhiều loại tấn công an toàn thông tin. Bộ ba an toàn thông tin giúp ta có được một sự minh họa tốt điều này. Bộ ba an toàn thông tin cho thấy ba mục tiêu chính của an ninh thông tin: tính toàn vẹn, tính bí mật, và tính sẵn sàng. Khi ba tính chất này phù hợp với nhau, thông tin sẽ được bảo vệ tốt.

Như chúng ta đã nói, công việc của người quản lý an toàn thông tin là rất khó. Có nhiều nhiệm vụ phải được thực hiện để bảo vệ đầy đủ các nguồn lực của một tổ chức, và một sự sai lệch bất kỳ phần nào trong đó cũng có thể dẫn đến sự vi phạm tính an toàn hệ thống. Đây là lý do tại sao nhiệm vụ bảo vệ hệ

thống thông tin là khá khó khăn. Trong phần tiếp theo chúng ta sẽ xem xét những cách khác nhau mà một hệ thống có thể bị tấn công.

2.3.1. Các hiểm họa ngẫu nhiên

Các hiểm họa ngẫu nhiên là những hiểm họa do lỗi hoặc những thiếu sót vô ý, những bất cẩn của con người, những hiểm họa tự nhiên (do sự tác động lên hệ thống và các thành phần, của các quá trình vật lý khách quan hoặc các hiện tượng thiên tai ngẫu nhiên, không phụ thuộc vào con người).

Các hiểm họa do lỗi hoặc sự bất cẩn của con người chẳng hạn như các thao tác không thận trọng dẫn đến giải mật các thông tin mật hoặc làm lộ các thông tin mật, hay một người dùng vô tình kích vào phím delete và làm xóa các dữ liệu quan trọng. Trên thực tế, dữ liệu sau khi xóa đi vẫn còn lưu trữ trên ổ cứng mà các phần mềm chuyên dụng vẫn có thể khôi phục lại chúng khi cần thiết. Mặc dù lỗi và sự bất cẩn không được các tin tặc quốc tế quan tâm nhiều nhưng theo một nghiên cứu mới nhất được thực hiện thông qua hệ thống thư điện tử, nó vẫn là mối đe dọa số một cho hệ thống của chúng ta. Bởi vì chúng ta không thể từ chối tất cả các truy cập của cộng đồng người dùng, Việc bảo vệ hệ thống trở nên khó khăn trước những người cần sử dụng nó ngày này qua ngày khác. Lỗi và sự bất cẩn tấn công vào thành phần bí mật và toàn vẹn của bộ ba CIA.

Để giúp chống lại những sai lầm này, chúng ta có thể sử dụng một số nguyên tắc bảo mật sau.

Nguyên tắc an toàn đầu tiên mà sẽ giúp chống lại lỗi và thiếu sót là "đặc quyền tối thiểu". Nếu chúng ta chỉ cung cấp cho người dùng tập tối thiểu nhất các quyền truy cập cần thiết để thực hiện chức năng công việc của họ, sau đó chúng ta sẽ giảm số lượng thông tin có thể vô tình bị làm hỏng.

Một nguyên tắc có thể giúp giảm thiểu vấn đề này là thực hiện sao lưu đầy đủ và thường xuyên các thông tin trên hệ thống. Khi người dùng làm mất tính toàn vẹn của thông tin thường trú trên hệ thống, cách đơn giản nhất để khôi phục lại các thông tin là từ một tệp sao lưu được thực hiện vào đêm hôm trước. Tệp sao lưu là một trong những công cụ cần thiết của người quản lý an toàn thông tin và thường chỉ cần đến đối với một cuộc tấn công thành công.

Các hiểm họa tự nhiên mà chúng ta phải đối mặt khi chúng ta xem xét vấn đề an toàn cho hệ thống như là: thiên tai, bão tố, phóng xạ, động đất, các sinh vật sống xâm nhập phá hủy hệ thống (chuột…) … Để đối phó hiệu quả với các hiểm họa tự nhiên này chúng ta cần đưa ra và thực hiện các chính sách an toàn vật lý phù hợp (sẽ được đề cập trong chương sau).

2.3.2. Gian lận và trộm cắp

Nếu người dùng cuối không vô tình phá hủy dữ liệu mà đang cố phá hủy các thông tin, thì ta có thể có một loại tấn công hoàn toàn khác. Đối với hầu hết nhân viên rất khó để tưởng tượng rằng một đồng nghiệp đến làm việc hàng ngày với một mưu đồ, nhưng điều đó có thể xảy ra. Như đã nói, các nhân viên có trách nhiệm hay được tin cậy sẽ có khả năng xâm nhập thành công lớn hơn so với những yếu tố bên ngoài. Điều này khiến cho việc tìm ra nguồn gốc của các cuộc tấn công nội bộ mà không cần cảnh báo với họ rằng bạn nghi ngờ họ đang làm sai, trở nên rất khó khăn. Một ví dụ khá phổ biến cho hiểm họa này là việc nhân viên hay cựu nhân viên lấy cắp mã nguồn của công ty cũ và làm thành sản phẩm mới.

Một giải pháp tốt nhất để tránh gian lận và trộm cắp bởi các nhân viên nội bộ là phải có chính sách rõ ràng, đầy đủ. Chính sách có thể giúp cho việc quản lý an toàn thông tin trở nên dễ dàng hơn trong việc thu thập dữ liệu về các hành động bị nghi ngờ là sai để chứng minh những hành vi xấu mà nhân viên đã thực hiện. Ví dụ như: Nhân viên trong hệ thống của bạn lấy trộm thông tin tài khoản của khách hàng hay không? Người dùng sau khi nghỉ việc có truy cập vào tài khoản của họ hay không?

Chúng ta đã xem xét những thiệt hại mà nhân viên nội bộ có thể thực hiện đối với hệ thống thông tin, phần tiếp theo chúng ta sẽ tìm hiểu về sự phá hủy do các cộng đồng khác có thể gây ra đối với dữ liệu của chúng ta - những người bên ngoài hệ thống.

2.3.3. Xâm nhập bất hợp pháp

Có một số nhóm người dùng Internet sẽ tấn công hệ thống thông tin. Ba nhóm chính là hacker, cracker và phreak. Trong khi thuật ngữ phổ biến để gọi tất cả ba nhóm này là "hacker" nhưng có một số sự khác biệt giữa các nhóm.

Một hacker là một người dùng thâm nhập vào một hệ thống chỉ để xem xét xung quanh và xem những gì có thể. Quy tắc của các hacker là sau khi họ đã thâm nhập vào hệ thống, họ sẽ thông báo cho quản trị hệ thống để cho người quản trị biết rằng hệ thống có một lỗ hổng. Người ta thường nói rằng một hacker chỉ muốn an toàn được cải thiện trên tất cả các hệ thống Internet. Nhóm tiếp theo, cracker, là nhóm thực sự nguy hiểm. Một cracker không có quy tắc nào để xâm nhập vào một hệ thống. Cracker sẽ gây thiệt hại hoặc phá hủy dữ liệu nếu họ có thể xâm nhập vào một hệ thống. Mục tiêu của cracker là gây ra càng nhiều thiệt hại cho tất cả các hệ thống trên Internet càng tốt. Nhóm cuối cùng - Phreak, cố gắng đột nhập vào hệ thống điện thoại của một tổ chức. Các Phreak sau đó có thể sử dụng truy cập điện thoại miễn phí để che giấu số điện thoại thực sự mà họ đang dùng để gọi, và cũng có thể làm cho tổ chức phải thanh toán hóa đơn với một số tiền lớn cho chi phí điện thoại đường dài.

Các cách một hacker tấn công một hệ thống có thể khác nhau rất nhiều. Mỗi kẻ tấn công có các thủ thuật riêng của mình có thể được sử dụng để xâm nhập vào một hệ thống. Chúng ta sẽ tìm hiểu phương pháp cơ bản của hacker ở dưới đây.

Phương pháp cơ bản của hacker có năm thành phần chính: trinh sát/thăm dò, quét, đoạt quyền truy cập, duy trì quyền truy cập, và xóa dấu vết. Điều này có vẻ kỳ lạ để các hacker suy nghĩ về một phương pháp luận, nhưng như với bất cứ cái gì khác, đó chỉ là vấn đề thời gian. Vì vậy, để tối đa hóa thời gian, hầu hết các hacker đi theo một phương pháp tương tự.

Giai đoạn đầu tiên trong phương pháp này là giai đoạn thăm dò. Trong giai đoạn này, kẻ tấn công cố gắng để thu được càng nhiều thông tin về các mạng mục tiêu càng tốt. Có hai cách chính một kẻ tấn công có thể thực hiện: chủ động và thụ động. Hầu hết các kẻ tấn công thường sẽ bắt đầu với các tấn công thụ động. Những tấn công thụ động thường có thể tạo ra rất nhiều thông tin tốt về mạng hoặc tổ chức mà các hacker muốn tấn công. Các hacker thường sẽ bắt đầu bằng cách đọc qua trang web của tổ chức đang nhằm tới để xem xét xem liệu có thể thu được thông tin gì. Những kẻ tấn công sẽ tìm kiếm thông tin liên lạc về nhân viên chủ chốt (điều này có thể được sử dụng cho tấn công lừa đảo hay tấn công dựa trên các kỹ nghệ xã hội), thông tin về các loại

công nghệ sử dụng tại các tổ chức, và bất kỳ thông tin quan trọng khác có thể được sử dụng cho một cuộc tấn công. Sau khi những kẻ tấn công đã xem qua các trang web, họ có thể sẽ chuyển sang các công cụ tìm kiếm trên Internet để tìm thêm thông tin về mạng mà họ muốn tấn công. Họ sẽ tìm kiếm những bài viết về nhóm tin xấu được đăng tại địa điểm dành cho những người đang có hiềm khích với công ty, và các chi tiết khác mà có thể giúp họ trong cuộc tấn công. Những kẻ tấn công sau đó sẽ tìm kiếm thông tin ở các máy chủ DNS của các tổ chức tấn công. Điều này sẽ cung cấp một danh sách các máy chủ và địa chỉ IP tương ứng. Một khi điều này được thực hiện, các hacker sẽ đi tiếp đến tấn công chủ động.

Để thực hiện một cuộc tấn công do thám chủ động, một hacker sẽ thực hiện quét ping, quét mạng SNMP, thu gom các banner, và các tấn công tương tự khác. Các cuộc tấn công sẽ giúp kẻ tấn công loại bỏ số lượng địa chỉ IP chết và tìm thấy những host còn sống để chuyển sang giai đoạn tiếp theo - quét.

Một kẻ tấn công sẽ bắt đầu quét, tìm kiếm các lỗ hổng để thỏa hiệp nhằm đạt được quyền truy cập vào mạng. Kẻ tấn công sẽ quét tất cả các máy chủ mà có sẵn trên Internet, tìm kiếm các lỗ hổng được biết đến. Những lỗ hổng bảo mật có thể là trong một ứng dụng Web được viết kém hoặc từ các ứng dụng đã được biết là có các lỗ hổng bảo mật trong đó. Sau đây là một số kiểu quét thông dụng:

a) Quét Ping

Phương pháp này đơn giản là chỉ ping các địa chỉ IP để kiểm tra xem các host tương ứng với các địa chỉ đó còn sống hay không. Các kiểu quét phức tạp hơn sử dụng các giao thức khác như quét SNMP cũng có cơ chế hoạt động tương tự.

b) Quét cổng TCP

Kiểu này dò quét các cổng TCP mở để tìm các dịch vụ đang chạy để có thể khai thác, lợi dụng hay phá hoại. Máy quét có thể sử dụng các kết nối TCP thông dụng hoặc là các kiểu quét trộm(sử dụng kết nối mở một bên) hoặc là kiểu quét FIN (không mở cổng mà chỉ kiểm tra xem có ai đó đang lắng nghe). Có thể quét danh sách các cổng liên tục, ngẫu nhiên hoặc là đã được cấu hình.

c) Quét cổng UDP

Loại quét này khó hơn một chút vì UDP là giao thức không kết nối. Kỹ thuật là gửi một gói tin UDP vô nghĩa tới một cổng nào đó. Hầu hết các máy đích sẽ trả lời bằng một gói tin ICMP "destination port unreachable", chỉ ra rằng không có dịch vụ nào lắng nghe ở cổng đó. Tuy nhiên, nhiều máy điều tiết các thông báo ICMP nên ta không thể làm điều này một cách nhanh chóng được.

d) Xác định hệ điều hành

Bằng việc gửi các gói tin TCP hay ICMP không đúng qui cách, kẻ tấn công có thể thu được thông tin về hệ điều hành.

e) Quét tài khoản

Cố gắng đăng nhập vào hệ thống với các Tài khoản (Account):

- Các Tài khoản không có mật khẩu
- Các Tài khoản với mật khẩu trùng với tên đăng nhập hoặc là 'password'
- Các Tài khoản mặc định đã được dùng để chuyển sản phẩm
- Các Tài khoản được cài cùng với các sản phẩm phần mềm
- Các vấn đề về tài khoản nặc danh FTP

Kẻ tấn công cũng sẽ xem xét tường lửa và bộ định tuyến của tổ chức để xem liệu có lỗ hổng tồn tại ở đó không. Khi kẻ tấn công đã biên soạn một danh sách các lỗ hổng bảo mật, sau đó sẽ chuyển sang giai đoạn tiếp theo – đoạt quyền truy cập.

Có nhiều cách cho một kẻ tấn công đạt được quyền truy cập vào các mạng mục tiêu. Một số điểm vào mạng phổ biến hơn là thông qua hệ điều hành máy chủ định tấn công (hệ điều hành), thông qua một ứng dụng đã được tự phát triển, cũng như thông qua một ứng dụng với lỗ hổng đã biết, thông qua các thiết bị mạng có thể được nhìn thấy từ Internet, và nếu vẫn thất bại những kẻ tấn công sẽ thực hiện một cuộc tấn công từ chối dịch vụ. Một khi kẻ tấn công có thể truy cập tất cả những gì mà hắn muốn làm là đảm bảo rằng hắn ta có thể giữ được truy cập này.

Để duy trì truy cập, một kẻ tấn công thường sẽ tải lên một ứng dụng tùy chỉnh trên máy chủ bị xâm nhập. Ứng dụng này sau đó sẽ là một cửa hậu để

vào tổ chức cần tấn công, và có thể cho phép kẻ tấn công vào và ra theo ý muốn. Ngoài việc tải lên các chương trình mới, một kẻ tấn công có thể thay đổi chương trình hiện có trên hệ thống. Ưu điểm của việc làm này là một quản trị viên thông thạo có thể biết các tập tin trên hệ thống của mình và anh ấy có thể nhận ra rằng các tập tin mới đã được cài đặt trên các máy chủ của mình. Bằng cách thay đổi các tập tin đã tồn tại, hệ thống sẽ như chưa hề bị sửa đổi khi thoạt nhìn qua. Một cách thông thường để thực hiện điều này là với việc sử dụng một nhóm các tập tin được gọi là rootkit. Rootkit cho phép kẻ tấn công thay thế các file hệ thống bình thường với các tập tin cùng tên mà cũng có chức năng Trojan horse (sẽ được đề cập chi tiết trong phần mã độc hại). Các tập tin hệ thống mới sẽ cho phép kẻ tấn công thực hiện theo cách đúng như như khi hắn ta thêm các tập tin bổ sung cho các máy chủ cần tấn công. Một kẻ tấn công có thể không cần phải truy cập vào hệ thống mục tiêu trong thời gian dài mà có thể chỉ muốn tải về các chương trình hiện có hoặc dữ liệu từ máy chủ mục tiêu. Khi kẻ tấn công đã xác định cơ chế cho việc truy cập trở lại máy chủ mục tiêu, bước cuối cùng trong phương pháp của hacker là che đậy những dấu vết của mình.

Để xóa những dấu vết của mình, một kẻ tấn công sẽ xem xét các tập tin ghi nhật ký kiểm toán của hệ thống và loại bỏ bất kỳ dấu vết của mình trên hệ thống. Điều này sẽ làm ẩn truy cập của kẻ tấn công trước những người quản trị hệ thống và cũng sẽ để lại ít bằng chứng trong trường hợp quản trị hệ thống muốn có một cuộc kiểm tra pháp y thực hiện trên các máy chủ bị xâm nhập. Cấp độ kỹ năng của kẻ tấn công thường được thể hiện rõ ràng trong giai đoạn này. Một kẻ tấn công bình thường có thể xóa toàn bộ một tập tin ghi nhật ký, do đó khiến cho quản trị hệ thống dễ dàng xác định rằng một người nào đó đã ở trong hệ thống, nhưng một kẻ tấn công có tay nghề cao hơn có thể chỉ sửa đổi các nội dung ghi nhật ký hành động của mình để cho thấy luồng thông tin có nguồn gốc từ một địa chỉ IP khác.

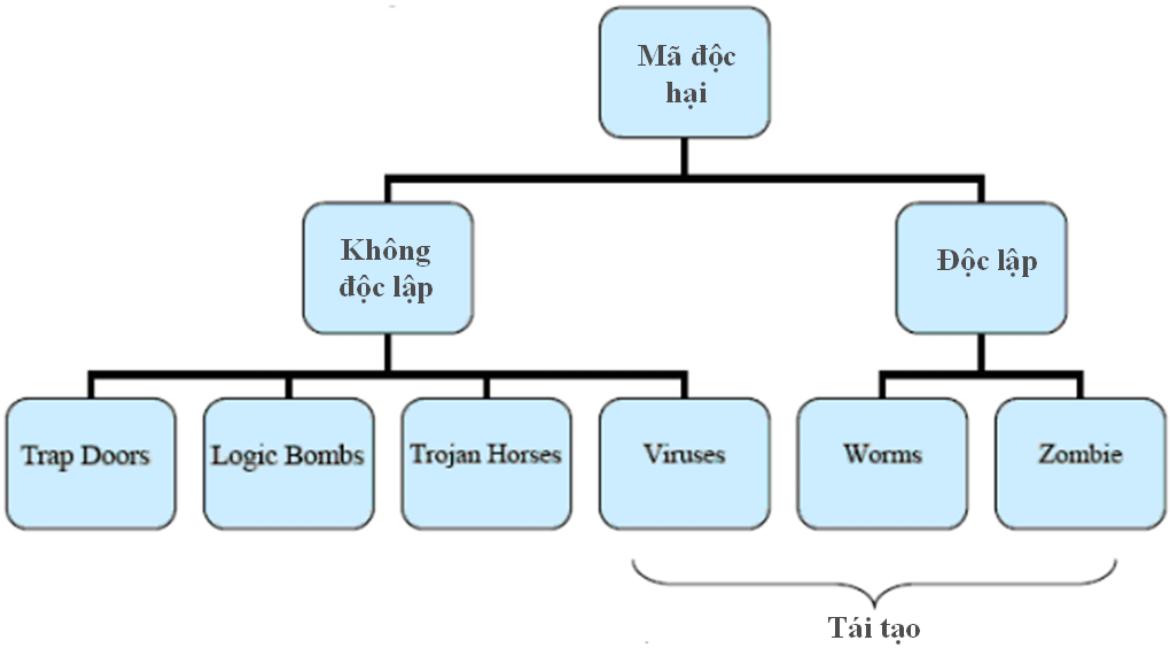
2.3.4. Mã độc hại

Trong khi những người dùng ác ý hay hacker có thể tấn công hệ thống, các chương trình được phát hành bởi cùng một nhóm người này thường sẽ thành công hơn trong việc tiếp cận các thành phần bảo vệ của tổ chức. Mã độc

hại được định nghĩa là bất kỳ đoạn mã trong một phần mềm hay kịch bản (script) được thiết kế với mục đích làm cho một hệ thống thực hiện bất kỳ hành động nào theo ý của người sử dụng (mã độc hại) với quyền của chủ sở hữu hệ thống. Một trong những cách nhanh nhất để đưa mã độc vào mạng được bảo vệ của một tổ chức mục tiêu là gửi các mã độc hại thông qua thư điện tử.

Có rất nhiều loại khác nhau của mã độc và có nhiều tiêu chí để phân loại mã độc hại, dưới đây là hai cách phân loại dựa vào hình thức lây nhiễm và theo phân loại của NIST-National Institute of Standart and Technology (Viện tiêu chuẩn – công nghệ quốc gia Hoa kỳ). Sự phân loại này chỉ mang tính chất tương đối.

2.3.4.1. Theo hình thức lây nhiễm



Hình 2.1 Phân loại mã độc hại

Theo hình trên mã độc hại gồm 2 loại chính: một loại cần vật chủ để tồn tại và lây nhiễm, vật chủ ở đây có thể là các file dữ liệu, các file ứng dụng, hay các file chương trình thực thi… và một loại là tồn tại độc lập.

Độc lập nghĩa đó là chương trình độc hại có thể được lập lịch và chạy trên hệ điều hành.

Không độc lập (needs host program) là một đoạn chương trình đặc biệt thuộc một chương trình nào đó không thể thực thi độc lập như một chương

trình thông thường hay tiện ích nào đó mà bắt buộc phải có bước kích hoạt chương trình chủ trước đó thì chương trình đó mới chạy.

a) Trap Door

Trap Door còn được gọi là Back Door. Trong đời sống thường, Trap Door mang ý nghĩa "cánh cửa" để vào một tòa nhà. Trap door là một điểm bí mật trong một chương trình, cho phép một ai đó có thể truy cập lại hệ thống mà không phải vượt qua các hàng rào an ninh như thông thường. Trap door được sử dụng bởi những nhà lập trình với mục đích dò lỗi, kiểm tra chương trình.

Trong các cuộc tấn công trap door là phần mềm độc hại thường trú và đợi lệnh điều khiển từ các cổng dịch vụ TCP hoặc UDP. Trap door khi chạy trên máy bị nhiễm, nó sẽ thường trú trong bộ nhớ và mở một cổng cho phép kẻ tấn công truy nhập vào máy nạn nhân thông qua cổng mà nó đã mở và kẻ tấn công có toàn quyền điều khiển máy bị nhiễm.

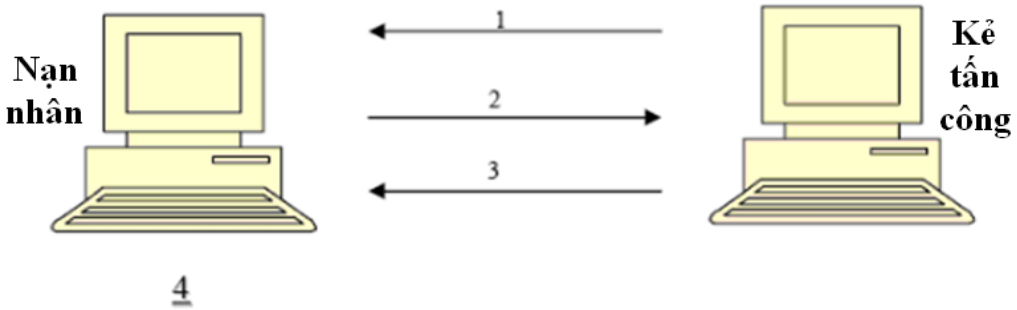
Trap door nguy hiểm ở chỗ nó hoàn toàn chạy ẩn trong máy. Nhiều Trap door được hẹn trước giờ để kết nối ra ngoài (đến một giờ nhất định mới mở một cổng để hacker đột nhập vào) nên rất khó phát hiện ngay cả quét cổng.

Ví dụ: Back door W32/TDSS là một chương trình chiếm quyền điều khiển từ xa, bí mật điều khiển hệ thống máy tính bị nhiễm.

b) Logic Bombs

Logic bomb là đoạn mã độc được nhúng vào một chương trình hợp pháp mà chúng có thể thực thi khi có một sự kiện nào đó xảy ra. Các đoạn mã thường được chèn vào các ứng dụng hoặc các hệ điều hành để thực hiện việc phá hủy hệ thống hoặc phá hủy các chức năng an toàn của hệ thống.

Logic bomb có thể gửi thông báo tới kẻ tấn công khi người dùng truy nhập Internet và sử dụng một chương trình đặc biệt nào đó như bộ xử lý văn bản. Từ đó kẻ tấn công có thể chuẩn bị cho các cuộc tấn công (chẳng hạn kết hợp với các máy tính khác bị nhiễm để bắt đầu một cuộc tấn công từ chối dịch vụ).



Hình 2.2 Mô hình hoạt động Logic bomb

1. Kẻ tấn công đưa bom logic vào máy nạn nhân thông qua một chương trình ứng dụng nào đó.

2. Máy nạn nhân cài đặt chương trình ứng dụng.

3. Kẻ tấn công gửi thông điệp tấn công.

4. Bom logic đã cài đặt trên máy nạn nhân.

c) Trojan Horses

Trojan Horse là loại mã độc hại được đặt theo sự tích "Ngựa thành Troy". Trojan horse không có khả năng tự nhân bản tuy nhiên nó lây vào hệ thống với biểu hiện rất bình thường nhưng thực chất bên trong có ẩn chứa các đoạn mã với mục đích gây hại. Trojan có thể gây hại theo ba cách sau:

Tiếp tục thực thi các chức năng của chương trình mà nó bám vào, bên cạnh đó thực thi các hoạt động gây hại một cách riêng biệt (ví dụ như gửi một trò chơi dụ cho người dùng sử dụng, bên cạnh đó là một chương trình đánh cắp mật khẩu).

Tiếp tục thực thi các chức năng của chương trình mà nó bám vào, nhưng sửa đổi một số chức năng để gây tổn hại (ví dụ như một trojan giả lập một cửa sổ đăng nhập để lấy mật khẩu) hoặc che giấu các hành động phá hoại khác (ví dụ như trojan che giấu cho các tiến trình độc hại khác bằng cách tắt các hiển thị của hệ thống).

Thực thi luôn một chương trình gây hại bằng cách núp dưới danh một chương trình không có hại (ví dụ như một trojan được giới thiệu như là một chò chơi hoặc một công cụ trên mạng, người dùng chỉ cần kích hoạt file này là lập tức dữ liệu trên máy tính sẽ bị xoá hết).

Có 7 loại trojan chính:

Trojan truy cập từ xa: Được thiết kế để cho kẻ tấn công có khả năng từ xa chiếm quyền điều khiển của máy bị hại. Các trojan này thường được giấu vào các trò chơi và các chương trình nhỏ làm cho người dùng mất cảnh giác.

Trojan gửi dữ liệu: Nó thực hiện việc lấy và gửi dữ liệu nhạy cảm như mật khẩu, thông tin thẻ tín dụng, các tệp nhật ký, địa chỉ email… cho kẻ tấn công. Trojan này có thể tìm kiếm cụ thể thông tin hoặc cài phần mềm đọc trộm bàn phím và gửi toàn bộ các phím bấm về cho kẻ tấn công.

Trojan hủy hoại: Thực hiện việc xóa các tệp tin. Loại trojan này giống với virus và thường có thể bị phát hiện bởi các chương trình diệt virus.

Trojan kiểu proxy: Sử dụng máy tính bị hại làm proxy, qua đó có thể sử dụng máy bị hại để thực hiện các hành vi lừa gạt hay đánh phá các máy tính khác.

Trojan FTP: Được thiết kế để mở cổng 21 và cho phép tin tặc kết nối vào máy bị hại sử dụng FTP.

Trojan tắt phần mềm an ninh: Thực hiện việc dừng hoặc xóa bỏ chương trình an ninh như phần mềm chống virus hay tường lửa mà người dùng không nhận ra.

Trojan DoS: Được sử dụng trong các cuộc tấn công từ chối dịch vụ. Ví dụ các con bot sử dụng trong DDoS cũng có thể coi là một loại trojan.

Ví dụ trojan có tên Zeus, Clampi đã mang về cho tội phạm hàng triệu USD bằng cách ghi lại thông tin tài khoản để làm thẻ giả hoặc chuyển tiền vào tài khoản của một bên trung gian - gọi là Mule. Mule sau đó được trả công để đảm nhận việc gửi tiền ra nước ngoài. Mule được thuê thông qua các trang tìm kiếm việc làm và họ không hề biết rằng số tiền họ nhận gửi đi là bất hợp pháp.

d) Virus

Virus là một loại mã độc hại có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính. Virus phải luôn bám vào vật chủ (có thể là file dữ liệu hoặc file ứng dụng) để lây lan. Virus có thể làm bất cứ việc gì mà các chương trình khác có thể làm. Virus chỉ khác ở điểm nó tự đính kèm vào một chương trình và thực thi bí mật khi chương trình mang virus được thực thi. Khi virus được thực thi nó có thể làm bất kỳ việc gì trên hệ thống như xóa file, chương trình. Vòng đời virus gồm 4 giai đoạn:

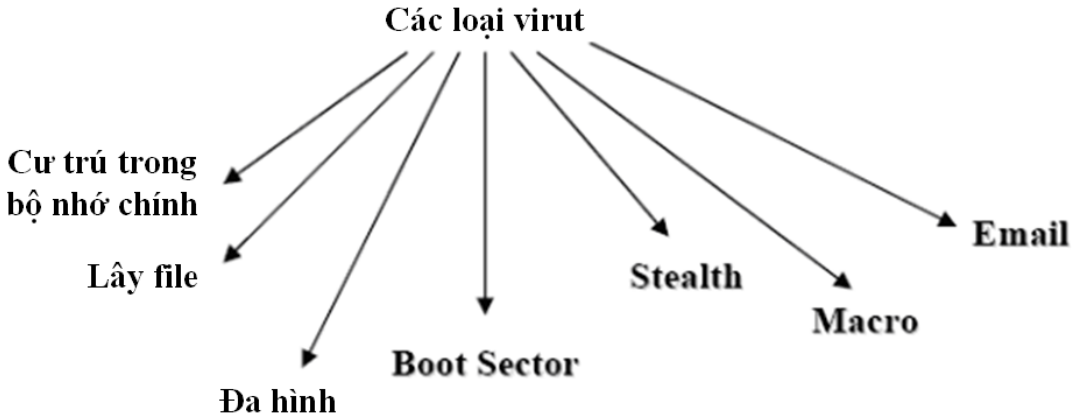
Dormant (nằm im): Trong giai đoạn này virus không làm gì cho đến khi được kích hoạt bởi một ai đó hay một sự kiện nào đó.

Propagation (lây lan): Trong giai đoạn này virus thực hiện việc sao chép chính nó tới các chương trình, vị trí khác trong ổ đĩa.

Triggering (kích hoạt): Trong giai đoạn này virus được kích hoạt để thực thi chức năng của nó.

Execution (thực thi): Chức năng của virus được thực thi. Chức năng có thể là vô hại như gửi một thông điệp nào đó tới màn hình, hoặc một chức năng có hại như phá hủy các chương trình, các file hệ thống.

Virus gồm 7 loại chính:



Hình 2.3 Phân loại virus

Memory – resident virus (virus cư trú trong bộ nhớ chính): Cư trú rong bộ nhớ chính như là một phần của chương trình hệ thống. Theo đó virus sẽ gây ảnh hưởng mỗi khi chương trình được thực thi.

Program file virus (virus lây file): Gây ảnh hưởng đến các file chương trình như exe/com/sys.

Polymorphic virus (virus đa hình): Loại virus này tự thay đổi hình thức của nó, gây khó khăn cho các chương trình diệt virus. Virus "Tequilla" là loại virus đa hình đầu tiên xuất hiện năm 1991.

Boot Sector virus: Là loại virus đầu tiên trên thế giới được phổ biến rộng rãi và được viết vào năm 1986. Boot virus lợi dụng tiến trình boot của máy tính để thực hiện việc kích hoạt mình. Khi máy tính được khởi động, nó luôn tìm đến master boot record được lưu trữ tại địa chỉ head 0, track 0, sector 1 để đọc thông tin. Boot Sector virus lây lan sang đĩa cứng khi khởi động hệ thống từ đĩa mềm bị nhiễm.

Stealth virus: Đây là loại virus có khả năng tự che giấu không để cho hệ điều hành và phần mềm chống virus biết. Nó nằm trong bộ nhớ để ngăn chặn sử dụng hệ điều hành và che giấu những thay đổi về kích thước các tập tin. Những virus này chỉ bị phát hiện khi chúng còn ở trong bộ nhớ. Có nhiều boot sector virus có khả năng Stealth. Ví dụ virus "The Brain" được tạo ra tại Pakistan bởi Basit và Amjad. Chương trình này nằm trong phần khởi động (boot sector) của một đĩa mềm 360Kb và nó sẽ lây nhiễm tất cả các ổ đĩa mềm. Đây là loại "stealth virus" đầu tiên.

Macro virus: Là tập lệnh được thực thi bởi một ứng dụng nào đó. Macro virus phổ biến trong các ứng dụng Microsoft Office khi tận dụng khả năng kiểm soát việc tạo và mở file để thực thi và lây nhiễm. Ví dụ: virus Baza, Laroux và một số virus Staog xuất hiện năm 1996 tấn công các file trong hệ điều hành Windows 95, chương trình bảng tính Excel và cả Linux. Virus Melisa cũng là một trong những Macro virus nổi tiếng.

Thư điện tử virus: Là những virus được phát tán qua thư điện tử. Ví dụ virus Melissa được đính kèm trong thư điện tử. Nếu người dùng mở file đính kèm Macro được kích hoạt sau đó thư điện tử virus này tự động gửi chính nó tới tất cả những hòm thư có trong danh sách thư của người đó.

e) Worm

Worm (sâu mạng) là chương trình độc hại có khả năng tự nhân bản và tự lây nhiễm trong hệ thống, nó có khả năng "tự đóng gói", điều đó có nghĩa là nó không cần file chủ để mang nó khi nhiễm vào hệ thống. Như vậy Worm không bám vào một file hoặc một vùng nào đó trên đĩa cứng, vì vậy không thể dùng các chương trình quét file để diệt Worm.

Mục tiêu của Worm là làm lãng phí băng thông của mạng, phá hoại hệ thống như xóa file, tạo back door, thả keylogger…

Tấn công của Worm có đặc trưng là lan rộng cực kỳ nhanh chóng do không cần tác dụng của con người (như khởi động máy, sao chép tập tin hay đóng/mở file).

Worm có thể chia làm 2 loại:

Network Service Worm lan truyền bằng cách lợi dụng các lỗ hổng bảo mật của mạng, của hệ điều hành hoặc của ứng dụng. Ví dụ Sasser (W32.Sasser.Worm) bắt đầu lây lan trên mạng vào 1/5/2004 có thể tự động

lây lan bất cứ máy tính nào kết nối Internet. Nó lợi dụng lỗ hổng bảo mật Local Security Authority Subsystem Service (LSASS - lỗi này đã được Microsoft công bố và phát hành bản sửa lỗi ngày 13-4-2004) để tấn công các máy cài Windows 2000/ XP/ Máy chủ 2003.

Mass Mailing Worm là một dạng tấn công qua dịch vụ mail, tuy nhiên nó tự đóng gói để tấn công và lây nhiễm chứ không bám vào vật chủ là email. Khi sâu này lây nhiễm vào hệ thống, nó thường cố gắng tìm kiếm sổ địa chỉ và tự gửi bản thân nó đến các địa chỉ thu nhặt được. Việc gửi đồng thời cho toàn bộ các địa chỉ thường gây quá tải cho mạng hoặc cho máy chủ mail. Ví dụ Mydoom là một trong những loại Worm khiến nhiều hệ thống máy tính bị tê liệt và gây thiệt hại tài chính lên đến hàng tỷ đôla.

f) Zombie

Zombie là chương trình độc hại bí mật liên kết với một máy tính khác ngoài internet để nghe lệnh từ các máy tính đó. Các Zombie thường sử dụng trong các cuộc tấn công từ chối dịch vụ DDoS để tấn công vào một website nào đó.

Kiểu thông dụng nhất của Zoombie là các agent dùng để tổ chức một cuộc tấn công DDoS. Kẻ tấn công có thể cài Zoombie vào một số lượng lớn các máy tính rồi ra lệnh tấn công cùng một lúc.

Ví dụ Trinoo và Tribe Flood Network là hai Zoombie nổi tiếng được sử dụng như các công cụ để thực hiện tấn công DDoS.

2.3.4.2. Phân loại của NIST

a) Virus

Với cách định nghĩa, phân loại này, virus là một loại mã độc hại (Maliciuos code) có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính. Như vậy virus máy tính phải luôn luôn bám vào một vật chủ (đó là file dữ liệu hoặc file ứng dụng) để lây lan. Các chương trình diệt virus dựa vào đặc tính này để thực thi việc phòng chống và diệt virus, để quét các file trên thiết bị lưu, quét các file trước khi lưu xuống ổ cứng… Điều này cũng giải thích vì sao đôi khi các phần mềm diệt virus tại PC đưa ra thông báo “phát hiện ra virus nhưng không diệt được” khi thấy có

dấu hiệu hoạt động của virus trên PC, bởi vì "vật mang virus" lại nằm ở máy khác nên không thể thực thi việc xoá đoạn mã độc hại đó.

Compiled Virus là virus mà mã thực thi của nó đã được dịch hoàn chỉnh bởi một trình biên dịch để nó có thể thực thi trực tiếp từ hệ điều hành. Các loại boot virus như (Michelangelo và Stoned), file virus (như Jerusalem) rất phổ biến trong những năm 80 là virus thuộc nhóm này, compiled virus cũng có thể là pha trộn bởi cả boot virus va file virus trong cùng một phiên bản.

Interpreted Virus là một tổ hợp của mã nguồn mà chỉ thực thi được dưới sự hỗ trợ của một ứng dụng cụ thể hoặc một dịch vụ cụ thể trong hệ thống. Một cách đơn giản, virus kiểu này chỉ là một tập lệnh, cho đến khi ứng dụng gọi thì nó mới được thực thi. Macro virus, scripting virus là các virus nằm trong dạng này. Macro virus rất phổ biến trong các ứng dụng Microsoft Office khi tận dụng khả năng kiểm soát việc tạo và mở file để thực thi và lây nhiễm. Sự khác nhau giữa macro virus và scripting virus là: Macro virus là tập lệnh thực thi bởi một ứng dụng cụ thể, còn scripting virus là tập lệnh chạy bằng một service của hệ điều hành. Melisa là một ví dụ điển hình về Macro virus, Love Stages là ví dụ cho scripting virus.

b) Worm

Giống với Worm trong tiêu chí phân loại phía trên.

c) Trojan Horse

Giống với Trojan Horse trong tiêu chí phân loại phía trên.

d) Malicious Mobile Code

Là một dạng mã phần mềm có thể được gửi từ xa vào để chạy trên một hệ thống mà không cần đến lời gọi thực hiện của người dùng hệ thống đó. Malicious Mobile Code được coi là khác với virus, worm ở đặc tính là nó không nhiễm vào file và không tìm cách tự phát tán. Thay vì khai thác một điểm yếu bảo mật xác định nào đó, kiểu tấn công này thường tác động đến hệ thống bằng cách tận dụng các quyền ưu tiên ngầm định để chạy mã từ xa. Các công cụ lập trình như Java, ActiveX, JavaScript, VBScript là môi trường tốt cho Malicious mobile code. Một trong những ví dụ nổi tiếng của kiểu tấn công này là Nimda, sử dụng JavaScript.

Kiểu tấn công này của Nimda thường được biết đến như một tấn công hỗn hợp (Blended Atatck). Cuộc tấn công có thể đi tới bằng một thư điện tử khi người dùng mở một thư điện tử đọc bằng trình duyệt web. Sau khi nhiễm vào máy này, Nimda sẽ cố gắng sử dụng sổ địa chỉ thư điện tử của máy đó để phát tán tới các máy khác. Mặt khác, từ máy đã bị nhiễm, Nimda cố gắng quét các máy khác trong mạng có thư mục chia sẻ mà không bảo mật, Nimda sẽ dùng dịch vụ NetBIOS như phương tiện để chuyển file nhiễm virus tới các máy đó. Đồng thời Nimda cố gắng dò quét để phát hiện ra các máy tính có cài dịch vụ IIS có điểm yếu bảo mật của Microsoft. Khi tìm thấy, nó sẽ sao chép bản thân nó vào máy chủ. Nếu một máy trạm web có điểm yếu bảo mật tương ứng kết nối vào trang web này, client đó cũng bị nhiễm (lưu ý rằng bị nhiễm mà không cần "mở thư điện tử bị nhiễm virus"). Quá trình nhiễm virus sẽ lan tràn theo cấp số nhân.

e) Tracking Cookie

Là một dạng lạm dụng cookie để theo dõi một số hành động duyệt web của người sử dụng một cách bất hợp pháp. Cookie là một file dữ liệu chứa thông tin về việc sử dụng một trang web cụ thể nào đó của web-client. Mục tiêu của việc duy trì các cookie trong hệ thống máy tính nhằm căn cứ vào đó để tạo ra giao diện, hành vi của trang web sao cho thích hợp và tương ứng với từng web-client. Tuy nhiên tính năng này lại bị lạm dụng để tạo thành các phần mềm gián điệp (spyware) nhằm thu thập thông tin riêng tư về hành vi duyệt web của cá nhân.

f) Phần mềm gián điệp

Spyware (phần mềm gián điệp) Là loại phần mềm chuyên thu thập các thông tin từ các máy chủ (thông thường vì mục đích thương mại) qua mạng Internet mà không có sự nhận biết và cho phép của chủ máy. Một cách điển hình, spyware được cài đặt một cách bí mật như là một bộ phận kèm theo của các phần mềm miễn phí (freeware) và phần mềm chia sẻ (shareware) mà người ta có thể tải về từ Internet. Một khi đã cài đặt, spyware điều phối các hoạt động của máy chủ trên Internet và lặng lẽ chuyển các dữ liệu thông tin đến một máy khác (thường là của những hãng chuyên bán quảng cáo hoặc của các tin tặc). Phần mềm gián điệp cũng thu thập tin tức về địa chỉ thư điện

tử và ngay cả mật khẩu cũng như là số thẻ tín dụng. Khác với worm và virus, Spyware không có khả năng tự nhân bản.

g) Phần mềm quảng cáo

Phần mềm quảng cáo (Adware) rất hay có ở trong các chương trình cài đặt tải từ trên mạng. Một số phần mềm vô hại, nhưng một số có khả năng hiển thị thông tin lên màn hình, cưỡng chế người sử dụng.

h) Attacker Tool

Là những bộ công cụ tấn công có thể sử dụng để đẩy các phần mềm độc hại vào trong hệ thống. Các bộ công cụ này có khả năng giúp cho kẻ tấn công có thể truy nhập bất hợp pháp vào hệ thống hoặc làm cho hệ thống bị lây nhiễm mã độc hại. Khi được tải vào trong hệ thống bằng các đoạn mã độc hai, Attacker tool có thể chính là một phần của đoạn mã độc đó (ví dụ như trong một trojan) hoặc nó sẽ được tải vào hệ thống sau khi nhiễm. Ví dụ như một hệ thống đã bị nhiễm một loại worm, worm này có thể điều khiển hệ thống tự động kết nối đến một trang web nào đó, tải attacker tool từ trang đó và cài đặt Attacker tool vào hệ thống. Có rất nhiều loại Attacker tool, trong đó thường gặp nhất là backdoor và keylogger

- Backdoor là một thuật ngữ chung chỉ các phần mềm độc hại thường trú và đợi lệnh điều khiển từ các cổng dịch vụ TCP hoặc UDP. Một cách đơn giản nhất, phần lớn các backdoor cho phép một kẻ tấn công thực thi một số hành động trên máy bị nhiễm như truyền file, dò mật khẩu, thực hiện mã lệnh… Backdoor cũng có thể được xem xét dưới 2 dạng: Zoombie và Remote Administration Tool

+ Zoombie (có thể đôi lúc gọi là bot) là một chương trình được cài đặt lên hệ thống nhằm mục đích tấn công hệ thống khác. Kiểu thông dụng nhất của Zoombie là các Agent dùng để tổ chức một cuộc tấn công DDoS. Kẻ tấn công có thể cài Zoombie vào một số lượng lớn các máy tính rồi ra lệnh tấn công cùng một lúc. Trinoo và Tribe Flood Network là hai Zoombie nổi tiếng.

+ Remote Administration Tool (RAT) là các công cụ có sẵn của hệ thống cho phép thực hiện quyền quản trị từ xa. Tuy nhiên hacker cũng có thể lợi dụng tính năng này để xâm hại hệ thống. Tấn công kiểu này có thể bao gồm hành động theo dõi mọi thứ xuất hiện trên màn hình cho đến tác động

vào cấu hình của hệ thống. Ví dụ về công cụ RAT là: Back Orifice, SubSeven…

- Keylogger là phần mềm được dùng để bí mật ghi lại các phím đã được nhấn bằng bàn phím rồi gửi tới hacker. Keylogger có thể ghi lại nội dung của thư điện tử, của văn bản, tên đăng nhập, mật khẩu, thông tin bí mật...Ví dụ một số loại keylogger như: KeySnatch, Spyster…

- Rootkits là tập hợp của các file được cài đặt lên hệ thống nhằm biến đổi các chức năng chuẩn của hệ thống thành các chức năng tiềm ẩn các tấn công nguy hiểm. Ví dụ như trong hệ thống Windows, Rootkit có thể sửa đổi, thay thế file, hoặc thường trú trong bộ nhớ nhằm thay thế, sửa đổi các lời gọi hàm của hệ điều hành. Rootkit thường được dùng để cài đặt các công cụ tấn công như cài backdoor, cài keylogger. Ví dụ về Rootkit là: LRK5, Knark, Adore, Hack Defender.

- Web Browser Plug-in là phương thức cài mã độc hại thực thi cùng với trình duyệt web. Khi được cài đặt, kiểu mã độc hại này sẽ theo dõi tất cả các hành vi duyệt web của người dùng (ví dụ như tên trang web đã truy nhập) sau đó gửi thông tin ra ngoài. Một dạng khác là phần mềm gián điệp có chức năng quay số điện thoại tự động, nó sẽ tự động kích hoạt modem và kết nối đến một số điện thoại ngầm định mặc dù không được phép của chủ nhân.

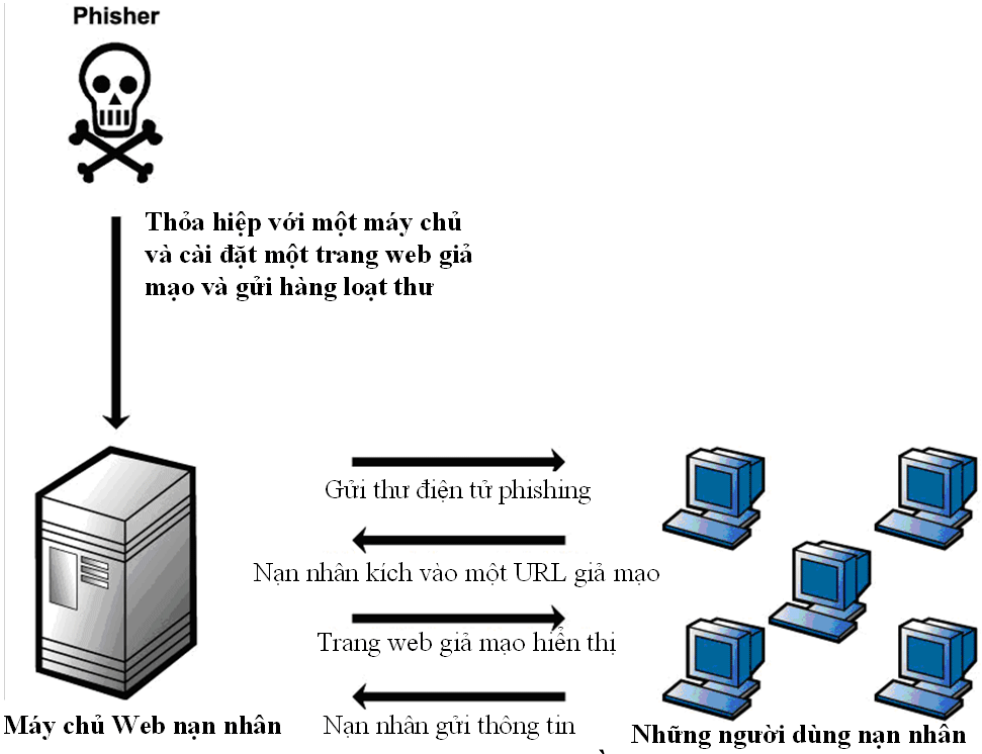
- Thư điện tử Generator là những chương trình cho phép tạo ra và gửi đi một số lượng lớn các thư điện tử. Mã độc hại có thể gieo rắc các Thư điện tử generator vào trong hệ thống. Các chương trình gián điệp, thư rác, mã độc hại có thể được đính kèm vào các thư điện tử được sinh là từ Thư điện tử generator và gửi tới các địa chỉ có trong sổ địa chỉ của máy bị nhiễm.

- Attacker Toolkit là các bộ công cụ có thể được tải xuống và cài vào hệ thống khi hệ thống đã bị khống chế bởi phần mềm độc hại. Các công cụ kiểu như các bộ dò quét cổng, bộ phá mật khẩu, bộ dò quét gói tin chính là các Attacker Toolkit thường hay được sử dụng.

i) Phishing

Phishing Là một hình thức tấn công thường có thể xem là kết hợp với mã độc hại. Phishing là phương thức dụ người dùng kết nối và sử dụng một hệ thống máy tính giả mạo nhằm làm cho người dùng tiết lộ các thông tin bí mật về danh tính (ví dụ như mật khẩu, số tài khoản, thông tin cá nhân…). Kẻ

tấn công phishing thường tạo ra trang web hoặc thư điện tử có hình thức giống hệt như các trang web hoặc thư điện tử mà nạn nhân thường hay sử dụng như trang của ngân hàng, của công ty phát hành thẻ tín dụng… Thư điện tử hoặc trang web giả mạo này sẽ đề nghị nạn nhân thay đổi hoặc cung cấp các thông tin bí mật về tài khoản, về mật khẩu… Các thông tin này sẽ được sử dụng để trộm tiền trực tiếp trong tài khoản hoặc được sử dụng vào các mục đích bất hợp pháp khác.



Hình 2.4 Mô tả về Phishing

j) Virus Hoax

Là các cảnh báo giả về virus. Các cảnh báo giả này thường núp dưới dạng một yêu cầu khẩn cấp để bảo vệ hệ thống. Mục tiêu của cảnh báo virus giả là cố gắng lôi kéo mọi người gửi cảnh báo càng nhiều càng tốt qua email. Bản thân cảnh báo giả là không gây nguy hiểm trực tiếp nhưng những thư gửi để cảnh báo có thể chứa mã độc hại hoặc trong cảnh báo giả có chứa các chỉ dẫn về thiết lập lại hệ điều hành, xoá file làm nguy hại tới hệ thống. Kiểu cảnh báo giả này cũng gây tốn thời gian và quấy rối bộ phận hỗ trợ kỹ thuật khi có quá nhiều người gọi đến và yêu cầu dịch vụ.

2.3.5. Tấn công từ chối dịch vụ

Đây là kiểu tấn công vào tính sẵn sàng của hệ thống, làm hệ thống cạn kiệt tài nguyên hoặc chiếm dụng băng thông của hệ thống, làm mất đi khả năng đáp ứng trả lời các yêu cầu đến. Trong trường hợp này, nếu hệ thống cần dùng đến tài nguyên thì rất có thể hệ thống sẽ gặp lỗi.

Tấn công từ chối dịch vụ là hành động mà các tin tặc lợi dụng đặc điểm hoặc lỗi an toàn thông tin của một hệ thống dịch vụ nhằm làm ngưng trệ hoặc ngăn cản người dùng truy nhập dịch vụ đó. Thường thì tấn công từ chối dịch vụ gây cho chương trình hoặc hệ thống bị đổ vỡ hoặc bị treo, tê liệt từng phần hoặc toàn bộ, buộc người quản trị dịch vụ đó phải tạm ngừng cung cấp dịch vụ và khởi động lại hệ thống.

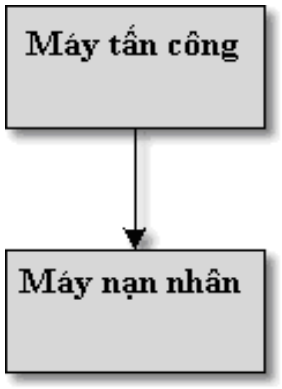
Đặc điểm đầu tiên của tấn công từ chối dịch vụ là cuộc tấn công này không lấy thông tin của hệ thống, nó thường chỉ gây cho hệ thống tê liệt, không hoạt động được và đôi khi gây hỏng hóc hoặc phá hoại thông tin có trên hệ thống. Việc ngừng hoạt động trong một thời gian nhất định của các hệ thống dịch vụ thường gây thiệt hại không thể ước tính chính xác được, đó là tổng của thiệt hại trực tiếp về tiền bạc, uy tín cho nhà cung cấp dịch vụ, và thiệt hại gián tiếp của khách hàng sử dụng dịch vụ. Đôi khi tấn công từ chối dịch vụ không làm tê liệt hệ thống, nhưng làm chậm và giảm khả năng phục vụ của hệ thống cũng dẫn tới những thiệt hại đáng kể. Đặc điểm thứ hai, trong cách tấn công này là người bị hại không thể chống đỡ lại được kiểu tấn công này vì công cụ được sử dụng trong cách tấn công này là các công cụ mà hệ thống dùng để vận hành hằng ngày.

Có thể phân biệt ra bốn dạng DoS sau :

- Tiêu thụ băng thông
- Làm nghèo tài nguyên
- Sai sót trong lập trình
- Tấn công Routing và DNS

Về mặt kỹ thuật có 3 kiểu tấn công từ chối dịch vụ chính là DoS (Denial of Service), DDoS (Distributed Denial of Service) và DRDoS (Distributed Reflection Denial of Service).

a) Tấn công từ chối dịch vụ truyền thống (DoS)



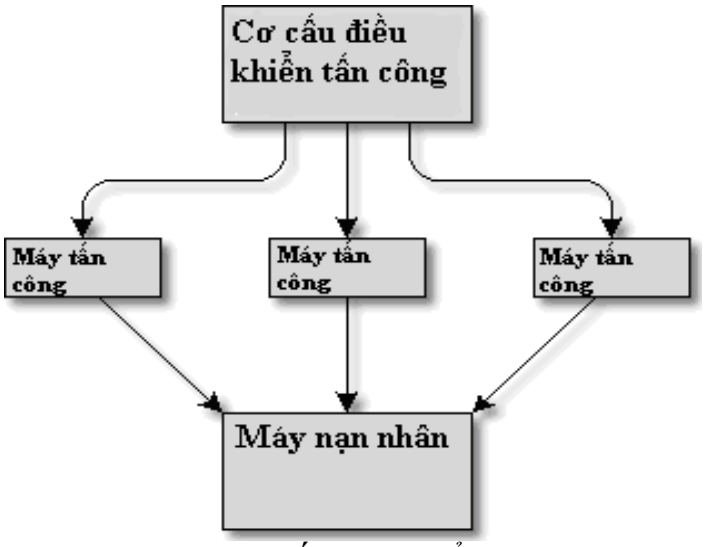
Hình 2.5 Tấn công kiểu DOS

Trong nhiều năm qua đã có một số lượng lớn các cuộc tấn công DoS "một-một" phổ biến. Trong các cuộc tấn công, hacker sẽ khởi động một tấn công từ hệ thống của mình chống lại các máy chủ hoặc mạng mục tiêu. SYN floods, Fin floods, Smurfs và Fraggles là các ví dụ về các tấn công "một-một". Trong khi tất cả các tấn công này ngày nay vẫn thành công đối với một số mạng mục tiêu, hầu hết các tổ chức cũng đã triển khai công nghệ để ngăn chặn những tấn công này tránh gây ra một sự gián đoạn dịch vụ trong tổ chức của họ. Đơn thuần máy tấn công có băng thông lớn hơn máy nạn nhân.

b) Tấn công từ chối dịch vụ phân tán - DDoS

Vào tháng Hai năm 2000, các tấn công DoS đạt đến cấp độ tiếp theo. Trong tháng này, một số mục tiêu cao cấp đã được thực hiện ngoại tuyến bởi thế hệ tiếp theo của tấn công DoS – tấn công từ chối dịch vụ phân tán (DDoS). Các tấn công DDoS không còn quen thuộc với tấn công "một-một" trong quá khứ. Những tấn công này sử dụng máy zombie để tạo ra một tấn công "nhiều-một". Sử dụng nhiều máy cùng tấn công vào một máy nạn nhân. Các máy zombie là thiết bị đã bị tổn hại và đã được tải lên đoạn mã vào trong, chính đoạn mã này sẽ cho phép một máy tổng liên hệ với chúng, và tất cả đều thực hiện các tấn công DoS cùng một lúc. Đã có hàng chục ngàn máy zombie có sẵn và những kẻ tấn công có thể sử dụng một số công cụ phổ biến (miễn phí) mà từ đó để khởi động các tấn công. Những công cụ này khá đơn giản để sử dụng và cho phép kẻ tấn công phát hành một cuộc tấn công nghiêm trọng chống lại mục tiêu.

Các tấn công DDoS mới là rất khó để bảo vệ chống lại. Hầu hết các công cụ từ chối dịch vụ không phải bằng cách làm quá tải các tiến trình của máy chủ, nhưng bằng cách làm ngập lụt các đường băng thông từ các nhà cung cấp dịch vụ Internet (ISP). Hầu hết các tổ chức vẫn còn dễ bị tổn thương đối với kiểu tấn công này. Cơ chế làm giảm bớt các tấn công DDoS nhiều nhất là bằng cách cố gắng để giảm thiểu số lượng máy bị nhiễm zombie sẵn. Ngay khi có một cơ chế lây nhiễm mới và tốt hơn xuất hiện, một vòng đời khác của các tấn công DDoS chắc chắn sẽ sinh ra.



Hình 2.6 Tấn công kiểu DDoS

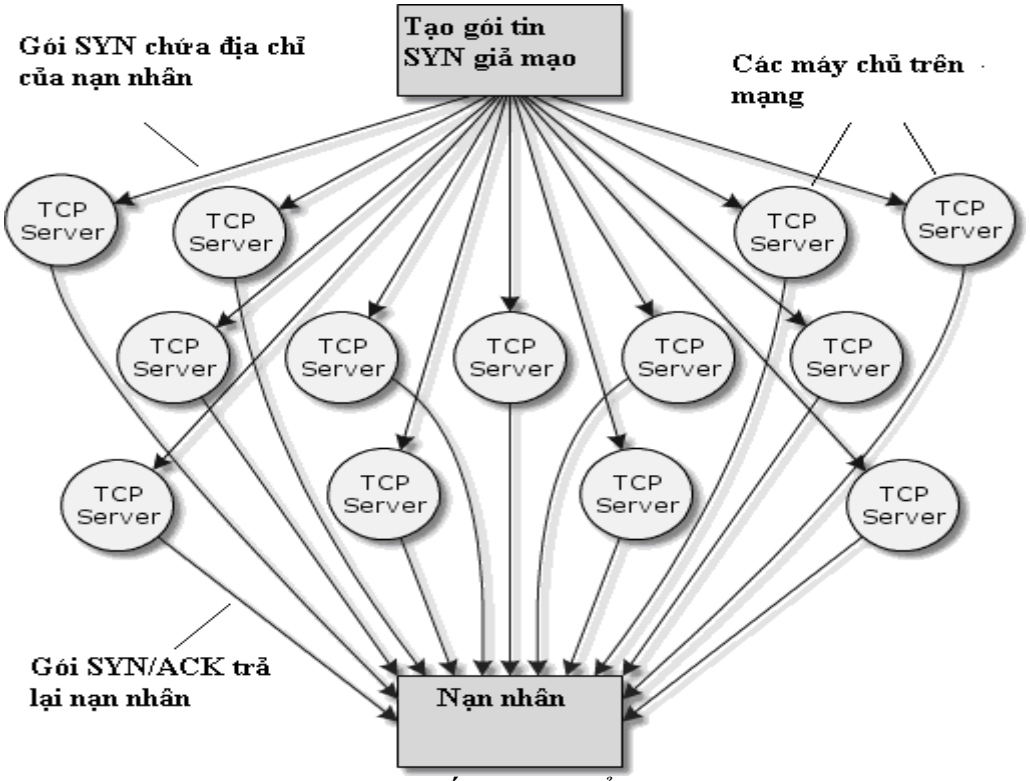
c) Tấn công từ chối dịch vụ theo phương pháp phản xạ phân tán (DRDoS)

Tấn công từ chối dịch vụ phản xạ chỉ mới xuất hiện gần đây nhưng lại là loại nguy hiểm nhất. Nếu được thực hiện bởi các hacker chuyên nghiệp, không một hệ thống nào có thể đứng vững được trước nó. Đáng nói hơn, hiện cũng đã xuất hiện nhiều loại virus, worm, trojan có chức năng tự động thực hiện tấn công DoS.

Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy đích, làm tắc nghẽn hoàn toàn đường kết nối từ máy đích vào xương sống của Internet và làm tiêu hao tài nguyên. Trong suốt quá trình máy đích bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy đích đó, tất cả các dịch vụ chạy trên nền TCP/IP như: DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa.

Sử dụng các máy chủ phản xạ, máy tấn công sẽ gửi yêu cầu kết nối tới các máy chủ có băng thông rất cao trên mạng – máy chủ phản xạ, các gói tin yêu cầu kết nối này mang địa chỉ IP giả - chính là địa chỉ IP của máy nạn nhân. Các máy chủ phản xạ này gửi lại máy nạn nhân các gói SYN/ACK dẫn tới hiện tượng nhân băng thông.

Đây có lẽ là kiểu tấn công lợi hại nhất và làm boot máy tính của đối phương nhanh gọn nhất. Cách làm thì cũng tương tự như DDoS nhưng thay vì tấn công bằng nhiều máy tính thì người tấn công chỉ cần dùng một máy tấn công thông qua các máy chủ lớn trên thế giới. Vẫn với phương pháp giả mạo địa chỉ IP của nạn nhân, kẻ tấn công sẽ gửi các gói tin đến các máy chủ mạnh nhất, nhanh nhất và có đường truyền rộng nhất như Yahoo… , các máy chủ này sẽ phản hồi các gói tin đó đến địa chỉ của nạn nhân. Việc cùng một lúc nhận được nhiều gói tin thông qua các máy chủ lớn này sẽ nhanh chóng làm nghẽn đường truyền của máy tính nạn nhân và làm crash, khởi động lại máy tính đó. Cách tấn công này lợi hại ở chỗ chỉ cần một máy có kết nối Internet đơn giản với đường truyền bình thường cũng có thể đánh bật được hệ thống có đường truyền tốt nhất thế giới nếu như ta không kịp ngăn chặn. Tất nhiên đối với "tấn công từ chối dịch vụ" mọi biện pháp chỉ hạn chế được một phần.



Hình 2.7 Tấn công kiểu DRDoS

Ngoài các cách cơ bản như trên, còn có thể tấn công từ chối dịch vụ kiểu Smurf Attack, kiểu Tear Drop, hay nhằm vào tài nguyên hệ thống như CPU, bộ nhớ, file hệ thống, tiến trình…

Hiện tại chưa có biện pháp hữu hiệu nào để phòng chống tấn công từ chối dịch vụ, nhất là kiểu tấn công gây quá tải hệ thống dịch vụ. Nhà cung cấp dịch vụ chỉ có thể hạn chế hoặc giữ cho hệ thống của mình không bị sụp đổ chứ khó có thể giữ cho dịch vụ của mình luôn sẵn sàng trước mọi cuộc tấn công từ chối dịch vụ.

Biện pháp tốt nhất hiện nay để chống lại các cuộc tấn công từ chối dịch vụ, nhất là kiểu tấn công dựa vào lỗi an toàn thông tin của hệ thống, là các nhà cung cấp dịch vụ phải liên tục cập nhật phiên bản sửa lỗi phần mềm mới nhất cho hệ thống của mình. Đồng thời các nhà cung cấp dịch vụ phải xây dựng và quản trị hệ thống sao cho chúng ít có khả năng bị lợi dụng để phát động tấn công từ chối dịch vụ đối các dịch vụ khác.

2.3.6. Tấn công lừa đảo

2.3.6.1. Định nghĩa tấn công lừa đảo

Tấn công lừa đảo là tên được đặt cho một loại tấn công bảo mật, trong đó một người nào đó sử dụng các kỹ nghệ xã hội của mình lôi kéo những người khác tiết lộ thông tin mà có thể được sử dụng để ăn cắp dữ liệu, truy cập vào hệ thống, truy cập vào điện thoại di động, tiền bạc, hoặc thậm chí nhận dạng riêng của bạn. Các tấn công như vậy có thể rất đơn giản hoặc rất phức tạp. Việc tiếp cận thông tin qua điện thoại hoặc qua các trang web mà bạn truy cập đã đưa thêm vào một chiều hướng mới đối với các kỹ sư xã hội hay kẻ lừa đảo.

Phần này xem xét các cách mà con người, các cơ quan chính phủ, các tổ chức quân sự, và các công ty đã bị lừa cung cấp thông tin mà được sử dụng để tấn công. Công nghệ thấp cũng như các hình thức mới hơn của hành vi trộm cắp điện tử cũng sẽ được thảo luận.

Kỹ nghệ xã hội là việc thu thập thông tin nhạy cảm hoặc đặc quyền truy cập một cách bất hợp pháp bởi một người bên ngoài, dựa trên việc xây dựng một mối quan hệ tin tưởng không chính tắc với những người bên trong. Chú ý rằng từ "người ngoài" không chỉ đề cập đến những người không phải là nhân

viên; một người ngoài có thể là một nhân viên đang cố gắng để phá vỡ các chính sách và chuẩn mực đã được thiết lập.

Mục đích của kỹ nghệ xã hội là để lừa một người nào đó cung cấp thông tin có giá trị hoặc truy cập tới các thông tin hoặc tài nguyên. Các đối tượng khai thác của kỹ nghệ xã hội là dựa trên những phẩm chất vốn có trong bản chất con người, chẳng hạn như:

❖ Mong muốn được hữu ích. Chúng ta đã đào tạo nhân viên của mình tốt, đảm bảo khách hàng hài lòng. Cách tốt nhất để có một sự thẩm định tốt là có nhiều phản hồi tốt từ những người cần được giúp đỡ. Hầu hết các nhân viên của chúng ta muốn thể hiện là hữu ích và điều này có thể dẫn đến việc cho đi quá nhiều thông tin.

❖ Xu hướng tin tưởng người. Bản chất con người là thực sự tin tưởng người khác cho đến khi họ chứng minh rằng họ không đáng tin cậy. Nếu ai đó nói với chúng ta rằng anh ta là một người nào đó, chúng ta thường chấp nhận điều đó. Chúng ta phải đào tạo nhân viên của mình phải tìm kiếm bằng chứng độc lập.

❖ Nỗi sợ hãi khi gây rắc rối. Quá nhiều người trong chúng ta đã thấy phản ứng tiêu cực của cấp trên vì việc xác minh danh tính đã kéo dài quá lâu hoặc bởi vì một số quan chức thấy bị xúc phạm. Quản lý phải hỗ trợ tất cả các nhân viên đang làm nhiệm vụ của họ và bảo vệ các nguồn tài nguyên thông tin của doanh nghiệp.

❖ Sự sẵn sàng/tự nguyện đi tắt. Đôi khi chúng ta lười biếng. Chúng ta dán mật khẩu trên màn hình hoặc để lại các tài liệu quan trọng nằm ở những nơi mà bất cứ ai cũng có thể nhìn thấy.

Những gì mà hầu hết các công ty sợ hãi về các cuộc tấn công dựa trên các kỹ nghệ xã hội là dấu hiệu của các kỹ sư xã hội thành công thực sự là họ nhận được những gì họ đang tìm kiếm mà không bị nghi ngờ.

Theo từ điển thuật ngữ, "wetware" là người được gắn liền với một hệ thống máy tính. Con người thường là liên kết yếu nhất trong chuỗi bảo mật. Trong những năm 1970, chúng ta có thể nói rằng nếu chúng ta cài đặt các gói điều khiển truy cập, chúng ta sẽ có an toàn. Trong những năm 1980, chúng ta có thể được khuyến khích để cài đặt phần mềm chống virus để đảm bảo rằng các hệ thống và các mạng lưới của chúng ta được an toàn. Trong những năm

1990, chúng ta có thể nói rằng tường lửa sẽ đem đến cho chúng ta sự an toàn. Trong thế kỷ 21, đó là hệ thống phát hiện xâm nhập hoặc cơ sở hạ tầng khóa công khai sẽ dẫn chúng ta đến an toàn thông tin. Nhưng trong thời đại hiện nay thì điều đó là chưa đủ, chúng ta cần phải quan tâm hơn nữa tới yếu tố con người.

Một kẻ lừa đảo có kỹ năng thường sẽ cố gắng khai thác điểm yếu này trước khi dành thời gian và công sức vào các phương pháp khác để bẻ mật khẩu hoặc truy cập vào hệ thống. Tại sao phải đi đến tất cả những rắc rối của việc cài đặt một sniffer trên mạng trong khi một cuộc gọi điện thoại đơn giản cho một nhân viên sẽ có được định danh và mật khẩu người dùng cần thiết. Kỹ nghệ xã hội là hình thức tấn công khó phòng thủ nhất bởi vì nó không thể được phòng thủ đơn lẻ với phần cứng hoặc phần mềm. Một phòng thủ thành công đòi hỏi phải có một kiến trúc an toàn thông tin hiệu quả, bắt đầu với các chuẩn và chính sách và sau đó thông qua với một quá trình đánh giá tổn thương.

2.3.6.2. Các loại phổ biến của tấn công dựa trên các kỹ nghệ xã hội

Trong khi khu vực thành công lớn nhất cho loại tấn công này là khu vực tương tác dựa trên yếu tố con người bởi các kỹ sư xã hội, cũng có một số phương pháp dựa trên máy tính để tìm cách lấy các thông tin mong muốn sử dụng các chương trình phần mềm để thu thập thông tin hoặc từ chối dịch vụ của một hệ thống. Một trong những phương pháp khéo léo nhất lần đầu tiên được giới thiệu trên Internet vào tháng 2 năm 1993, Người dùng cố gắng để đăng nhập vào hệ thống đã gặp dấu nhắc bình thường, và sau khi nhập id và mật khẩu, hệ thống lại có dấu nhắc bắt đầu lại từ đầu. Những gì đã xảy ra có phải đó là một cuộc tấn công sử dụng các kỹ nghệ xã hội hay không? Ở đó một kẻ lừa đảo đã thực thi một chương trình được cài đặt ở phía trước của phần đăng nhập bình thường hàng ngày, thu thập thông tin, và sau đó thông qua dấu nhắc tới quá trình đăng nhập thực tế. Theo bài báo xuất bản vào thời điểm đó, hơn 95% người dùng đã thường xuyên có mã truy cập bị tổn thương.

Ngày nay chúng ta thấy việc sử dụng các trang web như một mánh khóe phổ biến để cung cấp một cái gì đó miễn phí hoặc một cơ hội để giành

chiến thắng một cái gì đó trên trang web hoặc để có được thông tin quan trọng. Tại một công ty Michigan vào năm 1998, nhà quản trị mạng đã cài đặt một trang web thông tin 401(k) yêu cầu nhân viên phải đăng ký với các trang web để lấy được thông tin trong chương trình 401 (k) của họ. Sau khi đưa ra các thông tin như id tài khoản, mật khẩu, số bảo hiểm xã hội, và địa chỉ nhà, trang web trở lại một tin nhắn cho thấy nó vẫn còn đang được xây dựng. Trong vòng một tuần, gần như tất cả nhân viên với một kế hoạch 401 (k), bao gồm cả người quản lý cấp cao, đã cố gắng đăng ký trên trang web.

Các hình thức khác của lừa đảo có thể đã được phân loại thành các nhóm khác nhau. Hai hình thức đầu tiên là mạo danh và người dùng quan trọng. Hai hình thức này thường được sử dụng kết hợp với nhau. Cuốn sách Cyberpunk của Katie Hafner và John Markoff năm 1991 mô tả những hành động của một Susan Hadley (hay còn gọi là Susan Thunder). Sử dụng một thư mục máy tính quân sự dễ dàng truy cập, cô ấy có thể lấy được tên của các cá nhân phụ trách. Cô đã sử dụng kiến thức cơ bản của mình về các hệ thống và các thuật ngữ quân sự khi cô gọi cho một căn cứ quân sự để tìm ra các sĩ quan chỉ huy của cơ sở thông tin bị phân chia bí mật. Cô nói một cách ngọt ngào theo cách của mình để lấy tên của tổng thư ký và sau đó sẽ tìm cách trì hoãn. Sử dụng thông tin này, cô đã thay đổi chiến thuật. Cô chuyển giọng từ là lãnh đạm sang có thẩm quyền. Cấp trên của cô ta, người quan trọng nhất, đã gặp nhiều vấn đề khi truy cập hệ thống và cô ấy muốn biết lý do tại sao. Sử dụng các hiểm họa, cô đã có truy cập và theo đó cô đã truy cập vào trong các hệ thống trong thời gian 20 phút.

Giả vờ là một người nào đó hoặc hưởng ứng theo cách của bạn để lấy các thông tin cần thiết; Đây là những ví dụ điển hình về cách những kẻ lừa đảo thực hiện các hành động để có được các thông tin họ cần. Họ thường sẽ liên hệ với bộ phận hỗ trợ và tình cờ nói ra tên của các nhân viên khác. Một khi họ có những gì họ cần để được truy cập xa hơn nữa, họ sẽ tấn công một người dễ bị tổn thương hơn – một người có thông tin nhưng không nhất thiết phải ảnh hưởng đến việc thách thức bất cứ ai về "thẩm quyền".

Có lẽ hai trong các hình thức lâu đời nhất của lừa đảo là tìm trong thùng rác và nhìn lướt qua vai. Những người móc thùng rác sẵn sàng bị bẩn để có được những thông tin cần thiết. Các công ty rất thường xuyên vứt đi các

thông tin quan trọng. Thông tin nhạy cảm, hướng dẫn sử dụng, và các thư mục điện thoại nên được băm nhỏ trước khi xử lý.

Những người xem qua vai sẽ nhìn qua vai của ai đó để biết được mật khẩu hoặc số PIN. Một vài năm trước đây, một trong những chương trình tin tức đã làm một số về gian lận thẻ điện thoại. Trong suốt quá trình, phóng viên đã có được một chiếc thẻ gọi điện thoại mới và sử dụng nó ở nhà ga trung tâm ở thành phố New York. Trong khi cô thực hiện cuộc gọi, cảnh sát bí mật đã tính có ít nhất năm người nhìn lướt thấy số PIN của cô ấy. Một người thậm chí quay sang người quay phim chắc chắn rằng anh ta cũng có số đó.

Hai loại cuối cùng của lừa đảo dựa trên yếu tố con người là ủy quyền của bên thứ ba và hỗ trợ kỹ thuật. Việc ủy quyền của bên thứ ba điển hình xảy ra khi các kẻ lừa đảo nói ra tên của một người cấp cao có thẩm quyền để cấp quyền truy cập. Ví dụ như "Bà Lan nói rằng điều đó là được" hoặc "Trước khi bà Lan đi nghỉ, bà ấy đã cho biết tôi nên gọi cho bạn để lấy thông tin này". Các kẻ lừa đảo cũng có thể giả dạng các cơ quan của chính quyền để tìm hiểu xem nếu cô ấy đã ra ngoài. Nhớ rằng hầu hết các kẻ lừa đảo là ở trong nội bộ.

Phương pháp "hỗ trợ kỹ thuật" là phương pháp mà các kẻ lừa đảo giả vờ là một người nào đó từ một nhóm cơ sở hạ tầng và muốn một người dùng truy cập hệ thống trong khi anh ta có cơ hội sử dụng kết nối. Họ thường sẽ yêu cầu id tài khoản và mật khẩu của người dùng để họ có thể nhìn thấy nó qua mạng. Trong một đánh giá tổn thương gần đây của một nhà cung cấp bảo hiểm lớn Texasbased, 12 nhân viên được gọi bởi "quản trị mạng", người mà thực sự là nhân viên an ninh giả dạng là quản trị mạng. Những nhân viên được thông báo rằng mạng đang gặp phải vấn đề về kết nối, rằng họ đã cài đặt một lối thoát trên các kết nối cáp quang, và sau đó yêu cầu những nhân viên đăng nhập vào hệ thống. Họ yêu cầu id tài khoản và mật khẩu để sử dụng như một sự xác minh rằng các dữ liệu đã được gửi đúng. Ba nhân viên không trả lời các cuộc gọi điện thoại. Tám trong số chín người kia đã đưa ra các thông tin yêu cầu. Một nhân viên đã không thể đưa ra mật khẩu của mình bởi vì người đó không thể tìm thấy tờ ghi chú - nó ghi thông tin tài khoản bằng văn bản.

Một số lỗ hổng bảo mật tiềm năng quá tầm thường đến mức chúng hầu như không được xem là một mối quan tâm. Với tất cả các vụ cháy mà chúng

ta phải chiến đấu mỗi ngày và những thời hạn mà chúng ta đã đáp ứng, một số yếu tố rõ ràng nhất thường bị bỏ qua:

- Các mật khẩu: điểm truy cập số một cho các kẻ lừa đảo là mật khẩu cũ. Sau khi tất cả các chương trình nâng cao nhận thức và các thẻ nhắc nhở, chúng ta vẫn thấy các mật khẩu của nhân viên tạo ra là quá ngắn hoặc quá dễ đoán. Các mật khẩu hệ thống tạo ra quá dài và các nhân viên đã viết ra để ghi nhớ chúng. Thậm chí ngày nay, một số hệ thống không yêu cầu mật khẩu phải được thay đổi. Chúng ta tìm thấy điều này ở hầu hết trong các hệ thống thư điện tử và tài khoản Internet. Chúng ta khuyến cáo việc đánh giá về độ dài mật khẩu và các chuẩn về khoảng thời gian để thay đổi, xác định xem chúng vẫn đáp ứng các nhu cầu hiện tại của cộng đồng người dùng.
- Các modem: mỗi công ty có nhiều modem hơn là những gì họ biết. Các nhân viên và nhà thầu sẽ bổ sung thêm một modem vào một hệ thống và sau đó cài đặt các sản phẩm như pcAnywhere hoặc Carbon Copy để cải thiện thời gian truy cập từ xa của họ. Chúng ta khuyến nghị nên kiểm tra các modem ít nhất hai lần một năm.
- Quầy lễ tân: đặt ra các quy trình diễn ra có thể giúp các nhân viên lễ tân trong việc xác minh ai ở đầu bên kia của cuộc gọi điện thoại.
- Các trang web: có hai vấn đề ở đây: trang web giả để thu thập thông tin và các trang web hợp pháp cung cấp quá nhiều thông tin. Nhiều tin tặc sử dụng các thông tin mà họ thu thập từ trang web của doanh nghiệp để khởi động các cuộc tấn công trên mạng. Hãy chắc chắn rằng các thông tin có sẵn này sẽ không làm tổn thương tới tài nguyên thông tin của doanh nghiệp.

Một kẻ lừa đảo có thể chỉ đơn giản đi bộ vào bên trong và ứng xử như một nhân viên. Những nhân viên của chúng ta đã không được đào tạo để thử thách những người xa lạ. Hoặc nếu họ đã được đào tạo, nhưng chưa có đủ sự tăng cường cho quá trình thử thách. Yêu cầu tất cả những người trên trang web phải mang định danh thích hợp. Một số tổ chức chỉ yêu cầu khách phải đeo biển hiệu. Vì vậy, để trở thành một nhân viên, một người truy cập chỉ đơn giản là phải bỏ các biển hiệu. Nguyên tắc định danh nhân viên không chỉ là một biện pháp an ninh, mà là một quá trình để bảo vệ người đó tại nơi làm

việc. Bằng cách đảm bảo rằng chỉ những người dùng được xác thực mới được phép truy cập, các nhân viên sẽ có một môi trường làm việc an toàn.

2.3.6.3. Các pha trong tấn công lừa đảo

Một cuộc tấn công lừa đảo thường thực hiện theo các pha cơ bản như sau:

- Nghiên cứu, thu thập thông tin về tổ chức mục tiêu:

Có thể nghiên cứu và thu thập thông tin bằng các cách như thông qua việc sử dụng các công cụ tìm kiếm, có thể kết hợp sử dụng các kỹ thuật như Google Hacking, kỹ thuật bới rác, thu thập các thông tin được đăng tải trên trang web của tổ chức, thông tin về các nhân viên, người điều hành, gia đình của họ, hoặc trực tiếp đi thăm quan địa hình của tổ chức…

Sau quá trình nghiên cứu, thu thập và chọn lọc thông tin về tổ chức, kẻ tấn công lừa đảo sẽ dựa vào các thông tin đó để đưa ra các tiêu chí và lựa chọn mục tiêu hay nạn nhân. Bước này được thực hiện nhằm xác định các nhân viên có kiến thức bảo mật kém, nhẹ dạ cả tin, ít kinh nghiệm, những nhân viên tham lam, nản lòng với mục tiêu, đường lối, cách làm việc, có những mối quan hệ bất hòa… trong tổ chức để lợi dụng họ cho mục đích của kẻ tấn công lừa đảo.

- Phát triển các mối quan hệ:

Phát triển các mối quan hệ với mục tiêu được chọn, quá trình này giúp kẻ tấn công có được mối quan hệ tốt đẹp với nạn nhân và họ sẽ sẵn sàng giúp hắn những việc không đúng với thủ tục, chính sách làm việc của tổ chức một cách vô thức.

- Khai thác các mối quan hệ:

Trong pha này kẻ tấn công sẽ tận dụng những mối quan hệ đã xây dựng và phát triển được để khai thác lấy thông tin mong muốn. Tập hợp thông tin tài khoản nhạy cảm, thông tin tài chính, thiết bị, sơ đồ, cách bài trí, danh sách hồ sơ nhân viên, các công nghệ hiện đại của công ty, tổ chức… hoặc là nhận được quyền truy cập vào tài nguyên, hệ thống của tổ chức.

Tóm lại, Chuyên gia bảo mật có thể bắt đầu quá trình phòng chống kiểu tấn công này bằng cách làm sẵn một loạt các tài liệu hỗ trợ cho tất cả nhân viên. Nhiều nhân viên phản ứng tích cực với các câu chuyện liên quan đến các

trò lừa đảo dựa trên các kỹ năng xã hội. Đảm bảo cho thông tin được cập nhật và chính xác. Bao gồm chi tiết về những hậu quả của cuộc tấn công thành công. Không thảo luận về các cuộc tấn công này theo cách thức bảo mật đã bị phá vỡ, nhưng thay vào đó là tác động của chúng tới hoạt động hoặc nhiệm vụ của doanh nghiệp. Các cuộc tấn công có thể dẫn đến mất lòng tin của khách hàng, mất thị phần và công việc. Nhân viên ở tất cả các cấp của doanh nghiệp cần phải hiểu và tin rằng họ quan trọng đối với chiến lược bảo vệ tổng thể. Nếu không có tất cả các nhân viên là một phần của đội, các doanh nghiệp, các tài sản và các nhân viên của họ sẽ mở cửa cho tấn công từ cả hai phía: kẻ lừa đảo bên ngoài và nội bộ. Đào tạo và trợ giúp có thể giúp giảm bớt tác động của những cuộc tấn công.

2.3.7. Hiểm họa rò rỉ thông tin qua các kênh truyền

Kênh rò rỉ TT - Đó là một tổ hợp gồm nguồn tin, vật mang vật chất hoặc môi trường lan truyền tín hiệu mang TT và thiết bị tách TT khỏi tín hiệu hay vật mang. Đối với hệ thống TT – VT có thể chia ra các kênh rò rỉ TT sau đây:

2.3.7.1. Kênh điện từ

Nguyên nhân xuất hiện kênh này chính là trường điện từ sinh ra từ dòng điện chạy trong các thành phần máy móc của hệ thống. Trường điện từ có thể làm cảm ứng các dòng điện trong các dây dẫn ở gần nó (sự cảm ứng – xuyên điện). Kênh điện từ có thể chia ra thành các kênh:

1. Kênh vô tuyến (bức xạ cao tần)
2. Kênh tần số thấp
3. Kênh lưới điện (cảm ứng xuyên điện trên lưới điện nuôi)
4. Kênh nối đất (xuyên điện trên dây nối đất)
5. Kênh tuyến tính (xuyên điện trên các dây liên lạc giữa hệ máy tính)

2.3.7.2. Kênh âm thanh

Liên quan tới việc truyền các sóng âm trong không khí hoặc các dao động đàn hồi trong các môi trường khác. Chúng xuất hiện khi các thiết bị phản ánh TT làm việc.

2.3.7.3. Kênh hình ảnh

Kênh này liên quan tới khả năng kẻ xấu quan sát được bằng hình ảnh sự làm việc của các thiết bị phản xạ TT của hệ thống (màn hình chẳng hạn) mà không phải lọt vào địa điểm đặt các thiết bị của hệ thống. Các thiết bị tách TT khỏi vật mang ở đây là máy chụp hình, máy quay video (video camera)…

2.3.7.4. Kênh thông tin

Kênh này liên quan tới tiếp cận (trực tiếp hoặc từ xa) tới các yếu tố của HT, tới các vật mang TT, tới bản thân TT đầu vào và đầu ra (và các kết quả xử lý), tới bảo đảm toán học (kể cả các hệ điều hành). Nó cũng gồm cả việc trích các đường dây dẫn TT. Kênh TT có thể chia ra các loại:

1. Các đường dây TT liên lạc viễn thông
2. Các đường dây liên lạc đặc biệt (đường dây nóng)
3. Mạng cục bộ
4. Các vật mang tin trên máy
5. Các thiết bị đầu cuối

2.4. CÁC KIỂU TẤN CÔNG PHỔ BIẾN

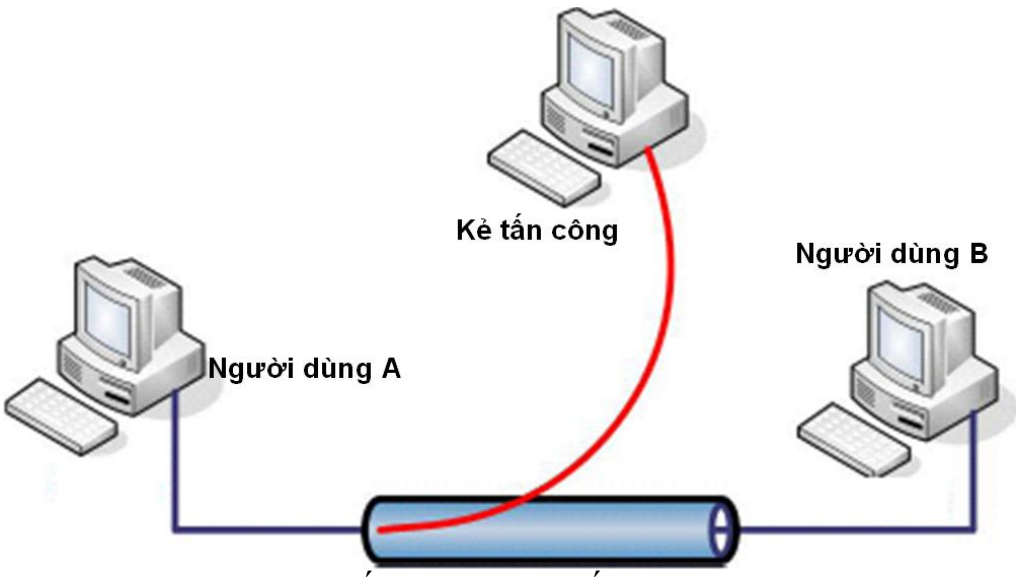
Chúng ta phải đối mặt với rất nhiều các tấn công từ hàng loạt các góc độ và phương pháp tiếp cận khác nhau. Khi chúng ta nhìn vào chính xác những gì tạo nên một cuộc tấn công, chúng ta có thể phân chúng theo loại tấn công đại diện, nguy cơ đại diện và các điều khiển mà chúng ta có thể sử dụng để giảm thiểu tấn công đó.

Khi chúng ta xem xét các kiểu tấn công mà chúng ta có thể gặp, chúng ta có thể phân chúng thành 4 loại sau: tấn công chặn bắt, tấn công ngăn chặn, tấn công sửa đổi, tấn công giả mạo. Mỗi loại tấn công này có thể ảnh hưởng đến một hoặc một số nguyên tắc trong bộ ba CIA như trong hình 2.8. Hơn nữa đường ranh giới giữa các kiểu tấn công và những ảnh hưởng cụ thể của nó có thể có một số điểm mờ. Phụ thuộc vào tấn công cụ thể chúng ta có thể bàn luận xem nó thuộc những kiểu tấn công nào hay nó có những kiểu ảnh hưởng nào.

Hình 2.8 Các loại tấn công phổ biến

2.4.1. Tấn công chặn bắt thông tin

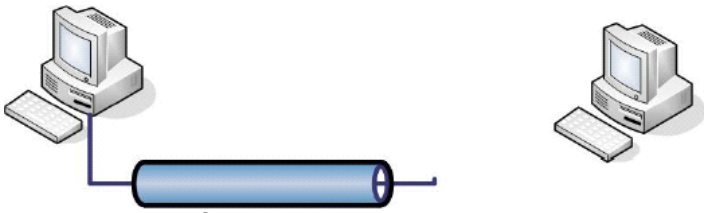
Các tấn công chặn bắt thông tin cho phép những người dùng không được xác thực truy cập tới dữ liệu, ứng dụng hay môi trường của chúng ta và chúng là các tấn công chủ yếu vào tính bí mật của thông tin. Tấn công chặn bắt có thể là việc người không được xác thực xem hoặc sao chép các tập tin, nghe trộm cuộc nói chuyện qua điện thoại hoặc đọc thư điện tử, và có thể được thực hiện đối với các tấn công ở chế độ tĩnh hay đang di chuyển. Nếu được thực hiện chính xác thì các tấn công chặn bắt thông tin có thể rất khó để phát hiện.



Hình 2.9 Tấn công chặn bắt thông tin

2.4.2. Tấn công ngăn chặn thông tin

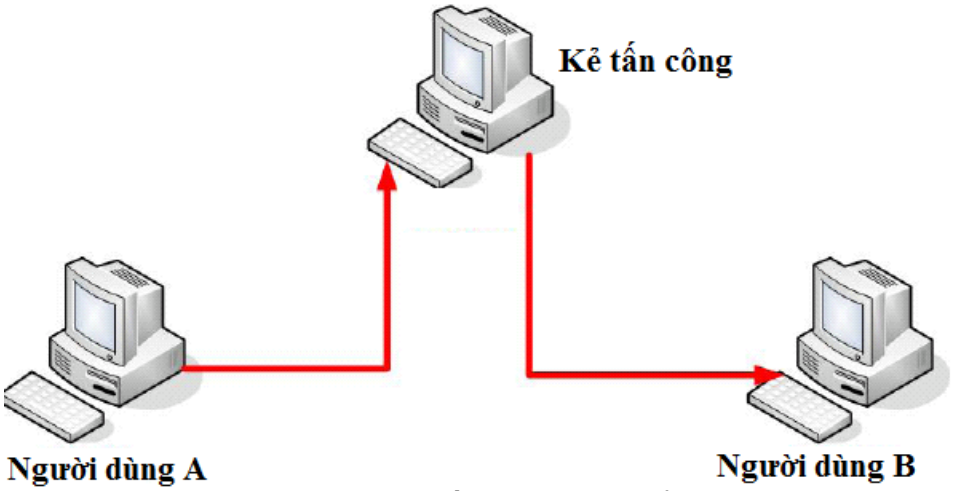
Các tấn công ngăn chặn gây ra việc các nguồn tài nguyên của chúng ta trở nên không sử dụng được hoặc không sẵn sàng để chúng ta sử dụng có thể là tạm thời hoặc vĩnh viễn. Các tấn công ngăn chặn thường ảnh hưởng đến tính sẵn sàng nhưng cũng có thể là tấn công vào tính toàn vẹn. Trong trường hợp tấn công từ chối dịch vụ vào máy chủ thư điện tử, chúng ta sẽ phân kiểu tấn công này như là tấn công vào tính sẵn sàng. Trong trường hợp một kẻ tấn công thao tác chạy các tiến trình trên một cơ sở dữ liệu để ngăn chặn các truy cập vào các dữ liệu chứa trong đó thì chúng ta có thể coi đó là một tấn công vào tính toàn vẹn, do có thể dữ liệu sẽ bị mất hoặc hư hỏng, hoặc chúng ta có thể coi đó là một tấn công kết hợp vào cả hai tính chất. Chúng ta cũng có thể xem xét cuộc tấn công cơ sở dữ liệu như vậy là một cuộc tấn công sửa đổi chứ không phải là một cuộc tấn công ngăn chặn.



Hình 2.10 Tấn công ngăn chặn thông tin

2.4.3. Tấn công sửa đổi

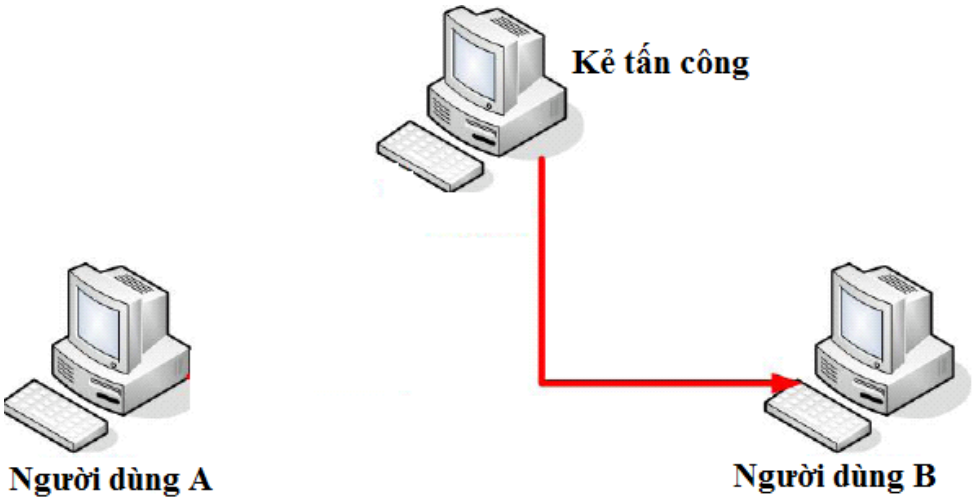
Các tấn công sửa đổi liên quan đến việc sửa đổi các tài nguyên của chúng ta. Các tấn công này có thể coi là tấn công chủ yếu vào tính toàn vẹn của thông tin nhưng cũng có thể là một tấn công vào tính sẵn sàng. Nếu chúng ta truy cập một tập tin một cách trái phép và thay đổi dữ liệu trong đó, chúng ta đã làm mất tính toàn vẹn của thông tin chứa trong tập tin. Tuy nhiên nếu chúng ta xem xét trường hợp tập tin đó là một tập tin cấu hình quản lý cách thức xử lý của một dịch vụ cụ thể, có thể một trong số đó là hoạt động như một máy chủ Web, chúng ta có thể làm ảnh hưởng tới tính sẵn sàng của dịch vụ đó bằng cách thay thế các nội dung của tập tin. Nếu chúng ta tiếp tục với khái niệm này và nói tập tin cấu hình mà chúng ta đã thay đổi cho máy chủ Web của chúng ta là một trong những thứ làm thay đổi cách thức máy chủ thỏa thuận các kết nối được mã hóa, thì chúng ta thậm chí có thể làm nó thành một cuộc tấn công vào tính bí mật.



Hình 2.11 Tấn công sửa đổi

2.4.4. Tấn công giả mạo

Các tấn công giả mạo liên quan đến việc tạo ra các dữ liệu, các tiến trình, các thông tin liên lạc hoặc các hành động tương tự khác đối với một hệ thống. Các tấn công giả mạo chủ yếu ảnh hưởng đến tính toàn vẹn nhưng cũng có thể được coi là một tấn công vào tính sẵn sàng. Nếu chúng ta tạo ra thông tin giả mạo trong một cơ sở dữ liệu, điều này được coi như là một tấn công giả mạo. Chúng ta cũng có thể tạo thư điện tử - thường được sử dụng như là một phương pháp để nhân bản phần mềm mã độc hại, chẳng hạn như chúng ta có thể thấy việc sử dụng phương pháp này để lây lan một con sâu. Đối với ý nghĩa là một tấn công vào tính sẵn sàng, nếu chúng ta tạo ra các tiến trình bổ sung, lưu lượng mạng, thư điện tử, lưu lượng Web hoặc những thứ khác tương tự đủ để tiêu thụ hết các nguồn tài nguyên, chúng ta có thể gặp phải khả năng các dịch vụ này không có sẵn cho người dùng hợp pháp của hệ thống.



Hình 2.12 Tấn công giả mạo

2.5. CÂU HỎI

1. Giải thích sự khác nhau giữa một hiểm họa và một lỗ hổng?
2. Hãy tạo và mô tả các trường hợp về một hệ thống TT – VT chịu các tấn công ác ý gây ra bởi mỗi loại hiểm họa (lộ tin, phá vỡ toàn vẹn tin và từ chối dịch vụ).
3. Sáng tác một kịch bản về hệ thống máy tính chịu một tấn công ác ý do tất cả 3 loại hiểm họa gây ra cùng một lúc.
4. Hãy đưa ra một liệt kê các hiểm họa có thể đe doạ tới an toàn của một hệ thống của một công ty và đối với hệ thống máy tính của cá nhân bạn. (Vòng ngoài, vòng trong…)
5. Loại tấn công nào đánh vào tính bí mật của thông tin?

CHƯƠNG 3. ĐẢM BẢO AN TOÀN THÔNG TIN TỔNG THỂ

3.1. CÁC NGUYÊN LÝ ĐẢM BẢO AN TOÀN THÔNG TIN

ATTT các hệ thống dựa trên các đòi hỏi của pháp luật hiện hành, các tiêu chuẩn, các tài liệu phương pháp chuẩn, được bảo đảm bằng tổ hợp các thiết bị kỹ thuật – chương trình và các biện pháp tổ chức trợ giúp chúng ở tất cả các giai đoạn công nghệ của xử lý TT và trong tất cả các chế độ hoạt động của các thiết bị kể cả khi sửa chữa và niêm cất.

Các thiết bị kỹ thuật – chương trình của bảo vệ không được gây ảnh hưởng xấu tới các đặc trưng hoạt động cơ bản của hệ thống (độ tin cậy, tính linh hoạt, khả năng thay đổi cấu hình…). Một trong những phần không thể bỏ qua của công việc về ATTT là việc đánh giá hiệu quả của các thiết bị bảo vệ, được tiến hành theo phương pháp có tính tới toàn bộ các đặc trưng kỹ thuật của đối tượng được đánh giá kể cả các giải pháp kỹ thuật và sự thực hiện trên thực tế các thiết bị bảo vệ. Việc bảo vệ hệ thống phải đi kèm sự kiểm soát hiệu quả các thiết bị bảo vệ được đề xuất định kỳ bởi người dùng hoặc bởi cơ quan kiểm tra.

Những đòi hỏi nêu trên có thể thực hiện nhờ 7 nguyên tắc sau đây:

3.1.1. Nguyên tắc tính hệ thống

Tiếp cận hệ thống trong ATTT nói rằng: cần phải kiểm kê tất cả các yếu tố, các điều kiện và các nhân tố có quan hệ với nhau, có tương tác với nhau và có biến đổi theo thời gian:

1. Trong tất cả các dạng hoạt động TT và thể hiện TT.
2. Với tất cả các thành tố của hệ thống.
3. Trong tất cả các chế độ hoạt động.
4. Ở tất cả các giai đoạn của chu kỳ sống.

5. Trong sự tương tác của đối tượng bảo vệ với môi trường bên ngoài.

Khi thực hiện ATTT hệ thống cần phải tính tới tất cả các điểm xung yếu, các vị trí dễ tổn thương của hệ thống xử lý TT, và cả đặc trưng, các đối tượng tiềm năng, các hướng của các tấn công và hệ thống từ phía những kẻ phá hoại (đặc biệt kẻ ác ý có trình độ chuyên môn cao), các con đường xâm nhập vào các hệ thống phân tán và các kênh tiếp cận trái phép (TCTP) tới thông tin. Hệ thống bảo vệ phải được thiết lập không chỉ tính tới tất cả các kênh xâm nhập đã biết, mà còn cả khả năng xuất hiện các kênh hoàn toàn mới của các nguy cơ an toàn.

3.1.2. Nguyên tắc tổng thể

Trong tay các chuyên gia an toàn máy tính có rất nhiều biện pháp, phương pháp và thiết bị bảo vệ hệ thống máy tính. Các thiết bị tính toán hiện đại, các hệ điều hành, các thiết bị chương trình ứng dụng và chỉ dẫn đều có cài đặt các yếu tố bảo vệ khác nhau. Sử dụng tổng thể đồng bộ các yếu tố này yêu cầu sự tương thích đồng bộ của các thiết bị khác loại khi xây dựng hệ thống toàn diện để bịt kín tất cả các kênh xâm nhập của các hiểm họa và không chứa các vị trí xung yếu ở nơi tiếp giáp của các thành tố của hệ thống.

3.1.3. Nguyên tắc bảo vệ liên tục

Bảo vệ TT - đó không phải là biện pháp một vài lần và thậm chí đó không phải là tập hợp cụ thể của các biện pháp đã thực hiện và các thiết bị đã cài đặt, mà đó là một quá trình liên tục hướng tới mục tiêu, yêu cầu phải đưa ra các giải pháp phù hợp ở tất cả các giai đoạn của chu kỳ sống của hệ thống (bắt đầu ngay từ lúc thiết kế chứ không phải chỉ trong khi khai thác hệ thống). Thiết kế hệ thống bảo vệ phải được tiến hành song song với thiết lập chính hệ thống được bảo vệ.

Phần lớn các thiết bị bảo vệ kỹ thuật và vật lý cần có sự trợ giúp thường xuyên của các biện pháp tổ chức (hành chính) để thực hiện có hiệu quả các chức năng của chúng (ví như sự thay đổi kịp thời, bảo quản chặt chẽ và ứng dụng linh hoạt các tên, mật khẩu, các khoá mã, sự phân quyền v.v…). Sự gián đoạn (hoặc ngừng tạm thời) trong hoạt động của các thiết bị bảo vệ có thể bị kẻ ác ý lợi dụng để đưa vào các chương trình đặc biệt, các thiết bị cài bẫy và

các phương tiện khác để qua mặt hệ thống bảo vệ khi hệ thống làm việc trở lại.

3.1.4. Nguyên tắc đầy đủ hợp lý

Thiết lập một hệ bảo vệ tuyệt đối không chọc thủng được là một điều không tưởng vì rằng với đầy đủ điều kiện và phương tiện có thể vượt qua mọi hệ bảo vệ. Ví dụ, các phương tiện bảo vệ mật mã trong phần lớn các trường hợp không bảo đảm độ bền vững tuyệt đối, mà chúng chỉ bảo đảm sự bí mật TT trong điều kiện bị tấn công mã thám liên tục bằng các máy tính hiện đại, trong một khoảng thời gian phù hợp với yêu cầu bảo vệ mà thôi. Do đó cần nói về một độ bảo vệ vừa đủ nào đó. Một hệ thống bảo vệ hiệu quả có chi phí khá đắt. Nó sử dụng công suất đáng kể của máy tính và các tài nguyên đi kèm và do đó nó có thể gây thêm cho người dùng hệ thống một sự bất tiện và rắc rối đáng kể. Điều quan trọng là phải lựa chọn đúng mức độ bảo vệ cần thiết, mà trong đó các chi phí, độ mạo hiểm và phạm vi các thiệt hại có thể là chấp nhận được (bài toán phân tích độ mạo hiểm).

3.1.5. Nguyên tắc mềm dẻo hệ thống

Thông thường phải thiết lập hệ bảo vệ trong các điều kiện bất định khá lớn. Cho nên các biện pháp thực hiện và các thiết bị lắp đặt cho bảo vệ, nhất là ở giai đoạn đầu đi vào hoạt động, có thể bảo đảm hoặc là một độ bảo vệ quá mức hoặc là quá thấp. Do vậy để có thể điều chỉnh độ bảo vệ, các thiết bị như vậy phải có sự mềm dẻo nhất định. Đặc biệt điều này quan trọng khi mà hệ bảo vệ được đưa vào một hệ thống đang làm việc mà không được phép phá vỡ quá trình hoạt động bình thường của nó. Ngoài ra, điều kiện bên ngoài, các yêu cầu bảo vệ theo thời gian cũng có thay đổi. Trong những tình huống như vậy, tính chất mềm dẻo hệ thống bảo vệ sẽ giúp cho việc nâng cấp hệ thống dễ dàng mà không phải thay thế mới toàn bộ máy móc thiết bị của hệ thống.

3.1.6. Nguyên tắc công khai của thuật toán và cơ chế bảo vệ

Bản chất của nguyên tắc này là ở chỗ, sự bảo vệ không được chỉ dựa vào bí mật của cơ cấu tổ chức và các thuật toán hoạt động của các tiểu hệ (bộ phận). Dù có biết thuật toán làm việc của hệ thống bảo vệ thì cũng không thể qua mặt được nó (thậm chí cả tác giả của hệ thống bảo vệ cũng vậy).

3.1.7. Nguyên tắc đơn giản trong sử dụng

Các cơ chế bảo vệ phải dễ hiểu và đơn giản trong sử dụng. Việc áp dụng các thiết bị bảo vệ không được buộc phải biết các ngôn ngữ đặc biệt hoặc buộc phải thực hiện các thao tác khó khăn đối với người dùng hợp pháp, kể cả việc thực hiện các thao tác khó hiểu rắc rối.

3.2. QUY TRÌNH AN TOÀN HOẠT ĐỘNG

Toàn bộ quá trình này liên quan đến không chỉ các biện pháp đối phó được thiết lập, mà trước khi làm như vậy cần phải xác định cẩn thận chính xác những gì chúng ta cần bảo vệ, và những gì chống lại cái mà chúng ta cần phải bảo vệ. Nếu chúng ta thực hiện ngay việc đặt các biện pháp bảo vệ tại chỗ, chúng ta đã "cầm đèn chạy trước ô tô" và có thể không hướng đúng vào những nỗ lực bảo vệ các tài sản thông tin thực sự quan trọng nhất cần bảo vệ. Điều quan trọng cần nhớ khi thiết lập các biện pháp an toàn, chúng ta cần phải thực thi các biện pháp an toàn với một mức độ phù hợp với những gì cần bảo vệ. Nếu chúng ta đều áp dụng cùng một mức độ bảo mật cho tất cả mọi thứ, chúng ta có thể bảo vệ không hợp lý một số tài sản có giá trị không cao và bảo vệ không tốt cho những tài sản có giá trị lớn hơn nhiều.

Quy trình an toàn hoạt động nhìn sẽ rất quen thuộc với bất kỳ ai đã làm việc với việc quản lý rủi ro. Về bản chất, quá trình này là để xác định những thông tin chúng ta cần bảo vệ, phân tích các hiểm họa và các lỗ hổng có thể ảnh hưởng đến nó, và phát triển các phương pháp giảm thiểu tác động đối với những hiểm họa và các lỗ hổng, như trong hình 3.1.

Mặc dù quá trình này tương đối đơn giản, nhưng nó rất hiệu quả.

3.2.1. Xác định các thông tin quan trọng

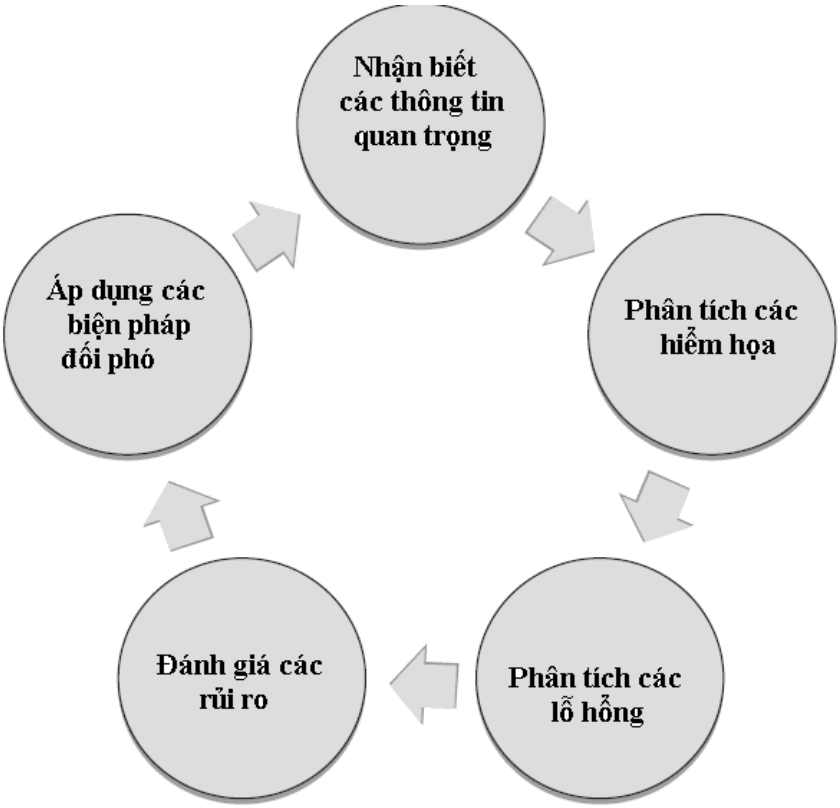
Bước đầu tiên và có thể là bước quan trọng nhất trong quá trình an toàn hoạt động là để xác định các tài sản thông tin quan trọng nhất của chúng ta. Mặc dù chúng ta có thể dành rất nhiều thời gian để xác định tất cả các phần rất nhỏ của thông tin mà thậm chí nhìn từ xa có thể là quan trọng, đây không phải là mục tiêu của bước này trong quy trình an toàn hoạt động. Đối với bất kỳ doanh nghiệp, cá nhân, hoạt động quân sự, quá trình, dự án nào, chắc chắn có ít nhất một phần nhỏ thông tin quan trọng mà các thứ khác phải phụ thuộc

vào. Đối với một công ty nước giải khát, nó có thể là công thức bí mật, đối với một nhà cung cấp ứng dụng thì đó có thể là các mã nguồn của chúng ta, đối với hoạt động quân sự đó có thể là thời gian biểu của các cuộc tấn công và những thứ tương tự. Đây là những tài sản mà cần được bảo vệ nhất và sẽ gây ra những thiệt hại lớn nhất nếu bị khám phá, và đây là những tài sản mà chúng ta nên nhận ra.

Ở bước này bên cạnh việc xác định các thông tin quan trọng nhất, chúng ta cũng cần phải nhận biết các tài sản quan trọng khác trong phạm vi hệ thống và người sở hữu 1 của các tài sản đó.

3.2.2. Phân tích các hiểm họa

Như đã thảo luận khi chúng ta xem xét các hiểm họa, lỗ hổng và các rủi ro, một hiểm họa là một cái gì đó mà có tiềm năng gây hại cho chúng ta. Trong trường hợp phân tích các hiểm họa đến tài sản thông tin của chúng ta, chúng ta sẽ bắt đầu với các thông tin quan trọng mà chúng ta đã xác định ở bước trước. Với danh sách các thông tin quan trọng, sau đó chúng ta có thể bắt đầu xem xét những gì có hại có thể gây ra khi thông tin quan trọng bị khám phá, và những ai có thể khám phá thông tin đó. Đây là quá trình tương tự được sử dụng bởi nhiều tổ chức chính phủ và quân đội để phân loại thông tin và xác định ai được phép xem nó.



Hình 3.1 Quy trình an toàn hoạt động

Ví dụ nếu chúng ta là một công ty phần mềm đã xác định các mã nguồn độc quyền của một trong số những sản phẩm chính của chúng ta là một mục thông tin quan trọng, chúng ta có thể xác định rằng các hiểm họa chính chẳng hạn như mã nguồn đó có thể bị tiếp xúc bởi kẻ tấn công hay đối thủ cạnh tranh của chúng ta. Nếu mã nguồn đã bị tiếp xúc bởi những kẻ tấn công, chúng có thể có khả năng xác định cơ chế mà chúng ta sử dụng để tạo ra các từ khóa bản quyền đối với sản phẩm của chúng ta để chống lại sự sao chép, và sử dụng truy cập vào mã nguồn để phát triển một tiện ích mà có thể tạo ra các từ khóa hợp pháp, do đó sẽ thất thoát một khoản phí mà chúng ta thu được từ các bản quyền phần mềm. Trong trường hợp đối thủ cạnh tranh của chúng ta, họ có thể sử dụng truy cập vào mã nguồn nhằm sao chép các tính năng để sử dụng trong các ứng dụng riêng của họ hay họ có thể sao chép phần lớn các ứng dụng của chúng ta và bán nó.

Trong quy trình thì bước này cần phải được lặp đi lặp lại cho mỗi mục thông tin mà chúng ta xác định là quan trọng, với mỗi bên có thể tận dụng lợi thế của nó nếu nó bị tiếp xúc, và với mỗi lần sử dụng chúng có thể tạo ra các thông tin. Một cách logic, các tài sản thông tin mà chúng ta nhận dạng là quan

trọng sẽ tham gia nhiều hơn từ bước này trở đi. Trong một số trường hợp chúng ta có thể thấy chỉ có một số nhỏ các bên tham gia có khả năng sử dụng thông tin và sau đó chỉ có một số cách nhất định và trong một số trường hợp chúng ta có thể thấy hoàn toàn ngược lại.

3.2.3. Phân tích lỗ hổng

Như thảo luận về các hiểm họa, chúng ta cũng đã nói về các lỗ hổng ở phần trước. Lỗ hổng là điểm yếu mà có thể được sử dụng để làm hại chúng ta. Trong trường hợp phân tích các lỗ hổng trong hệ thống cần bảo vệ, chúng ta đã đặt sự bảo vệ đối với những tài sản thông tin, chúng ta sẽ xem xét cách các quá trình tương tác với các tài sản này thường được thực hiện như thế nào, và chúng ta có thể tấn công để làm tổn thương chúng. Khi chúng ta xem xét về các hiểm họa, chúng ta sử dụng mã nguồn của một công ty phần mềm như là một ví dụ về một mục thông tin quan trọng mà có thể gây hại cho chúng ta nếu nó đã bị rơi vào tay của đối thủ cạnh tranh của chúng ta bằng cách này hay cách khác.

Khi chúng ta xem xét về các lỗ hổng, chúng ta có thể thấy rằng kiểm soát an toàn của chúng ta đối với các mã nguồn quan trọng không phải là rất chặt chẽ, và rằng nó có thể bị truy cập, sao chép, xóa hay chỉnh sửa mà không cần sự ủy quyền nào ngoài việc cần phải truy cập hệ điều hành hay mạng chia sẻ. Điều này có thể khiến cho nó có thể bị một kẻ tấn công đã xâm nhập vào hệ thống sao chép, làm xáo trộn hoặc xóa hoàn toàn các mã nguồn, hoặc có thể làm cho các tập tin dễ bị tổn thương do những thay đổi vô tình trong khi hệ thống đang bảo trì. Chúng ta cũng có thể thấy không có chính sách quy định cách các mã nguồn được xử lý, nơi mà nó nên được lưu trữ, cho dù các bản sao nên tồn tại trong các hệ thống khác hoặc trong các phương tiện thông tin sao lưu, và cách nó nên được bảo vệ nói chung. Kết hợp những vấn đề này có thể gây ra nhiều lỗ hổng mà có thể có tiềm năng dẫn đến vi phạm nghiêm trọng sự an toàn của chúng ta.

3.2.4. Đánh giá rủi ro

Đánh giá rủi ro với ý nghĩa là quyết định những vấn đề mà chúng ta thực sự cần phải quan tâm trong quy trình an toàn hoạt động. Như chúng ta đã

thảo luận, rủi ro xảy ra khi chúng ta có một hiểm họa phù hợp với khả năng dễ bị tổn thương và chỉ xảy ra sau đó. Quay lại với ví dụ về mã nguồn phần mềm của chúng ta, chúng ta đã xác định rằng chúng ta thấy một hiểm họa tiềm năng đối với mã nguồn ứng dụng khi nó bị tiếp xúc trái phép. Hơn nữa chúng ta thấy rằng chúng ta đã có một lỗ hổng trong việc kiểm soát yếu kém các truy cập tới mã nguồn và thiếu một chính sách xác định chính xác cách kiểm soát. Hai vấn đề này kết nối với nhau có thể dẫn đến sự tiếp xúc các thông tin quan trọng của chúng ta từ các đối thủ cạnh tranh hay các kẻ tấn công.

Điều quan trọng cần lưu ý là chúng ta chỉ cần có sự kết nối một hiểm họa với một lỗ hổng thì có thể tạo thành một rủi ro. Nếu tính bí mật của mã nguồn của chúng ta không phải là một vấn đề, ví dụ nếu chúng ta đã tạo ra một dự án mã nguồn mở và mã nguồn là miễn phí thì chúng ta sẽ không có rủi ro trong trường hợp này. Tương tự như thế nếu mã nguồn của chúng ta là đối tượng có các yêu cầu an ninh nghiêm ngặt, cái mà sẽ làm cho nó hầu như không thể được công bố một cách trái phép thì chúng ta cũng sẽ không có rủi ro.

Ở bước này chúng ta sẽ phải:

- Đánh giá các tác động kinh doanh đến tổ chức mà có thể là kết quả từ các lỗi sai về an ninh bảo mật, tính đến hậu quả của việc mất độ tin cậy, tính toàn vẹn và tính sẵn sàng của các tài sản.

- Đánh giá khả năng có thể xảy ra trên thực tế của các lỗi sai về an ninh bảo mật diễn ra trong các mối đe doạ phổ biến, các điểm yếu và các tác động liên quan tới các tài sản này, các phương pháp kiểm soát được thực hiện gần đây.

- Ước lượng mức độ rủi ro.

- Xác định rõ các rủi ro có thể chấp nhận hoặc yêu cầu xử lý theo các tiêu chí chấp nhận rủi ro đã thiết lập.

Lưu ý rằng, quá trình an toàn hoạt động có thể kết thúc với sự đánh giá rủi ro. Có nghĩa là khi sự rủi ro được chấp nhận là đủ thấp. Định nghĩa như vậy sẽ chịu ảnh hưởng lớn bởi mục tiêu và sứ mệnh của hệ thống. Ví dụ, nếu một hệ MT chứa các thành tố được sử dụng cho các hoạt động vô hại như là các trò chơi điện tử thì sự giảm thiểu rủi ro trong quá trình an toàn hoạt động

có thể coi là một thao tác dưới tới hạn. Tuy nhiên, nếu một hệ được dùng cho hoạt động như là kiểm soát vũ khí hay là sự duy trì sự sống thì việc giảm thiểu rủi ro trở nên rất quan trọng.

3.2.5. Áp dụng các biện pháp đối phó

Một khi chúng ta đã phát hiện ra những gì rủi ro có thể xảy ra đối với các thông tin quan trọng của chúng ta, sau đó chúng ta nên đưa ra các biện pháp để giảm thiểu chúng. Các biện pháp đó được đề cập đến trong an toàn hoạt động như các biện pháp đối phó. Như chúng ta đã thảo luận, để tạo thành một rủi ro, chúng ta cần có một bộ phù hợp giữa hiểm họa và lỗ hổng. Khi chúng ta xây dựng một biện pháp đối phó cho một rủi ro cụ thể, chúng ta chỉ cần giảm thiểu hiểm họa hoặc lỗ hổng. Trong trường hợp ví dụ mã nguồn của chúng ta, hiểm họa là việc mã nguồn có thể bị tiếp xúc bởi các đối thủ cạnh tranh hay những kẻ tấn công và lỗ hổng là sự yếu kém trong việc điều khiển an toàn mà chúng ta có thể thiết lập để bảo vệ nó. Trong trường hợp này, không phải là có nhiều vấn đề mà chúng ta có thể thực hiện để bảo vệ trước những hiểm họa của nó mà không thay đổi bản chất của toàn bộ ứng dụng, vì vậy việc chúng ta thực hiện giảm thiểu các hiểm họa thực sự không phải là một bước đi tốt. Tuy nhiên, chúng ta có thể đưa ra biện pháp để giảm thiểu khả năng dễ tổn thương.

Trong trường hợp của ví dụ mã nguồn, chúng ta đã có một lỗ hổng phù hợp với hiểm họa vì sự yếu kém trong kiểm soát việc xử lý của bản thân mã nguồn. Nếu chúng ta thiết lập các biện pháp mạnh mẽ hơn trong việc kiểm soát truy cập tới mã nguồn và cũng đưa ra chính sách với một bộ quy tắc để quy định cách mã nguồn được xử lý, chúng ta sẽ loại bỏ phần lớn lỗ hổng này. Một khi chúng ta đã phá vỡ cặp hiểm họa/lỗ hổng, chúng ta sẽ có khả năng giảm thiểu được một rủi ro nghiêm trọng.

Điều quan trọng cần lưu ý đây là một quá trình lặp đi lặp lại, một khi chúng ta đạt được sự kết thúc vòng lặp, trong mọi trường hợp chúng ta sẽ cần phải đi qua vòng lặp này nhiều hơn một lần để giảm thiểu hoàn toàn bất kỳ vấn đề nào. Mỗi thời điểm chúng ta đi qua vòng lặp, chúng ta sẽ làm như thế dựa trên kiến thức và kinh nghiệm chúng ta đã có từ những nỗ lực giảm thiểu rủi ro trước đây, và chúng ta sẽ có thể điều chỉnh các giải pháp để có một mức

độ bảo mật cao hơn. Ngoài ra, khi có sự thay đổi môi trường và yếu tố mới phát sinh, chúng ta sẽ cần phải xem xét lại quá trình này.

Đối với những người quen thuộc với quy trình quản lý rủi ro, chúng ta có thể nhận thấy thiếu một bước ở bên an toàn hoạt động khi chúng ta so sánh hai quy trình, cụ thể là việc đánh giá sự hiệu quả của các biện pháp đối phó của chúng ta. Tuy nhiên, quá trình này chắc chắn không phải thiết lập cố định và hoàn toàn không có lý do nào để không bao gồm chính thức bước này nếu nó là cần thiết. Trong thực tế chúng ta có thể thấy lợi ích lớn từ việc làm này.

Quy trình an toàn hoạt động gồm năm bước chính. Chúng ta bắt đầu bằng việc xác định những thông tin quan tọng nhất để chúng ta biết được những gì chúng ta cần bảo vệ. Sau đó chúng ta phân tích tình huống để xác định chúng ta có thể phải đối mặt với những hiểm họa và tiếp theo là những lỗ hổng bảo mật tồn tại trong môi trường của chúng ta. Một khi chúng ta biết chúng ta phải đối mặt với những hiểm họa và lỗ hổng nào, chúng ta có thể cố gắng để xác định những rủi ro mà chúng ta có thể gặp phải. Những rủi ro thực sự mà đang hiện hữu là sự kết hợp phù hợp giữa hiểm họa và lỗ hổng. Khi chúng ta biết những rủi ro phải đối mặt, sau đó chúng ta có thể lập kế hoạch các biện pháp đối phó, có thể đưa ra các biện pháp để giảm thiểu các rủi ro.

Ngoài việc sử dụng các quy trình an toàn hoạt động trong các tổ chức thương mại và chính phủ, chúng ta cũng sử dụng các khái niệm bảo mật này trong cuộc sống hàng ngày của chúng ta mặc dù không thể làm như thế một cách chính thức. Chúng ta thường xuyên thực hiện các bước xác định thông tin quan trọng và lập kế hoạch các biện pháp để bảo vệ nó trong quá trình thường ngày của cuộc sống. Riêng với khối lượng thông tin cá nhân của chúng ta di chuyển thông qua một loạt các hệ thống và mạng thì điều này trở nên ngày càng quan trọng để thực hiện các bước bảo vệ nó.

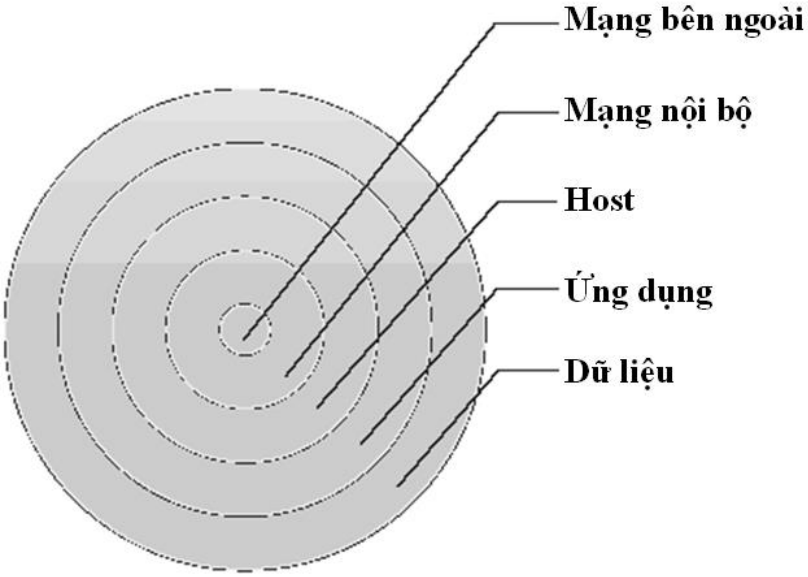
3.3. MÔ HÌNH BẢO VỆ THÔNG TIN THEO CHIỀU SÂU

Trong lĩnh vực quân sự, phòng ngự chiều sâu là một phương cách phòng thủ mà trong đó bên phòng ngự tăng bề dày của tuyến phòng ngự với ý định sẵn sàng nhượng bộ diện tích trận địa để đổi lấy khả năng hấp thụ sức đột phá, hãm dần tốc độ đột phá của đối phương, và cuối cùng chặn mũi đột phá khi đã bị mài mòn. Phòng ngự chiều sâu là một chiến lược chung trong cả

các cuộc diễn tập quân sự và an toàn thông tin. Trong cả hai trường hợp, khái niệm cơ bản về phòng ngự chiều sâu là để xây dựng một biện pháp phòng thủ nhiều lớp, biện pháp này sẽ cho phép chúng ta vẫn có thể gắn kết một biện pháp phòng thủ thành công với một hoặc một số biện pháp bị lỗi.

Khi đảm bảo an toàn thông tin cho một tổ chức, người ta cũng sử dụng mô hình này để thiết lập hệ thống phòng thủ cho hệ thống. Khi thiết kế một hệ thống phòng thủ, chúng ta phải thiết kế sao cho hệ thống đó có cấu trúc tương tự như "củ hành tây". Kẻ tấn công lột một lớp vỏ bên ngoài, sẽ còn rất nhiều lớp vỏ bên trong bảo vệ cho phần lõi của củ hành. Phòng thủ có chiều sâu giúp chúng ta bảo vệ hệ thống của mình bất chấp một hoặc nhiều "lớp" bảo vệ bên ngoài bị xâm hại. Một hệ thống phòng thủ chỉ an toàn khi nào càng đi sâu vào bên trong, kẻ tấn công càng gặp phải nhiều khó khăn, tốn nhiều công sức và dễ bị phát hiện hơn. Một chi tiết cần phải lưu ý là không có bất kì lớp bảo vệ nào đủ sức chống lại mọi loại tấn công, sức mạnh của hệ thống phòng thủ là sự kết hợp sức mạnh của từng lớp bảo vệ, mỗi lớp thực thi nhiệm vụ của riêng mình, nghĩa là ngăn cản và phòng ngừa một loại tấn công cụ thể nhất định.

Trong hình 3.2 chúng ta có thể thấy một ví dụ về các lớp mà chúng ta có thể muốn đưa vào để bảo vệ nguồn tài nguyên của chúng ta từ quan điểm logic, ít nhất chúng ta sẽ muốn bảo vệ các lớp mạng bên ngoài, mạng nội bộ, các host, ứng dụng và dữ liệu. Do thực hiện tốt việc phòng thủ ở mỗi lớp nên khả năng để thành công trong việc thâm nhập sâu vào mạng lưới của chúng ta và tấn công trực tiếp các tài nguyên của chúng ta là rất khó.



Hình 3.2 Phòng thủ chiều sâu

Một trong những điều cần lưu ý khi lập kế hoạch cho một chiến lược phòng thủ chiều sâu là không phải vấn đề chúng ta đưa ra bao nhiêu lớp hay có bao nhiêu biện pháp phòng thủ tại mỗi lớp, chúng ta sẽ không thể ngăn cản tất cả các kẻ tấn công trong một khoảng thời gian không xác định và đây cũng không phải là mục tiêu cuối cùng của phòng thủ chiều sâu trong thiết lập an toàn thông tin. Mục đích ở đây là để đưa ra đủ các biện pháp phòng ngự ở giữa các tài nguyên thật sự quan trọng và kẻ tấn công để chúng ta sẽ có cả hai thông báo rằng một tấn công đang được tiến hành và bản thân chúng ta cũng có đủ thời gian để thực hiện các biện pháp tích cực hơn ngăn các cuộc tấn công đạt được thành công.

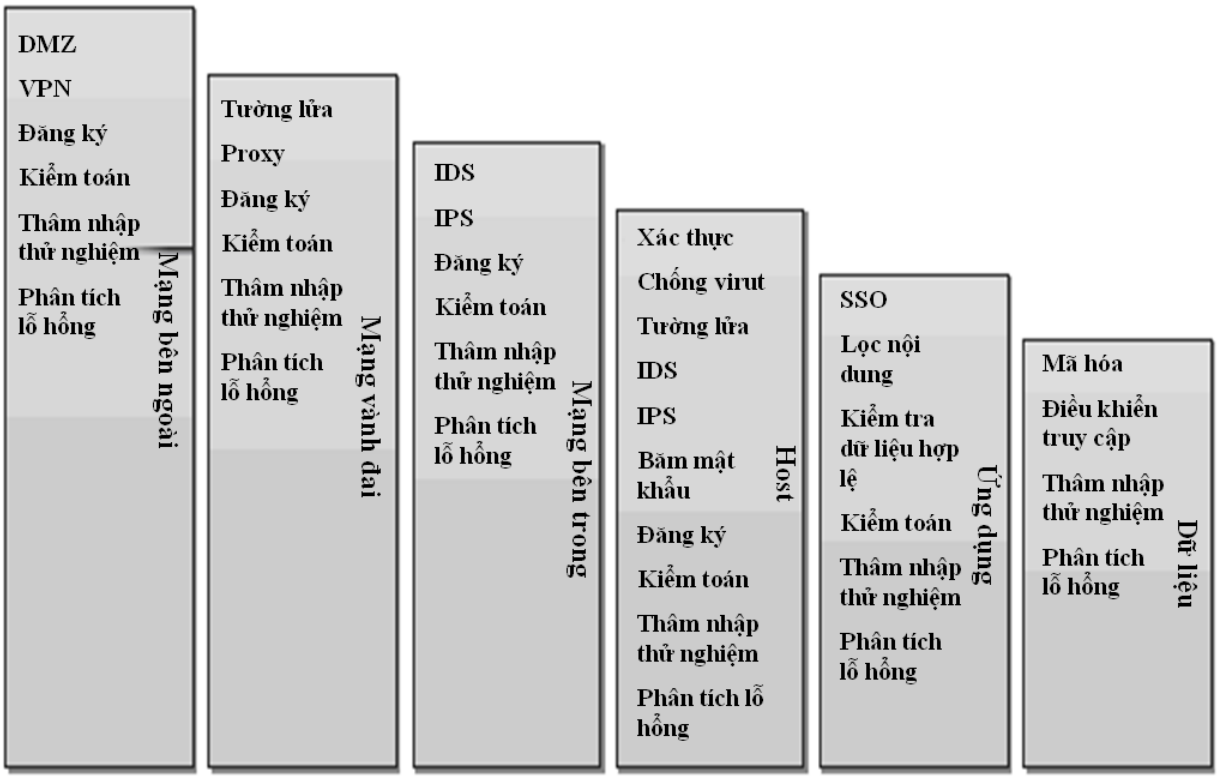
Chúng ta có thể thấy chính xác một chiến lược như vậy trong bản phát hành rạp chiếu của bộ phim Người dơi, "kỵ sĩ bong đêm", năm 2008. Công ty sản xuất bộ phim, Warner Bros, đã dành sáu tháng để phát triển một chiến lược phòng vệ nhiều lớp để giữ cho bộ phim không bị vi phạm bản quyền và không được xuất hiện trên các mạng chia sẻ tập tin càng lâu càng tốt. Những biện pháp này bao gồm một hệ thống giám sát những người có quyền truy cập vào các bản sao của bộ phim tại mọi thời điểm, vận chuyển các cuộn phim đã được tách thành các phần riêng biệt tới rạp chiếu để giữ cho toàn bộ bộ phim không bị đánh cắp trong khi vận chuyển, giám sát các rạp chiếu với thiết bị nhìn ban đêm để xem có ai cố gắng ghi lại bộ phim trong rạp hay không và các biện pháp khác. Mặc dù tất cả thời gian và tài nguyên được sử dụng để

ngăn chặn việc vi phạm bản quyền của bộ phim, nhưng bộ phim đã xuất hiện trên một mạng chia sẻ tập tin 38 giờ sau khi bộ phim được phát hành. Đối với Warner Bros, điều này đã được coi là thành công vì công ty đã có thể ngăn chặn việc bộ phim bị vi phạm bản quyền trong một khoảng thời gian đủ lâu để doanh thu tuần đầu công chiếu không bị ảnh hưởng gì đáng kể.

Khi chúng ta xem xét các lớp mà có thể thiết lập chiến lược phòng thủ theo chiều sâu, chúng ta sẽ thấy rằng chúng có thể được thay đổi tùy thuộc vào tình hình và môi trường cụ thể mà chúng ta đang bảo vệ. Như chúng ta đã thảo luận, từ góc độ an toàn thông tin logic chặt chẽ, chúng ta sẽ muốn xem xét các lớp mạng bên ngoài, mạng vành đai, mạng nội bộ, host – máy chủ, ứng dụng, lớp dữ liệu và nhân tố con người như là các khu vực để đặt hệ thống phòng thủ của mình. Chúng ta có thể tăng thêm độ phức tạp vào trong mô hình phòng thủ bằng cách thêm một số lớp quan trọng khác như các phòng thủ vật lý và nhiều lớp khác nữa.

Các lớp cơ bản tạo thành một hệ thống phòng thủ theo chiều sâu: mạng bên ngoài, mạng vành đai, mạng nội bộ, host, ứng dụng, dữ liệu và nhân tố con người.

Như chúng ta có thể thấy ở hình 3.3, liệt kê một số các biện pháp phòng thủ chúng ta có thể sử dụng đối với mỗi lớp mà chúng ta đã thảo luận. Trong một số trường hợp chúng ta có thể thấy một biện pháp phòng thủ được liệt kê trong nhiều lớp vì nó có thể được áp dụng trong nhiều khu vực. Một ví dụ minh họa tốt cho vấn đề này là một cuộc thâm nhập thử nghiệm. Thâm nhập thử nghiệm là một phương pháp tìm kiếm các lỗ hổng trong hệ thống an ninh của chúng ta bằng việc sử dụng một số phương pháp giống như một kẻ tấn công sẽ sử dụng nhằm phá vỡ hệ thống của chúng ta, và là một chiến thuật mà chúng ta có thể muốn sử dụng tại tất cả các lớp phòng thủ của mình.



Hình 3.3 Các phương pháp phòng ngự trong từng lớp

Ở đây chúng ta thấy có các phương pháp phòng ngự như: DMZ, VPN, logging, kiểm toán, thâm nhập thử nghiệm, phân tích điểm yếu, tường lửa, Proxy, Statefull packet inspection, IDS, IPS, xác thực, chống virus, băm mật khẩu, đăng nhập một lần, lọc nội dung, kiểm tra tính hợp lệ của dữ liệu, mã hóa, kiểm soát truy cập, sao lưu. Đây chỉ là một số phương pháp kỹ thuật chúng ta có thể áp dụng để bảo vệ hệ thống của mình, ngoài ra còn có các phương pháp khác như bảo vệ vật lý, giáo dục người dùng trong hệ thống, cưỡng chế bằng pháp luật, quy tắc của tổ chức. Những phương pháp này sẽ được nói sâu hơn trong các phần tiếp theo.

3.4. CÁC PHƯƠNG PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

Tất cả các giải pháp bảo đảm ATTT phải giúp đạt đến các mục đích sau đây:

- Cảnh báo sự xuất hiện các hiểm họa
- Làm rõ các hướng tiềm năng và mức độ nguy hiểm của hiểm họa phá vỡ ATTT
- Phát hiện các dấu vết thực tế phá vỡ ATTT
- Ngăn chặn sự hoá giải, rò rỉ và tiếp cận trái phép tới TT

- Triệt tiêu hoặc làm giảm mức độ thiệt hại do phá vỡ ATTT và do việc TT bị lọt vào tay tin tặc

Chúng ta sẽ xem xét một số phương pháp đảm bảo an toàn thông tin:

3.4.1. Phương pháp đảm bảo an toàn vật lý

Một trong những cách đơn giản nhất nhưng hiệu quả nhất để bảo vệ tài sản thông tin là sử dụng điều khiển vật lý. Nó gồm một chuỗi các biện pháp, chẳng hạn như khóa giấy tờ nhạy cảm trong một ngăn kéo cuối mỗi ngày làm việc tới các giải pháp phức tạp hơn như tích hợp hệ thống kiểm soát cửa với camera truyền hình mạch đóng (Closed Circuit Television Cameras - CCTV).

Phương pháp sử dụng sẽ phụ thuộc vào ngân sách, kích thước, loại hình kinh doanh và sự nhạy cảm của thông tin.

An toàn vật lý phần lớn liên quan đến sự bảo vệ của ba loại tài sản chính: con người, trang thiết bị và dữ liệu. Tất nhiên trọng tâm của chúng ta là bảo vệ con người. Con người là yếu tố khó khăn để thay thế hơn trang thiết bị và dữ liệu một cách đáng kể, đặc biệt khi họ có kinh nghiệm trong lĩnh vực cụ thể và đã quen thuộc với các quy trình và nhiệm vụ mà họ thực hiện.

Thứ tự ưu tiên tiếp theo là bảo vệ dữ liệu. Nếu chúng ta lập kế hoạch một cách đầy đủ và có sự chuẩn bị trước, chúng ta có thể dễ dàng bảo vệ dữ liệu trước bất kỳ thảm họa mà không phải là trên phạm vi toàn cầu. Nếu chúng ta không chuẩn bị cho vấn đề này, chúng ta có thể dễ dàng bị mất dữ liệu của mình vĩnh viễn.

Cuối cùng, chúng ta bảo vệ thiết bị và các cơ sở chứa đựng nó. Điều này có vẻ là một tập rất quan trọng các đối tượng mà chúng ta có thể muốn gán một mức độ ưu tiên cao hơn khi lập kế hoạch các biện pháp an toàn vật lý. Tuy nhiên điều này nói chung không phải là trường hợp đặc biệt, ngoài một số tình huống, hầu hết trong số đó thực sự xoay quanh việc đảm bảo an toàn con người. Trong thế giới công nghệ, nhiều phần cứng chúng ta sử dụng là tương đối phổ biến và dễ dàng thay thế. Ngay cả nếu chúng ta đang sử dụng nhiều thiết bị chuyên dụng, chúng ta thường có thể thay thế nó trong một vài ngày hay một vài tuần.

Các hiểm họa mà chúng ta phải đối mặt khi chúng ta xem xét vấn đề an toàn vật lý thường rơi vào một số loại chính như:

- Nhiệt độ quá cao
- Các chất khí
- Các chất lỏng
- Sinh vật sống
- Các vật phóng đi tự động như tên lửa…
- Các chuyển động
- Các bất thường về năng lượng
- Con người
- Các chất độc
- Khói và lửa

Bảy loại đầu tiên trong số các loại hiểm họa này được xác định bởi Donn Parker trong sách Cuộc chiến chống tội phạm máy tính.

Chúng ta có thể sử dụng các công cụ để thực hiện phương pháp này như: các tín hiệu báo động điện tử (máy báo cháy, máy báo sự thay đổi bất thường về nhiệt độ, máy báo động đất…), các loại camera theo dõi, các loại khoá cửa, các lưới chắn cửa sổ, hàng rào, nhân viên bảo vệ, chó bảo vệ, các biển cảnh báo, các thiết bị để duy trì nhiệt độ thích hợp, cân bằng độ ẩm, máy phát điện …

Trong nhiều trường hợp, các doanh nghiệp lớn có cơ sở dữ liệu, máy chủ tập tin và máy trạm có chứa thông tin khách hàng, dự báo bán hàng, tài liệu chiến lược kinh doanh, sơ đồ mạng, và một lượng lớn dữ liệu khác mà họ không muốn công khai hoặc rơi vào tay của đối thủ cạnh tranh. Nếu bảo mật vật lý tại địa điểm có dữ liệu đó là yếu, kẻ tấn công có thể chỉ đơn giản là đi vào tòa nhà và ăn cắp một máy tính xách tay, tài liệu giấy, ổ đĩa flash hoặc đĩa từ một máy chủ và phải đi bộ ra với dữ liệu.

Chúng ta cũng cần phải nhận thức về các khu vực có thể không thể bảo vệ vật lý và cần phải hạn chế các dữ liệu rời khỏi không gian đã được bảo vệ. Trong một tòa nhà văn phòng, chúng ta có một diện tích khá hạn chế để bảo vệ và chúng ta có thể áp dụng nhiều hơn các lớp bảo vệ vật lý đến các khu vực quan trọng, chẳng hạn như các trung tâm dữ liệu trong đó có các máy chủ. Nếu dữ liệu nhạy cảm rời khỏi khu vực này, chúng ta rất hạn chế trong việc chúng ta có thể làm những gì để bảo vệ vật lý cho nó, ngoài việc sử dụng mã hóa (sẽ được trình bày trong phần sau). Một số biện pháp nữa mà chúng ta

cần nói đến ở đây đó là việc sao lưu dữ liệu, loại bỏ các dữ liệu nhạy cảm khi không cần dùng nữa (làm cho dữ liệu không thể truy cập khi không còn cần thiết: cắt nhỏ một tập giấy có chứa dữ liệu nhạy cảm trước khi vất đi)…

Theo các nguyên tắc phòng ngự theo chiều sâu, càng nhiều lớp an toàn vật lý mà chúng ta đưa ra thì chúng ta sẽ càng an toàn.

Một điều quan trọng khi thực hiện an toàn vật lý là chỉ thiết lập an toàn sao cho phù hợp với giá trị của tài sản mà chúng ta đang bảo vệ. Nếu chúng ta có một nhà kho trống rỗng, thì không cần phải đưa khóa bảo mật cao, hệ thống báo động và bảo vệ vũ trang. Tương tự như vậy, nếu chúng ta có một ngôi nhà đầy đủ các thiết bị điện tử và máy tính đắt tiền, thì thật vô nghĩa khi trang bị cho nó ổ khóa rẻ tiền và loại bỏ toàn bộ hệ thống báo động.

Sau đây là một loạt các bước thực tế ta có thể làm để giúp bảo vệ an ninh vật lý cho các hệ thống của mình:

• Khảo sát các tòa nhà và giải quyết các vấn đề rõ ràng. Đặt ổ khóa bền vững trên cửa ra vào, lắp đặt các cửa sổ tốt, và chắc chắn rằng mọi người ngừng hoạt động vào cuối ngày.

• Đặt máy chủ và các thiết bị chuyên môn quan trọng khác trong phòng chuyên dụng với khóa cửa bên trong và không có cửa sổ.

• Cài đặt hệ thống điều hòa không khí và phát hiện lửa thích hợp trong các phòng đặc biệt.

• Tránh để các thiết bị quan trọng gần lỗ thông hơi, đường ống, nhà bếp, nhà vệ sinh, bộ tản nhiệt và các mối nguy hiểm tương tự khác.

• Tắt màn hình vào ban đêm (điều này ngăn cản việc ánh sáng làm lộ).

• Giữ một danh sách (hoặc kiểm kê tài sản) của tất cả các hệ thống, bộ nhớ, bộ xử lý, các số seri, các địa điểm và ngày mua.

• Đặt các nhãn vĩnh viễn trên thiết bị có giá trị. Có lẽ cố gắng đánh dấu thiết bị bằng tia cực tím - điều này có thể giúp tìm lại các thiết bị bị đánh cắp.

• Giữ các bản sao lưu các thông tin cách xa khỏi các hệ thống nguồn, và nếu có thể tắt trang web.

• Trong khu vực chia sẻ, các khu vực công cộng hoặc mở (ví dụ như phòng tiếp khách) sử dụng khóa Kensington (cáp) để gắn các thiết bị có giá trị với bàn.

• Giảm thiểu số lượng giấy và các thông tin nhạy cảm để lại trên bàn làm việc. Khóa tài liệu trong tủ (thiết lập chính sách “bàn sạch" nếu có thể). Điều này không chỉ tốt cho an ninh: nếu có hỏa hoạn, nước được sử dụng để kiểm soát nó có thể gây ra thiệt hại lớn cho các giấy tờ, đôi khi chính những giấy tờ này sẽ làm đám cháy lan nhanh và gây ra thiệt hại lớn. Ngoài ra, hãy nhớ rằng thậm chí bị thiệt hại nhỏ với một cửa sổ vào một ngày lộng gió có thể gây ra việc mất giấy tờ vì bị thổi bay xung quanh.

• Nếu công ty bao gồm khoảng hơn 15-20 người, nên sử dụng biển hiệu khách truy cập và khuyến khích nhân viên kiểm tra những khách không có người đi kèm.

• Hộ tống tất cả các khách - không để cho họ đi lang thang xung quanh mà không có sự giám sát.

• Duy trì sổ nhật ký khách truy cập và thời gian khi khách truy cập vào và rời trụ sở. Duy trì một sổ nhật ký khác cho việc vào ra đối với khu vực nhạy cảm, chẳng hạn như phòng máy tính.

• Xem xét các camera quan sát trong lĩnh vực CNTT quan trọng (ví dụ như phòng máy chủ) và các khu vực tiếp tân.

• Thực hiện việc bảo hiểm thích hợp cho tổ chức ngay cả khi đó là một tổ chức nhỏ.

3.4.2. Phương pháp mã hóa

Đây là phương pháp dùng mật mã để che giấu (mã hoá) TT. Phương pháp này rất hiệu quả và được áp dụng rộng rãi trong các hệ thống TT – VT hiện nay. Đặc biệt khi TT được truyền đi khoảng cách xa thì đây là phương pháp an toàn duy nhất để bảo vệ TT. Thiết bị thực hiện mã hoá thông thường sử dụng là các chương trình phần mềm (hoặc các thiết bị – chương trình).

Các phương pháp mật mã BVTT bảo đảm mã hoá và giải mã các dữ liệu mật (tính bí mật), và cũng được sử dụng để khẳng định tính chân thực (xác thực) nguồn dữ liệu và kiểm soát toàn vẹn của dữ liệu (tính toàn vẹn). Các phương pháp mật mã là yếu tố bắt buộc của các HAT, nhưng nó có ý nghĩa đặc biệt với việc phát triển của các hệ phân tán và các mạng mở, mà ở đó ta không thể duy trì được sự bảo vệ vật lý các kênh liên lạc.

3.4.2.1. Lịch sử phát triển

Lịch sử đối với việc sử dụng mật mã là rất phong phú, với một số ví dụ cổ xưa nhất được sử dụng bởi những người Hy Lạp và La Mã cổ đại. Thông tin được ẩn bởi một loạt các mã, xăm mình trên các đầu cạo của sứ giả và sau đó nuôi tóc, và vô số các phương pháp khác. Để đề cập đến lịch sử tồn tại và phát triển của mật mã cần rất nhiều thời lượng và thực sự đã có rất nhiều sách viết về đề tài này, vì thế chúng ta sẽ đi chỉ đi lướt qua một vài điểm nổi bật.

a) Mật mã Caesar

Mật mã Caesar là một ví dụ điển hình của mật mã cổ đại và được cho là đã được sử dụng bởi Julius Caesar. Mật mã Caesar liên quan đến việc dịch chuyển mỗi chữ cái của thông điệp rõ đi một số lượng nhất định của các chữ cái, chuyển ba vị trí như thể hiện trong hình 3.4. Các bản mã có thể được giải mã bằng cách áp dụng cùng một số thay đổi theo hướng ngược lại. Kiểu mã hóa này được biết đến như một mật mã thay thế, do sự thay thế của một chữ cho một chữ khác một cách nhất quán.

Một sự thay đổi gần đây của các mật mã Caesar có thể được tìm thấy trong mật mã ROT13. ROT13 sử dụng cơ chế tương tự như thuật toán mã hóa Caesar nhưng di chuyển mỗi chữ 13 vị trí về phía trước. Sự tiện lợi của việc di chuyển 13 vị trí nằm ở thực tế việc áp dụng một đợt mã hóa với ROT13 cũng có chức năng như giải mã, hai lần quay như thế sẽ trở lại vị trí bắt đầu bản gốc trong bảng chữ cái. Tiện ích để thực hiện ROT13 có thể được tìm thấy trong các thiết lập cơ bản của các công cụ mà đi kèm với nhiều hệ điều hành Linux và UNIX.

S	E	C	R	E	T	M	E	S	S	A	G	E
V	H	F	U	H	W	P	H	V	V	D	J	H

Hình 3.4 Mật mã Caesar

b) Máy mật mã

Trước khi máy tính hiện đại ra đời, các máy móc để thực hiện việc mã hóa đơn giản đã tồn tại. Ban đầu, các thiết bị như vậy là máy móc cơ khí đơn giản, nhưng khi công nghệ phát triển, chúng ta bắt đầu nhìn thấy sự xuất hiện của các thiết bị điện tử và các hệ thống phức tạp hơn.

Disk Jefferson, phát minh bởi Thomas Jefferson năm 1795, là một cỗ máy mã hóa hoàn toàn cơ khí. Nó bao gồm một loạt các ổ đĩa, từng được đánh dấu bằng các chữ cái a đến z xung quanh cạnh của nó, như thể hiện trong hình 3.5.

Hình 3.5 Jefferson Disk

Trên mỗi đĩa, các chữ cái được sắp xếp theo một thứ tự khác nhau, mỗi đĩa cũng được đánh dấu bằng một định danh duy nhất để tạo điều kiện sắp xếp chúng theo một thứ tự cụ thể. Các thiết bị được xây dựng bởi Jefferson chứa 36 đĩa, mỗi đĩa đại diện cho một ký tự trong bản tin. Để mã hóa một bản tin, chúng ta sẽ sắp xếp các chữ trong một hàng trên toàn bộ đĩa để tạo ra các thông báo trong bản rõ, như thể hiện trong hàng A của Hình 3.6, và sau đó chọn một hàng các chữ khác để sử dụng như các bản mã, như thể hiện trong hàng B.

	A	F	T	K	D	A	R	X	Z	X	Z	X
	B	K	O	E	E	Q	U	T	Y	U	I	A
	P	I	P	Q	U	W	Z	W	V	Y	U	C
	I	L	Y	G	L	B	C	V	D	Z	P	R
	U	Q	G	B	M	K	W	B	T	W	F	U
	L	A	L	D	A	R	N	U	E	P	E	P
	H	V	C	O	Z	P	M	N	W	S	L	Q
A	M	E	E	T	I	N	G	I	S	A	G	O
	X	C	H	W	V	U	O	S	M	O	Y	J
	O	U	Z	N	Y	H	B	E	X	T	D	B
	E	Z	A	P	N	F	Q	M	U	B	A	G
	V	J	U	X	F	J	I	C	P	E	N	F
	Y	G	R	L	Q	E	A	L	L	K	S	W
	C	Y	M	V	P	O	P	G	K	C	O	D
	G	M	K	A	B	G	S	A	I		H	V
	X	W	N	M	W	I	F	D	F	N	R	L
	K	D	F	U	J	D	T	R	B	D	L	M
	F	O	W	H	R	M	J	Q	H	G	X	E
	S	X	N	I	S	T	E	K	O	R	M	Y
	D	B	D	Y	G	V	Y	F	Q	V	T	H
	R	H	Q	Z	K	S	L	J	A	I	J	S
B	T	N	J	R	O	C	H	O	N	L	Q	I
	Q	P	I	F	C	X	K	P	G	F	V	N
	J	R	B	S	X	Z	D	Z	C	M	W	K
	W	S	V	J	H	L	V	H	J	J	B	Z
	N	T	G	C	P	Y	X	Y	R	Q	C	T

Hình 3.6 Hiển thị Jefferson Disk

Khóa của hình thức mật mã này là nằm ở thứ tự của các ổ đĩa. Miễn là các thiết bị mã hóa và giải mã có đĩa với các chữ theo cùng một thứ tự, và bản thân các đĩa cũng có cùng thứ tự, tất cả công việc mà chúng ta cần phải làm để giải mã thông điệp là phải xếp theo hàng các ổ đĩa với cùng một thứ tự như bản mã, và sau đó nhìn qua các hàng để tìm bản tin gốc. Tất nhiên, Đây chỉ là một phiên bản phức tạp hơn của một mật mã thay thế, có thể thực hiện thông qua việc sử dụng một sự hỗ trợ cơ khí.

Một ví dụ phức tạp hơn của một máy mật mã có thể được tìm thấy trong máy Enigma do Đức chế tạo. Enigma được tạo ra bởi Arthur Scherbius

vào năm 1923 và đã được sử dụng để đảm bảo thông tin liên lạc của Đức trong Thế chiến II. Trong thực tế, đã có nhiều mô hình của máy Enigma, và một loạt các phụ kiện và tiện ích mà có thể được đính kèm với chúng. Máy cụ thể trong hình 3.7 là một mô hình sau đó của Enigma, được phát triển vào năm 1932.

Hình 3.7 Máy mã Enigma của Đức

Bình thường trông Enigma như một chiếc máy chữ kì quái nhét trong một cái hộp gỗ nhưng cấu trúc của nó lại vô cùng phức tạp. Enigma được cấu thành bởi ba bộ phận chính: một bàn phím để nhập bức điện, một bộ mã hóa để biến chữ cái vừa nhập thành mật mã, và một bảng gồm những bóng đèn nhấp nháy thể hiện những chữ cái được mã hóa đó. Bộ phận mã hóa gồm các bánh xe quay chữ, được gọi là cánh quạt, có thể đổi chỗ cho nhau. Dưới bàn phím là bảng điện chứa các sợi cáp. Mỗi cánh với 26 chữ cái và 26 tiếp xúc điện trên chúng, tương tự như trong khái niệm chung với đĩa Jefferson. Để bổ sung thêm khả năng tùy biến, một số mô hình cũng đã có một bảng vá lỗi, cho phép một số hoặc tất cả các chữ cái được trao đổi bằng cách cắm cáp vào các vị trí khác nhau. Trên mỗi cánh quạt, vòng có chứa các chữ cái trong bảng

chữ cái cũng có thể được luân chuyển một cách độc lập các tiếp xúc điện, để thay đổi mối quan hệ giữa các ký tự được lựa chọn và các ký tự đầu ra.

Khi một phím được nhấn trên bàn phím, một hoặc nhiều hơn các cánh quạt sẽ xoay vật lý, tùy thuộc vào cấu hình của nó, do đó thay đổi hướng của các tiếp xúc điện giữa các cánh quạt. Dòng điện sẽ chảy qua toàn bộ loạt các ổ đĩa, và sau đó trở lại thông qua chúng một lần nữa để tới đĩa gốc. Tương đương với ký tự sẽ sáng trên hàng loạt các ký tự trên bàn phím và được ghi lại. Để cho hai máy Enigma giao tiếp, chúng cần phải được cấu hình giống nhau.

3.4.2.2. Các công cụ mật mã hiện đại

Mặc dù hệ thống mật mã điện rất hiệu quả đã tồn tại, chẳng hạn như của Enigma cho phép các giải pháp truyền thông an toàn cao trong một khoảng thời gian, sự ra đời của hệ thống máy tính với sự gia tăng liên tục về sức mạnh và độ phức tạp khiến cho các hệ thống này lỗi thời. Các hệ thống này vẫn chủ yếu phụ thuộc vào nguyên tắc an toàn đóng (sự bí mật về thuật toán mã hóa) để bảo vệ các dữ liệu mà chúng xử lý.

Để thực sự có thể sử dụng thuật toán mã hóa mở, công nghệ mới được phát triển phụ thuộc vào các bài toán khó, đôi khi được gọi là các bài toán một chiều. Các vấn đề một chiều nói chung là dễ thực hiện theo một hướng nhưng rất khó để thực hiện theo một hướng khác. Phân tích thừa số của các số rất lớn là một ví dụ về một vấn đề một chiều. Các vấn đề như vậy là cơ sở của nhiều hệ thống mã hóa hiện đại. Chúng ta sẽ xem xét cụ thể các thuật toán mã hóa.

a) Mật mã khóa đối xứng

Mật mã khóa đối xứng, còn được gọi là mật mã khóa bí mật, sử dụng một khóa duy nhất cho cả việc mã hóa bản rõ và giải mã bản mã. Khóa chính phải được chia sẻ giữa người gửi và người nhận, và quá trình này, được gọi là trao đổi khóa, tạo thành một chủ đề con hoàn chỉnh của mật mã. Chúng ta sẽ thảo luận về quá trình trao đổi khóa sâu hơn ở các phần sau trong chương này. Đối xứng trong mật mã khóa đối xứng có nghĩa là sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã.

Một trong những điểm yếu chính của mật mã khóa đối xứng nằm trong việc sử dụng một khóa. Nếu khóa bị tiếp xúc bởi người khác ngoài người gửi

và người nhận, nó có thể cho phép một kẻ tấn công người mà đã tìm cách đánh chặn để giải mã các thông điệp hoặc tệ hơn nữa là để giải mã thông điệp, thay đổi nó, sau đó mã hóa nó một lần nữa và gửi nó cho người nhận thay cho các thông điệp ban đầu. Trong trường hợp này, mật mã khóa đối xứng chỉ cung cấp tính bảo mật và không cung cấp tính toàn vẹn, bởi chúng ta sẽ không biết được rằng thông điệp trong ví dụ trên đã bị thay đổi.

Mật mã khóa đối xứng chia thành hai loại chính: mã khối và mã dòng. Một thuật toán mã hóa khối có một số định trước của các bit, được biết đến như là một khối, trong thông điệp rõ và mã hóa khối đó. Khối thường bao gồm 64 bit nhưng có thể lớn hơn hoặc nhỏ hơn tùy thuộc vào các thuật toán cụ thể được sử dụng và các chế độ khác nhau, trong đó các thuật toán có thể có khả năng hoạt động. Một mật mã dòng mã hóa các bit của thông điệp rõ, 1 bit tại một thời điểm. Ta cũng có thể sử dụng một thuật toán mã hóa khối để hoạt động như một mật mã dòng bằng cách thiết lập kích thước khối là 1 bit.

Đa số các thuật toán mã hóa được sử dụng hiện nay là mã khối. Mặc dù mã khối thường chậm hơn so với thuật toán mã hóa dòng nhưng chúng có xu hướng hiệu quả hơn. Kể từ khi mật mã khối hoạt động trên các khối lớn hơn của các thông báo tại một thời điểm, chúng có xu hướng được nhiều nguồn lực chuyên sâu và phức tạp hơn để thực hiện trong phần cứng hay phần mềm. Mật mã khối cũng nhạy cảm hơn với những sai sót trong quá trình mã hóa như chúng đang làm việc với nhiều dữ liệu hơn. Một lỗi trong quá trình mã hóa của một thuật toán mã hóa khối có thể làm cho không sử dụng được một phân đoạn lớn hơn của dữ liệu hơn so với những gì chúng ta sẽ tìm thấy trong một mật mã dòng, bởi mật mã dòng sẽ chỉ được làm việc với 1 bit cụ thể.

Nói chung, một số chế độ mã khối có thể được sử dụng cùng với một thuật toán dựa trên mã hóa khối để phát hiện và bù đắp cho các lỗi như vậy. Chúng ta có thể thấy chế độ làm việc như vậy trong việc sử dụng với các thuật toán như chuẩn mã hóa dữ liệu (DES) và tiêu chuẩn mã hóa tiên tiến (AES - Advanced Encryption Standard), và chúng ta sẽ xem xét một số chế độ này trong phần tiếp theo khi chúng ta nói về các thuật toán sử dụng chúng.

Thông thường, mật mã khối là tốt hơn để sử dụng trong trường hợp kích thước của thông điệp là cố định hoặc được biết trước, chẳng hạn như khi chúng ta đang mã hóa một tập tin hoặc kích thước thông điệp được cung cấp

trong tiêu đề của giao thức. Mật mã dòng thường tốt hơn để sử dụng trong những trường hợp mà chúng ta có dữ liệu có kích cỡ không rõ hoặc dữ liệu trong một dòng liên tục, chẳng hạn như chúng ta có thể nhìn thấy di chuyển qua mạng.

- Các thuật toán mã hóa đối xứng chính

Có một số thuật toán mã hoá đối xứng được phổ biến hơn, trong số này, DES, 3DES và AES, đang hoặc đã đang được sử dụng thường xuyên bởi chính phủ Hoa Kỳ và những tổ chức khác như các thuật toán chuẩn để bảo vệ dữ liệu nhạy cảm.

DES đầu tiên đưa vào sử dụng vào năm 1976 tại Hoa Kỳ và từ đó đã được sử dụng bởi nhiều tổ chức trên toàn cầu. DES là một thuật toán mã hóa khối dựa trên mật mã khóa đối xứng và sử dụng một khóa 56-bit. Mặc dù DES được coi là rất an toàn cho một khoảng thời gian, nhưng nó đã không còn được coi là như vậy. Trong năm 1999, một dự án tính toán phân tán đã được đưa ra để phá vỡ một khóa DES bằng cách kiểm tra các khoá có thể trong toàn bộ không gian khoá, và dự án thành công với việc làm như vậy trong một khoảng thời gian ít hơn 22 giờ. Điểm yếu này mang lại bởi chiều dài khóa ngắn và đã được bù đắp trong một khoảng thời gian sau thông qua việc sử dụng 3DES, mà chỉ đơn giản là DES được sử dụng để mã hóa mỗi khối ba lần, mỗi lần với một khóa khác nhau. DES có thể hoạt động trong một số chế độ khối khác nhau, bao gồm chế độ liên kết khối mã (Cipher Block Chaining - CBC), chế độ quyển mã điện tử (Electronic Code Book - ECB), chế độ phản hồi mã (Cipher Feedback - CFB), chế độ phản hồi đầu ra (Output Feedback - OFB), và chế độ đếm (Counter Mode - CTR). Mỗi chế độ thay đổi cách các chức năng mã hóa và cách các lỗi được xử lý.

AES được sử dụng bởi chính phủ Mỹ, và một số tổ chức khác, và nó là sự thay thế cho DES - thuật toán mã hóa tiêu chuẩn cho chính phủ liên bang Hoa Kỳ. AES sử dụng ba thuật toán mã hóa khác nhau: một với một khóa 128-bit, một với một khóa 192 bit, và một với một khóa 256 bit, tất cả đều có khối dữ liệu đầu vào chiều dài 128 bit. Một loạt các cuộc tấn công đã cố gắng chống phá AES, hầu hết trong số họ chống phá mã hóa bằng cách sử dụng khóa 128-bit, và hầu hết trong số đó không thành công, thành công một phần, hoặc hoàn toàn đáng ngờ. Tại thời điểm năm 2011, chính phủ Mỹ vẫn coi

AES là an toàn. AES có cùng các chế độ khối mà DES sử dụng và cũng bao gồm các chế độ khác như chế độ XEX-based Tweaked CodeBook (TCB).

Có một số lượng lớn các mã khối đối xứng nổi tiếng khác, trong đó có Twofish, Serpent, Blowfish, CAST5, RC6, và IDEA, cũng như các thuật toán mã hóa dòng như RC4, Oryx, và SEAL.

Ưu điểm chính của mã hoá đối xứng là tác động nhanh và đơn giản. Còn nhược điểm lớn ở đây là, khoá mật phải được cả người gửi và người nhận biết trước. Điều này làm phức tạp đáng kể trong việc quy ước và phân phối khoá giữa những người dùng. Về bản chất, trong các mạng mở khi đó cần phải duy trì một kênh an toàn vật lý để trao đổi khoá. Chính nhược điểm lớn này đã dẫn tới thiết kế một phương pháp mã hoá mới – mã hoá với khoá công khai hay là mật mã phi đối xứng.

b) Mật mã khóa bất đối xứng

Mặc dù mật mã khóa đối xứng chỉ sử dụng có một khóa, mã hóa khóa phi đối xứng, còn được gọi là mật mã khóa công khai, sử dụng hai khóa: một khóa công khai và một khóa riêng. Khóa công khai được sử dụng để mã hóa dữ liệu được gửi từ người gửi đến người nhận và được chia sẻ với tất cả mọi người. Chúng ta thấy khóa công khai được chứa trong chữ ký thư điện tử, đăng trên các máy chủ mà tồn tại đặc biệt để lưu trữ khóa công khai, được đăng trên các trang Web, và hiển thị theo một số cách khác. Khóa riêng được sử dụng để giải mã dữ liệu mà đến người nhận cuối và được bảo vệ rất cẩn thận bởi người nhận. Các thao tác toán học phức tạp được sử dụng để tạo ra các khóa riêng và khóa công khai. Hiện nay các thao tác này có đủ độ khó để các phương tiện không thể thực hiện việc tính ngược các khóa riêng từ khóa công khai. Mật mã khóa bất đối xứng lần đầu tiên được mô tả bởi Martin Hellman và Whitfield Diffie trong bài báo năm 1976 của họ, "Hướng mới trong mật mã".

Ưu điểm chính của mã hóa khóa bất đối xứng hơn mật mã khóa đối xứng là không cần thiết phải phân phối khóa. Như chúng ta đã thảo luận trước đó, khi chúng ta sử dụng một thuật toán đối xứng, chúng ta cần phải phân phối khóa theo một số cách. Chúng ta có thể làm điều này bằng cách trao đổi các khoá trực tiếp giữa những người cần giao tiếp, gửi khóa trong thư điện tử, hoặc lặp đi lặp lại nó bằng lời nói qua điện thoại, nhưng chúng ta thường

không muốn gửi khóa cùng với bản tin, vì điều này sẽ khiến cho bản tin của chúng ta dễ dàng có được bởi một kẻ nghe trộm. Khi chúng ta sử dụng mật mã khóa bất đối xứng, chúng ta đã không cần phải chia sẻ một khóa duy nhất. Chúng ta chỉ đơn giản là làm cho khóa công khai của chúng ta dễ dàng có được, và bất kỳ ai cần gửi cho chúng ta một thông điệp được mã hóa bằng cách sử dụng nó.

- Các thuật toán mật mã khóa bất đối xứng

Thuật toán RSA, được đặt tên cho tác giả của nó Ron Rivest, Adi Shamir và Leonard Adleman, là một thuật toán bất đối xứng được sử dụng trên toàn thế giới, bao gồm cả trong các giao thức Secure Sockets Layer (SSL), được sử dụng để bảo đảm cho nhiều giao dịch phổ biến như Web và lưu lượng truy cập thư điện tử. RSA đã được tạo ra vào năm 1977 và vẫn là một trong những thuật toán được sử dụng rộng rãi nhất trên thế giới cho đến ngày nay.

Mật mã đường cong elliptic (ECC) là một lớp các thuật toán mã hóa, mặc dù đôi khi được gọi như thể nó là một thuật toán trong và của chính nó. ECC được đặt tên cho các kiểu vấn đề toán học mà chức năng mã hóa của nó dựa vào. ECC có nhiều lợi thế hơn các loại thuật toán mã hóa khác. Nó có một sức mạnh mã hóa cao hơn với các khóa ngắn hơn so với nhiều loại thuật toán khác, có nghĩa là chúng ta có thể sử dụng các khóa ngắn hơn với ECC trong khi vẫn duy trì một mức độ rất an toàn của mã hóa. Nó cũng là một loại thuật toán rất nhanh và hiệu quả, cho phép chúng ta thực hiện nó trên phần cứng với một tập các nguồn tài nguyên hạn chế hơn, dễ dàng hơn, chẳng hạn như điện thoại di động hoặc thiết bị cầm tay. Chúng ta có thể thấy ECC được triển khai trong một loạt các thuật toán mã hóa, bao gồm Secure Hash Algorithm 2 (SHA-2) và thuật toán ký số đường cong Elliptic (Elliptic Curve Digital Signature Algorithm - ECDSA).

Tồn tại một số thuật toán bất đối xứng khác, bao gồm ElGamal, Diffie-Hellman, và Digital Signature Standard (DSS). Chúng ta cũng có thể thấy một loạt các giao thức và các ứng dụng dựa trên mật mã phi đối xứng, bao gồm Pretty Good Privacy (PGP) cho các tin nhắn và các tập tin bảo mật, SSL và Transport Layer Security (TLS) cho nhiều loại luồng lưu thông bao gồm cả web và thư điện tử, và một số giao thức bằng giọng nói qua IP (VoIP) cho các

cuộc hội thoại. Mật mã phi đối xứng đã cho phép nhiều phương pháp hiện đại của truyền thông an toàn tồn tại và có khả năng sẽ tiếp tục là cơ sở của chúng trong một thời gian.

Nhược điểm cơ bản của các thuật toán phi đối xứng là tác động chậm – nó chậm hơn thuật toán đối xứng tới hàng nghìn lần. Để hạn chế nhược điểm này, người ta sử dụng công nghệ kết hợp cả hai phương pháp mã hoá đối xứng và phi đối xứng. Ví dụ, bản rõ có thể mã hoá bằng mật mã đối xứng (tác động nhanh), còn khoá mật (ngẫu nhiên) gửi kèm theo bản rõ được mã bằng mật mã phi đối xứng.

Một ưu việt quan trọng của các thuật toán phi đối xứng là khả năng nhận biết (nhận dạng) người gửi bằng cách dùng chữ ký điện tử của anh ta (nhất là trong các giao dịch điện tử). Tư tưởng của công nghệ chữ ký điện tử như sau: Người gửi truyền đi 2 phiên bản của cùng một bản tin (một bản rõ và một bản là mã hóa của nó bằng khoá riêng, tức là mã hoá nghịch đảo). Người nhận dùng khoá công khai của người gửi giải mã bản mã nhận được ở trên. Nếu kết quả thu được trùng với bản rõ thì cá nhân và chữ ký của người gửi coi như được xác định.

Trên thực tế áp dụng chữ ký điện tử, thì không phải tất cả bản tin được mã hoá, mà chỉ có một tổng kiểm tra đặc biệt – hash total (tổng băm) – giữ bản tin không bị xuyên tạc, được mã hoá thôi. Quan trọng ở đây là, chữ ký điện tử bảo đảm được cả toàn vẹn bản tin và cả tính chân thực của người gửi.

Các vấn đề liên quan đến việc triển khai chữ ký điện tử và tính tổng băm (hash total) của nó được xác định trong các luật về giao dịch điện tử của các quốc gia. Ví dụ, chuẩn các hàm băm (Hash functions) trong GOST R34-10-2012 của Liên bang Nga chẳng hạn.

c) Hàm băm

Hàm băm đại diện cho một loại mật mã thứ ba bên cạnh mật mã đối xứng và bất đối xứng, những gì chúng ta có thể gọi là mật mã không khóa. Hàm băm, cũng được gọi là tóm lược bản tin, không sử dụng khóa, nhưng thay vào đó là tạo ra một giá trị băm có chiều dài cố định và có tính duy nhất cao, thường được gọi là một giá trị băm, dựa trên các thông báo ban đầu, một cái gì đó dọc theo cùng các dòng như một dấu vân tay.

Các giá trị băm không thể được sử dụng để phát hiện các nội dung của thông báo ban đầu, hoặc bất kỳ đặc điểm khác của nó, nhưng có thể được sử dụng để xác định xem liệu các thông báo có bị thay đổi hay không. Giá trị băm rất hữu ích khi phân phối các tập tin hoặc gửi thông tin liên lạc, như giá trị băm có thể được gửi đi với bản tin để người nhận có thể xác minh tính toàn vẹn của nó. Người nhận chỉ đơn giản là băm lại bản tin bằng cách sử dụng cùng một thuật toán, sau đó so sánh hai giá trị băm. Nếu hai giá trị phù hợp, bản tin đã không thay đổi. Nếu chúng không phù hợp, bản tin đã bị thay đổi.

Mặc dù theo lý thuyết có thể thiết kế một giá trị băm phù hợp cho hai bộ dữ liệu khác nhau, được gọi là một va chạm, đây là một nhiệm vụ thực sự rất khó khăn, và thường đòi hỏi rằng các thuật toán băm được phân chia để thực hiện. Một số thuật toán, chẳng hạn như thuật toán tóm lược thông báo 5 (Message-Digest 5 - MD5), đã bị tấn công theo kiểu này, mặc dù việc tạo ra một va chạm không phải là dễ. Khi trường hợp này xảy ra, các thuật toán bị tổn hại thường rơi ra khỏi các sử dụng phổ biến. Các thuật toán băm như SHA-2 và SHA-3 đã thay thế MD5 trong các trường hợp an ninh nghiêm ngặt băm là bắt buộc. Nhiều thuật toán băm khác tồn tại và được sử dụng trong một loạt các tình huống, chẳng hạn như MD2, MD4, và RACE.

Tiếp theo chúng ta sẽ tìm hiểu về những ứng dụng mở rộng của hàm băm: chữ ký số và chứng chỉ.

(1) Chữ ký số

Chữ ký số là cách sử dụng khác mà chúng ta có thể đặt các thuật toán bất đối xứng và sự liên kết giữa khóa bí riêng và khóa công khai. Chữ ký kỹ thuật số cho phép chúng ta ký một bản tin để giúp phát hiện những thay đổi trong nội dung bản tin, để đảm bảo rằng thông điệp đã được gửi hợp pháp từ bên dự kiến, và để ngăn chặn người gửi từ chối việc người đó đã gửi bản tin, gọi là việc chống chối bỏ. Để ký một bản tin, người gửi sẽ tạo ra một giá trị hash của bản tin, và sau đó sử dụng khóa riêng của mình để mã hóa giá trị băm, do đó tạo ra một chữ ký số. Người gửi sau đó sẽ gửi các chữ ký số cùng với thông báo, thường là bằng cách gắn thêm nó vào thông báo.

Khi bản tin đến người nhận cuối, người nhận sẽ sử dụng khóa công khai của người gửi để giải mã chữ ký số, do đó khôi phục lại giá trị băm gốc của bản tin. Sau đó người nhận có thể xác minh tính toàn vẹn của thông điệp

bằng cách băm lại bản tin và so sánh hai giá trị băm. Mặc dù điều này nghe có vẻ như mất một lượng đáng kể công việc để xác minh tính toàn vẹn của thông điệp, nhưng nó thường được thực hiện bởi một phần mềm ứng dụng trong một số loại và quá trình này phần lớn thường là trong suốt đối với người dùng cuối.

(2) Chứng chỉ

Ngoài các giá trị băm và chữ ký số, chúng ta có một cấu trúc mà chúng ta có thể mở rộng quy mô sử dụng ký bản tin, dưới dạng thức chứng chỉ số, thường được gọi là chứng chỉ. Các chứng chỉ được tạo ra để liên kết một khóa công khai với một cá nhân cụ thể và thường được sử dụng như một hình thức nhận dạng điện tử cho người cụ thể. Chứng chỉ thường được hình thành bằng cách kết hợp khóa công khai và các thông tin nhận dạng, chẳng hạn như tên, địa chỉ, và chúng có chữ ký của cơ quan chứng nhận (CA). Một CA là một thực thể đáng tin cậy để xử lý chứng chỉ số. Một CA nổi tiếng, hiện nay, là VeriSign và ở Việt Nam cũng có một số CA như Ban Cơ yếu Chính phủ - cung cấp chứng chỉ cho các tổ chức chính phủ, Bkis – cung cấp chứng chỉ cho các tổ chức thương mại. Ngoài ra, một số tổ chức lớn mà sử dụng một số lượng lớn các chứng chỉ có thể chọn để thực hiện CA riêng của mình để giảm chi phí.

Lợi thế của việc có một chứng chỉ là nó cho phép chúng ta xác minh rằng một khóa công khai thực sự liên quan đến một cá nhân cụ thể. Trong trường hợp chữ ký số, chúng ta đã thảo luận trong phần trước, nó có thể có khả năng rằng một người nào đó đã giả mạo các khóa được sử dụng để ký vào các bản tin và các khóa không thực sự thuộc về người gửi ban đầu. Nếu chúng ta có một chứng chỉ số cho người gửi, chúng ta có thể dễ dàng kiểm tra với CA để đảm bảo rằng khóa công khai của người gửi là hợp pháp.

Một CA chỉ là một phần nhỏ của cơ sở hạ tầng có thể được đưa ra để xử lý chứng chỉ trên một quy mô lớn. Cơ sở hạ tầng này được biết đến như một cơ sở hạ tầng khóa công khai (PKI). Một PKI thường bao gồm hai thành phần chính, mặc dù một số tổ chức có thể tách một số chức năng ra thành nhiều hơn hai thành phần này. Trong một PKI, chúng ta thường thấy các CA cấp phát và xác minh chứng chỉ và cơ quan đăng ký (RAS) xác minh danh tính của các cá nhân liên quan đến chứng chỉ.

Trong PKI, chúng ta cũng đối phó với các khái niệm về thu hồi chứng chỉ, trong trường hợp chứng chỉ đến ngày hết hạn của nó, chứng chỉ bị tổn thương, hoặc một lý do khác phát sinh mà chúng ta cần phải đảm bảo rằng các chứng chỉ có thể không còn được sử dụng. Trong trường hợp này, chúng ta sẽ có thể xem xét bổ sung những chứng chỉ này vào danh sách thu hồi chứng chỉ (CRL). CRL là một danh sách chung công cộng chứa tất cả các chứng chỉ bị thu hồi trong một thời gian nhất định, tùy thuộc vào các tổ chức cụ thể.

3.4.2.3. Bảo vệ dữ liệu ở chế độ tĩnh, vận chuyển và sử dụng

Chúng ta có thể phân chia cụ thể ứng dụng thực tế của mật mã thành hai loại chính: bảo vệ dữ liệu ở chế độ tĩnh và bảo vệ dữ liệu trong chuyển động. Bảo vệ dữ liệu ở chế độ tĩnh là rất quan trọng vì số lượng lớn các dữ liệu được lưu trữ có thể được tìm thấy trên các thiết bị như băng sao lưu, ổ đĩa flash, và ổ đĩa cứng trong các thiết bị di động như máy tính xách tay. Bảo vệ dữ liệu trong chuyển động là rất quan trọng cũng vì số lượng rất lớn các giao dịch của các doanh nghiệp được tiến hành qua Internet, bao gồm cả giao dịch tài chính, thông tin y tế, hồ sơ thuế, và trao đổi nhạy cảm tương tự khác.

a) Bảo vệ dữ liệu lưu trữ bằng mật mã

Bảo vệ dữ liệu ở chế độ lưu trữ là một lĩnh vực mà khi tiến hành đảm bảo an toàn thường lơ là và là một khu vực đặc biệt xấu nếu chúng ta lựa chọn không nhấn mạnh tính an toàn. Nói chung, dữ liệu được coi là tĩnh khi nó đang ở trên một thiết bị lưu trữ của một số loại và không được di chuyển qua mạng, thông qua một giao thức… Điều này hơi phi logic, dữ liệu tĩnh trên phương tiện truyền thông cũng có thể được chuyển động, ví dụ, chúng ta có thể mang theo trong túi một ổ đĩa flash có chứa một bản sao của các mẫu thuế của chúng ta, hoặc để lại ở ghế sau xe một máy tính xách tay có chứa các nội dung của một cơ sở dữ liệu khách hàng.

Một giải pháp hiệu quả để bảo vệ dữ liệu tĩnh. Phương pháp chính mà chúng ta sử dụng để bảo vệ loại dữ liệu này là mã hóa, đặc biệt là khi chúng ta biết rằng các phương tiện lưu trữ, hoặc các phương tiện truyền thông và các thiết bị mà nó được chứa trong đó, sẽ có khả năng bị tiếp xúc với hành vi trộm cắp vật lý, chẳng hạn như trên một băng sao lưu hoặc trong một máy tính xách tay.

Một số lượng lớn các sản phẩm thương mại có sẵn mà sẽ cung cấp việc mã hóa cho các thiết bị di động, thường tập trung vào các ổ đĩa cứng và các thiết bị lưu trữ di động, bao gồm cả các sản phẩm từ các công ty lớn như McAfee, Symantec, và PGP. Các tính năng của sản phẩm thương mại như vậy thường bao gồm khả năng mã hóa toàn bộ ổ đĩa cứng, được gọi là mã hóa đĩa đầy đủ, và một loạt các phương tiện truyền thông di động, cũng như các tính năng quản lý tập trung, bảo mật và các tính năng quản trị khác. Ngoài ra còn có một số sản phẩm mã hóa miễn phí hay mã nguồn mở trên thị trường.

Chúng ta cũng cần phải nhận thức được vị trí dữ liệu có tính chất nhạy cảm mà chúng ta phải chịu trách nhiệm đang được lưu trữ và cần phải thực hiện các biện pháp thích hợp để đảm bảo rằng nó được bảo vệ ở đó.

b) Bảo vệ dữ liệu chuyển động

Một mối quan tâm lớn đối với việc bảo vệ dữ liệu của chúng ta khi nó đang chuyển động qua một mạng đa dạng. Điều này có thể trên một mạng WAN hoặc mạng LAN đóng, trên một mạng không dây, qua Internet, hoặc bằng các cách khác. Phương pháp chính của bảo mật dữ liệu từ việc tiếp xúc trên mạng truyền thông là mã hóa, và chúng ta có thể lựa chọn để áp dụng nó theo hai cách: bằng cách mã hóa chính các dữ liệu để bảo vệ nó, hoặc bằng cách bảo vệ toàn bộ kết nối.

(1) Bảo vệ dữ liệu

Chúng ta có thể có nhiều cách tiếp cận để bảo vệ dữ liệu chúng ta đang gửi qua mạng, phụ thuộc vào dữ liệu gì chúng ta đang gửi và các giao thức mà thông qua đó chúng ta đang gửi đi.

SSL và TLS thường được sử dụng để bảo vệ thông tin gửi qua mạng và qua Internet, và chúng hoạt động kết hợp với các giao thức khác như Internet Message Access Protocol (IMAP) và Post Office Protocol (POP) cho thư điện tử, Hypertext Transfer Protocol (HTTP) cho lưu lượng truy cập web, VoIP cho các cuộc hội thoại, nhắn tin tức thời, và hàng trăm các giao thức khác. SSL thực sự là tiền thân của TLS và TLS dựa chủ yếu trên phiên bản mới nhất của SSL. Các thuật ngữ thường được sử dụng thay thế cho nhau, và chúng gần như giống hệt nhau. Cả hai phương pháp vẫn đang được sử dụng phổ biến.

Khi SSL/TLS được sử dụng, nó mã hóa kết nối giữa hai hệ thống giao tiếp qua mạng nhưng nói chung đặc trưng cho một ứng dụng hoặc giao thức cụ thể. Vì vậy, mặc dù chúng ta có thể sử dụng SSL/TLS để mã hóa thông tin liên lạc của chúng ta với máy chủ chứa thư điện tử của chúng ta, điều này không có nghĩa là các kết nối được thực hiện thông qua trình duyệt web của chúng ta cũng được áp dụng cùng một mức độ an toàn nâng cao. Nhiều ứng dụng phổ biến có khả năng hỗ trợ SSL/TLS, nhưng chúng thường cần phải được cấu hình để thực hiện như vậy một cách độc lập.

(2) Bảo vệ kết nối

Một cách tiếp cận chúng ta có thể lựa chọn thực hiện là mã hóa tất cả lưu lượng truy cập mạng của chúng ta với một mạng riêng kết nối ảo(VPN). Các kết nối VPN sử dụng một loạt các giao thức để thực hiện một kết nối an toàn giữa hai hệ thống. Chúng ta có thể sử dụng một VPN khi chúng ta đang kết nối từ một mạng có khả năng không an toàn, chẳng hạn như kết nối không dây trong một khách sạn, tới các nguồn tài nguyên nội bộ mà được an toàn đằng sau tường lửa công ty.

Việc sử dụng mạng riêng ảo có thể cung cấp cho chúng ta một giải pháp cho việc gửi lưu lượng nhạy cảm trên các mạng không an toàn. Một kết nối VPN, thường được gọi là một đường hầm, là một kết nối được mã hóa giữa hai điểm. Điều này thường được thực hiện thông qua việc sử dụng một ứng dụng máy khách VPN trên một đầu của kết nối, và một thiết bị được gọi là một bộ tập trung VPN ở đầu bên kia. Các khách hàng sử dụng phần mềm để xác thực với bộ tập trung VPN, thường là qua Internet, và sau khi kết nối được thiết lập, tất cả lưu lượng trao đổi từ giao diện mạng kết nối với các luồng VPN thông qua các đường hầm VPN được mã hóa.

Các VPN thường được sử dụng để cho phép những người làm việc từ xa kết nối với các nguồn tài nguyên nội bộ của một tổ chức. Khi kết nối như vậy được thiết lập, các thiết bị kết nối có thể thực hiện như thể nó đã được kết nối trực tiếp vào mạng nội bộ của tổ chức nắm giữ các kết nối. Điều này có thể rất hữu ích vì nó cho phép chúng ta có thể cho phép nhiều truy cập đối với người làm việc từ xa hơn chúng ta thường sẽ có thể thực hiện an toàn khi các nhân viên ở bên ngoài biên giới mạng của chúng ta.

Mặc dù một loạt các giao thức có thể được sử dụng để đảm bảo một kết nối VPN, và nhiều loại đã được phát triển và sử dụng trong những năm qua,

hai phương pháp chính được sử dụng hiện nay là: Internet Protocol Security (IPsec) VPN và SSL VPN. Hai loại kết nối VPN có thể được cấu hình để cho một tập các tính năng và chức năng gần giống nhau, từ quan điểm của người sử dụng, nhưng chúng yêu cầu một tập hơi khác nhau về phần cứng và phần mềm để thiết lập. Thông thường, một IPsec VPN đòi hỏi một cấu hình phần cứng phức tạp hơn và một phần mềm client được cài đặt, trong khi một SSL VPN thường hoạt động từ một plug-in có trọng lượng nhẹ được tải về từ một trang web và một cấu hình phần cứng ít phức tạp. Theo một số quan điểm bảo mật, hai phương pháp là tương đối tương đương về mã hóa. Có thể là máy khách SSL VPN có thể được tải về máy tính công cộng hoặc máy tính ngẫu nhiên khác, do dễ cài đặt, và cung cấp một con đường rò rỉ dữ liệu hoặc tấn công bởi trạng thái không an toàn của hệ thống.

c. Bảo vệ dữ liệu trong sử dụng

Một hướng mới trong bảo vệ dữ liệu liên quan đến việc bảo vệ nó trong khi nó đang được sử dụng. Mặc dù chúng ta có thể sử dụng mã hóa để bảo vệ dữ liệu trong khi nó được lưu trữ hoặc di chuyển qua mạng, chúng ta đang có một số hạn chế trong khả năng bảo vệ dữ liệu trong khi nó đang được sử dụng bởi những người hợp pháp có quyền truy cập vào nó. Người sử dụng có thẩm quyền có thể in các tập tin, chuyển chúng sang các máy khác hoặc các thiết bị lưu trữ, thư điện tử cho họ, chia sẻ chúng trên mạng chia sẻ file peer-to-peer (P2P), và nói chung những việc làm này tạo ra một sự phủ nhận đối với các biện pháp an toàn đã thiết lập cẩn thận của chúng ta.

Trong năm 2009, người ta đã được phát hiện ra rằng thông tin mật có chứa chi tiết về các thông tin liên lạc, định vị và hệ thống điện tử quản lý cho Marine One, máy bay trực thăng được sử dụng để vận chuyển tổng thống của Hoa Kỳ, đã bị rò rỉ trên mạng P2P từ máy tính của một nhà thầu chính phủ. Một bản sao của dữ liệu cũng đã được tìm thấy là đã được chia sẻ từ một máy tính với một địa chỉ IP của Iran. Rõ ràng, đây là một trường hợp dữ liệu cực kỳ nhạy cảm bị mất trong khi sử dụng, nhưng chúng ta cũng có thể thấy nhiều ví dụ về các công ty tổ chức và làm việc với dữ liệu nhạy cảm cho các doanh nghiệp và cá nhân một cách thường xuyên.

Nhìn chung, mật mã cho chúng ta một cơ chế để bảo vệ dữ liệu ở dạng tĩnh, chuyển động, và đến một mức độ nhất định trong sử dụng. Nó cung cấp cái cốt lõi cho nhiều cơ chế bảo mật cơ bản cho phép chúng ta liên lạc và thực

hiện các giao dịch khi các dữ liệu liên quan có tính chất nhạy cảm và chúng ta muốn rằng nó không được tiếp xúc với công chúng hoặc một kẻ tấn công.

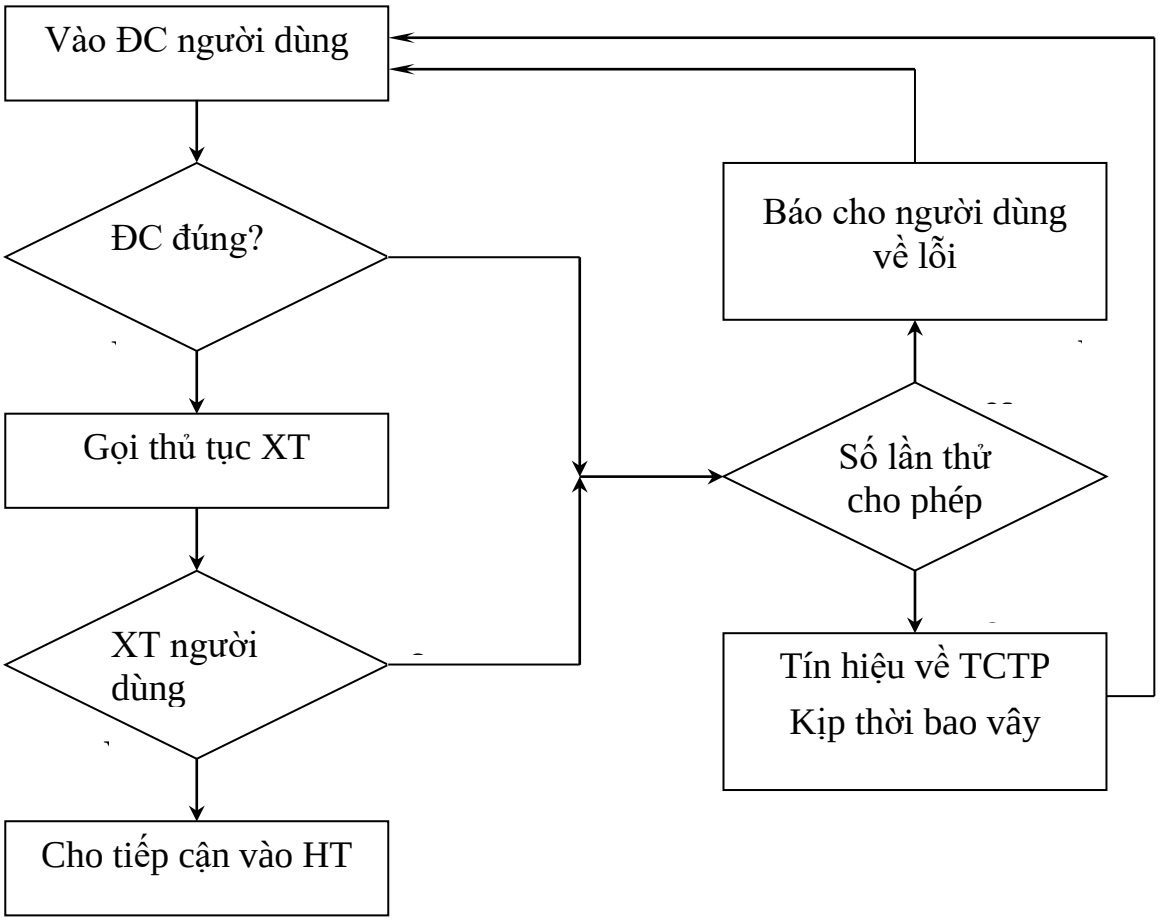
3.4.3. Phương pháp nhận dạng và xác thực

Khi chúng ta đang phát triển các biện pháp an toàn, cho dù quy mô của một cơ chế cụ thể hay toàn bộ cơ sở hạ tầng thì nhận dạng và xác thực là các khái niệm quan trọng, bởi vì tất cả các cơ chế BVTT đều dựa trên sự tương tác của các chủ thể và các đối tượng của HT, mà chúng (các S – chủ thể và O – đối tượng) cần có các tên gọi cụ thể. Các chủ thể của hệ thống thường là các người dùng, các quá trình, các đối tượng của hệ thống là bản thân TT và các tài nguyên TT của hệ thống (các file, các thư mục, CSDL…). Theo nghĩa hẹp thì nhận dạng là sự khẳng định về một ai đó hoặc một cái gì đó, và xác thực là một hành động nhằm thiết lập hoặc chứng thực một cái gì đó (hoặc một người nào đó) đáng tin cậy, có nghĩa là, những lời khai báo do người đó đưa ra hoặc về vật đó là sự thật. Chúng ta có thể thấy những quá trình giống như này diễn ra hàng ngày theo nhiều cách thức khác nhau.

Một ví dụ rất thông dụng về giao dịch nhận dạng và xác thực có thể thấy trong việc sử dụng các thẻ thanh toán, nó đòi hỏi phải có một số nhận dạng cá nhân (PIN). Khi chúng ta quẹt dải từ trên thẻ, chúng ta khẳng định rằng chúng ta là người được ghi danh trên thẻ. Tại thời điểm này thì chúng ta đã đưa ra được định danh của chúng ta nhưng không có gì hơn thế. Khi chúng ta được nhắc nhở để nhập mã PIN liên kết với thẻ, chúng ta sẽ hoàn thành phần xác thực của giao dịch với hi vọng kết quả xác thực thành công.

Nhận dạng (ND) chỉ đơn giản là một sự khai báo chúng ta là ai. Sự xác thực (XT) là việc kiểm tra sự phù hợp của S tiếp cận với định danh dành cho S đó và khẳng định quyền của nó (nói cách khác là kiểm tra tính chân thực của lời khai báo của S).

Sơ đồ chung của ND&XT người dùng khi tiếp cận hệ thống có dạng như hình sau:



Hình 3.8 Sơ đồ nhận dạng và xác thực người dùng

Trong ý nghĩa an toàn thông tin thì xác thực là tập hợp các phương thức chúng ta sử dụng để thiết lập một định danh là đúng. Điều quan trọng cần lưu ý là xác thực chỉ thiết lập liệu việc nhận dạng có được thực hiện chính xác hay không. Xác thực không suy ra hoặc hàm ý bất cứ điều gì về những gì mà các bên được xác thực được phép làm, đây là một nhiệm vụ riêng được gọi là ủy quyền. Chúng ta sẽ thảo luận về ủy quyền kỹ hơn trong phần tiếp, nhưng điều quan trọng phải hiểu bây giờ là xác thực cần thực hiện đầu tiên.

Nếu trong quá trình XT, sự chân thực của S đã được xác lập, thì hệ thống bảo vệ cần phải xác định các quyền của S nữa. Điều này cần thiết cho các kiểm soát tiếp theo.

3.4.3.1. Các yếu tố trong xác thực

Xác thực có thể được thực hiện dựa trên một trong các yếu tố sau:

■ Điều gì đó mà chúng ta biết: đây là một yếu tố xác thực rất phổ biến. Điều này thường liên quan đến kiến thức về một điều bí mật duy nhất được

chia sẻ bởi các bên xác thực. Đối với người dùng, điều bí mật này có thể là một mật khẩu, một mã PIN hoặc một khóa mã riêng…

■ Xác thực thường dựa trên việc sở hữu vật chất của một sản phẩm hay thiết bị mà là duy nhất với người sử dụng. Chúng ta có thể thấy các yếu tố này cùng được sử dụng trong hình thức thẻ ATM, các chứng minh thư, hay các thẻ an toàn dựa trên phần mềm (software-based security tokens) có thể thấy như trong hình 3.9. Một số tổ chức như các ngân hàng đã bắt đầu sử dụng truy cập tới các thiết bị logic như điện thoại di động hay các tài khoản thư điện tử như là một phương thức xác thực tốt. Độ mạnh của yếu tố này có thể thay đổi phụ thuộc vào việc thực hiện.

Hình 3.9 Thẻ an toàn dựa trên phần mềm

■ Xác thực dựa trên các thuộc tính vật lý tương đối riêng của một các nhân, thường được gọi là sinh trắc học. Nhân tố này có thể được dựa trên các thuộc tính đơn giản như cân nặng, chiều cao, màu tóc hay màu mắt, nhưng những thuộc tính này không có xu hướng là duy nhất đủ để làm cho việc nhận dạng được an toàn. Các thuộc tính thường được sử dụng phổ biến hơn là các đặc điểm nhận dạng có tính phức tạp hơn chẳng hạn như vân tay, mống mắt/tròng đen, mô hình võng mạc, hoặc các đặc điểm trên khuôn mặt. Yếu tố này cung cấp khả năng xác thực mạnh hơn, ví như việc giả mạo hoặc ăn cắp một bản sao của một định danh vật lý là một nhiệm vụ có phần khó khăn hơn, mặc dù không phải không thể.

■ Xác thực dựa trên những hành động hay hành vi của một cá nhân. Yếu tố đó có thể bao gồm phân tích dáng đi của cá nhân, sự chậm trễ thời gian giữa các tổ hợp phím khi nhập cụm từ mật khẩu, hay các yếu tố tương tự như vậy. Yếu tố này thể hiện một phương pháp xác thực rất mạnh và rất khó để

làm sai lệch. Việc xác thực này tuy nhiên cũng có thể có khả năng không chính xác sẽ từ chối người dùng hợp pháp với một tỷ lệ cao hơn so với một số yếu tố khác, dẫn đến việc không cho người dùng thực sự cần phải được xác thực.

■ Yếu tố xác thực dựa trên vị trí địa lý. Yếu tố này hoạt động khác với các yếu tố khác, bởi vì phương pháp xác thực của nó phụ thuộc vào người được xác thực như là một hiện diện vật lý tại một hay nhiều địa điểm cụ thể. Chúng ta có thể thấy một ví dụ khá lỏng lẻo của yếu tố này trong các hành động rút tiền từ máy ATM. Mặc dù điều này chắc chắn không phải là một quyết định thiết kế vì lý do an toàn, sự thật là điều này chỉ có thể được thực hiện tại các địa điểm địa lý cụ thể. Yếu tố này mặc dù khả năng khả dụng của nó ít hơn so với một số yếu tố khác, rất khó để chống lại việc tính toán mà không lật đổ hoàn toàn hệ thống thực hiện việc xác thực.

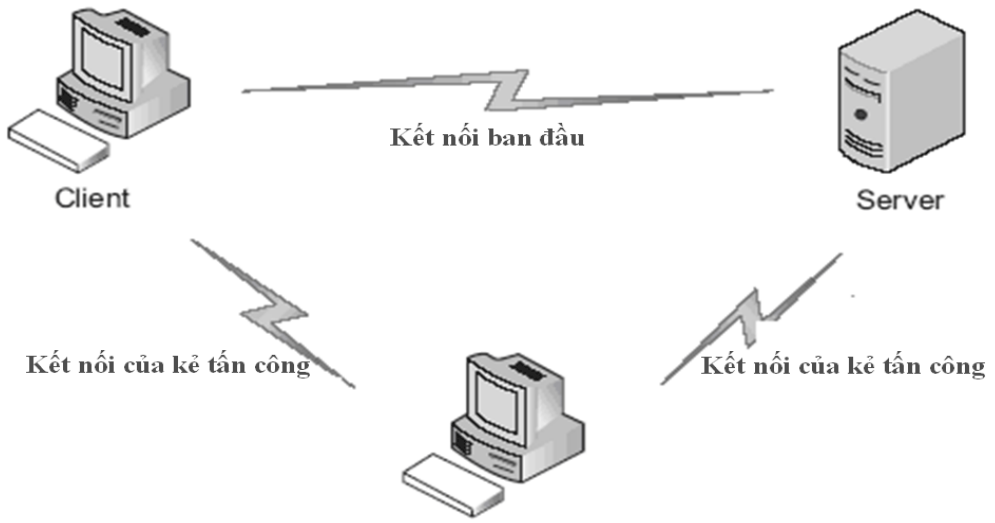
Nhiều hệ thống sử dụng nhiều nhân tố xác thực, được gọi là xác thực đa nhân tố. Chúng ta có thể thấy một ví dụ phổ biến của chứng thực đa nhân tố trong việc sử dụng máy ATM. Trong trường hợp này chúng ta có "cái gì đó chúng ta biết" đó là số PIN của chúng ta, và "cái gì đó mà chúng ta có", đó là thẻ ATM của chúng ta. Thẻ ATM của chúng ta thực hiện nhiệm vụ gấp đôi, vừa là một yếu tố để xác thực, vừa là một cách để nhận dạng.

Tùy thuộc vào các yếu tố cụ thể được lựa chọn, chúng ta có thể lắp ráp các chương trình xác thực đa nhân tố mạnh hơn hay yếu hơn trong một hoàn cảnh nhất định. Trong một số trường hợp, mặc dù một số phương pháp nhất định có thể rất khó để đánh bại nhưng chúng cũng không thể thực hiện được trong thực tế. Ví dụ DNA là một yếu tố xác thực rất mạnh nhưng thực tế không cho phép thực hiện thường xuyên. Như đã thảo luận ở những phần trước, chúng ta cần phải xây dựng an toàn sao cho phù hợp với những gì mà chúng ta đang bảo vệ. Chúng ta có thể cài đặt các máy quét mống mắt trên tất cả các thiết bị đầu cuối thẻ tín dụng thay vì việc khách hành ký nhận thẻ tín dụng của mình và chắc chắn sẽ tăng cường mức độ an toàn, nhưng điều này sẽ rất tốn kém và không thực tế và có thể gây khó chịu cho các khách hàng của chúng ta.

3.4.3.2. Xác thực lẫn nhau

Xác thực lẫn nhau đề cập đến một cơ chế xác thực mà trong đó cả hai bên xác thực lẫn nhau. Trong quá trình xác thực chuẩn, mà chỉ là xác thực một chiều, máy trạm xác thực tới máy chủ để chứng minh rằng nó là bên mà sẽ được truy cập tới tài nguyên mà máy chủ cung cấp. Trong xác thực lẫn nhau thì không chỉ máy trạm thực hiện xác thực với máy chủ mà máy chủ cũng phải thực hiện xác thực với máy trạm. Xác thực lẫn nhau thường được thực hiện thông qua việc sử dụng các chứng chỉ số, cái mà chúng đã thảo luận ở phần phương pháp mã hóa. Tóm lại, cả máy trạm và máy chủ sẽ có một chứng chỉ để xác thực lẫn nhau.

Trong các trường hợp mà chúng ta không thực hiện xác thực lẫn nhau, bản thân chúng ta đã mở cửa cho các tấn công mạo danh, thường được gọi với cái tên là các tấn công kẻ đứng giữa. Trong tấn công này kẻ tấn công chèn giữa máy trạm và máy chủ và đóng vai các máy chủ đối với máy trạm, và máy trạm đối với máy chủ, như trong hình 3.10. Điều này được thực hiện bằng cách phá vỡ các mô hình bình thường của các giao dịch, sau đó chặn và chuyển tiếp lưu lượng truy cập mà thường sẽ được chuyển trực tiếp giữa máy trạm và máy chủ. Điều này thường có thể được thực hiện bởi kẻ tấn công chỉ phải phá hoại hay làm sai lệch xác thực từ máy trạm tới máy chủ. Nếu chúng ta thực hiện việc xác thực lẫn nhau thì điều này sẽ trở nên khó khăn đáng kể cho kẻ tấn công.



Hình 3.10 Tấn công kẻ đứng giữa

Xác thực lẫn nhau cũng có thể sử dụng kết hợp với xác thực đa nhân tố, với việc thực hiện sau đó thường chỉ ở phía máy trạm. Xác thực đa yếu tố từ phía máy chủ tới máy trạm sẽ không chỉ là thách thức về mặt kỹ thuật mà còn không thực tế trong hầu hết các môi trường. Có thể hình dung chúng ta có thể thực hiện xác thực đa nhân tố lẫn nhau trong một môi trường bảo mật cao, nhưng điều này sẽ dẫn đến một mất mát rất lớn về năng suất.

3.4.3.3. Một số phương pháp xác thực

Có rất nhiều phương pháp thực hiện XT, chúng ta hãy xem xét 4 phương pháp cơ bản sau đây:

a) Dùng mật khẩu

Đây là phương pháp thường được dùng hơn cả. MK là các đặc tính bí mật của các chủ thể, mà khi đăng nhập hệ thống các S đưa vào và tiểu hệ XT sẽ so sánh chúng với MK mẫu được lưu giữ ở dạng mã hoá trong cơ sở MK mẫu và trong trường hợp trùng nhau tiểu hệ sẽ cho phép tiếp cận với các tài nguyên hệ thống.

Người ta chia ra làm 2 loại MK: MK cố định (dùng nhiều lần) và MK thay đổi (dùng 1 lần).

Trong nhiều hệ thống người ta dùng MK sử dụng nhiều lần. Ở đây MK của khách hàng không thay đổi (trong các phiên làm việc) và trong khoảng thời gian do nhà quản trị quy định. Hệ MK như vậy là đơn giản cho quản trị nhưng lại có nhiều nguy cơ bị khám phá. Ngày nay tồn tại nhiều phương pháp khám phá MK: từ ăn cắp bằng mắt thường (nhìn trộm, thu thập các giấy vụn ghi MK…) cho đến chặn bắt các phiên liên lạc, vét cạn các MK có thể bằng MTĐT hiện đại nhất. Khả năng khám phá mật khẩu tăng lên, nếu MK đơn giản, trực tiếp (tên người thân, ngày tháng sinh nhật,…), nếu MK có độ dài nhỏ, không có chu kỳ tồn tại …

Thường người ta đưa MK vào hệ thống ở chế độ hội thoại. Nhưng cũng có thể chọn MK từ chương trình.

Phương pháp MK dùng một lần (MK thay đổi) có độ an toàn cao hơn. Có 3 phương pháp dùng MK thay đổi thường được áp dụng:

- Biến tướng hệ MK đơn giản: Theo phương pháp này người ta cho khách hàng một danh sách các MK. Khi XT, hệ thống sẽ hỏi khách hàng MK

mà số thứ tự của nó (ở trong liệt kê đó) là ngẫu nhiên (ví dụ, trùng với thời điểm của đồng hồ chẳng hạn). Độ dài và số thứ tự các ký hiệu của MK cũng có thể được hỏi theo cách ngẫu nhiên.

- Phương pháp "Hỏi - Đáp": Đó là phương pháp mà trong đó hệ thống hỏi khách hàng một số câu hỏi có đặc tính chung, nhưng trả lời đúng thì chỉ từng cá nhân cụ thể mới có được. Ví dụ:

Login, Minh

XT: Hãy nói họ tên của mẹ anh? Vũ Thị Bình

XT: Anh đã học trường THPT nào? Đống Đa

XT: OK!

Có thể tăng câu hỏi lên theo các chủ đề khác nhau (và đáp án đúng tất nhiên hệ thống đã lưu trước ở dạng mã).

- Phương pháp hàm số: Đó là phương pháp sử dụng một hàm số đặc biệt biến đổi MK – f(x), cho phép làm thay đổi MK (theo công thức xác định) của khách hàng theo thời gian. Hàm f(x) phải thoả mãn một số yêu cầu như: với MK x cho trước dễ dàng tính được MK mới y=f(x); dù biết x và y, rất khó hoặc không thể xác định được f(x). Ví dụ MK của ta là một số có 4 chữ số là d1d2d3d4 (chẳng hạn là các số 1312, 4752, …). Hàm f(x) ta chọn như sau:

f(x)=2(d1.d4+d2.d3)mod(d1d2d3d4)

Khi đó ta có MK mới, ví dụ:

y= f(4752) = 2(4.2+7.5)mod(4.7.5.2) = 2(8+35)mod280 = 86mod280=86

Ta có bảng tương ứng sau:

x	y=f(x)
1312	4
4752	86
5472	76
6836	120
8831	64

HT và khách hàng đều biết trước f(x). hệ thống gửi cho khách hàng MK x và yêu cầu khách hàng trả lời. Khách hàng tính y=f(x) và gửi cho hệ thống. hệ thống xác thực bằng cách so sánh y với kết quả có sẵn của mình. Cho dù

kẻ công phá MK có biết x và y cũng khó đoán được hàm cũng khó đoán được hàm f(x).

Có 2 phương pháp thông dụng trong biến đổi hàm số. Đó là phương pháp biến hàm và phương pháp "bắt tay".

Phương pháp biến hàm thực hiện bằng cách biến đổi bản thân hàm f(x) theo chu kỳ nào đó. Thường người ta đưa vào biểu thức của f(x) các tham số có thể thay đổi mềm dẻo (ví dụ phụ thuộc ngày, giờ nào đó). Khách hàng được biết MK ban đầu, hàm f(x) và chu kỳ thay đổi mật khẩu.

Bản chất của phương pháp "bắt tay" như sau: Hàm biến đổi MK f(x) chỉ có khách hàng và hệ thống biết. Khi đăng nhập HT, tiểu hệ XT sinh ra một dãy số ngẫu nhiên x và gửi cho khách hàng. Khách hàng tính kết quả y=f(x) và gửi lại cho hệ thống. hệ thống sẽ so sánh kết quả đó với kết quả của chính hệ thống. Nếu trùng nhau thì coi như XT đã được chứng minh. Trong nhiều trường hợp, một khách hàng nào đó có thể rất cần kiểm tra XT một khách hàng từ xa khác hoặc một hệ thống nào đó mà anh ta định truy nhập. Khi đó phù hợp hơn cả là dùng chế độ MK "bắt tay", vì trong quá trình trao đổi MK này không có thành viên nào nhận được bất cứ TT mật nào (họ chỉ "bắt tay" nhau thôi).

b) Dùng thẻ bài

Đây là một phương pháp tổ hợp để XT. Nó đòi hỏi không chỉ biết MK mà còn phải có một tấm thẻ (token) – là một thiết bị đặc biệt khẳng định sự chân thực của chủ thể. Thẻ bài chia làm 2 loại: loại thụ động (có bộ nhớ) và loại tích cực (thẻ thông minh hay smart-card).

Phổ biến nhất là loại thẻ thụ động (thẻ từ), có băng từ. Thẻ từ đòi hỏi phải có thiết bị đọc với bàn phím và bộ xử lý. Khi sử dụng thẻ từ, khách hàng phải đưa ra số XT của mình (tức đặc chỉ). Trong trường hợp nó trùng với phương án điện tử có trong thẻ từ, thì khách hàng được cho phép tiếp cận hệ thống. Dùng thẻ từ như vậy cho phép XT chính xác người được quyền tiếp cận hệ thống và loại trừ được việc sử dụng bất hợp pháp thẻ bởi kẻ xấu (ví dụ, khi mất cắp hoặc rơi thẻ). Cách dùng như vậy thường gọi là XT hai nhân tố.

Đôi khi (thường là trong các kiểm soát vật lý cửa ra – vào) các thẻ từ chỉ được đưa vào máy đọc mà người ta không hỏi số XT (tức đặc chỉ) của chủ sở hữu thẻ.

Việc sử dụng thẻ từ để XT có ưu điểm là: có thiết bị riêng để xử lý các TT xác thực (thiết bị đọc) mà không cần đưa chúng vào bộ nhớ của MTĐT, do đó loại trừ được khả năng bắt trộm chúng trên các kênh liên lạc. Phương pháp này cũng có các nhược điểm sau: nó đắt giá hơn các MK, đòi hỏi phải có thiết bị đọc riêng, khi dùng cần có các tính toán và phân phối sao cho an toàn, phải đề phòng kẻ xấu lấy cắp và không bỏ quên ở thiết bị đọc, cũng đã có trường hợp làm thẻ giả…

Thẻ thông minh (Smart-card) có bộ nhớ và còn có thêm bộ vi xử lý gắn trên đó. Điều này cho phép thực hiện được các phương án khác nhau của MK: MK dùng nhiều lần, MK dùng một lần, MK hỏi - đáp… Thẻ thông minh đều bảo đảm XT hai nhân tố. Thẻ thông minh còn kết hợp các chức năng khác như làm thẻ rút tiền… Nhược điểm là giá cả rất đắt.

c) Dùng các đặc điểm sinh trắc của con người

Đây là phương pháp XT cực mạnh, bảo đảm độ chính xác tới gần100% mà không phải lo về vấn đề rơi, mất MK và các đặc chỉ. Tuy nhiên phương pháp chỉ thích hợp với con người (động vật), khó áp dụng cho việc XT các quá trình hoặc dữ liệu. Phương pháp này cũng đòi hỏi phải có các thiết bị phức tạp và đắt tiền. Do vậy người ta chỉ áp dụng nó đối với hệ thống đặc biệt quan trọng (XT người dùng theo đồng tử mắt, theo dấu vân tay, hình dái tai, theo ảnh hồng ngoại động mạch, theo chữ viết, theo mùi, theo tiếng nói và thậm chí theo ADN…). Chúng ta điểm qua một số phương pháp sinh trắc điển hình.

Dấu vân tay: Các máy quét dấu vân tay (scanner) tương đối nhỏ, đặc biệt hấp dẫn và cũng không đắt tiền. Sự trùng hợp dấu vân tay có xác suất cỡ 10^{-3} %. Các máy quét như vậy hiện được dùng nhiều trong lĩnh vực hình sự vì ở đó lượng dấu vân tay tích trữ được đã rất lớn.

Đồng tử mắt: Thiết bị XT theo đồng tử mắt có độ chính xác rất cao. Về mặt lý thuyết, thì xác suất trùng lặp của hai đồng tử mắt là cỡ 10^{-78} %.

Tiếng nói: Kiểm tra tiếng nói thường được dùng trong khi liên lạc bằng điện thoại. Một thiết bị ghi âm 16 quãng và một mirco tụ điện là có thể thực hiện được xác suất lỗi ở đây cỡ 2% – 5%. Trạng thái con người ở đây cũng phải tính tới: kích động, ốm đau, say xỉn…

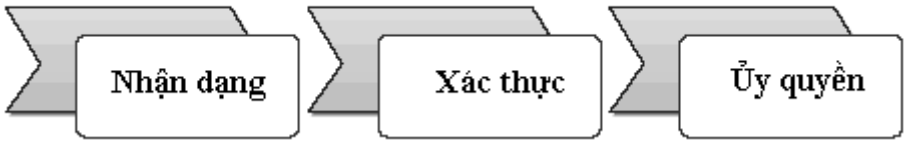
d) Dùng hệ thống định vị toàn cầu (GPS)

Đây là phương pháp XT mới xuất hiện gần đây nhất dựa vào hệ thống định vị toàn cầu (GPS – Global Positioning System) để chứng minh tính chân thực của người dùng ở xa theo vị trí mà anh ta đang ở đó. Người dùng có máy GPS gửi (nhiều lần) toạ độ của các vệ tinh nằm trong vùng nhìn thấy của anh ta. Tiểu hệ XT của hệ thống nhận được toạ độ ấy và biết được quỹ đạo của các vệ tinh sẽ xác định được vị trí của khách hàng với độ chính xác cỡ 1m. Trường hợp này đòi hỏi người dùng hợp pháp (ở xa) phải ở cố định một địa điểm.

3.4.4. Cấp quyền

Sau khi nhận dạng đã hoàn tất, cần phải xác lập quyền của chủ thể hay ủy quyền cho chủ thể. Điều này cần thiết để kiểm soát việc sử dụng các tài nguyên hệ thống sau này. Quá trình xác lập quyền còn được gọi là phân giới tiếp cận (tức là giới hạn để quản lý logic tiếp cận).

Ủy quyền là bước kế tiếp sau khi chúng ta hoàn thành việc nhận dạng và xác thực, như trong hình 3.11. Ủy quyền cho phép chúng ta xác định chính xác những gì mà người được xác thực đúng được phép làm.



Hình 3.11 Nhận dạng, xác thực và ủy quyền

Khi chúng ta xác định những truy cập sẽ cung cấp cho bên đã được xác thực, có một khái niệm quan trọng mà chúng ta nên nhớ kỹ, được gọi là nguyên tắc đặc quyền tối thiểu. Nguyên tắc này chỉ ra rằng chúng ta chỉ nên cho phép tối thiểu quyền truy cập cho bên được xác thực, có thể là một người dùng, một tài khoản người dùng hay một quá trình để cho phép thực hiện các chức năng cần thiết của nó. Ví dụ một người nào đó làm việc trong một bộ phận bán hàng không cần truy cập vào dữ liệu trong hệ thống nguồn nhân lực nội bộ của chúng ta để làm công việc của họ. Vi phạm nguyên tắc đặc quyền tối thiểu là vấn đề chính trong số các vấn đề an toàn mà chúng ta đang phải đối mặt ngày nay.

Bằng cách tuân thủ nguyên tắc đặc quyền tối thiểu khi cấu hình hệ thống, phân quyền truy cập cho các tài khoản và lập kế hoạch an toàn, chúng ta có thể làm mất đi một số công cụ truy cập dễ dàng mà kẻ tấn công có thể sử dụng để chống lại chúng ta. Nếu chúng ta chỉ cung cấp cho người dùng tập tối thiểu nhất các quyền truy cập cần thiết để thực hiện chức năng công việc của họ, thì chúng ta sẽ giảm số lượng thông tin có thể vô tình bị làm hỏng. Đây là một biện pháp bảo mật rất đơn giản mà chúng ta có thể đưa ra và nó rất hiệu quả.

Thông thường, các quyền của chủ thể được thể hiện bằng liệt kê các tài nguyên cho phép được dùng và các quyền tiếp cận tới từng tài nguyên trong danh sách đó. Các tài nguyên hệ thống có thể là chương trình, dữ liệu, thiết bị lôgic, vùng nhớ, thời gian bộ xử lý, các ưu tiên…

Có các phương pháp phân giới tiếp cận (xác lập quyền) cơ bản sau đây:

- Phân quyền theo liệt kê

Cần có sự tương ứng sau đây trong các liệt kê: mỗi người dùng – liệt kê các tài nguyên và các quyền tiếp cận tới chúng hoặc là, mỗi tài nguyên – liệt kê các người dùng và các quyền tiếp cận của họ tới tài nguyên này. Các liệt kê cho phép xác lập quyền với độ chính xác đến từng người dùng. Ở đây dễ dàng cho thêm quyền hoặc trực tiếp cấm tiếp cận. Các liệt kê thường dùng trong các Hệ điều hành và trong hệ quản trị CSDL (DBMS).

- Dùng ma trận quyền

Ma trận quyền còn gọi là bảng quyền. Trong ma trận quyền, các hàng là các đặc chỉ của các chủ thể tiếp cận HT, còn các cột – là các đối tượng của hệ thống (hay là các tài nguyên). Mỗi yếu tố của ma trận có thể chứa tên, kích thước của tài nguyên cho phép, quyền tiếp cận (đọc, ghi, v.v…), chú giải về chương trình điều khiển quyền… Trong hình vẽ sau đưa ra một mảng của ma trận quyền:

Bảng 3.1 Ví dụ về một mảng của ma trận quyền

Chủ thể	Thư mục D:\Heap	Chương trình BMT	Máy in
Người dùng 1	Cdrw	E	W
Người dùng 2	R		w từ 9:00 đến 17:00

Ký hiệu : c – sinh tạo, d – xoá, r - đọc, w – ghi, e – thực hiện.

Ma trận quyền là phương pháp thuận tiện, tất cả TT về quyền đều chứa trong một bảng. Tuy nhiên kích thước của ma trận có thể lớn và không tối ưu (nhiều ô rỗng). Vấn đề nén ma trận quyền đã được xử lý khá tốt trong hệ điều hành.

- Phân giới tiếp cận theo độ mật và thứ hạng

Tài nguyên hệ thống được nhóm lại và phân chia theo độ mật hoặc theo thứ hạng. Theo độ mật chia thành các nhóm tiếp cận chung, mật, tối mật, tuyệt mật. Người dùng được cấp quyền tương ứng với mức mật cao nhất mà anh ta được cho phép. Khi đó anh ta được tiếp cận tới tất cả các dữ liệu với độ mật không cao hơn độ mật đã được cho phép. Trong phân giới theo thứ hạng thì phân chia theo độ quan trọng của người dùng (ví dụ, lãnh đạo, nhà quản trị, khách hàng, …).

Có 2 cơ chế cấp quyền thường được áp dụng: cơ chế tùy chọn (DAC – Discretionary Access Control) và cơ chế bắt buộc (MAC – Mandatory Access Control).

- Cơ chế cấp quyền DAC: Với mỗi cặp (S – O) phải liệt kê rõ và đơn nghĩa các loại tiếp cận (đọc, viết…) tức là các tiếp cận được phép của chủ thể S tới đối tượng O. Cơ chế này được thực hiện nhờ danh sách quyền hoặc nhờ ma trận quyền.

Cơ chế này là một mô hình kiểm soát truy cập dựa trên các truy cập được xác định bởi chủ sở hữu của các tài nguyên được đòi hỏi. Chủ sở hữu của các tài nguyên có thể quyết định ai có quyền và ai không có quyền truy cập, và xác định những truy cập nào họ được phép có quyền. Trong hệ điều hành của Microsoft, chúng ta có thể thấy việc thực hiện DAC. Nếu chúng ta quyết định tạo một mạng chia sẻ, ví dụ chúng ta có thể quyết định những người mà chúng ta muốn cho phép truy cập.

- Cơ chế cấp quyền MAC: Cơ chế này dựa trên sự phân cấp theo độ mật các TT chứa trong các đối tượng O của hệ thống và sự cho phép chính thức các chủ thể S được tiếp cận tới TT với độ mật tương ứng. Nói cách khác, mỗi chủ thể S và mỗi đối tượng O được gán cho các nhãn an toàn, phản ánh vị trí của S và O trong các tập có thứ tự của chúng. Các nhãn an toàn có chứa các đặc trưng trong phân cấp có thứ tự (tức độ mật) và cả các đặc trưng phi

thứ tự (tức hạng mục an toàn). MAC được thực hiện nhờ phương pháp phân giới theo mức (độ) mật và theo hạng mục an toàn.

Cơ chế này là một mô hình kiểm soát truy cập mà trong đó các chủ sở hữu các tài nguyên không được quyết định ai sẽ truy cập vào tài nguyên đó mà thay vào đó những truy cập được quyết định bởi một nhóm hoặc các cá nhân có thẩm quyền để thiết lập truy cập vào tài nguyên. Chúng ta thường thấy việc thực hiện MAC trong các tổ chức của chính phủ, nơi mà các truy cập vào một tài nguyên phần lớn được quyết định bởi nhãn nhạy cảm áp dụng cho nó (bí mật, tối mật,…), mức độ thông tin nhạy cảm cá nhân được phép truy cập (có lẽ chỉ có bí mật), và liệu cá nhân thực sự có nhu cầu để truy cập vào tài nguyên, như chúng ta đã thảo luận khi chúng ta nói về các nguyên tắc đặc quyền tối thiểu ở phần trước của chương.

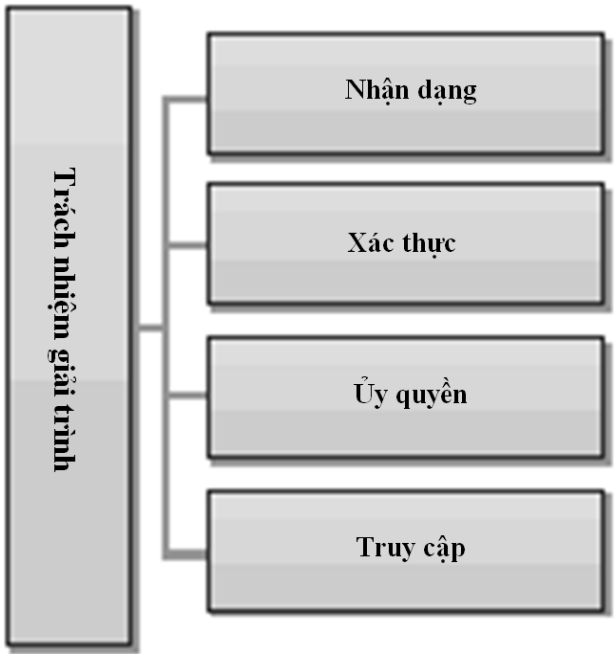
3.4.5. Đăng ký và kiểm toán

Khi chúng ta trải qua quá trình nhận dạng, xác thực và ủy quyền hoặc thậm chí trong khi chúng ta vẫn đang trong quá trình này, chúng ta cần phải theo dõi các hoạt động diễn ra, như trong hình 3.12. Mặc dù chúng ta có thể đã cho phép các bên truy cập tài nguyên của chúng ta, chúng ta vẫn cần phải đảm bảo rằng họ thực hiện đúng với các quy định có liên quan đến vấn đề an toàn, ứng xử kinh doanh, đạo đức, quấy rối tình dục và những thứ tương tự.

Trong những năm gần đây, có thể đảm bảo rằng chúng ta và những người dùng trong môi trường của chúng ta tuân thủ theo các quy tắc quy định sử dụng đã trở thành một nhiệm vụ quan trọng. Bây giờ chúng ta có một ngôi nhà lớn các thông tin ở dạng dữ liệu số hóa, bao gồm cả các dữ liệu y tế, thông tin tài chính, tố tụng, bí mật thương mại, và hàng loạt các thông tin khác. Nếu chúng ta không thiết lập và thực hiện theo nguyên tắc nghiêm ngặt đối với các truy cập tới dữ liệu nhạy cảm được lưu trữ theo cách này, chúng ta có thể bị lỗ trong kinh doanh, trộm cắp sở hữu trí tuệ, trộm cắp danh tính, gian lận và nhiều tội phạm khác. Một số loại dữ liệu ví dụ như y tế và tài chính, thường được bảo hộ theo quy định của pháp luật ở một số quốc gia.

Chúng ta thực hiện kiểm toán để đảm bảo rằng việc tuân thủ pháp luật, chính sách, và các quy định khác của cơ quan kiểm soát hành chính đang được thực thi. Chúng ta có thể kiểm toán một loạt các hoạt động bao gồm cả

việc tuân thủ các chính sách, kiến trúc an toàn phù hợp, các cài đặt ứng dụng, hành vi cá nhân hay các hoạt động hoặc cấu hình khác.



Hình 3.12 Trách nhiệm giải trình

Đăng ký là một cơ chế của Hệ BVTT, để ghi chép tất cả các sự kiện liên quan đến an toàn của hệ thống (vào và ra của các chủ thể tiếp cận, chạy và thực hiện các chương tình, in các tài liệu, các ý đồ tiếp cận tới các tài nguyên nhạy cảm, sự thay đổi quyền của các chủ thể và trạng thái các đối tượng tiếp cận…). Với các hệ thống được kiểm chuẩn về ATTT, ở các nước như Nga, Mỹ, danh sách các sự kiện mà Đăng ký ghi chép do Uỷ ban đặc biệt của Nhà nước quy định (ví dụ ở Nga là do Ủy ban Kiểm tra Nhà nước quyết định). Ghi nhật ký cung cấp cho chúng ta một lịch sử của các hoạt động đã diễn ra trong môi trường đang được ghi. Chúng ta thường tạo các bản ghi theo cách tự động trong các hệ điều hành, và theo dõi các hoạt động diễn ra trên các thiết bị máy tính, mạng và viễn thông, cũng như hầu hết bất kỳ thiết bị nào có thể được điều khiển từ xa để kết hợp hoặc được kết nối với một máy tính. Ghi nhật ký là một công cụ phản ứng , trong đó nó cho phép chúng ta xem hồ sơ những gì xảy ra sau khi nó đã xảy ra. Để ngay lập tức phản ứng với một cái gì đó đang diễn ra, chúng ta sẽ cần phải sử dụng một công cụ dòng IDS/IPS.

Cơ chế ghi nhật ký thường được cấu hình và có thể được thiết lập để ghi bất kỳ cái gì tới chỉ ghi các sự kiện quan trọng, thường là điển hình, tới mọi hành động được thực hiện bởi hệ thống hay phần mềm, thường chỉ được

thực hiện cho các mục đích khắc phục sự cố khi chúng ta thấy có vấn đề. Chúng ta thường sẽ thấy các sự kiện như lỗi phần mềm, lỗi phần cứng, người dùng đăng nhập hoặc truy cập tài nguyên, và nhiệm vụ đòi hỏi gia tăng đặc quyền trong hầu hết các bản ghi, tùy thuộc vào các thiết lập ghi nhật ký và hệ thống yêu cầu.

Nhật ký thường chỉ có sẵn cho các quản trị viên hệ thống để xem và thường không thể thay đổi bởi người dùng hệ thống, có lẽ ngoại trừ bằng cách viết/ghi vào chúng. Điều quan trọng cần lưu ý là thu thập các bản ghi mà không xem xét chúng là một việc khá vô ích. Nếu chúng ta không bao giờ xem xét nội dung của các bản ghi, ngay từ đầu chúng ta cũng có thể đã không thu thập chúng. Điều quan trọng là chúng ta lập lịch xem xét thường xuyên các bản ghi của chúng ta để nắm bắt được bất cứ điều gì bất thường trong nội dung của chúng.

Chúng ta cũng có thể được yêu cầu để phân tích các nội dung của các bản ghi liên quan đến một sự cố hoặc tình huống cụ thể. Những hoạt động này thường rơi vào những nhân viên an ninh trong trường hợp điều tra, các sự cố, và kiểm tra việc tuân thủ. Trong nhiều trường hợp điều này có thể là một việc khó khăn nếu khoảng thời gian đòi hỏi là lớn hơn một vài ngày. Ngay cả việc tìm kiếm các nội dung của một bản ghi tương đối đơn giản, chẳng hạn như được tạo ra từ một máy chủ Web proxy, có nghĩa có thể phải lọc thông qua một lượng lớn dữ liệu từ một hoặc nhiều máy chủ. Trong những trường hợp này các kịch bản tùy chỉnh hay thậm chí một công cụ như grep có thể là không có giá trị để thực hiện các công việc như thế trong một khoảng thời gian hợp lý.

Để tăng hiệu quả của đăng ký, người ta tiến hành kiểm toán các bản ghi chép được. Cho nên người ta thường gọi phương pháp này là kiểm toán (audit). Kiểm toán là phân tích các TT ghi chép được, là một trong những phương pháp chính để đảm bảo trách nhiệm giải trình thông qua các phương tiện kỹ thuật và bằng cách đảm bảo rằng chúng ta có một hồ sơ chính xác những người, những hành động của họ và thời gian diễn ra hành động đó. Nó cho phép kịp thời phát hiện các sai phạm, xác định các điểm xung yếu của hệ bảo vệ, đánh giá các công việc của người dùng …

Khi chúng ta thực hiện một cuộc kiểm toán, có một số thành phần mà chúng ta có thể kiểm tra, chủ yếu tập trung vào việc tuân thủ pháp luật và các chính sách có liên quan. Trong thế giới an toàn thông tin, chúng ta có xu hướng xem xét các truy cập vào ra hệ thống như là một tiêu điểm chính, nhưng thường mở rộng vào các lĩnh vực khác, chẳng hạn như an toàn vật lý.

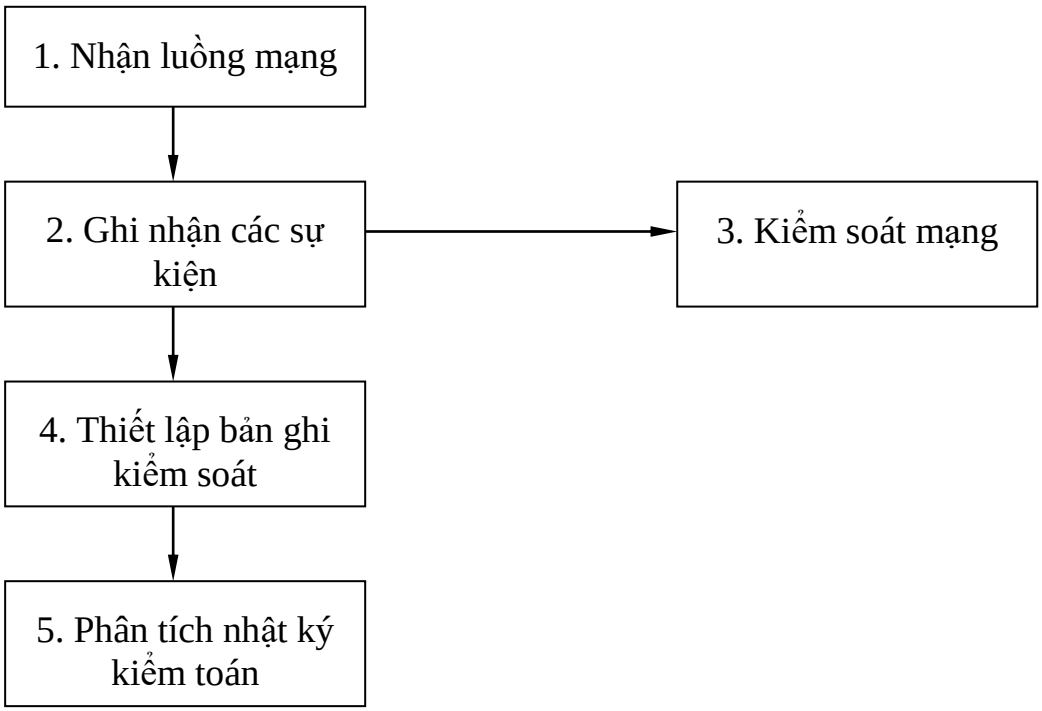
Công cụ dùng cho kiểm toán là bản ghi kiểm toán. Đó là tập hợp có thứ tự về thời gian các bản ghi kết quả hoạt động của các S của HT, đủ để khôi phục lại, xem xét lại và phân tích dãy các thao tác và các thủ tục khác nhau hoặc diễn biến các sự kiện. Dạng thường gặp của bản ghi kiểm toán giống như sau:

Bảng 3.2 Ví dụ về bản ghi kiểm toán thường gặp

Loại ghi chép	Ngày	Thời gian	Terminal	Người dùng	Sự kiện	Kết quả
81	11.8	10:14:06	1A5	NDVINH	LOGIN	OK
91	11.8	10:15:11	1A5	NDVINH	LOGIN	INCORPASS

Bản ghi kiểm toán nhiều khi còn được gọi là dấu vết kiểm toán, là một công cụ để kiểm soát truy nhập rất quan trọng.

Quá trình thực hiện đăng ký gồm 4 giai đoạn: thu thập và lưu dữ liệu; bảo vệ vết kiểm toán; tổng hợp; phân tích. Sơ đồ chức năng của tiểu hệ đăng ký có dạng sau (dùng cho một mạng):



Hình 3.13 Sơ đồ chức năng của tiểu hệ đăng ký

Ở giai đoạn đầu (thu thập và lưu dữ liệu), người ta xác định các dữ liệu cần thu thập và lưu (từ luồng mạng), chu kỳ làm sạch (lấy ra và in) và lưu trữ nhật ký, mức độ kiểm soát tập trung, vị trí và phương tiện lưu nhật ký, khả năng đăng ký TT được mã hoá v.v…

Trước hết, các dữ liệu đăng ký được phải được bảo vệ khỏi các tiếp cận trái phép và các công phá. Giai đoạn tổng hợp cần thiết để liên kết và đồng bộ (về định dạng) các dữ liệu đăng ký được từ các mảng khác nhau của hệ thống. Giai đoạn quan trọng nhất là phân tích các TT kiểm toán. Có 2 phương pháp phân tích TT nhằm phát hiện các tiếp cận trái phép (phát hiện xâm nhập).

- Phương pháp thống kê: Dựa trên cơ sở xác định các giá trị thống kê trung bình của các thông số hoạt động của các tiểu hệ (cái gọi là dáng dấp "lịch sử" của luồng mạng) và sự so sánh chúng (các giá trị này) với cái đang diễn ra. Tồn tại sự sai khác nhất định (giữa "lịch sử" và hiện tại) có thể là tín hiệu về khả năng xuất hiện sự xâm nhập, gồm cả sự dừng máy chủ (máy chủ) do tràn ngập yêu cầu, do lan truyền virus, do các chương trình giả mạo v.v…

- Phương pháp tiên đoán: Trong trường hợp này thì tại các luật logic phát hiện xâm nhập đã có lập trình các kịch bản quen thuộc đối với HT; đã lập trình các đặc trưng của hệ thống báo hiệu về sự công phá hoặc là mô hình các

hành động (thao tác) của kẻ phá hoại dẫn đến xâm nhập. Rõ ràng là, phương pháp này chỉ nhận biết được các hiểm họa đã có, xác định trên cơ sở hiểu biết hệ phát hiện xâm nhập mà thôi.

Khi chúng ta thực hiện theo dõi và ghi nhật ký trong mạng và hệ thống, chúng ta có thể sử dụng thông tin này để duy trì một thế trận an toàn cao hơn, sẽ có thể bằng cách này hay cách khác. Nó cho phép chúng ta thực hiện trách nhiệm giải trình cũng cho phép chống chối bỏ, ngăn chặn những người có thể lạm dụng tài nguyên của chúng ta, giúp chúng ta trong việc phát hiện và ngăn chặn xâm nhập, và trợ giúp chúng ta trong việc chuẩn bị tài liệu cho các thủ tục pháp lý.

Chúng ta có thể tạo bằng chứng của hoạt động trực tiếp từ các bản ghi hệ thống hay mạng, hoặc phục hồi bằng chứng thông qua việc sử dụng các kỹ thuật số giám định pháp y của hệ thống hoặc các thiết bị liên quan đến. Chúng ta cũng có thể thiết lập chống chối bỏ thông qua việc sử dụng các công nghệ mã hóa, cụ thể hơn thông qua việc sử dụng các hàm băm để ký vào một thông tin liên lạc hay một tập tin (phần này sẽ trình bày kỹ hơn ở phần sau).

Một trong những động cơ của việc giám sát và ghi nhật ký trong môi trường của chúng ta là để phát hiện và ngăn chặn xâm nhập ở cả phương diện logic và vật lý. Nếu chúng ta thực hiện các cảnh báo dựa trên các hoạt động bất thường trong môi trường của chúng ta và kiểm tra thông tin mà chúng ta đăng nhập một cách thường xuyên, chúng ta sẽ có một cơ hội tốt hơn để phát hiện các cuộc tấn công đang được tiến hành và ngăn chặn những người mà chúng ta có thể thấy có nguy cơ.

Đặc biệt trong khía cạnh logic, nơi mà các cuộc tấn công có thể xảy ra trong vài phần của giây, chúng ta cũng sẽ khôn ngoan thực hiện các công cụ tự động để thực hiện các nhiệm vụ như vậy. Chúng ta có thể phân chia hệ thống như vậy thành hai loại chính: hệ thống phát hiện xâm nhập (IDS) và hệ thống phòng chống xâm nhập (IPS). Một IDS thực hiện đúng như là một công cụ giám sát và cảnh báo, chỉ thông báo cho chúng ta biết rằng một cuộc tấn công hoặc một hành động không mong muốn đã xảy ra. Một IPS thường làm việc từ các thông tin được gửi bởi IDS, thực sự có thể thực hiện hành động dựa trên những gì đang xảy ra trong môi trường. Trong một cuộc tấn công qua

mạng, một IPS có thể từ chối lưu lượng truy cập từ địa chỉ của cuộc tấn công. Chúng ta sẽ thảo luận về IDS và IPS sâu hơn trong các phần sau.

3.4.6. Tường lửa

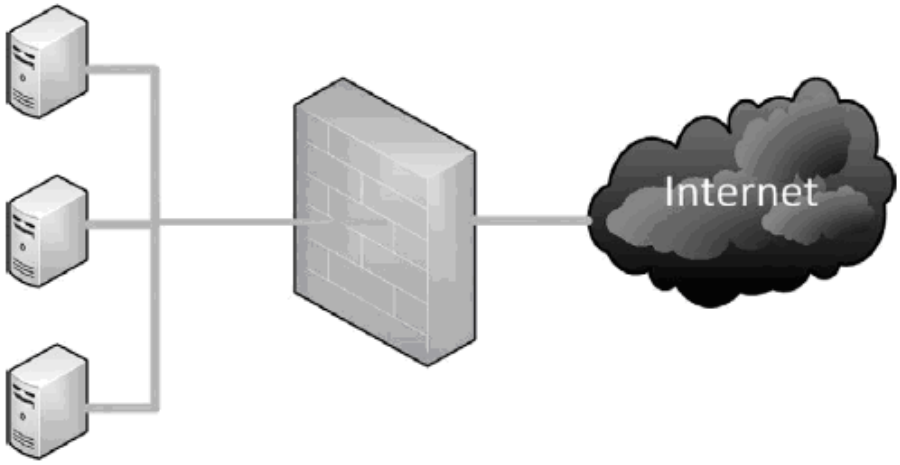
Đây là phương pháp dùng cơ chế màn chắn để BVTT trong các mạng máy tính. Nó dùng để kiểm soát các luồng TT ở cổng ra vào các máy tính, mạng LAN, WAN được bảo vệ và nó thực hiện 2 chức năng cơ bản:

- Nó tăng cường sự an toàn của các đối tượng bên trong mạng bằng việc bỏ qua các yêu cầu không hợp pháp từ môi trường bên ngoài. Điều đó làm giảm tính tổn thương của các đối tượng bên trong, vì tin tặc buộc phải vượt qua một hàng rào bảo vệ là màn chắn liên mạng (firewall), trong đó các cơ chế ATTT được tập trung rất chặt chẽ và cẩn thận.
- Nó cho phép kiểm soát các luồng TT đi ra môi trường bên ngoài do đó nâng cao được chế độ mật của hệ thống.

Ngoài chức năng kiểm soát tiếp cận, màn chắn còn bảo đảm được việc đăng ký (và kiểm toán) các trao đổi TT.

Chức năng màn chắn được thực hiện nhờ màn chắn liên mạng gọi là tường lửa (Firewall). Tường lửa là các chương trình phần mềm hoặc các thiết bị – chương trình, thực hiện việc kiểm soát các luồng TT vào và/hoặc ra khỏi hệ thống và bảo vệ hệ thống bằng cách lọc các TT.

Tường lửa thường được đặt trong mạng nơi mà chúng ta thấy mức độ tin tưởng bị thay đổi. Chúng ta có thể thấy một tường lửa nằm giữa biên giới mạng bên trong của chúng ta và mạng Internet, như hình 3.14. Chúng ta cũng có thể thấy tường lửa đặt ở vị trí bên trong mạng nội bộ của chúng ta để ngăn chặn lưu thông mạng tới các vị trí nhạy cảm bởi những người không có lý do để thực hiện điều đó.



Hình 3.14 Tường lửa

Nhiều tường lửa được sử dụng ngày nay dựa trên các khái niệm về kiểm tra các gói dữ liệu qua mạng. Việc kiểm tra này xác định cái gì nên được phép vào hoặc ra. Cho dù lưu thông là được phép hay bị cấm có thể được dựa trên một số các yếu tố khác nhau và phần lớn phụ thuộc vào độ phức tạp của các tường lửa. Ví dụ, chúng ta có thể cho phép hoặc cấm lưu lượng truy cập dựa trên giao thức được sử dụng, cho phép các lưu lượng Web và thư điện tử đi qua, nhưng cấm mọi lưu lượng khác.

Tường lửa có thể ở trong các hình thức:

- Một gói phần mềm được cài đặt trên một hệ thống máy chủ/host
- Một dụng cụ hoặc một thiết bị mạng
- Một tính năng của một số thiết bị mạng khác (chẳng hạn như một bộ định tuyến)

Ngoài ra còn có tường lửa cá nhân mà làm công việc tương tự, nhưng chỉ bảo vệ một hệ thống, chẳng hạn như một máy tính xách tay hoặc máy PC.

Tường lửa bảo đảm rằng lưu lượng truy cập mạng của một số loại nhất định (hoặc từ các ứng dụng nhất định) được phép chuyển từ mạng này sang mạng khác theo một chính sách bảo mật đã được thiết lập. Nó có thể ngăn chặn các cuộc tấn công dựa trên mạng mà thường nhằm chống lại hệ thống.

Trong số các nhiệm vụ khác, tường lửa có thể:

- Ghi lại các lưu lượng truy cập và các nỗ lực kết nối
- Xác thực những người dùng đang cố gắng để tạo ra các kết nối mạng
- Kiểm tra các gói dữ liệu mạng và theo dõi trạng thái của các kết nối để đảm bảo chúng hoạt động như mong đợi

- Kiểm tra lưu lượng truy cập ứng dụng, ví dụ, virus thư điện tử hoặc các trang web

- Bảo vệ mạng nội bộ bằng cách thực hiện dịch địa chỉ mạng (NAT)

Bằng cách ngăn chặn truy cập không mong muốn vào mạng của tổ chức, nguy cơ một hành vi vi phạm an ninh thông tin sẽ giảm đáng kể.

Một tường lửa có thể không:

- Ngăn chặn các cuộc tấn công từ Internet trên giao thức được xác định.

- Chặn tấn công dial-up vào các máy chủ truy cập từ xa và các modem trong mạng của bạn

Sự lọc TT ở đây gồm: phân tích TT theo tập hợp các tiêu chí nhất định và đưa ra quyết định cho phép TT đi vào (hoặc ra) khỏi hệ thống.

Nói chung màn chắn liên mạng khi thực hiện các chức năng của mình, tiến hành phân tích tất cả các luồng TT giữa hai mảng của một mạng hoặc giữa các mạng riêng biệt.

Màn chắn liên mạng phân loại như sau:

- Theo vị trí đặt trong mạng: bên ngoài và bên trong để bảo vệ khỏi mạng ngoài hoặc giữa các mảng.

- Theo mức lọc: tương ứng với mô hình chuẩn mạng mở OSI của ISO.

Các màn bên ngoài liên quan đến phân tích giao thức TCP/IP siêu mạng Internet. Đối với màn chắn bên trong đặc trưng là đa giao thức. Ví dụ, nếu sử dụng Hệ điều hành mạng Nowell Netware thì cần tính tới giao thức SPX/IPX.

Hoạt động của các màn chắn liên mạng đều sử dụng TT của các mức khác nhau của mô hình OSI. Màn liên mạng lọc TT ở mức càng cao thì mức bảo vệ an toàn của nó càng cao.

Theo mức lọc các gói tin, Tường lửa chia ra 4 loại cơ bản:

- Tường lửa lọc gói
- Cổng gác mức phiên
- Cổng gác mức ứng dụng
- Thanh tra trạng thái

3.4.6.1. Tường lửa lọc gói

Đó là tập hợp các chương trình làm việc trên máy chủ sao cho có thể lọc tất cả các gói tin đi vào và đi ra. Đây là một trong những công nghệ tường lửa

lâu đời và đơn giản nhất. Sự lọc được thực hiện bằng cách phân tích địa chỉ IP của nguồn và đích, và cả của các port (socket) trong thành phần của các gói TCP và UDP và so sánh chúng với một bảng quyền được cấu hình trong tường lửa lọc gói. Tưởng lửa loại này đơn giản trong sử dụng, rẻ tiền, ít ảnh hưởng tới năng suất hệ thống. Nhược điểm cơ bản của chúng là tính dễ bị tổn thương của địa chỉ IP. Chẳng hạn, IP-spoofing là một ví dụ điển hình. IP-spoofing (nghĩa là sự giả mạo địa chỉ IP), khi mà một tin tặc sử dụng một địa chỉ IP giả danh để tấn công vào mạng. Tường lửa lọc gói cũng phức tạp trong cấu hình: để lắp đặt nó đòi hỏi phải biết các thủ tục mức mạng, mức vận tải và mức ứng dụng. Sau đây là bảng các loại tường lửa và các mức mạng tương ứng của mô hình mạng mở OSI (Open System Interconnection):

Bảng 3.3 Các loại tường lửa và các mức mạng tương ứng

Các mức OSI	Thủ tục Internet (IP)	Loại Firewalls
7. Ứng dụng	Telnet, FTP, DNS, NPS, PING, SMTP, HTTP	Cổng gác ứng dụng Thanh tra trạng thái
6. Biểu diễn dữ liệu		
5. Phiên	TCP, UDP	Cổng gác tầng phiên
4. Vận tải	TCP, UDP	
3. Mạng	IP, ICMP	Tường lửa lọc gói
2. Liên kết dữ liệu		
1. Vật lý		

3.4.6.2. Cổng gác tầng phiên

Tường lửa loại này kiểm soát sự cho phép một phiên liên lạc (tức là khép kín mạng liên lạc, vì thế tiếng Anh gọi là Circuit – level Gateway). Nó theo dõi việc xác lập liên lạc giữa client hợp pháp với máy chủ host bên ngoài (và ngược lại) và quyết định cho phép (hay không?) yêu cầu phiên liên lạc. Trong việc lọc các gói, cổng gác tầng phiên dựa vào TT chứa trong đầu các gói của tầng phiên của thủ tục TCP, tức là nó hoạt động ở mức cao hơn (2 tầng) so với tường lửa lọc gói (firewall lọc gói hoạt động ở tầng mạng 3 còn cổng gác này làm việc ở tầng phiên 5). hệ thống tường lửa này thường có chức năng truyền các địa chỉ mạng trong đó có chứa các địa chỉ IP, tức là nó loại bỏ các IP-spoofing. Tuy nhiên, vì nó chỉ kiểm soát các gói ở tầng phiên nên việc

kiểm soát nội dung các gói tin do các dịch vụ khác nhau tạo thành vẫn không có được. Để khắc phục nhược điểm này người ta dùng Tường lửa Cổng gác tầng ứng dụng.

3.4.6.3. Cổng gác tầng ứng dụng

Tường lửa loại này kiểm tra nội dung của mỗi gói tin đi qua cổng gác và nó có thể lọc các loại lệnh riêng biệt hoặc các TT trong tầng ứng dụng. Đây là một loại firewall hoàn thiện và chắc chắn hơn cả. Nó sử dụng các chương trình – trung gian proxies (uỷ nhiệm) của mức ứng dụng hay là các chương trình – nhân viên agent. Các agent dùng để cho các dịch vụ cụ thể của Internet (HTTP, FTP, TELNET, …), chúng được đưa vào với mục đích kiểm tra các gói mạng về các dữ liệu chính xác. Tuy nhiên cổng gác tầng ứng dụng làm giảm hiệu suất của hệ thống do việc xử lý lại trong các chương trình – trung gian (trong các chương trình – agent).

Nhược điểm của nó còn là việc phải thiết kế các chương trình – trung gian mới mỗi khi có một dịch vụ mới được đưa vào Internet.

3.4.6.4. Tường lửa thanh tra trạng thái

Thanh tra trạng thái bao gồm các yếu tố của cả 3 loại tường lửa ở trên. Như một bộ lọc gói, nó làm việc ở tầng mạng lọc tất cả các gói ra vào trên cơ sở kiểm tra địa chỉ IP và số các cổng. Nó cũng thực hiện chức năng của cổng gác tầng phiên bằng cách xác định các gói tin thuộc mỗi phiên liên lạc. Và cuối cùng, nó thực hiện chức năng Gác tầng ứng dụng, đánh giá nội dung mỗi gói tin theo chính sách an toàn được mỗi tổ chức, cơ quan cụ thể đưa ra.

Đặc thù của Thanh tra trạng thái là: nó chặn bắt và phân tích từng gói tin tại tầng ứng dụng của mô hình OSI. Thay vì dùng các chương trình – trung gian liên quan tới các ứng dụng, Thanh tra trạng thái sử dụng các thuật toán nhận biết và xử lý dữ liệu, đặc biệt tại mức ứng dụng, trong đó các gói được so sánh với các tập dữ liệu đã biết; điều đó bảo đảm sự lọc gói hiệu quả cao hơn nhiều.

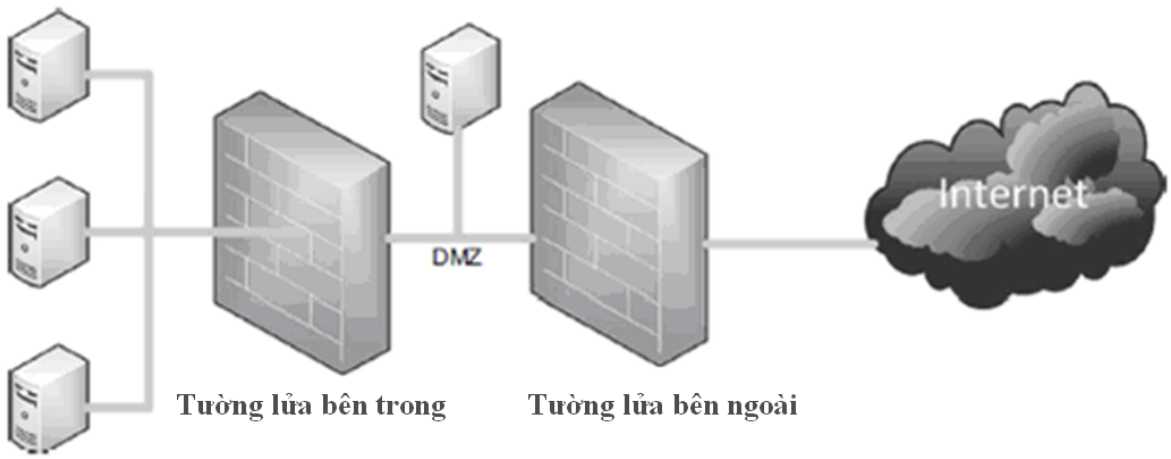
Một tường lửa thanh tra trạng thái sử dụng bảng trạng thái để theo dõi trạng thái của các kết nối và sẽ chỉ cho phép các lưu thông đi qua là một phần của kết nối mới hoặc của một kết nối đã được thiết lập và chưa bị đóng. Ví dụ, kiểu tường lửa này có thể xác định và theo dõi lưu lượng truy cập liên

quan đến kết nối của một người dùng cụ thể tới một trang Web, và biết được khi kết nối bị đóng thì các lưu thông tiếp tục của kết nối này sẽ là bất hợp pháp và không được đi qua.

Ngoài ra, khi chúng ta nghiên cứu về tường lửa, chúng ta cần phải đề cập đến một kiểu đặc biệt của tường lửa: DMZ.

3.4.6.5. DMZ

Một vùng DMZ, hay vùng phi quân sự, nói chung là sự kết hợp giữa một tính năng thiết kế mạng và một thiết bị bảo vệ chẳng hạn như một tường lửa. Chúng ta thường có thể làm tăng mức độ bảo mật trên mạng của chúng ta bằng cách phân chia chúng một cách hợp lý. Khi chúng ta xem xét một hệ thống mà cần phải được tiếp xúc với các mạng bên ngoài như Internet để hoạt động, chẳng hạn như máy chủ thư điện tử, máy chủ web, chúng ta cần đảm bảo an toàn cho chúng và an toàn cả các thiết bị trên mạng phía sau chúng. Chúng ta thường có thể làm điều này bằng cách đặt một lớp bảo vệ giữa các thiết bị, chẳng hạn như máy chủ thư của chúng ta và Internet, và giữa phần còn lại trong mạng của chúng ta và các thiết bị như trong hình dưới đây:



Hình 3.15 DMZ

Điều này chỉ cho phép các lưu thông mà cần phải đến được máy chủ mail, ví dụ, giao thức IMAP (Internet Message Access Protocol) và giao thức SMTP (Simple Message Transfer Protocol) trên cổng 143 và 25, tương ứng – truy cập tới máy chủ thư của chúng ta, và các cổng tương tự để đi vào trong mạng của chúng ta. Giả sử không có các dịch vụ khác đang chạy trên cùng hệ

thống, chúng ta có thể hạn chế lưu thông đi vào và đi ra khỏi vùng DMZ nơi mà máy chủ thư của chúng ta ở đó với những cổng cụ thể.

3.4.7. Hệ thống phòng chống và phát hiện xâm nhập

Hiện nay, hệ thống IDS/IPS đã được triển khai rộng rãi trên toàn thế giới, với đặc điểm mô hình triển khai đơn giản, cách thức phát hiện các truy nhập hiệu quả đã góp phần nâng cao độ tin cậy của hệ thống an ninh.

3.4.7.1. Hệ thống phát hiện xâm nhập

IDS là từ viết tắt tiếng anh của Intrusion Detection System hay còn gọi là hệ thống phát hiện các truy nhập trái phép. IDS có nhiệm vụ rà quét các gói tin trên mạng, phát hiện các truy nhập trái phép, các dấu hiệu tấn công vào hệ thống từ đó cảnh báo cho người quản trị hay hệ thống biết về nguy cơ xảy ra tấn cống trước khi nó xảy ra.

IDS có thể được triển khai theo một số cách tùy thuộc vào mục tiêu hay mục đích của hệ thống. Nó có thể bảo vệ các máy chủ nội bộ quan trọng, xác định các cuộc tấn công dựa trên Internet và giám sát các điểm truy cập mạng.

a) Vai trò, chức năng của IDS

* Phát hiện các nguy cơ tấn công và truy nhập trái phép

- Đây là vai trò chính của một hệ thống phát hiện xâm nhập IDS, nó có nhiệm vụ xác định những tấn công và truy nhập trái phép vào hệ thống mạng bên trong.

- Hệ thống IDS có khả năng hỗ trợ phát hiện các nguy cơ an ninh đe dọa mạng mà các hệ thống khác (như tường lửa) không có, kết hợp với hệ thống ngăn chặn xâm nhập IPS giúp cho hệ thống chặn đứng, hạn chế các cuộc tấn công, xâm nhập từ bên ngoài.

* Tăng khả năng hiểu biết về những gì đang hoạt động trên mạng

IDS cung cấp khả năng giám sát xâm nhập và khả năng mô tả an ninh để cung cấp kiến thức tổng hợp về những gì đang chạy trên mạng từ góc độ ứng dụng cũng như góc độ mạng cùng với khả năng liên kết với phân tích, điều tra an ninh nhằm đưa ra các thông tin về hệ thống nhờ đó giúp người quản trị nắm bắt và hiểu rõ những gì đang diễn ra trên mạng.

* Khả năng cảnh báo và hỗ trợ ngăn chặn tấn công

- IDS có thể hoạt động trong các chế độ làm việc của một thiết bị giám sát thụ động (sniffer mode) hỗ trợ cho các thiết bị giám sát chủ động hay như là một thiết bị ngăn chặn chủ động (khả năng loại bỏ lưu lượng khả nghi).

- IDS hỗ trợ cho các hệ thống an ninh đưa ra các quyết định về lưu lượng dựa trên địa chỉ IP hoặc cổng cũng như đặc tính của tấn công.

- Ví dụ: Như mẫu tấn công hoặc bất thường về giao thức hoặc lưu lượng tương tác đến từ những máy chủ không hợp lệ.

- IDS còn có thể cảnh báo và ghi lại các biến cố cũng như thực hiện bắt giữ gói lưu lượng khi phát hiện tấn công để cung cấp cho nhà quản trị mạng các thông tin để phân tích và điều tra các biến cố.

- Ngay sau khi các phép phân tích và điều tra được thực hiện, một quy tắc loại bỏ lưu lượng sẽ được đưa ra dựa trên kết quả phân tích, điều tra đó.

- Tổ hợp của những thuộc tính và khả năng này cung cấp cho nhà quản trị mạng khả năng tích hợp IDS vào mạng và tăng cường an ninh đến một mức độ mà trước đây không thể đạt đến bằng các biện pháp đơn lẻ như bức tường lửa.

Ta nên xem xét việc cài đặt một IDS nếu ta:

- Đã bị vi phạm an ninh trong vòng mười hai tháng qua
- Chạy một trang web cho giao dịch kinh doanh
- Muốn phân vùng nội bộ của mạng
- Có một tổ chức cấu hình cao chịu trách nhiệm thu hút các cuộc tấn công độc hại
- Có một trang web từ xa không được giám sát với các liên kết ISP
- Đã thuê ngoài một phần hoặc tất cả các hoạt động CNTT
- Có kết nối với khách hàng hay đối tác kinh doanh
- Không có nhân viên an ninh vĩnh viễn hay toàn thời gian

b) Các phương pháp phát hiện xâm nhập

Các IDS thường được phân loại thông qua cách thức phát hiện các cuộc tấn công. Nói chung, chúng được chia thành hai loại chính: phát hiện dựa trên các mẫu (signature-based) và phát hiện dựa những bất thường (anomaly-based).

IDS dựa trên mẫu làm việc theo cách tương tự như hầu hết các hệ thống chống virus. Chúng duy trì một cơ sở dữ liệu chữ ký mà có thể báo hiệu một

loại hình cụ thể của cuộc tấn công và so sánh lưu lượng truy cập đến với những chữ ký. Nói chung, phương pháp này hoạt động tốt, trừ khi chúng ta gặp phải một cuộc tấn công mới, hoặc đã được xây dựng đặc biệt để không phù hợp với mẫu tấn công hiện có. Một trong những hạn chế lớn để phương pháp này là nhiều hệ thống dựa trên chữ ký chỉ dựa vào cơ sở dữ liệu mẫu của chúng để phát hiện các cuộc tấn công. Nếu chúng ta không có một mẫu cho các cuộc tấn công, chúng ta không thể thấy tất cả các cuộc tấn công đó. Thêm vào đó, kẻ tấn công thủ công vào lưu thông có thể có quyền truy cập vào các công cụ IDS mà chúng ta đang sử dụng, và có thể có thể kiểm tra các tấn công chống lại họ để có thể tránh được các biện pháp an ninh của chúng ta.

Phương pháp phát hiện chính khác của IDS là phát hiện dựa trên bất thường. IDS dựa trên bất thường thường làm việc bằng cách lấy một đường cơ sở của lưu thông và các hành vi bình thường đang diễn ra trên mạng. Chúng có thể đo tình trạng lưu thông trên các mạng so sánh với đường cơ sở này để phát hiện các mẫu mà không có mặt trong các lưu thông bình thường. Như vậy phương pháp này có thể làm việc rất tốt khi chúng ta đang tiến hành tìm kiếm để phát hiện các cuộc tấn công mới hoặc các cuộc tấn công đã được cố tình lắp ráp để tránh các IDS. Mặt khác, chúng ta cũng có thể thấy có một số lượng lớn cảnh báo giả từ IDS dựa trên bất thường hơn là từ IDS dựa trên mẫu. Nếu lưu thông trên mạng thay đổi so với những gì đã có khi chúng ta lấy đường cơ sở, IDS có thể xem đây là dấu hiệu của một cuộc tấn công, và tương tự đối với các hoạt động hợp pháp gây ra các mẫu lưu thông bất thường hoặc đột biến trong lưu thông.

Tất nhiên chúng ta có thể đặt một IDS tại vị trí mà cung cấp cho chúng ta một số lợi thế của từng loại hình phát hiện và sử dụng cả hai phương pháp dựa trên mẫu và dựa trên bất thường trong một IDS duy nhất. Điều này sẽ cho phép chúng ta linh hoạt nhiều hơn nữa trong việc phát hiện các cuộc tấn công, mặc dù có lẽ sẽ mất chi phí về sự chậm trễ trong hành động phát hiện và gây ra một tụt hậu trong việc phát hiện.

c) Các thành phần của IDS ở mức vật lý

Một hệ thống IDS bao gồm các thành phần:

Bộ phát hiện (Sensor): Là bộ phận làm nhiệm vụ phát hiện các sự kiện có khả năng đe dọa an ninh của hệ thống mạng, Sensor có chức năng rà quét

nội dung của các gói tin trên mạng, so sánh nội dung với các mẫu và phát hiện ra các dấu hiệu tấn công hay còn gọi là sự kiện.

Bộ giao diện (Console): Là bộ phận làm nhiệm vụ giám sát các sự kiện, các cảnh báo được phát hiện và sinh ra từ các Sensor và điều khiển hoạt động của các bộ Sensor.

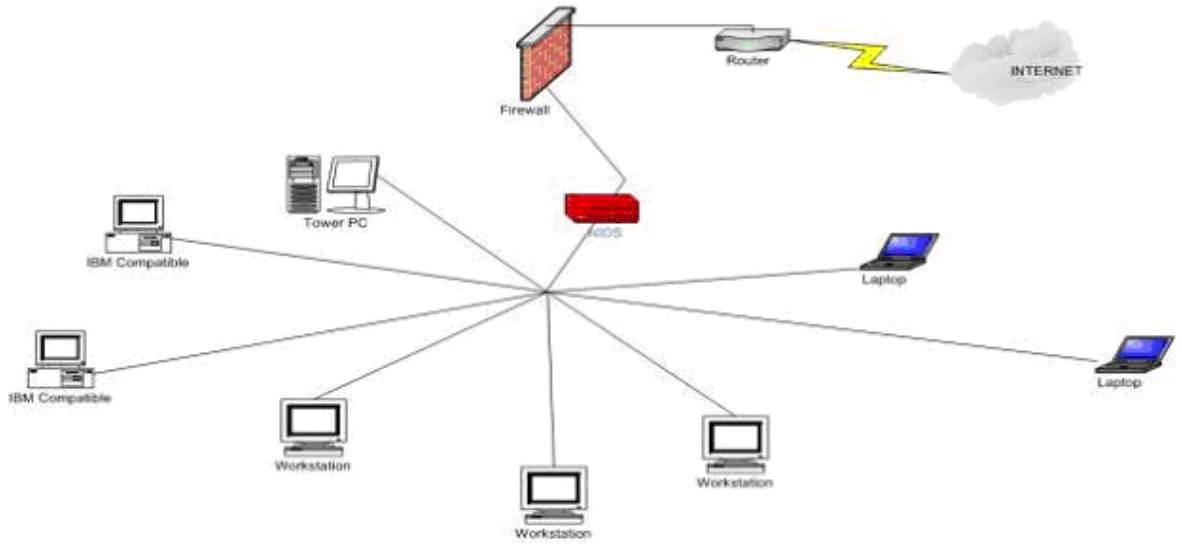
Bộ xử lý (Engine): Có nhiệm vụ ghi lại tất cả các báo cáo về các sự kiện được phát hiện bởi các Sensor trong một cơ sở dữ liệu và sử dụng một hệ thống các luật để đưa ra các cảnh báo trên các sự kiện an ninh nhận được cho hệ thống hoặc cho người quản trị.

Như vậy, hệ thống IDS hoạt động theo cơ chế "phát hiện và cảnh báo". Các Sensor là bộ phận được bộ trí trên hệ thống tại những điểm cần kiểm soát, Sensor bắt các gói tin trên mạng, phân tích gói tin để tìm các dấu hiệu tấn công, nếu gói tin có dấu hiệu tấn công, Sensor lập tức đánh dấu đấy là một sự kiện và gửi báo cáo kết quả về cho Engine, Engine ghi nhận tất cả các báo cáo của tất cả các Sensor, lưu các báo cáo vào trong cơ sở dữ liệu của mình và quyết định đưa ra mức cảnh báo đối với sự kiện nhận được. Console làm nhiệm vụ giám sát các sự kiện và cảnh báo đồng thời điều khiển hoạt động của các Sensor.

d) Phân loại

IDS được chia làm hai loại chính:

• NIDS (Network Intrusion Detection System): đặt tại những điểm quan trọng của hệ thống mạng, để phát hiện xâm nhập cho khu vực đó.



Hình 3.16 NIDS (Network Intrusion Detection System)

NIDS thường sẽ được gắn vào mạng ở một vị trí nơi mà chúng có thể theo dõi lưu lượng truy cập đi qua, nhưng chúng cần phải được đặt một cách cẩn thận để không bị quá tải. Việc đặt một NIDS đằng sau một thiết bị lọc, chẳng hạn như một bức tường lửa, có thể giúp loại trừ một số lưu lượng truy cập giả mạo vì thế sẽ giảm lưu lượng truy cập NIDS cần kiểm tra. Bởi vì NIDS cần phải kiểm tra một số lượng lớn lưu lượng truy cập trên một mạng cụ thể, chúng thường chỉ có thể làm một kiểm tra tương đối qua loa để xác định tình hình trên mạng là bình thường hay không. Bởi vì điều này, một NIDS có thể bỏ lỡ một số loại tấn công, đặc biệt là những người sử dụng những mánh khóe thủ công đặc biệt để vượt qua kiểm tra. Các tấn công thủ công gói tin liên quan đến các gói tin được thiết kế đặc biệt của lưu lượng truy cập để chứa đựng các cuộc tấn công hoặc mã độc hại, nhưng được thiết kế để tránh sự phát hiện của IDS, tường lửa, và các thiết bị tương tự khác.

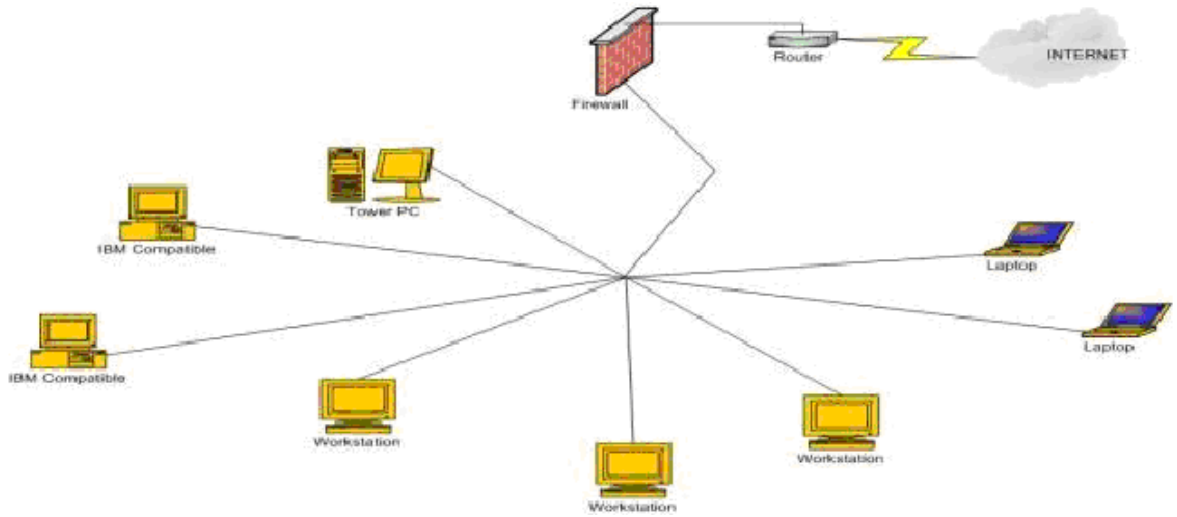
Theo chức năng sử dụng, hệ thống NIDS còn được phân thành hai hệ thống nhỏ đó là Protocol-based Intrusion Detection System (PIDS) và Application Protocol-based Intrusion Detection System (APIDS).

PIDS và APIDS được sử dụng để giám sát các giao vận và giao thức không hợp lệ hoặc không mong muốn trên luồng dữ liệu hoặc hạn chế các ngôn ngữ giao tiếp. Hệ thống Protocol-based Intrusion Detection System (PIDS) chứa một hệ thống (System) hoặc một thành phần (Agent) thường

được đặt ngay trước một máy chủ, giám sát và phân tích các giao thức trao đổi giữa các thiết bị được nối mạng (Một máy trạm hoặc một hệ thống).

Một hệ thống Application Protocol-based Intrusion Detection System (APIDS) bao gồm một hệ thống (System) hoặc một thành phần (Agent) thường nằm giữa một nhóm các máy chủ, giám sát và phân tích các trao đổi ở lớp ứng dụng của một giao thức định sẵn. Ví dụ; trên một máy chủ web với một cơ sở dữ liệu thì nó giám sát giao thức SQL để ngăn chặn các truy nhập vào ứng dụng khi trao đổi với cơ sở dữ liệu.

• HIDS (Host Intrusion Detection System): triển khai trên máy trạm hoặc máy chủ quan trọng, chỉ để bảo vệ riêng từng máy.



Hình 3.17 HIDS (Host Intrusion Detection System)

Hệ thống phát hiện xâm nhập dựa trên host (HIDS) được sử dụng để phân tích các hoạt động ở trên hoặc hướng vào các giao diện mạng của một host cụ thể. Chúng có nhiều lợi thế tương tự như hệ thống phát hiện xâm nhập dựa trên mạng (NIDS) có nhưng với phạm vi hoạt động giảm đi đáng kể. Như với phần mềm tường lửa, các công cụ này có thể dao động từ phiên bản sử dụng đơn giản tới các phiên bản thương mại phức tạp hơn nhiều, cho phép giám sát và quản lý tập trung.

Trong hệ thống HIDS, các Sensor thường thường là một phần mềm trên máy trạm (Software agent), nó giám sát tất cả các hoạt động của máy trạm mà nó nằm trên đó.

Hệ thống Host-based Intrusion Detection System bao gồm thành phần (Agent) cài đặt trên các máy trạm, nó xác định các truy nhập trái phép vào hệ

thống bằng cách phân tích các trao đổi của hệ thống, các bản ghi của các ứng dụng, sự sửa đổi các tệp tin trên hệ thống (Các file dạng binary, mật khẩu của file, dung lượng và các acl của các cơ sở dữ liệu) các hoạt động và trạng thái khác của hệ thống để từ đó phát hiện ra các dấu hiệu truy nhập trái phép vào hệ thống. Khi phát hiện ra các truy nhập trái phép, Agent lập tức sinh ra một sự kiện và gửi báo cáo về Engine, Engine tiến hành lưu các báo cáo của Agent vào cơ sở dữ liệu và tiến hành phân tích thông tin để đưa ra các cảnh báo cho người quản trị hoặc hệ thống.

Một lỗ hổng tiềm năng với HIDS quản lý tập trung là để cho các phần mềm báo cáo một cuộc tấn công tới bộ máy quản lý trong thời gian thực, thông tin cần phải được truyền qua mạng. Nếu các host đang xem xét đang bị tấn công chủ động thông qua cùng một mạng chúng ta sẽ báo cáo ở phía trên, chúng ta có thể không có khả năng để làm điều này. Chúng ta có thể cố gắng để giảm thiểu các vấn đề như vậy bằng cách gửi một tín hiệu thường xuyên từ thiết bị đến cơ chế quản lý, cho phép chúng ta giả định một vấn đề nếu chúng ta không nhìn thấy nhiều thiết bị một cách bất ngờ, nhưng điều này có thể không phải là một cách tiếp cận hoàn toàn.

* So sánh giữa hệ thống HIDS và NIDS:

Bảng 3.4 So sánh giữa HIDS và NIDS

NIDS	HIDS
Áp dụng trong phạm vi rộng (theo dõi toàn bộ hoạt động của mạng)	Áp dụng trong phạm vi một Host
Phát hiện tốt những tấn công, xâm nhập từ bên ngoài	Phát hiện tốt những tấn công, xâm nhập từ bên trong.
Phát hiện dựa trên các dữ liệu, thông tin thu thập trong toàn bộ mạng	Phát hiện dựa trên thông tin, dữ liệu trên Host
Độc lập với hệ điều hành	Phụ thuộc vào hệ điều hành trên Host đó
Tiết kiệm kinh phí khi triển khai	Yêu cầu chi phí cao
Dễ dàng cài đặt, triển khai	Phức tạp khi cài đặt, triển khai

3.4.7.2. Hệ thống IPS

IPS là viết tắt tiếng Anh của Intrusion Prevention System hay thường được gọi là hệ thống ngăn chặn truy nhập trái phép.

IPS là hệ thống kết hợp giữa hệ thống IDS và hệ thống Firewall, nó có ba thành phần chính đó là: Hệ thống Firewall, hệ thống IDS và thành phần trung gian kết nối hai hệ thống trên lại với nhau.

Firewall: là thành phần bảo vệ hệ thống mạng ở vùng biên, Firewall căn cứ trên tập luật mà nó được thiết lập từ trước để xác định cho phép hay không cho phép các gói tin được hay không được phép đi qua nó.

IDS: làm nhiệm vụ quét tất cả các gói tin trước khi hoặc sau khi đi vào mạng, đọc nội dung gói tin, phát hiện ra các dấu hiệu tấn công chứa đựng trong gói tin, nếu phát hiện có dấu hiệu tấn công, nó sinh ra cảnh báo cho hệ thống.

Thành phần trung gian kết nối: Thành phần trung gian kết nối nhận các cảnh báo và thông tin đưa ra từ hệ thống IDS, phân tích mức độ cảnh báo, tiến hành tác động lên hệ thống Firewall để cấu hình lại tập luật trên đó nhằm ngăn chặn các cuộc tấn công.

Như vậy, hệ thống IPS là một hệ thống chủ động, có khả năng phát hiện và ngăn ngừa các truy nhập trái phép, có khả năng ngăn chặn các cuộc tấn công, các nguy cơ tiềm ẩn trong nội dung của gói tin. Vì vậy hình thành lên một thế hệ Firewall mới có khả năng hoạt động ở lớp ứng dụng hay còn gọi là Application Layer Firewall.

3.4.8. Đánh giá khả năng dễ bị tổn thương và thâm nhập thử nghiệm

Đánh giá khả năng dễ bị tổn thương thường liên quan đến việc sử dụng các công cụ quét các tổn thương để xác định vị trí các lỗ hổng đó. Các công cụ này thường làm việc bằng cách quét các hệ thống mục tiêu để khám phá những cổng đang được mở trên đó, và sau đó thẩm vấn mỗi cổng mở này để tìm chính xác những dịch vụ đang lắng nghe trên cổng đó. Với thông tin này, công cụ đáng giá tổn thương sau đó có thể tham khảo cơ sở dữ liệu các thông tin dễ bị tổn thương của nó để xác định xem có lỗ hổng nào có thể có mặt. Mặc dù các cơ sở dữ liệu của các công cụ này có xu hướng khá hoàn thiện, các cuộc tấn công mới hơn hoặc những thứ mà rất ít được sử dụng bởi những

kẻ tấn công thường sẽ thoát khỏi sự chú ý của chúng. Điều này có nghĩa rằng các máy quét lỗ hổng chỉ có thể tìm thấy những vấn đề nó đã biết. Nó không thể tìm thấy những lỗ hổng mới. Ta cần phải đảm bảo rằng máy quét như vậy được cập nhật những vấn đề mới nhất bằng cách tải về bản cập nhật thường xuyên (giống như máy quét virus).

Các phần mềm máy quét được chia sẻ có sẵn miễn phí trên Internet. Một số chuyên gia sử dụng các máy quét là cơ sở duy nhất cho việc kiểm tra lỗ hổng hay thâm nhập thử nghiệm, không có sự phân tích hỗ trợ.

Bởi vì các báo cáo của máy quét có thể tạo ra các lỗi sai tích cực và tiêu cực, điều này không phải là một cách sử dụng hiệu quả về thời gian và công sức. Chúng có hiệu quả nhất khi được sử dụng làm cơ sở đánh giá tính dễ tổn thương, không phải là toàn bộ.

Thâm nhập thử nghiệm là một phương pháp tích cực hơn trong việc tìm kiếm các lỗ hổng bảo mật. Thâm nhập thử nghiệm, mặc dù nó có thể sử dụng các đánh giá tổn thương như là một điểm xuất phát, quá trình này còn gồm nhiều bước hơn nữa. Khi chúng ta tiến hành thâm nhập thử nghiệm, chúng ta mô phỏng càng giống các kỹ thuật mà một kẻ tấn công thực tế sẽ sử dụng càng tốt. Chúng ta có thể cố gắng để thu thập thêm các thông tin về môi trường mục tiêu từ người dùng các ứng dụng dựa trên Web hay các kết nối cơ sở dữ liệu Web, tiến hành các cuộc tấn công thông qua lỗ hổng chưa được vá trong các ứng dụng hay hệ điều hành, hoặc các phương pháp tương tự.

3.4.9. Phương pháp tổ chức

Đây là một phương pháp không chính tắc, được áp dụng chủ yếu với môi trường nhân viên (con người) làm việc trong hệ thống. Vì nhân viên là những người thao tác nhiều thiết bị, nhiều công việc liên quan trực tiếp tới TT được bảo vệ, nên họ phải được xem là đối tượng của bảo vệ. Các lỗi vô tình hoặc cố ý của họ có thể tạo điều kiện cho các tiếp cận trái phép xảy ra.

Bản chất phương pháp này là ở chỗ phải quy tắc hoá (đưa ra và thực hiện các quy tắc) quá trình hoạt động của hệ thống xử lý TT. Các quy tắc bao gồm một tổ hợp các biện pháp để tạo ra các điều kiện tự động xử lý và lưu giữ TT sao cho trong đó khả năng tiếp cận trái phép tới TT là nhỏ nhất. Các chuyên gia cho rằng, ngay từ khâu xây dựng công trình nhà đặt HT, phòng đặt thiết bị

nội thất, cổng, cửa… cho đến các bước của công nghệ tự động xử lý TT, tổ chức và duy trì chế độ làm việc của các nhân viên đều phải tuân thủ những quy tắc nghiêm túc. Trong hệ thống phải xác lập các quy định rõ ràng và đơn nghĩa về các công việc của người dùng, của nhân viên lập trình, của các yếu tố CSDL và các vật mang tin. Cần phải định rõ các ngày trong 1 tuần lễ và các giờ trong ngày cho phép các người dùng và nhân viên làm việc trên hệ thống. Trong từng ngày làm việc của nhân viên cần phải liệt kê rõ ràng các tài nguyên hệ thống được cho phép tiếp cận và thứ tự tiếp cận tới chúng. Cần phải có danh sách các người dùng được phép sử dụng các thiết bị kỹ thuật, các chương trình… Đối với các yếu tố CSDL, cần chỉ rõ danh sách những người được quyền tiếp cận và các thủ tục cho phép họ thực hiện. Đối với các vật mang TT phải quy định rõ, chỗ cất thường xuyên, danh sách các cá nhân có quyền nhận chúng và liệt kê các chương trình cho phép được làm việc với chúng.

Để thực hiện quy tắc hoá thường áp dụng các biện pháp tổ chức – kỹ thuật và tổ chức – pháp lý. Các biện pháp tổ chức như vậy bao phủ tất cả các yếu tố cấu thành của hệ thống xử lý TT ở tất cả các giai đoạn trong vòng đời của HT: xây dựng nhà cửa, thiết kế HT, lắp đặt và chạy thử thiết bị, thí nghiệm và kiểm tra, đưa vào sử dụng…

3.4.10. Phương pháp cưỡng chế

Đó là cách bảo vệ mà trong đó, khi người dùng và các nhân viên của hệ thống trao đổi dữ liệu buộc phải tuân thủ đầy đủ các điều luật về xử lý và sử dụng các TT được bảo vệ và cách bảo vệ này đặt họ trước pháp luật về trách nhiệm vật chất, hành chính hoặc tội phạm hình sự. Ở đây thường có các pháp lệnh, các bộ luật quy định các luật lệ sử dụng và xử lý các TT nhạy cảm, bí mật và các biện pháp trừng phạt vì phá vỡ các điều luật đó. Chúng ta có thể kể ra một số pháp lệnh và bộ luật: Pháp lệnh số 30/2000/PL-UBTVQH10 ngày 28/12/2000 về bảo vệ bí mật nhà nước, Luật Giao dịch điện tử ngày 29/11/2005, Luật Công nghệ thông tin ngày 29/6/2006, Luật Viễn thông ngày 23 tháng 11 năm 2009, Luật Cơ yếu ngày 26/11/2011, Nghị định của Chính phủ số 73/2007/NĐ-CP ngày 28 tháng 5 năm 2007 về hoạt động nghiên cứu, sản xuất, kinh doanh và sử dụng mật mã để bảo vệ thông tin không thuộc

phạm vi bí mật nhà nước, nghị định số 26/2007/NĐ-CP ngày 15/2/2007 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số, nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, nghị định số 97/2008/NĐ-CP ngày 28/8/2008 của Chính phủ quy định về quản lý, cung cấp, sử dụng Internet và thông tin điện tử trên Internet…

Mọi vi phạm phải được điều tra làm rõ. Người có hành vi vi phạm, tùy theo tính chất, hậu quả tác hại gây ra sẽ bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc truy cứu trách nhiệm hình sự.

Nếu ta có các chính sách được xác định rõ trong tổ chức, người quản lý an toàn thông tin có thể sử dụng kỹ thuật pháp y để thu thập chứng cứ có thể giúp cung cấp bằng chứng về người thực hiện vụ tấn công. Mặc dù toàn bộ nội dung của kỹ thuật pháp y là vượt quá phạm vi của giáo trình này, chúng ta dành một ít thời gian thảo luận về pháp y ở mức độ tổng quát.

Pháp y máy tính cho phép một người được đào tạo có thể phục hồi bằng chứng từ các hệ thống máy tính. Nguyên tắc đầu tiên của việc pháp y máy tính là: "không làm hại". Điều này có nghĩa rằng nếu bạn đang không biết phải làm gì, thì không làm bất cứ điều gì đối với hệ thống. Mục tiêu đầu tiên của việc pháp y máy tính là giữ cho hệ thống ở tình trạng nguyên sơ nhất có thể. Điều này có thể trái với trực quan của các chuyên gia công nghệ có bản năng muốn xem xét hệ thống để xác định chính xác những gì đang xảy ra và làm thế nào nó xảy ra. Mỗi khi chuyên gia kỹ thuật di chuyển chuột hoặc chạm vào bàn phím để nhập lệnh, hệ thống sẽ thay đổi. Điều này làm cho các bằng chứng thu thập được từ hệ thống bị nghi ngờ hơn. Sau cùng, làm thế nào người ta sẽ xác định những hành động nào đã được thực hiện bởi các nhân viên bị nghi ngờ và những hành động nào đã được thực hiện bởi các chuyên gia điều tra hành vi?

Có nhiều nơi mà bằng chứng về hoạt động có thể bị bỏ lại. Tường lửa, các bản ghi máy chủ và máy trạm làm việc là tất cả những nơi cần được nghiên cứu để xác định nếu vẫn còn có bằng chứng. Khi nói đến các máy trạm làm việc, bước đầu tiên trong pháp y máy tính là mang tính chất rất phi kỹ thuật. Trong bước đầu tiên này, các nhân viên an ninh hoặc nhân viên hỗ trợ

nên được liên hệ để xem chi tiết những gì họ biết về hệ thống. Một trong những vấn đề lớn nhất sẽ là khả năng máy trạm đang sử dụng một tiện ích mã hóa ổ cứng. Lý do cho điều này là ở bước thứ hai - "rút phích cắm". Nếu rút phích cắm của một hệ thống có một ổ cứng được mã hóa, ta có thể không bao giờ có thể xác định được những thông tin nào ở trong hệ thống. Chúng ta sẽ nói thêm về mã hóa trong phần sau của giáo trình này.

Giả sử chúng ta có thể xác nhận rằng không có mã hóa ổ đĩa cứng trên hệ thống nghi ngờ, bước tiếp theo như đã đề cập ở trên - rút phích cắm. Bây giờ, nếu hệ thống là một máy tính xách tay, việc rút ổ cắm sẽ không tắt hệ thống, nó sẽ chỉ chạy bằng năng lượng của một pin. Trong trường hợp máy tính xách tay, ta cần phải rút phích cắm và tháo pin ra. Trong mọi trường hợp, một khi hệ thống được tắt, ổ đĩa cứng trong hệ thống nên được giao cho một nhà chuyên môn có trình độ. Xin lưu ý rằng thực sự có nhiều hơn nữa các bước trong quá trình pháp y này mà những điều đó vượt khỏi phạm vi của giáo trình này.

Một khi chuyên gia có kinh nghiệm có hệ thống nghi ngờ, hoặc ít nhất là ổ đĩa cứng, người đó sẽ tạo một bản sao lưu dòng bit của ổ cứng. Một bản sao lưu dòng bit khác với một bản sao lưu tệp thông thường ở chỗ nó đưa ra một bản sao chính xác của ổ cứng. Một bản sao dòng bit không chỉ cần sao chép các tập tin và hệ thống tập tin, nó sao chép tất cả mọi thứ. Các không gian trống, không gian chùng, các mảnh tập tin, và mọi thứ khác được nhân bản vào một ổ đĩa cứng thứ hai. Lý do của việc làm này là tất cả các quá trình phục hồi dữ liệu sẽ được thực hiện trên ổ đĩa cứng thứ hai, giữ ổ cứng ban đầu trong trạng thái nguyên sơ của nó và nó sẽ không được sửa đổi. Tất cả quá trình phục hồi dữ liệu được thực hiện trên hệ thống cũng sẽ được thực hiện trên các bản sao lưu của ổ đĩa cứng.

Một khi các bản sao được thực hiện, một sự so sánh của các ổ đĩa cứng sẽ được thực hiện bằng cách sử dụng công nghệ tích hợp được gọi là băm MD5 (xem hình 3.18). Định nghĩa của băm MD5, như được lấy từ các trang web MD5, như sau:

Các thuật toán MD5 có đầu vào một bản tin có độ dài tùy ý và tạo ra một số 128 bit, là một dạng “vân tay” hay “mã số thông điệp” (message digest) của đầu vào. Người ta cho rằng sẽ không khả thi về mặt tính toán để tạo ra 2

thông điệp có cùng mã số thông điệp, hoặc tạo ra một thông điệp với mã số cho trước. Thuật toán MD5 được dự tính áp dụng cho những ứng dụng chữ ký điện tử, ở đó một file lớn phải được "nén" một cách an toàn trước khi mã hóa với một khóa riêng dưới một hệ mã hóa công khai như RSA.

Thuật toán MD5 được thiết kế để chạy tương đối nhanh trên các máy 32 bit, có thể được thực hiện một cách khá gọn.

Về bản chất, MD5 là một cách để xác minh tính toàn vẹn dữ liệu, và là phương pháp đáng tin cậy hơn nhiều so với kiểm tra và nhiều phương pháp thường được sử dụng khác.

Sau khi thực hiện băm MD5 đối với mỗi ổ đĩa, các giá trị tương ứng sau đó được so sánh. Nếu các giá trị là như nhau, thì hai ổ đĩa giống hệt nhau, nếu các giá trị MD5 là khác nhau, thì sao lưu dòng bit thất bại và các ổ đĩa là khác nhau. Băm MD5 rất hay được sử dụng để xác minh tính toàn vẹn của một tập tin. Các giá trị có thể được sử dụng để đảm bảo rằng một tập tin đã không thay đổi trong suốt quá trình tải về và cũng có thể được sử dụng như một thành phần của một chữ ký số.

Sau khi các ổ đĩa cứng đã được so sánh và tìm thấy là giống nhau, các chuyên gia pháp y sẽ bắt đầu xem xét các ổ đĩa cứng để tìm bằng chứng cho thấy các cuộc tấn công đã được đưa ra từ máy đó. Các chuyên gia pháp y sẽ cố gắng phục hồi các file đã xóa, sẽ tìm kiếm các mảnh tập tin trong không gian chùng, và cũng sẽ xem xét thông qua các tập tin dữ liệu trên hệ thống nghi ngờ để xem nếu có bằng chứng hiện diện. Nếu bất kỳ bằng chứng nào được tìm thấy trên hệ thống, chuyên gia pháp y sẽ viết tài liệu về bằng chứng đó và biến nó thành một bản báo cáo cuối cùng.


.: Archive Search Results for: wireless

#	Rank	File Name	MD5 Checksum
1	Full Match	9907-exploits/ATT_DoS.txt	16dcd9165b23bf5d2e952fa134284b43
DoS attack on AT&T Wireless text-messaging service			
2	Full Match	advisories/linux-security/linux-security.1-9.txt	61dfd39ef48fbea8f6afa7dbfb9027df
Linux Security Week June 26 - In this issue: The default configuration of wu-ftpd is vulnerable to remote users gaining root access, Simple Object Access Protocol (SOAP), Network Intrusion Detection Using Snort, Updates for Mandrake bind, cdrecord, dump, fdutils, kdesu, xemacs, and xlockmore, Remote users can cause a FreeBSD system to panic and reboot via bugs in the processing of IP options in the FreeBSD IP stack, Remote vulnerabilities exist with all Zope-2.0 releases, NetBSD: libdes vulnerability, RedHat: 2.2.16 Kernel Released, Bastille Linux Review, and Intel admits wireless security concerns. Homepage: http://www.linuxsecurity.com. By Benjamin Thomas			

Hình 3.18 Trang web với giá trị MD5

3.4.11. Phương pháp giáo dục

Đó là phương pháp bảo vệ, trong đó tạo ra các điều kiện mà các điều luật xử lý và sử dụng TT được bảo vệ quyết định bởi các tiêu chuẩn đạo đức và thói quen. Đó là các chuẩn mực đã hình thành hoặc đang hình thành theo sự phát triển và phổ biến của các máy tính điện tử. Các chuẩn mực này đa phần không là bắt buộc như các điều luật định, tuy nhiên việc không tuân thủ chúng thường dẫn đến mất uy tín, danh dự của cá nhân hoặc tổ chức (mất thương hiệu). Các chuẩn mực đạo đức nhiều khi không "thành văn" (ví dụ các chuẩn được công nhận chung về danh dự, về yêu nước…) và nhiều khi được quy định theo trật tự pháp luật ở dạng các bảng luật lệ hoặc hướng dẫn. Điển hình ở đây có thể nêu ví dụ là "Các quy tắc ứng xử chuyên môn" của các thành viên Hiệp hội người dùng MTĐT Hoa Kỳ.

Cập nhật và nâng cao kiến thức về ATTT và nhận thức về vai trò của nó trong hệ thống công nghệ thông tin là một điều rất quan trọng và cấp bách vì xét cho cùng hành động của con người là yếu tố quyết định . Mặc dù ATTT được biết đến rộng rãi nhưng yếu tố con người thường ít được các tổ chức quan tâm đến. Đối với những nhà quản trị, họ cần một chính sách an toàn và một chương trình nhận thức cũng như đánh giá chất lượng về ATTT nhưng tiếc rằng hiện nay chưa có nhiều giải pháp thực sự quan tâm vào vấn đề làm sao để tăng cường sự vững chắc cho mối liên kết vốn dĩ rất yếu ớt này trong mắt xích ATTT.

Để có hiệu quả, các chính sách, thủ tục và tiêu chuẩn phải được đào tạo và củng cố cho người lao động. Quá trình này phải được thực hiện liên tục và không được quá sáu tháng giữa các lần gia cố. Việc chỉ cần công bố các chính sách và mong đợi nhân viên đọc, hiểu, và thực hiện những gì được yêu cầu là không đủ. Họ cần phải được đào tạo để nhấn mạnh những gì là quan trọng và làm thế nào nó sẽ giúp họ làm công việc của mình. Việc đào tạo này nên được bắt đầu từ định hướng nhân viên mới và tiếp tục trong quá trình làm việc. Khi một người không còn là nhân viên nữa, thời điểm củng cố cuối cùng nên được thực hiện trong quá trình phỏng vấn thôi việc.

Một phương pháp khác để giữ nhân viên đã được thông báo và đào tạo là có một trang web dành riêng cho vấn đề an toàn. Nó phải được cập nhật thường xuyên và nên bao gồm các thủ đoạn kỹ nghệ xã hội mới. Nó có thể

chứa một "mẹo an toàn trong ngày" và nhắc nhở nhân viên phát hiện những dấu hiệu lừa đảo điển hình. Những dấu hiệu này có thể bao gồm các hành vi như:

- Từ chối cung cấp thông tin liên hệ
- Thực hiện vội vã các quá trình
- Vội vã đưa ra và loại bỏ các tên người một cách lúng túng
- Hăm dọa nếu không cung cấp thông tin
- Những lỗi nhỏ
- Yêu cầu thông tin hoặc truy cập bị cấm
- Bỗng dưng khen ngợi, ca tụng một cách khác thường
- Tỏ ra khó chịu, bực bội khi được hỏi

Là một phần của quá trình đào tạo hay giáo dục này, việc củng cố thêm giúp nắm bắt tốt hơn. Khi những nhân viên làm điều đúng, chắc chắn rằng họ được ghi nhận là thích hợp. Đào tạo các nhân viên sẽ gọi cho ai nếu họ nghi ngờ họ đang bị tấn công lừa đảo.

Một kẻ tấn công với đủ thời gian, kiên nhẫn và quyết tâm cuối cùng sẽ khai thác một số điểm yếu trong môi trường kiểm soát của doanh nghiệp. Nâng cao nhận thức của nhân viên và chấp nhận biện pháp tự vệ sẽ trở thành màn chắn đầu tiên của chúng ta trong việc phòng thủ trong trận chiến chống lại những kẻ tấn công này. Phòng ngự tốt nhất chống lại các tấn công nhằm vào con người là đòi hỏi người lao động được kiểm tra và nâng cao nhận thức một cách thường xuyên.

Một lực lượng lao động được đào tạo, có đầy đủ thông tin là một trong những vũ khí mạnh nhất trong kho vũ khí của một người quản lý an ninh thông tin. Có nhiều lý do tại sao, bao gồm:

- Con người rất giỏi trong việc phát hiện các bất thường; tốt hơn nhiều so với máy
- Một tỷ lệ lớn các sự cố an ninh thông tin xảy ra thông qua các nhân viên không biết hoặc hiểu biết
- Đội ngũ nhân viên năng động sẽ báo cáo (và hành động theo) các xu hướng và các sự cố mà không có quá trình cơ giới hóa thực tế có thể hy vọng phát hiện

Vấn đề chính là động lực. Nếu không có động lực đúng đắn, không có số lượng kiến thức hay sự hiểu biết sẽ thay đổi hành vi của nhân viên. Những gì cần thiết là kiến thức và sự hiểu biết thích hợp đi kèm với hành động thích hợp.

Bất kỳ sáng kiến an toàn thông tin đều phải được đi kèm giữa một sự chủ động với sự giáo dục và nhận thức. Làm thế nào để điều này được thực hiện phụ thuộc vào nhiều yếu tố khác nhau, bao gồm:

- Mức độ rủi ro được nhận thức
- Ngân sách có sẵn - thường phụ thuộc vào mức độ rủi ro được nhận thức
- Cơ sở hạ tầng kỹ thuật của các tổ chức bị ảnh hưởng
- Lan truyền địa lý
- Văn hóa doanh nghiệp

Vấn đề giáo dục và nhận thức đã được giải quyết theo một số cách khác nhau, một số thành công và một số khác hiển nhiên không như vậy. Nhiều sáng kiến thất bại bởi vì chúng không có cấu trúc.

Hiện nay, một số doanh nghiệp tại Việt Nam đã có sự chuyển biến tích cực trong vấn đề nhận thức về ATTT. Họ sẵn sàng đầu tư ngân sách đào tạo nguồn nhân lực nhằm tạo nền tảng vững chắc về nhận thức và kiến thức ATTT cho đội ngũ nhân viên của doanh nghiệp. Điển hình là như: Sở Khoa học và Công nghệ Đồng Nai, Công ty Bảo hiểm Bảo Minh, Fujitsu Vietnam, Ngân hàng Á Châu ...

Bên cạnh đó vẫn còn nhiều doanh nghiệp nhất là các doanh nghiệp vừa và nhỏ vẫn chưa tiếp cận và hiểu hết tầm quan trọng của việc thiết lập các chính sách về ATTT và quản lý tiêu chuẩn chất lượng ATTT theo ISO (sẽ được trình bày ở chương 5) thực sự vẫn còn xa lạ và mới mẻ đối với họ.

3.5. CÂU HỎI

1. Kể tên theo thứ tự quan trọng ba mối quan tâm lớn đối với an toàn vật lý?
2. Thuật toán xác thực có những ưu điểm và nhược điểm gì so với sơ đồ dùng mật khẩu?
3. Chúng ta gọi quá trình mà trong đó máy trạm xác thực với máy chủ và máy chủ xác thực với máy trạm là gì?

4. Nếu chúng ta đang sử dụng một mật khẩu 8 ký tự và chỉ chứa các chữ thường, sẽ tăng sức mạnh như thế nào khi ta tăng lên thành 10 ký tự ?
5. Hãy trình bày sự khác nhau giữa MAC và DAC trong kiểm soát truy cập?
6. Những loại kiểm soát truy cập nào có thể được sử dụng trong trường hợp chúng ta muốn ngăn chặn người dùng đăng nhập vào tài khoản của họ sau giờ làm việc?
7. Giải thích vấn đề người được ủy quyền nhầm lẫn có thể cho phép leo thang đặc quyền xảy ra như thế nào?
8. Sự khác biệt giữa đánh giá lỗ hổng và thâm nhập thử nghiệm là gì?
9. Phân biệt sự giống và khác nhau giữa Hệ phát hiện xâm nhập với Đăng ký và kiểm toán?
10. Mã hoá TT là phương pháp bảo vệ chống lại những hiểm họa loại gì?
11. Hãy giải thích khả năng của phương pháp mã hoá TT chống lại:
    a) Việc nghe trộm trên các đường liên lạc.
    b) Tiếp cận vật lý từ xa tới các file.
12. Giải thích sự khác biệt giữa phát hiện dựa vào mẫu và phát hiện bất thường trong IDS.
13. Hãy so sánh ưu và nhược điểm của việc mã hoá TT bằng thiết bị mật mã (máy) và bằng chương trình phần mềm?
14. Với một môi trường có chứa các máy chủ có thể xử lý dữ liệu khách hàng nhạy cảm, một số trong đó được tiếp xúc với Internet, chúng ta nên tiến hành đánh giá tổn thương, thâm nhập kiểm tra hay cả hai? Tại sao?
15. Trong quá trình an toàn hoạt động, sự khác biệt giữa đánh giá các hiểm họa và đánh giá lỗ hổng là gì?
16. Chúng ta sẽ sử dụng một DMZ để bảo vệ khi nào?

CHƯƠNG 4. CHÍNH SÁCH VÀ MÔ HÌNH AN TOÀN THÔNG TIN

4.1. CHÍNH SÁCH AN TOÀN THÔNG TIN

Như chúng ta đã nói ở chương 1, ATTT là một mắt xích liên kết hai yếu tố: yếu tố công nghệ và yếu tố con người.

1. Yếu tố công nghệ: bao gồm những sản phẩm như Firewall, phần mềm phòng chống virus, giải pháp mật mã, sản phẩm mạng, hệ điều hành và những ứng dụng như: trình duyệt Internet và phần mềm nhận Thư điện tử từ máy trạm.

2. Yếu tố con người: Là những người sử dụng máy tính, những người làm việc với thông tin và sử dụng máy tính trong công việc của mình.

Hai yếu tố trên được liên kết lại thông qua các chính sách về ATTT. Phần này chúng ta sẽ tìm hiểu kỹ về chính sách an toàn thông tin.

4.1.1. Các khái niệm cơ bản

Khi nghiên cứu các vấn đề ATTT trong các hệ thống TT – VT, chúng ta muốn nói về những trạng thái nhất định của hệ thống và trạng thái an toàn TT của hệ thống là điều chúng ta mong muốn. Một hệ thống tự động bao giờ cũng phải được biểu diễn bởi một mô hình (ít nhất là mô hình cấu trúc, nó gồm những thành tố gì, các tương tác giữa chúng ra sao). Vấn đề an toàn hệ thống phải được mô tả trong mô hình đó. Mặt khác, khái niệm bảo vệ an toàn liên quan chặt chẽ với khái niệm hiểm họa, kẻ phá hoại, kẻ xấu, kẻ lạm dụng… như là nguyên nhân gây ra mất an toàn cho hệ thống. Cho nên vấn đề an toàn của hệ thống phải được biểu diễn bằng mối liên hệ giữa các yếu tố cấu thành hệ thống với nhau và sự tương tác giữa chúng với nguyên nhân gây ra mất an toàn đó. Trước tiên, chúng ta xem xét khái niệm về mô hình hệ thống.

4.1.1.1. Mô hình chủ thể - đối tượng

Đây là mô hình cấu trúc thường dùng nhất để miêu tả một hệ thống TT – VT.

- Theo mô hình này, các thực thể của một hệ thống TT – VT được chia làm 2 loại: các chủ thể (subjects) và các đối tượng (objects). Các chủ thể (S) là các thực thể tích cực nó có thể đưa ra các yêu cầu về tài nguyên, sử dụng các tài nguyên đó để thực hiện các tính toán nào đó. Có thể hình dung chủ thể là các khách hàng, các chương trình, các quá trình… Đối tượng (O) là các thực thể thụ động như là một "kho" chứa thông tin, là các file, các thư mục…

- Các chủ thể và các đối tượng tương tác với nhau trong quá trình xử lý TT. Ta nói chúng tương tác với nhau về mặt TT. Các tương tác TT điển hình là các thao tác xử lý TT như read, write, create, delete,… Các tương tác TT như vậy xác định trạng thái TT của hệ thống.

- Các chủ thể thực hiện các thao tác TT trên tập hợp các đối tượng. Các mối quan hệ tương tác này được thể hiện qua khái niệm truy nhập. Ta nói chủ thể S. tiếp cận tới đối tượng O.

- Trạng thái an toàn của hệ thống (trạng thái ATTT) là trạng thái duy trì được các tương tác TT an toàn, hay nói cách khác là trạng thái đó phải duy trì được các tiếp cận an toàn và loại bỏ được các tiếp cận trái phép.

- Kẻ phá hoại, kẻ xấu, kẻ lạm dụng, tin tặc… là nguồn bên ngoài HT, là nguyên nhân phá vỡ tính an toàn TT của hệ thống. Rõ ràng kẻ xấu muốn tấn công vào ATTT của hệ thống thì nó phải tìm cách xâm nhập hệ thống tức là nó phải tiếp cận tới hệ thống (các chủ thể và các đối tượng của HT) qua cái gọi là "Kênh tác động" - Đó chính là các kênh rò rỉ TT đã nói ở phần trên.

4.1.1.2. Khái niệm chính sách an toàn và thiết bị kiểm soát

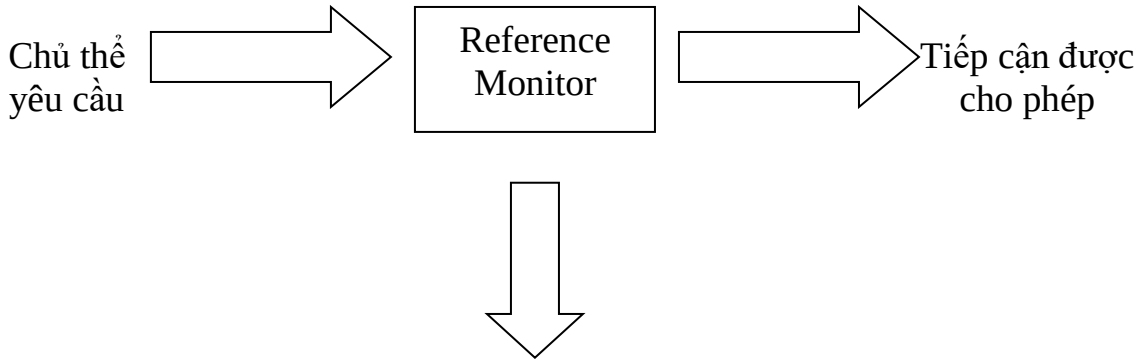
Định nghĩa CSAT: Theo "Sách da cam" (1983), chính sách an toàn là tập hợp các điều luật, các quy định và các giải pháp thực tế để giám sát sự điều khiển, sự bảo vệ và việc phân phối các thông tin nhạy cảm trong hệ thống.

Nói cách khác, các CSAT sẽ giúp cho hệ thống loại bỏ được các TCTP tới TT trong đó, để duy trì các tiếp cận an toàn tức là các trạng thái ATTT của hệ thống.

Các tương tác TT đều thực hiện nhờ các tiếp cận, ví dụ một phiên làm việc của một khách hàng được khởi động và thực hiện qua một chuỗi các truy

nhập (tiếp cận) tới các đối tượng của hệ thống. Quan điểm này về hoạt động của hệ MT dẫn ta đến hình dung rằng, có tồn tại một số thủ tục để làm trung gian dàn xếp xem tiếp cận nào được cho phép và tiếp cận nào thì không. Có thể coi sự trung gian này là một bộ lọc mà tất cả các đòi hỏi truy nhập của các chủ thể đều phải đi qua.

- Kiểu sơ đồ lọc này được gọi là thiết bị kiểm soát hay còn gọi là thiết bị tham chiếu (Reference Monitor). Về mặt chức năng nó được minh hoạ trong hình sau:



Hình 4.1 Sơ đồ thiết bị kiểm soát (Reference Monitor)

Từ đây thấy rõ rằng, thiết bị kiểm soát là bộ phận quan trọng để duy trì các chính sách an toàn của hệ thống.

- CSAT khác với TCTP ở chỗ: Nó xác định các tiếp cận cho phép và cả các tiếp cận bị nghiêm cấm (TCTP). Nó có tính cấu trúc tức là nó là cơ sở để xác định một thiết bị hoặc một cơ cấu tự động nào đó để thực hiện nó (thiết bị kiểm soát).

- CSAT bao gồm:

  - Tập hợp tất cả các thao tác có thể trên đối tượng của hệ thống.
  - Với mỗi cặp "chủ thể, đối tượng" (S^i,O^j) tập hợp các thao tác cho phép là tập con của tập hợp tất cả các thao tác có thể.

Ví dụ điển hình một CSAT như sau:

$\forall$ $s \in S$, $o \in O$, $a \in A$: Allow(s,o,a) iff P

Khi nghiên cứu CSAT cần giải quyết 4 loại nhiệm vụ liên quan chặt chẽ với nhau:

1. Phát biểu và khảo sát các dạng CSAT
2. Thể hiện chúng trên thực tế
3. Sự bảo đảm duy trì CSAT
4. Vấn đề quản lý an toàn

4.1.2. Vai trò của chính sách an toàn thông tin

Chính sách an toàn thông tin (CSATTT) là cội nguồn của tất cả các chỉ thị, các chuẩn, các thủ tục, các hướng dẫn và các tài liệu hỗ trợ khác. Bởi vì với bất kỳ cơ sở hạ tầng nào thì điều quan trọng là phải thiết lập một nền tảng vững chắc. Như sẽ được thảo luận, một chính sách thực hiện hai vai trò: đối nội và đối ngoại.

Phần đối nội chỉ ra cho nhân viên biết cái gì được mong đợi từ họ và những hành động của họ sẽ được đánh giá như thế nào. Phần đối ngoại chỉ ra cho thế giới biết doanh nghiệp được điều hành như thế nào, có chính sách hỗ trợ các hoạt động kinh doanh hay không và cho thấy tổ chức đó có hiểu được việc bảo vệ tài sản quan trọng là để thực hiện thành công sứ mệnh của mình.

Chính sách thể hiện chương trình bảo đảm an toàn thông tin của chúng ta được thực hiện như thế nào, mục tiêu, nhiệm vụ của nó, và trách nhiệm của mỗi người trong tổ chức.

Trong bất kỳ cuộc thảo luận về các yêu cầu bằng văn bản, thuật ngữ "chính sách" có nhiều hơn một nghĩa. Đối với một số người, chính sách là sự chỉ đạo của nhà quản lý cấp cao tất nhiên là trong một chương trình đang chạy như thế nào, mục tiêu và đối tượng của nó là gì và ai là người được giao trách nhiệm. Thuật ngữ "chính sách" có thể tham khảo các quy tắc an toàn cụ thể đối với một hệ thống cụ thể, như tập luật ACF2, các giấy phép RACF, hoặc các chính sách hệ thống phát hiện xâm nhập. Ngoài ra, các chính sách còn có thể tham chiếu đến các vấn đề hoàn toàn khác như các quyết định quản lý cụ thể mà thiết lập chính sách bảo mật thư điện tử của tổ chức hoặc chính sách sử dụng Internet.

Việc phát triển chính sách an toàn thông tin không đơn thuần là vấn đề kỹ thuật hay trách nhiệm kiểm tra, cũng không phải là chỉ đơn thuần một lĩnh vực nào đó mà nó phải xuyên suốt tất cả các chính sách của tổ chức.

Chính sách cung cấp cho toàn bộ tổ chức một sự quản trị rõ ràng, súc tích, sự quản lý nội bộ có thể mang lại lợi ích thực sự về tính hiệu quả cũng như một cách để giảm rủi ro thông tin. Một chính sách an toàn thông tin rõ ràng có thể:

• Giảm sự nhập nhằng

• Cung cấp hướng chỉ đạo và cam kết quản lý rõ ràng

• Thiết lập trách nhiệm và vai trò đã được thỏa thuận

Chính sách là một thể hiện của dự định. Nó cần phải được hỗ trợ bởi các chính sách cấp dưới và các thủ tục thực dụng. Chương này sẽ xem xét cụ thể về các chính sách an toàn thông tin của một tổ chức.

4.1.3. Các loại chính sách an toàn thông tin

Chúng ta cần lưu ý rằng, CSAT thể hiện rõ ràng tính chất mở của hệ thống. hệ thống có thể thay đổi, được tăng cường các thực thể mới (chủ thể, đối tượng, các thao tác mới). Các CSAT phải được duy trì theo thời gian. Cho nên trong quá trình nghiên cứu các tính chất của hệ thống phải xác định các thủ tục quản lý an toàn. Mặt khác, tính mở của hệ thống và vấn đề thực hiện CSAT trong cấu trúc cụ thể của hệ thống (ví dụ, lập trình chủ thể kiểm soát trong các lệnh của bộ vi xử lý cụ thể) lại đặt ra sự cần thiết phải xem xét nhiệm vụ bảo đảm hoạt động liên tục cho mỗi CSAT.

Chúng ta có thể sử dụng 2 loại chính sách an toàn (CSAT): Chính sách tuỳ chọn (discretionary) và Chính sách bắt buộc (mandatory).

- Chính sách an toàn tuỳ chọn (CSAT – D)

Còn gọi là CSAT thận trọng. Cơ sở của CSAT này là kiểm soát tiếp cận lựa chọn (Discretionary Access Control: DAC). DAC có 2 thuộc tính cơ bản sau:

- Tất cả các chủ thể và các đối tượng đều phải được nhận dạng.
- Các tiếp cận của một chủ thể tới một đối tượng của hệ thống được xác định trên cơ sở một điều luật bên ngoài hệ thống (lựa chọn trước từ bên ngoài HT).

CSAT tuỳ chọn có ưu điểm là, nó được thực hiện bởi các cơ chế bảo vệ tương đối đơn giản. Đa số các hệ thống tự động hiện nay tuân thủ các điều luật của loại CSAT này.

Có thể xem ma trận truy cập, mà các hàng của nó là các chủ thể và các cột là các đối tượng là ví dụ điển hình của CSAT – D; các yếu tố ma trận ở đây thể hiện các quyền truy cập và được lựa chọn trước. Nhược điểm ở đây là, tính cứng nhắc của mô hình. Nghĩa là, CSAT loại này không tính tới sự thay đổi trạng thái của HT, không có đòi hỏi gì tới trạng thái của hệ thống khi có sự thay đổi đó.

Cần lưu ý rằng, khi sử dụng CSAT – D sẽ xuất hiện vấn đề, phải xác định các luật trao quyền tiếp cận và phải phân tích ảnh hưởng của chúng tới an toàn hệ thống. Nói chung, khi sử dụng CSAT loại này, luôn xuất hiện bài toán khó giải về mặt thuật toán, đó là phải kiểm tra xem các điều luật chọn trước từ bên ngoài như vậy trong quá trình tương tác TT có dẫn tới việc phá vỡ an toàn hay không?

- Chính sách an toàn bắt buộc (toàn quyền) – CSAT – M.

Cơ sở của CSAT bắt buộc (còn gọi là CSAT toàn quyền) là kiểm soát tiếp cận bắt buộc (Mandatory Access Control – MAC). Nội dung của nó như sau:

o Tất cả các chủ thể và các đối tượng của hệ thống phải được nhận dạng.

o Cho trước một tập tuyến tính có trật tự các nhãn an toàn.

o Mỗi đối tượng của hệ thống được gán cho một nhãn an toàn xác định độ nhạy cảm của TT chứa trong nó – tức là độ mật của nó trong hệ thống.

o Mỗi chủ thể của hệ thống được gán cho một nhãn AT xác định mức độ tin cậy của nó trong hệ thống – Giá trị cực đại trong số các nhãn AT của các đối tượng mà chủ thể đó được tiếp cận được gọi là mức tiếp cận của một chủ thể.

Mục đích cơ bản của CSAT – M là ngăn chặn luồng TT từ các đối tượng với mức tiếp cận cao xuống các đối tượng với mức tiếp cận thấp hơn, tức là chống lại việc xuất hiện trong hệ thống các kênh TT "từ trên xuống". Trong các tài liệu, người ta hay mô tả CSAT – M nhờ một mô hình có tên là mô hình Bell – Lapadula (mô hình BLP). Chúng ta sẽ nghiên cứu mô hình này sau.

Trong khuôn khổ mô hình BLP có thể chứng minh kết luận quan trọng (chỉ ra sự khác nhau về nguyên tắc giữa các hệ thống thực hiện CSAT – M và các hệ thống thực hiện CSAT – D) sau đây:

"Nếu trạng thái ban đầu của hệ thống là an toàn và tất cả các biến đổi hệ thống từ trạng thái này sang trạng thái kia không vi phạm các điều luật do CSAT quy định, thì mọi trạng thái của hệ thống đều là an toàn".

Như vậy, đối với các hệ thống thực hiện CSAT – M thì cơ chế thực hiện nó cần phải theo dõi không chỉ các điều luật truy cập của các chủ thể tới các đối tượng mà còn cần kiểm soát trạng thái của hệ thống nữa. Do vậy thực hiện CSAT này làm cho tính tin cậy của hệ thống cao hơn.

Một ưu điểm nữa của CSAT – M là các điều luật của nó minh bạch và đơn giản hơn để các nhà sản xuất và phát triển dễ hiểu và thực hiện.

4.1.4. Các chính sách an toàn thông tin của một tổ chức

Có rất nhiều thuật ngữ khác nhau được sử dụng để mô tả một chính sách an toàn thông tin. Ví dụ ở Mỹ, người ta thường sử dụng thuật ngữ "chính sách" cho các tài liệu mà thường được mô tả ở Vương quốc Anh là "các tiêu chuẩn". Điều này có thể dẫn đến sự hiểu lầm. Trong tài liệu này sử dụng các thuật ngữ sau:

- Chính sách bảo mật thông tin doanh nghiệp
- Các chính sách cụ thể
- Các tiêu chuẩn
- Các thủ tục

4.1.4.1. Chính sách bảo mật thông tin doanh nghiệp

Chính sách này phải tính toán tới trách nhiệm cuối cùng để đáp ứng các mục tiêu hoặc nhiệm vụ kinh doanh, quản lý cấp cao phải đảm bảo rằng các nguồn tài nguyên cần thiết được sử dụng có hiệu quả để phát triển các khả năng nhằm đáp ứng các yêu cầu nhiệm vụ. Quản lý cấp cao phải phối hợp các kết quả của tiến trình phân tích rủi ro vào tiến trình ra quyết định. Quản lý cấp cao cũng có trách nhiệm phát hành các chính sách tổng thể để thiết lập sự định hướng của tổ chức trong việc bảo vệ tài sản thông tin.

Một chính sách bảo mật thông tin doanh nghiệp hay chính sách tổng thể (chính sách mức 1) đặt ra các mục đích và các nguyên tắc liên quan đến an

ninh thông tin của một tổ chức. Nó phải là vượt thời gian trong đó nó nên ít thay đổi từ năm này sang kia

Chính sách công ty phải:

• Rõ ràng và không nhập nhằng

• Trong chính sách này bao gồm các thành phần chính sau:

- Chủ đề
- Phạm vi
- Các nghĩa vụ pháp lý và quy định
- Các vai trò và trách nhiệm
- Cách tiếp cận chiến lược và các nguyên tắc
- Tiếp cận quản lý rủi ro
- Hành động trong trường hợp vi phạm chính sách

Chính sách này nên được thông qua ở mức cao nhất - ví dụ, Giám đốc điều hành. Người quản lý cấp cao phải có trách nhiệm phát hành chính sách chung để thiết lập định hướng của tổ chức trong việc bảo vệ tài sản của mình.

Bảng 4.1 Chính sách an toàn thông tin doanh nghiệp mẫu

Thông tin kinh doanh là một tài sản thiết yếu của công ty. Điều này thật sự đúng với tất cả các thông tin kinh doanh trong công ty, bất kể nó được tạo ra, phân phối hoặc lưu trữ như thế nào và cho dù nó được đánh máy, viết tay, in, quay phim, được tạo ra từ máy tính hay được nói ra. Tất cả các nhân viên có trách nhiệm bảo vệ thông tin doanh nghiệp trước những truy cập, sửa đổi, sao chép trái phép hoặc tiết lộ dù vô tình hay cố ý. Trách nhiệm ấy là điều cần thiết cho việc kinh doanh của công ty. Khi thông tin không được bảo vệ tốt, công ty có thể bị tổn hại bởi nhiều cách khác nhau, chẳng hạn như thiệt hại đáng kể đối với việc chia sẻ thị trường và danh tiếng bị hư hỏng. Thông tin chi tiết về trách nhiệm bảo vệ thông tin công ty của nhân viên được mô tả trong chính sách bảo vệ thông tin và hướng dẫn sử dụng các tiêu chuẩn. Người quản lý có trách nhiệm đảm bảo rằng tất cả các nhân viên đều hiểu và tuân thủ các chính sách và tiêu chuẩn/quy định. Người quản lý cũng có trách nhiệm ghi nhận sai lệch từ việc thiết lập thực thi an toàn và bắt đầu những hành động khắc phục.

Kiểm toán viên nội bộ sẽ thực hiện đánh giá định kỳ để đảm bảo sự tuân thủ liên tục các chính sách bảo vệ thông tin công ty. Việc vi phạm chính sách này sẽ được giải quyết theo quy định trong hướng dẫn chính sách quản lý nguồn nhân lực cho quản lý.

4.1.4.2. Các chính sách cụ thể

Những sự thay đổi của loại chính sách này nhanh hơn so với các chính sách chung. Vì chúng là chi tiết hơn nên chúng cần phải được xem xét thường xuyên hơn. Ví dụ về các chính sách cụ thể bao gồm:

- Chính sách phân loại tài sản
- Chính sách kiểm soát truy cập
- Chính sách về các hoạt động
- Chính sách quản lý sự cố
- Chính sách an ninh vật lý
- Chính sách nguồn nhân lực
- Chính sách truy cập của bên thứ ba
- Chính sách quản lý kinh doanh liên tục

Những chính sách là chính sách ở mức 2, mức chi tiết của chính sách chung, là các chính sách về các vấn đề cụ thể chẳng hạn như về việc sử dụng Internet…

4.1.4.3. Các tiêu chuẩn

Các tiêu chuẩn an toàn cung cấp hướng dẫn để đạt được các chính sách an ninh cụ thể, thường liên quan đến các công nghệ hoặc các sản phẩm cụ thể. Chúng được sử dụng như một điểm chuẩn cho mục đích kiểm toán và có nguồn gốc từ:

- Thực tiễn công nghiệp tốt nhất
- Kinh nghiệm
- Các trình điều khiển kinh doanh
- Thử nghiệm nội bộ

Chúng phải được xem xét thường xuyên để đảm bảo rằng đó là phiên bản mới và các vấn đề về lỗ hổng được giải quyết. Ví dụ về các tiêu chuẩn bao gồm:

- Xây dựng máy chủ UNIX

• Cấu hình tường lửa

• Các giao thức kết nối

Khi phát triển chính sách an toàn thông tin, sẽ rất cần thiết để thiết lập một tập các chuẩn hỗ trợ. Bảng sau cho thấy một ví dụ mẫu về những gì các chuẩn cho một chủ đề cụ thể.

Bảng 4.2 Ví dụ về các tiêu chuẩn

Người quản lý các hệ thống thông tin/người đứng đầu một nhóm Những người quản lý có trách nhiệm đối với hệ thống thông tin phải thực hiện tất cả các trách nhiệm phù hợp với việc quản lý khu vực của họ. Ngoài ra, họ sẽ thực hiện các hành động như người giám sát các thông tin được sử dụng trong hệ thống nhưng lại được sở hữu bởi những người quản lý khác. Họ phải đảm bảo rằng các chủ sở hữu này được xác định, bổ nhiệm và nhận thức được các trách nhiệm của họ. Tất cả các nhà quản lý, các giám sát, các giám đốc và những nhà quản lý ở các cấp cũng phải có vai trò cố vấn và hỗ trợ đối với những nhà quản lý hệ thống thông tin và hệ thống phi thông tin/IS đối với việc: - Xác định và đánh giá các hiểm họa - Xác định và thực hiện các phương pháp bảo vệ (bao gồm cả việc tuân thủ với những công việc này) - Duy trì một mức độ thỏa đáng về nhận thức bảo mật - Giám sát hoạt động phù hợp với các biện pháp an toàn trong đơn vị - Điều tra những điểm yếu và các sự cố - Gia tăng bất kỳ các vấn đề và hoàn cảnh mới mà ở đó họ có hiểu biết thông qua vai trò chuyên môn của họ - Giữ liên lạc với kiểm toán nội bộ và bên ngoài

4.1.4.4. Các thủ tục

Các thủ tục là bắt buộc, từng bước, chi tiết các hành động được yêu cầu để hoàn thành nhiệm vụ. Các thủ tục có thể là rất chi tiết. Thủ tục cần phải:

• Rõ ràng

• Không nhập nhằng

• Luôn được cập nhật

• Được thử nghiệm

• Được lập tài liệu

Ví dụ về các thủ tục bao gồm:

• Báo cáo sự cố

• Quản lý sự cố

• Thêm hay loại bỏ ID người dùng

• Sao lưu máy chủ

4.1.5. Cấu trúc của chính sách an toàn thông tin

Chúng ta có thể thấy rằng chúng ta cần phải tuân theo một định dạng đã được thiết lập để công bố các chính sách nội bộ. Nó không phải là luôn luôn có thể thực hiện theo các đề mục được đề nghị dưới đây, nhưng ta nên cố gắng làm như vậy.

Lưu ý rằng định dạng này là gợi ý cho các chính sách cụ thể chứ không phải là chính sách bảo mật thông tin công ty đã được đưa ra trước đó.

Các đề mục gợi ý cho các chính sách nội bộ

Những đề mục này được liệt kê dưới đây và sau đó tóm tắt trong các nội dung của từng mục cụ thể:

Tóm tắt

Số phiên bản và ghi lại sự thay đổi

1.0 Giới thiệu

1.1 Các định nghĩa và phạm vi

1.2 Thẩm quyền (bao gồm cả các vấn đề pháp lý hoặc quy định)

2.0 Các mục tiêu và các nguyên tắc cơ bản

3.0 Các vai trò và trách nhiệm

4.0 Chính sách

4.1 Phát biểu đề mục 1

4.2 Phát biểu đề mục 2

4.3 Phát biểu đề mục 3 v.v..

• **Tóm tắt**, phải minh bạch, dễ hiểu, thông tin được trình bày trong một trang duy nhất (tối đa) cho phép người đọc nhanh chóng hiểu được mục đích, quyền hạn và phạm vi của chính sách.

• **Số phiên bản và ghi lại sự thay đổi** là quan trọng vì nó đảm bảo rằng các chính sách mới nhất được áp dụng.

• **Các định nghĩa** (đặc biệt là các thuật ngữ kỹ thuật) là rất cần thiết. Có một số thuật ngữ (chẳng hạn như "toàn vẹn") có một ý nghĩa rất đặc biệt trong bối cảnh an toàn thông tin. Tất cả các thuật ngữ này cần được giải thích trong phần này. Điều quan trọng là phải nhớ rằng ta không cố gắng để cung cấp một định nghĩa từ điển thực sự, các định nghĩa nên được sử dụng trong bối cảnh của chính sách (tức là các định nghĩa, thuật ngữ sử dụng thống nhất trong toàn bộ một bộ tài liệu).

• **Phạm vi** của chính sách cần xác định những người mà chính sách áp dụng, và trong những hoàn cảnh nào. Ví dụ, có chính sách áp dụng riêng cho nhân viên toàn thời gian. Những chính sách khác có thể áp dụng đặc biệt cho những nhà quản lý cấp cao trong khi các chính sách hơn nữa chỉ có thể có liên quan trong các trường hợp nhất định, chẳng hạn như khi nhân viên làm ca đêm hoặc khi nhân viên đang đi du lịch ở nước ngoài.

• Mỗi chính sách phải bao gồm các chi tiết của bất cứ **cơ quan thẩm quyền** hỗ trợ chính sách (Chẳng hạn như Hội đồng quản trị, Tổng giám đốc Công ty hoặc người đứng đầu nhân sự).

• Mỗi chính sách cần phải có một loạt các **mục tiêu** (nếu ta không thể xác định điều này, ta nên xem xét các lý do của mình để có chính sách ở nơi đầu tiên). Các **nguyên tắc cơ bản** bao gồm các phát biểu như "Chúng ta sẽ hoạt động trên một cơ sở "cần để biết" (hoặc ngược lại, trên một cơ sở "cần để hạn chế"). Điều này cho phép ta thiết lập các nguyên tắc mà ta muốn hoạt động. Chúng có liên quan đến các tuyên bố chính sách thực tế, nhưng độc lập.

• Các vai trò và trách nhiệm liên quan đến tuyên bố phạm vi. Như ví dụ, vai trò và trách nhiệm sau đây có thể được thoả thuận và công bố.

Hội đồng quản trị là trách nhiệm cuối cùng đảm bảo rằng an ninh thông tin được quản lý đúng cách. Quản lý an ninh thông tin có trách nhiệm:

- Sự phát triển và bảo trì của chính sách này

- Đảm bảo chính sách này được hỗ trợ bởi các tài liệu thích hợp, chẳng hạn như thủ tục hướng dẫn

- Đảm bảo rằng các tài liệu có liên quan và được cập nhật mới nhất

- Đảm bảo chính sách này và các cập nhật tiếp theo được truyền đạt đến các phòng ban và nhân viên có liên quan.

Tất cả các nhân viên chịu trách nhiệm tuân thủ những chính sách này, và báo cáo bất kỳ vi phạm an ninh, sự cố cho người quản lý an ninh.

• **Các phát biểu chính sách** cần phải rõ ràng, súc tích và thiết lập mục đích. Các phát biểu sau đây được cung cấp như một ví dụ về những gì ta có thể mong đợi để thấy trong việc quản lý tài khoản người dùng máy tính có đặc quyền.

Bảng 4.3 Ví dụ về các phát biểu chính sách

Các tài khoản đặc quyền Thiết lập các tài khoản đặc quyền phải được giữ ở mức tối thiểu. Quá trình chính thức này sẽ được áp dụng trong trường hợp được coi là thích hợp để phát hành ưu đãi đặc biệt cho người dùng. Các quá trình này sẽ: - Xác định các đặc quyền liên quan với mỗi thành phần của một hệ thống (ví dụ: hệ điều hành, hệ thống quản lý cơ sở dữ liệu hoặc ứng dụng) - Xác định các nhóm của người sử dụng đòi hỏi ưu đãi đặc biệt (ví dụ như quản trị viên hệ thống) - Phân bổ quyền trên cơ sở hạn chế (ví dụ như các cơ sở "cần để sử dụng" hay "sự kiện kế tiếp sự kiện") - Lưu trữ hồ sơ các đặc quyền được phân bổ - Đảm bảo rằng quá trình cấp phép đã được hoàn thành trước khi truy cập đặc quyền được cho phép. Người sử dụng ban hành kèm theo ưu đãi đặc biệt sẽ có ID khác nhau cho đặc quyền và các tài khoản không đặc quyền. Các ID người dùng nhóm chỉ nên được sử dụng trong những trường hợp đặc biệt.

4.1.6. Cách xây dựng chính sách an toàn thông tin

Việc xây dựng một chính sách an ninh thông tin không nên được xem như một nhiệm vụ khó khăn. Những gì quan trọng là cần phải đưa ra phương hướng chính sách rõ ràng và hỗ trợ quản lý việc thực hiện và bảo đảm an ninh thông tin. Để có hiệu quả các chính sách phải phù hợp, dễ tiếp cận và dễ hiểu đối với tất cả người sử dụng dự định trong toàn tổ chức.

Khi chuẩn bị viết một chính sách cho một đối tượng cụ thể, nhớ rằng người viết sẽ không có cơ hội ngồi với từng người đọc và giải thích từng mục hoặc từng câu có nghĩa là gì. Người viết sẽ không thể nói cho mọi người

chính sách sẽ tác động đến các nhiệm vụ hàng ngày của họ như thế nào. Khi viết một chính sách, chúng ta phải nhận biết được đối tượng trực tiếp của chính sách. Đối với một chính sách tổng thể, đối tượng là tất cả các nhân viên.

Một chính sách cần có sự cam kết quản lý, hỗ trợ các thủ tục, một khuôn khổ kỹ thuật phù hợp mà trong đó nó có thể được thực hiện, một mức độ phù hợp của người có thẩm quyền, một phương tiện mà tuân thủ có thể được kiểm tra và đồng ý về mặt pháp lý phản ứng trong trường hợp nó bị xâm phạm.

Chính sách phù hợp là cơ sở để bảo mật thông tin tốt. Vai trò của chúng là cung cấp các trọng tâm chỉ đạo và hành động như các yếu tố liên kết tất cả các khía cạnh của thông tin quản lý an ninh.

Các đặc tính của bất kỳ chính sách nào phụ thuộc vào nhiều yếu tố. Đây có thể được gọi chung là văn hóa của tổ chức. Một số tổ chức có một văn hóa 'Mệnh lệnh và kiểm soát ' mạnh mẽ. Điều này có thể dẫn đến trong các chính sách có chứa các câu lệnh mạnh mẽ/tuyên bố bắt buộc (ví dụ, "Bạn sẽ log off vào cuối mỗi ngày làm việc"). Các tổ chức khác có thể sử dụng cụm từ tinh vi hơn, được thiết kế để thuyết phục những người là đối tượng của chính sách.

Cho dù kiểu văn hóa hoặc quản lý nào mà tổ chức chấp nhận, mục đích của một chính sách an ninh thông tin là giúp quản lý rủi ro và làm giảm nó đến mức có thể chấp nhận được.

Chính sách thường được dựa trên các tiêu chuẩn được công bố hiện tại, chẳng hạn như tiêu chuẩn ISO/IEC 27001, cung cấp một số đặc điểm kỹ thuật cho một hệ thống quản lý an ninh thông tin (ISMS).

4.1.6.1. Thẩm quyền/cấp phép

Ta sẽ cần phải đảm bảo rằng chính sách và các tài liệu hỗ trợ được ủy quyền phù hợp. Trong một số tổ chức, chữ ký của giám đốc có thể đủ. Trong các công ty khác, ta có thể tìm kiếm thẩm quyền từ một loạt các giám đốc điều hành cao cấp thuộc các lĩnh vực sau đây:

- Lĩnh vực tài chính
- Những người đứng đầu vận hành
- Lĩnh vực nhân sự
- Lĩnh vực pháp luật

4.1.6.2. Thực hiện

Sẽ rất khó để thực hiện toàn bộ chính sách thiết lập trên một tổ chức tại một thời điểm nhất định. Cách tiếp cận từng giai đoạn thường có hiệu quả nhất, lựa chọn một khu vực có ranh giới dễ dàng xác định và một trong đó hỗ trợ một loạt các dịch vụ khác, ví dụ như trung tâm hoạt động CNTT.

Lý do cần các trung tâm hoạt động CNTT

• Điều này là bình thường một nhà cung cấp dịch vụ nội bộ quan trọng, trong đó đảm bảo cao là cần thiết.

• Nhiều biện pháp an toàn được phân phối thông qua công nghệ.

• Cung cấp CNTT thường đã được quản lý tốt.

• Phạm vi không phải bao gồm tất cả người dùng.

Giai đoạn tiếp theo có thể tập trung vào các lĩnh vực kinh doanh cốt lõi và người dùng cuối CNTT, như các hoạt động CNTT sau đó sẽ phù hợp với chính sách.

Một mục tiêu thứ hai có thể là nhân viên hoặc chức năng nguồn nhân lực. Lý do lựa chọn này nhìn chung tương tự như đối với lựa chọn các chức năng CNTT ban đầu.

Các khu vực mục tiêu tiếp theo sẽ được hưởng lợi từ công việc này, và nó sẽ được dễ dàng hơn để thực hiện chính sách như “nhà cung cấp dịch vụ" trung tâm sẽ được bao phủ bởi chính sách đã có.

4.1.6.3. Hoạt động

Hoạt động là một phần của vấn đề rộng hơn về quản lý an ninh thông tin đến sự cần thiết phải giám sát việc tuân theo (và hiệu quả) các chính sách. Ta sẽ thấy rằng một số phát biểu chính sách không được tôn trọng (ví dụ như mọi người có thể chia sẻ mật khẩu). Điều này có thể bởi vì chúng sẽ làm ảnh hưởng đến hoạt động bình thường, hoặc được coi như là quá mức tốn kém.

Trong hầu hết các trường hợp chìa khóa để bảo mật hiệu quả là thiết lập chính sách có thể đạt được và để đảm bảo tuân thủ. Ta cũng sẽ cần phải có các quy trình phù hợp để đối phó với các trường hợp không thể tránh khỏi, nhưng rất ít, trường hợp các ngoại lệ chính sách hợp lệ. Tuy nhiên, chúng ta cần chuẩn bị để thay đổi các phát biểu của mình dựa trên các thông tin phản

hồi. Mọi người sẽ thực hiện dễ dàng hơn nếu họ đã được tham gia xây dựng chính sách và cảm thấy họ là các bên liên quan.

Trong thời gian này, các thiết lập chính sách nên trở thành chuẩn mực cho bất kỳ quy trình kiểm toán được sử dụng.

4.2. CÁC MÔ HÌNH AN TOÀN THÔNG TIN

Các mô hình an toàn (MHAT) là cơ sở lý thuyết để xây dựng các CSAT. Trong các mô hình của các CSAT có thể phân ra hai loại cơ bản:

- Mô hình an toàn tuỳ chọn (bất kỳ) (MHAT- D)
- Mô hình an toàn bắt buộc (chuẩn) (MHAT-M)

Chúng ta sẽ nghiên cứu các mô hình tiêu biểu cho mỗi loại nói trên. Điển hình cho mô hình tuỳ chọn (tương ứng với chính sách điều khiển truy nhập tuỳ chọn) là mô hình an toàn HRU. Và tiêu biểu cho loại MHAT bắt buộc là mô hình bí mật BLP.

4.2.1. Mô hình ma trận truy nhập HRU

4.2.1.1. Các luận điểm cơ bản của mô hình HRU

Mô hình HRU (Harison M., Ruzzo W., Ullman J.) thường dùng để phân tích hệ bảo vệ thực hiện CSAT-D, và yếu tố cơ bản của nó là Ma trận truy nhập. Ở đây trạng thái của hệ thống được coi như một ôtômat hữu hạn, hoạt động theo các luật di chuyển xác định.

Mô hình HRU lần đầu tiên được đưa ra vào năm 1971, và đến năm 1976 xuất hiện mô tả hình thức của nó.

Ký hiệu O - tập các đối tượng của HT; S – tập các chủ thể của hệ thống. Để tính tới cả mối quan hệ giữa các chủ thể, mô hình coi các chủ thể đồng thời cũng là các đối tượng ($S \subseteq O$); R – tập các quyền truy cập của các chủ thể tới các đối tượng, ví dụ như read, write, own; M – ma trận truy nhập, các hàng tương ứng với các chủ thể và các cột – các đối tượng; $M[s,o] \subseteq R$ – quyền truy nhập của chủ thể s tới đối tượng o.

Mỗi ôtômat được xây dựng trên cơ sở các luận điểm của mô hình HRU sẽ được gọi là một hệ thống. Chức năng của một hệ thống được xem xét chỉ trong khuôn khổ các thay đổi trong ma trận truy nhập M. Diễn biến của hệ thống được mô tả qua khái niệm trạng thái của nó.

Không gian trạng thái của hệ thống xác định bởi tích Đề-các của 3 tập các yếu tố cấu thành hệ thống là S, O và R: O x S x R.

Trạng thái hiện thời Q của hệ thống trong không gian trên được xác định bởi bộ ba: gồm yếu tố từ tập các chủ thể, tập các đối tượng và ma trận truy nhập M: Q = (S,O,M).

Sự thay đổi có thể trong hệ thống được xác định nhờ 6 toán tử cơ bản sau:

1. Enter r into M[s,o]: cấp cho chủ thể s quyền truy nhập r tới đối tượng o. Khi đó tại yếu tố M[s,o] của ma trận truy nhập thêm r vào.

2. Delete r from M[s,o]: xoá khỏi chủ thể s quyền truy nhập r tới đối tượng o.

3. Create subject S: tạo một chủ thể mới trong hệ thống. Trong ma trận truy nhập sẽ thêm một hàng mới và một cột mới.

4. Create object O: tạo một đối tượng mới trong hệ thống. Trong ma trận M sẽ thêm một cột mới.

5. Destroy subject S: xoá khỏi hệ thống chủ thể S. Trong ma trận M sẽ mất đi một hàng và một cột tương ứng.

6. Destroy object O: xoá khỏi hệ thống đối tượng O. Trong ma trận M sẽ bớt đi một cột tương ứng.

Ta gọi đây là các toán tử nguyên thuỷ và ký hiệu chúng là toán tử α. Kết quả tác động của toán tử α là hệ thống chuyển từ trạng thái Q = (S,O,M) sang trạng thái mới Q' = (S',O',M'). Dịch chuyển này ta sẽ ký hiệu là $Q\vdash_{\alpha} Q'$. Ta có bảng trạng thái sau đây:

Bảng 4.4 Bảng liệt kê các toán tử nguyên thủy

Toán tử nguyên thuỷ HRU	Điều kiện thực hiện	Trạng thái mới của HT
Enter r into M[s,o]	$s \in S$, $o \in O$	$S'=S$, $O'=O$, $M'[s,o]=M[s.o] \cup \{r\}$
Delete r from M[s,o]	$s \in S$,$o \in O$	$S'=S$, $O'=O$, $M'[s,o]=M[s.o] \setminus \{r\}$
Create subject s'	$s' \notin S$	$S'=S \cup \{s'\}$, $O'=O \cup \{s'\}$
Create object o'	$o' \notin O$	$S'=S$, $O'=O \cup \{o'\}$

Destroy subject s	$s \in S$	S'=S \ {s}, O'=O \ {s}
Destroy object o	$o \in O$	S'=S, O'=O \ {o}

Có thể cấu tạo từ các toán tử nguyên thuỷ α các toán tử lệnh. Các lệnh này gồm 2 phần:

- Các điều kiện để thực hiện lệnh.
- Dãy các toán tử nguyên thuỷ tiếp theo.

Các lệnh loại này có dạng sau:

Command C (x_1,…,x_k)

If $r_1 \in M[x_{s1},x_{o1}]$ and …and $r_m \in M[x_{sm},x_{om}]$ then

α_1

…

α_n

End.

Ở đây C – tên lệnh; x_i – tham số lệnh, là các đặc chỉ của các chủ thể và đối tượng, i – các chỉ số của các chủ thể và đối tượng (từ 1 đến k); α - các toán tử nguyên thuỷ; $r_1,…r_m \in R$ – các quyền truy nhập.

Khi hoàn thành câu lệnh C (x_1,…,x_k) hệ thống thực hiện bước chuyển từ trạng thái Q sang trạng thái mới Q'.

Ta ký hiệu bước chuyển này như sau: $Q \vdash C(x_1,…,x_k)\ Q'$. Lưu ý ở đây:

- Q'=Q, nếu như một trong những điều kiện của câu lệnh C(x_1,…,x_k) không được thực hiện.
- $Q'=Q_n$, nếu tất cả các điều kiện của câu lệnh C(x_1,…,x_k) được thực hiện và tồn tại các trạng thái Q_1,…,Q_n:

$$Q=Q_0 \vdash \alpha_1 Q_1 \vdash \alpha_2 \ldots \vdash \alpha_n Q_n$$

Ta hãy xem mấy ví dụ đơn giản nhất.

• Ví dụ 1: Lệnh tạo một file riêng cho bởi chủ thể s

Command "Create File" (s,f):

Create object f;

enter own into M[s,f];

enter read into M[s,f];

enter write into M[s,f];

End.

• Ví dụ 2: Lệnh chuyển cho chủ thể s' quyền read file f mà chủ sở hữu của f là chủ thể s

Command "Enter Read" (s,s',f):

If own ∈ M[s,f] then

enter read into M[s',f];

End.

4.2.1.2. Tính an toàn của hệ thống

Theo các đòi hỏi của hầu hết các tiêu chí đánh giá ATTT, các MT phải được thiết lập trên các mô hình toán học xác định, từ đó phải chứng tỏ được, về mặt lý luận (triết lý) sự tương ứng của hệ bảo vệ với các đòi hỏi của CSAT cho trước. Để giải quyết bài toán, cần phải có một thuật toán cho phép kiểm tra được sự tương ứng nói trên. Chúng ta hãy xem xét điều này.

Định nghĩa 4.1: Ta coi rằng, sự rò rỉ quyền r ∈ R có thể xảy ra do thực hiện lệnh Command C, nếu trong bước chuyển hệ thống tới trạng thái Q' có thực hiện toán tử nguyên thuỷ, đưa r vào yếu tố ma trận truy nhập M, mà trước đó yếu tố này không chứa r.

Định nghĩa 4.2: Trạng thái ban đầu Q_0 coi là an toàn đối với một quyền r nào đó, nếu không thể xảy ra bước chuyển của hệ thống tới trạng thái Q, trong đó có thể xuất hiện sự rò rỉ quyền r.

Định nghĩa 4.3: Một hệ thống được gọi là đơn toán tử, nếu mỗi lệnh chỉ thực hiện một toán tử nguyên thuỷ.

a) Định lý 4.1: (về tồn tại thuật toán kiểm tra)

Tồn tại một thuật toán cho phép kiểm tra xem một trạng thái cho trước của một hệ thống đơn toán tử có an toàn hay không đối với quyền r đã cho.

Chứng minh: Để chứng minh định lý 1 chỉ cần chứng tỏ rằng, số các dãy lệnh Command của hệ thống mà ta cần kiểm tra là hữu hạn. Trong trường hợp này, thuật toán kiểm tra an toàn là thuật toán chọn tổng toàn bộ các dãy lệnh và kiểm tra trạng thái cuối cùng mỗi dãy xem có rò rỉ quyền r hay không.

Lưu ý rằng, không cần thiết xem xét trong các dãy lệnh các toán tử "Delete" và "Destroy", vì rằng ta cần kiểm tra sự tồn tại một quyền truy nhập chứ không phải sự vắng mặt của nó. Hơn nữa, cần để ý rằng không cần phải xem xét các dãy lệnh có chứa nhiều hơn một toán tử "Create". Đó là do, tất cả

các dãy lệnh hoặc là kiểm tra, hoặc là enter các quyền truy nhập vào các yếu tố mới của ma trận truy nhập M, có thể bằng phép thế đơn giản các tham số, biểu diễn ở dạng các dãy lệnh tác động chỉ lên các chủ thể và các đối tượng đang tồn tại (không cần có các S. và O. mới sinh ra). Cần chỉ một toán tử Create cho trường hợp nếu Q_0 = (S,O,M) và S = ∅.

Như vậy, chúng ta chỉ cần xem xét các dãy lệnh có chứa các toán tử "Enter…into" và cực đại là một toán tử Create subject. Số các toán tử "Enter" khác nhau là n=$|R|(|S_0|+1)(|O_0|+1)$. Vì trật tự các thao tác Enter trong dãy lệnh là không quan trọng nên cùng với một thao tác "Create", thì số các dãy lệnh bị giới hạn bởi đại lượng 2^{n+1}.

b) Định lý 4.2: (không tồn tại thuật toán kiểm tra)

Bài toán kiểm tra tính an toàn của hệ thống bất kỳ là không có lời giải về mặt thuật toán.

Để chứng minh định lý 2 phải dựa vào kết luận quan trọng trong lý thuyết máy Turing: không tồn tại một thuật toán kiểm tra đối với máy Turing bất kỳ và một từ ban đầu bất kỳ. Chúng ta sẽ công nhận điều này mà không đi sâu vào các lập luận toán học và phức tạp.

Định lý 1 và định lý 2 ở trên cho ta 2 cách chọn bộ bảo vệ. Một mặt, mô hình HRU có thể biểu diễn đa dạng các CSAT tuỳ chọn, nhưng lại không tồn tại thuật toán để kiểm tra tính an toàn của chúng; mặt khác, có thể sử dụng các hệ đơn toán tử, mà với hệ thống này có tồn tại thuật toán kiểm tra an toàn, nhưng loại hệ thống như vậy lại rất hạn hẹp.

Phương hướng phát triển tiếp theo của mô hình HRU là xác định các điều kiện mà hệ thống phải tuân thủ, để sao cho bài toán kiểm tra an toàn với hệ thống có thể giải được về thuật toán. Ví dụ năm 1978, người ta chứng tỏ rằng, các hệ thống đơn điệu và đơn điều kiện, tức là nó không chứa các toán tử "Destroy" hoặc "Delete" và chỉ chứa các lệnh, mà phần điều kiện của chúng có không hơn một mệnh đề, sẽ có tồn tại thuật toán kiểm tra.

4.2.2. Mô hình trao quyền truy nhập Take – Grant

4.2.2.1. Mô hình Take – Grant cơ bản

a) Các luận điểm cơ bản của mô hình

Mô hình trao quyền truy nhập Take-Grant (ra đời vào năm 1976) dùng để phân tích các hệ thống bảo đảm kiểm soát truy nhập tuỳ chọn (DAC), trước hết là để phân tích các cách trao quyền truy nhập trong các hệ thống như vậy. Trong mô hình có sử dụng các giản đồ truy nhập và các luật biến đổi của chúng. Mục đích của mô hình là tìm lời giải cho câu hỏi về khả năng một chủ thể của hệ thống nhận các quyền truy nhập tới một đối tượng tại trạng thái được mô tả bằng một giản đồ truy nhập.

Về cách phân chia các thực thể của hệ thống vẫn tuân theo mô hình S-O, và vẫn coi $S \subseteq O$. Vậy:

S-tập các chủ thể và O-tập các đối tượng của hệ thống.

$R=\{r_1,r_2,\ldots,r_m\} \cup \{t,g\}$ – tập các quyền truy nhập, ở đây t (take) là quyền truy nhập, g (grant) là quyền cho quyền truy nhập.

G=(S,O,E)-là một giản đồ có định hướng đầu cuối được đánh dấu và không có vòng khép kín; giản đồ này thể hiện các truy nhập đang xảy ra trong hệ thống. Tập S,O tương ứng với các đỉnh của giản đồ và được ký hiệu như sau: $\otimes$ - vừa là chủ thể vừa là đối tượng; $\bullet$ - chủ thể (yếu tố của tập S). Các yếu tố của tập $E \subseteq OxOxR$ thể hiện các cung của giản đồ, đánh dấu các tập con không rỗng từ tập các quyền truy nhập R.

Trạng thái của hệ thống được mô tả bằng giản đồ truy nhập của nó. Bước chuyển của hệ thống từ trạng thái này sang trạng thái khác được xác định bởi các toán tử hoặc bằng các luật biến đổi giản đồ truy nhập. Biến đổi giản đồ G vào giản đồ G' sau khi thực hiện luật op thường ký hiệu là $G \vdash op\ G'$.

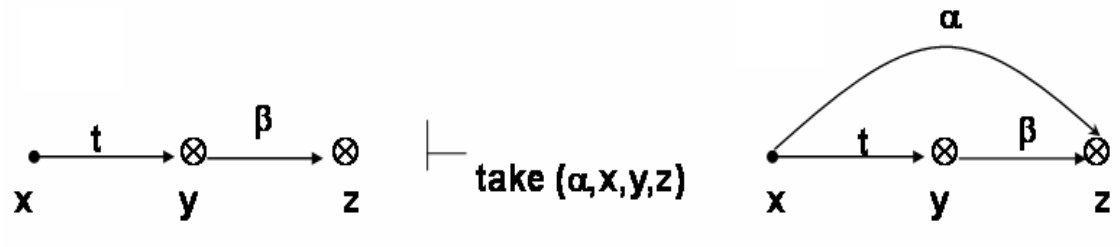
Trong mô hình Take-Grant cơ bản, có 4 loại luật biến đổi giản đồ truy nhập sau đây:

1. Luật Take (α,x,y,z) – Lấy quyền

Giả sử $x \in S$, $y,z \in O$ – là các đỉnh khác nhau của giản đồ G;

$\beta \subseteq R$ và $\alpha \in \beta$. Giản đồ truy nhập thể hiện trạng thái G của HT, trong đó chủ thể x đang nhận quyền t từ đối tượng y và đối tượng y có các quyền β truy nhập tới đối tượng z.

Luật Take (α,x,y,z) xác định thứ tự nhận giản đồ mới G' từ G như sau:

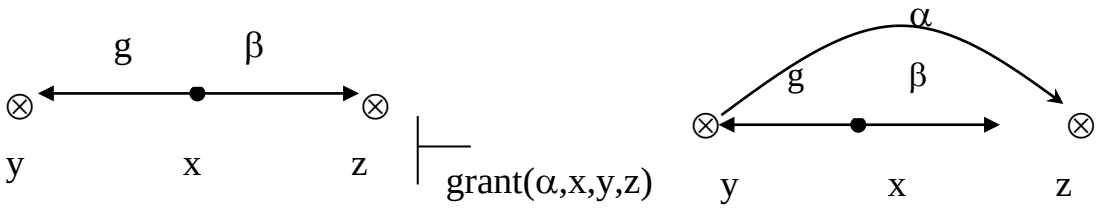


Chủ thể x lấy từ đối tượng y quyền α truy nhập tới đối tượng z. ($\alpha \subseteq \beta$)

2. Luật Grant (α,x,y,z) – Trao quyền

Giả sử $x \in S$, $y,z \in O$ – là các đỉnh của giản đồ G; $\beta \subseteq R$ và $\alpha \subseteq \beta$.

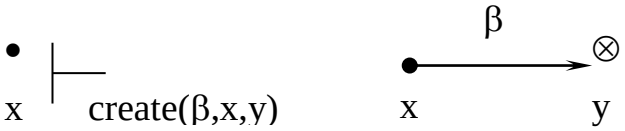
Luật này xác định trật tự thu được giản đồ mới G' từ giản đồ G như hình sau:



Chủ thể x trao cho đối tượng y quyền $\alpha \subseteq \beta$ tới đối tượng z.

3. Luật Create (β, x, y) – Tạo lập quyền β cho đối tượng mới

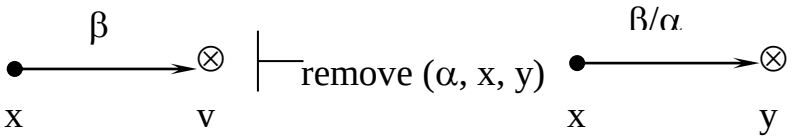
Giả sử: $x \in S$; $\beta \subseteq R$; $\beta \neq \varnothing$, y - đối tượng mới (hoặc chủ thể). Luật này xác định trật tự nhận G' từ G như sau:



Chủ thể x tạo ra một đối tượng mới y mà nó có quyền truy nhập tới β. (x có quyền β truy nhập tới y).

4. Luật Remove (α, x, y) – Tháo bỏ quyền

Giả sử: x ∈ S, y ∈ O – các đỉnh của giản đó G, β ∈ R; α ⊆ β. Luật này xác định trật tự nhận G’ từ G như sau.



Chủ thể x tháo bỏ quyền truy nhập α tới đối tượng y.

Các luật nêu ở trên gọi là các luật cơ bản. Ta có bảng các luật cơ bản sau đây:

Bảng 4.5 Các luật cơ bản của mô hình take - grant

Các luật cơ bản của mô hình T - G	Các điều kiện	Trạng thái kết quả của hệ thống G’=(S’,O’,E’)
Take (α,x,y,z)	x ∈ S, (x,y,t) ∈ E (y,z, β) ∈ E. x ≠ z, α ⊆ β	S’=S, O’=O E’=E ∪ {(x,z, α)}
Grant (α,x,y,z)	x ∈ S, (x,y,g) ∈ E (x,z, β) ∈ E. y ≠ z, α ⊆ β	S’=S, O’=O E’=E ∪ {(y,z, α)}
Create (β, x, y)	X ∈ S, y ∉ O	O’=O ∪ {y},S’=S∪{y}, nếu y là chủ thể, E’=E ∪ {(x,y, β)}
Remove (α, x, y)	x ∈ S, y ∈ O (x,z, β) ∈ E; α ⊆ β	S’=S, O’=O E’=E \ {(x,y, α)}

Trong mô hình Take – Grant, quan trọng là xác định các điều kiện, mà trong hệ thống có thể diễn ra sự trao quyền truy nhập theo một cách nhất định. Chúng ta hãy xem xét các điều kiện thực hiện:

- Phương pháp nhận bất hợp pháp các quyền truy nhập.
- Phương pháp chiếm quyền truy nhập

4.2.2.2. Trao quyền trái phép

Đây còn gọi là phương pháp trao bất hợp pháp quyền truy nhập. Phương pháp này có đặc trưng chính là, trong việc trao quyền truy nhập không có một

sự hạn chế nào đối với sự phối hợp của các chủ thể tham gia quá trình đó (tức là không phân biệt chủ thể hợp pháp hay bất hợp pháp).

Giả sử x,y $\in$ O - các đối tượng khác nhau của giản đồ truy nhập $G_0=(S_0,O_0,E_0)$; $\alpha \subseteq R$. Chúng ta hãy định nghĩa mệnh đề "truy nhập cho phép" (α,x,y,G_0) sao cho mệnh đề này sẽ đúng khi và chỉ khi có tồn tại các giản đồ $G_1=(S_1,O_1,E_1)$, … $G_N=(S_N,O_N,E_N)$ để cho $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$ và $(x,y,\alpha) \in E_N$.

• Định nghĩa 4.4: Người ta nói các đỉnh của một giản đồ truy nhập là tg-liên kết với nhau hoặc chúng được nối với nhau bằng tg-con đường nếu (không tính tới hướng của các cung) trong giản đồ đó giữa chúng (các đỉnh) có tồn tại một đường, mà mỗi cung của nó được chỉ thị t hoặc g. Sẽ gọi là các đỉnh trực tiếp liên kết tg với nhau, nếu đường tg giữa chúng chỉ gồm có một cung duy nhất.

• *Định lý 4.3.* Giả sử $G_0=(S_0,O_0,E_0)$ – giản đồ truy nhập chỉ chứa các đỉnh-chủ thể. Mệnh đề "có thể chia sẻ quyền" (α,x,y,G_0) đúng khi và chỉ khi thoả mãn các điều kiện 1 và 2 sau đây:

Điều kiện 1: Tồn tại các chủ thể $s_1,\ldots,s_m$ sao cho $(s_0,y,\gamma_1) \in E_0$ đối với i=1,…,m và $\alpha=\gamma_1 \cup \ldots \cup \gamma_m$.

Điều kiện 2: Chủ thể x trong giản đồ G_0 được nối bằng đường tg với mỗi chủ thể s_i ,với i=1,…,m.

Chứng minh: Đây là định lý có chứng minh khá phức tạp. Chúng ta không dẫn ra toàn bộ chứng minh mà sẽ chỉ ra phương pháp thực hiện nó.

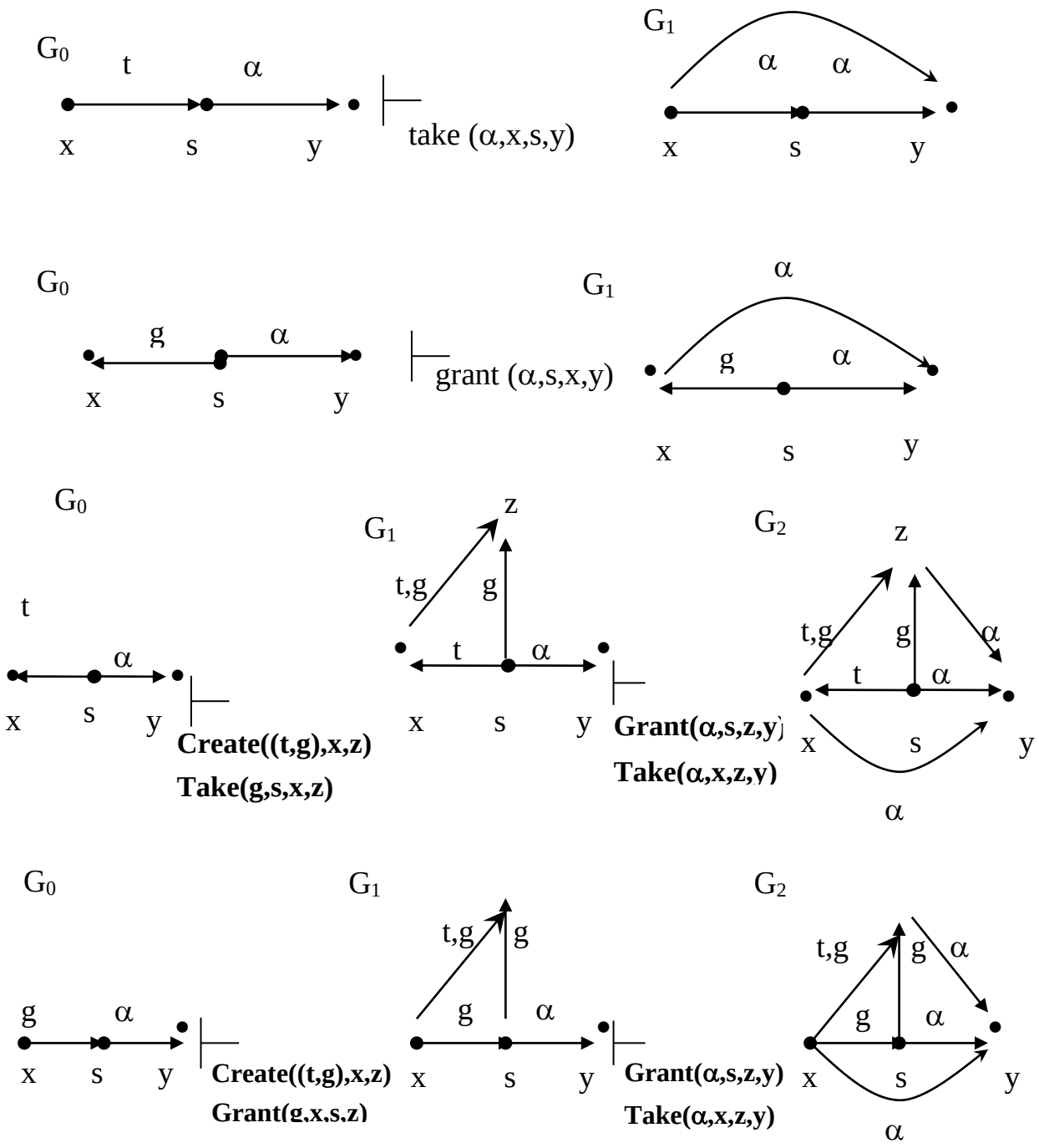
Đầu tiên người ta chứng minh định lý với m=1 (trường hợp m >1 dễ dàng suy ra.

Sau đó áp dụng phương pháp quy nạp toán học chứng minh tính cần và đủ của định lý.

Chứng minh tính cần: Giả sử mệnh đề là đúng sẽ suy ra sự cần thiết của các mệnh đề 1 và 2.

Chứng minh tính đủ: Giả sử hoàn thành các điều kiện 1 và 2 sẽ dẫn tới mệnh đề phải đúng.

Trong hình vẽ sau, chúng ta sẽ đưa ra tất cả các trường hợp có thể của liên kết tg trực tiếp của x và s.



Hình 4.2 Tất cả các trường hợp có thể của liên kết tg trực tiếp của hai thực thể

• *Định lý 4.4:* Người ta có thể chứng minh định lý 2 về khả năng trao quyền trái phép xảy ra ở các điều kiện kém chặt chẽ hơn so với các điều kiện của định lý 1. Ở đây chúng tôi chỉ giới thiệu về sự tồn tại của định lý này.

Tuy cả 2 trường hợp trao quyền nói tới ở định lý 1 và 2 vẫn đều giả định có sự hợp tác, tác động nhất định của các chủ thể, đặc biệt là đều có tác động tham gia của chủ thể ban đầu có một số quyền truy nhập để trao đổi.

4.2.2.3. Khả năng chiếm quyền truy nhập (Định lý 3)

Trong trường hợp trao quyền bất hợp pháp đều giả định sự hợp tác chặt chẽ của các chủ thể tham gia (các điều kiện của định lý 1 và định lý 2).

Trong khuôn khổ mô hình Take-Grant có thể chứng minh được khả năng tồn tại việc chiếm quyền truy nhập.

Giả sử x,y $\in$ O – là các đối tượng khác nhau của giản đồ truy nhập $G_0=(S_0,O_0,E_0)$; $\alpha \subseteq R$. Ta định nghĩa mệnh đề "cướp quyền có thể" (α,x,y,G_0) mà sẽ đúng khi và chỉ khi $(x,y,\alpha) \in E_0$ và tồn tại cácgiản đồ $G_1=(S_1,O_1,E_1)$, …, $G_N=(S_N,O_N,E_N)$ sao cho $G_0 \vdash op_1 G_1 \vdash op_2 \ldots \vdash op_N G_N$ và $(x,y,\alpha) \in E_N$; trong đó, nếu $\exists (x,y,\alpha) \in E_0$ thì $\forall z \in S_j$, j = 0,1,…,N opK $\neq$ grant(α,s,z,y) K=1,…N.

• *Định lý 4.5:* Giả sử $G_0=(S_0,O_0,E_0)$ là giản đồ truy nhập bất kỳ. Mệnh đề "cướp quyền có thể" đúng khi và chỉ khi thoả mãn các điều kiện 1,2,3 sau:

Điều kiện 1: $(x,y,\alpha) \notin E_0$.

Điều kiện 2: Tồn tại các đối tượng $S_1,\ldots,S_m$ sao cho $(s_i,y,\gamma_i) \in E_0$ với i=1,…m và $\alpha = \gamma_i \cup \ldots \cup \gamma_m$

Điều kiện 3: Các mệnh đề "có thể chia sẻ quyền" (t,x,s_i,G_0) với i=1,…,m là đúng.

Chứng minh tương tự như định lý 2.

4.2.3. Mô hình bí mật Bell – Lapadula

4.2.3.1. Khái niệm mức AT, hạng mục AT và nhãn AT

a) Mức an toàn

Mức an toàn được định nghĩa như một đặc trưng phân cấp (hierarchical attribute) được gắn liền với các thực thể trong hệ máy tính, giúp cho ta đánh dấu mức độ nhạy cảm an toàn của chúng.

Thực tế cho thấy, trong nhiều hệ thống MT tồn tại mối quan hệ thứ bậc giữa các độ nhạy cảm an toàn của các thực thể của chúng. Ví dụ, một file này có thể có nhạy cảm an toàn cao nhất, file khác có thể có nhạy cảm an toàn thấp hơn, file khác nữa sẽ có nhạy cảm an toàn khác... Tình huống này giống như sự nhạy cảm quen thuộc thường gắn với các hồ sơ và các nhân viên trong một cơ quan. Trong mỗi cơ quan hay mỗi công ty, thì các ghi nhớ, các báo cáo, các nhân viên và các tài nguyên khác thường được coi là có một độ nhạy cảm và một tầm quan trọng nào đó trong khuôn khổ thứ bậc đã được xác định.

Khi mối tương quan thứ bậc đã được hình thành, cần một cơ chế cho việc lập thẻ tên các thực thể cơ bản trong hệ MT sao cho nhạy cảm an toàn của chúng thể hiện được. Một trong những biện pháp để làm việc này là gắn cho mỗi thực thể một mức an toàn. Các nhãn an toàn luôn luôn thuộc về một cấp bậc đã xác định. Ví dụ, trong quân sự, tập các mức bao gồm: mức không phân loại (không xếp vào loại mật), mức mật, mức tối mật, mức tuyệt mật. Thứ bậc của các mức an toàn trong quân sự được xác lập như sau: Tuyệt mật được coi là cao hơn tối mật; Tối mật coi là cao hơn mật; Mật coi là cao hơn không phân loại (không mật). Trong môi trường thương mại, các mức tương ứng có thể là: Hạn chế, độc quyền, nhạy cảm, và công cộng. Hình 4.2 thể hiện điều đó.

Tuyệt mật	Hạn chế
Tối mật	Sở hữu
Mật	Nhạy cảm
Không phân loại	Công cộng
a) Mức an toàn quân sự	b) Mức an toàn thương mại

Hình 4.3 Các mức an toàn quân sự và thương mại

Để giúp cho việc biểu diễn các mức an toàn và các khái niệm tương tự trong chương này và tiếp sau, chúng ta cần đưa vào các cấu trúc toán học đơn giản và các quan hệ toán học cần thiết. Trong các thảo luận như vậy, một tập các mức an toàn sẽ được nói đến bằng tên " levels " (các mức). Còn quan hệ thứ bậc giữa các yếu tố khác nhau của "levels " sẽ được ghi nhận bằng các ký hiệu điều kiện:

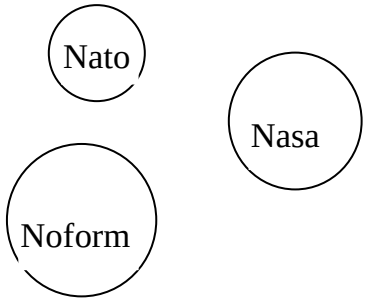
$<$ nhỏ hơn ; $\leq$ nhỏ hơn hoặc bằng ; $>$ lớn hơn ; $\geq$ lớn hơn hoặc bằng.

Trong ý nghĩa đó, " levels " có thể được coi là một tập hợp có thứ tự. Nghĩa là, hai phần tử bất kỳ của "levels" đều có thể được so sánh để xác định xem chúng là bằng nhau hay có một lớn hơn.

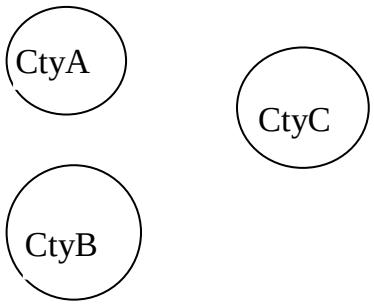
b) Hạng mục an toàn

Các hạng mục an toàn được định nghĩa như sự nhóm không thứ bậc các thực thể của hệ MT để giúp chỉ ra mức độ nhạy cảm an toàn của chúng.

Để hiểu điều này, hãy coi rằng, trong một hệ MT ngoài các mức an toàn, cần phải chia nhỏ các thực thể khác nhau của hệ thành các nhóm không có thứ bậc. Điều này được thực hiện bằng việc dùng các hạng mục an toàn categories. Các category quân sự điển hình có thể là các nhóm nato, nhóm nasa, nhóm nga, nhóm đông-nam á, nhóm nội địa và nhóm noform. Sự tương tự như vậy có thể dựa trên cơ sở là nhiều tập đoàn và công ty được chia ra theo các dự án khác nhau mà các tài nguyên của chúng được cung cấp cho hệ thống. Các hạng mục an toàn phi thứ bậc nói chung, cung cấp mô hình có ý nghĩa cho các tình huống tương tự. Ví dụ, các hạng mục an toàn thương mại có thể được xác định bởi thành viên của tập đoàn, của công ty (xem hình dưới).



Hình 4.4 Hạng mục AT quân sự điển hình



Hình 4.5 Hạng mục AT thương mại điển hình

Lưu ý rằng, không có gì ngăn cản việc cho phép các thực thể hay các nhân viên của một hệ được gắn với hơn một category an toàn. Hiển nhiên là nhà thiết kế hoặc quản trị hệ thống có thể lựa chọn để lập ra bản phân hoạch nhờ dùng các category an toàn sao cho: tất cả các đối tượng chỉ nằm đúng ở một category an toàn mà thôi, nhưng điều này không phải là nhất thiết. Cũng cần lưu ý rằng, không loại trừ trường hợp hệ thống không có category an toàn nào hoặc chỉ có một tập con các đối tượng của hệ được gắn với các category an toàn đã xác định.

Một khái niệm hữu ích trong quân sự thường được mô tả bởi các category an toàn là khái niệm Cần-để-Biết (Need-to-Know), trong đó thông tin không chỉ được gắn các mức an toàn quân sự mà còn được gắn với thuộc tính quân sự Cần-để-Biết. Điều đó cho phép thông tin chỉ được chuyển tới những ai cần nó nếu các mức an toàn cho phép. Thuộc tính Cần-để-Biết trong quân sự là phi thứ bậc, vì rằng các cá nhân làm việc trong khuôn khổ một mức an toàn nào đó có thể không cần biết một số thông tin tại mức này. Ví dụ, các cá nhân nằm trong khoảng cho phép Tuyệt Mật có thể không được quyền khảo sát thông tin tuyệt mật nếu họ không có nhu cầu đáng kể Cần-để-Biết thông tin này.

Trong các thảo luận có tính chất toán học tiếp sau đây, tập các hạng mục an toàn sẽ được ký hiệu là "categories", và chúng ta thường khảo sát các tập con khác nhau của "categories" bằng quan hệ bao hàm "$\subseteq$". Tất cả các tập con của "categories" không giống như các phần tử của tập "levels" không phải tất cả đều có thứ bậc dưới quan hệ bao hàm. Nghĩa là, nếu "categories" = { C , C* }, thì các tập con { C } và {C*} không bằng nhau mà cũng không có tập con nào là phủ lên tập con kia.

c) Các nhãn an toàn

Nhãn an toàn được định nghĩa như một đặc trưng gắn liền với các thực thể của hệ MT để đánh dấu mức nhạy cảm có thứ bậc và tính chất Cần-để-Biết của chúng. Một cách đặc thù, một nhãn an toàn bao gồm hai thành tố: một mức an toàn có thứ bậc và một tập (có thể là rỗng) các hạng mục an toàn phi thứ bậc. Chúng ta sẽ nói về tập các nhãn an toàn trong các thảo luận tiếp theo là "labels" với định nghĩa toán học như sau (ở đây, ký hiệu viết hoa P(categories) đánh dấu tập của tất cả các tập con của các hạng mục):

" labels " = "levels " × P(categories)

Tại đây ta đã dùng ký hiệu toán học quan hệ tích chéo, được định nghĩa như sau:

Cho các tập X và Y, tích chéo X × Y là một tập hợp tất cả các cặp có thứ tự (x,y), trong đó x là một yếu tố của X và y là một yếu tố của Y. Ví dụ, nếu X = {1,2} và ta có Y = {a,b} thì

X × Y+= = {(1,a),(1,b),(2,a),(2,b)}

Như vậy, các nhãn là một tập tất cả các cặp có thứ tự (a,b) trong đó a là một yếu tố của các mức (levels) và b là một yếu tố của P(categories). Ta thấy, một nhãn an toàn bao giờ cũng cấu tạo từ một mức an toàn và một tập các hạng mục an toàn (có thể là tập rỗng). Ta hãy xét một ví dụ cụ thể. Giả sử rằng, trong môi trường quân sự, các định nghĩa sau đây là đúng:

"levels" = {mật,tối mật}

"categories" = {army,navy}

P(categories) = {∅,{army},{navy},{army,navy}}.

Nói cách khác, hai mức an toàn Mật và Tối mật được định nghĩa trong môi trường quân sự và hai hạng mục an toàn army và navy (quân đội và hải quân) cũng được xác định. Định nghĩa này cung cấp cho ta tập các nhãn an toàn trong môi trường quân sự là tích chéo của hai tập này, cụ thể như sau :

"labels" = {(mật,{army}),(tối mật,{army}),
(mật,{navy}),(tối mật,{navy}),
(mật,{army,navy}),(tối mật,{army,navy}),
(mật,∅),(tối mật,∅)}

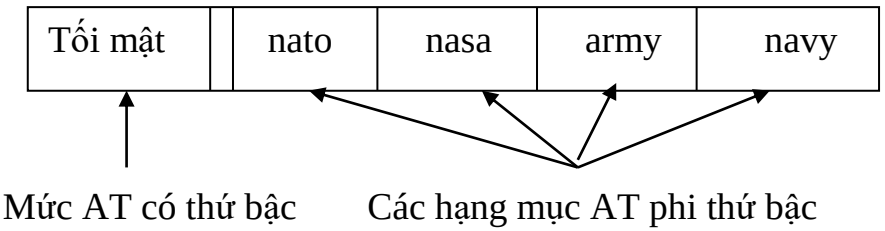
Để cho thuận tiện, một nhãn an toàn đã cho x= (lev,cats), chúng ta dùng lev để ký hiệu toán tử hình chiếu lev(x) và cats để ký hiệu toán tử hình

chiếu cats(x). Như vậy, lev((tối mật,∅)) sẽ là (tối mật) và cats((mật,{army})) sẽ là {army}. Hơn nữa, chúng ta sẽ tiếp tục sử dụng ký hiệu cặp có thứ tự để biểu diễn các nhãn an toàn. Ví dụ

x = (không phân loại,{a, b, c})

Ví dụ trên thể hiện nhãn an toàn x với mức an toàn có thứ bậc là không phân loại, nghĩa là lev(x) = không phân loại và các hạng mục an toàn phi thứ bậc là a, b và c, nghĩa là cats(x) = {a, b, c}.

Thông thường có thể thấy rằng, các nhãn an toàn cũng được biểu diễn bằng sơ đồ mô tả mức an toàn và các hạng mục an toàn đi kèm. Chẳng hạn, giản đồ trong hình vẽ sau mô tả nhãn an toàn quân sự điển hình với mức an toàn và tiếp sau là bốn hạng mục an toàn



Hình 4.6 Nhãn an toàn quân sự điển hình

4.2.3.2. Khái niệm quan hệ trội

a) Quan hệ hai ngôi

Chúng ta nhớ rằng, một quan hệ hai ngôi (a binary relation) trên tập X là một tập con của tích chéo X × X. Ví dụ, quan hệ thứ tự giữa cặp hai số nguyên bất kỳ trên tập các số nguyên Z là một quan hệ hai ngôi điển hình. Nếu a là một yếu tố của Z và b cũng là một yếu tố khác của Z, thì rõ ràng là quan hệ a > b là một yếu tố của một tập con của tích chéo Z × Z. Các yếu tố của một quan hệ bất kỳ được xác định, nói chung, đều chia sẻ một tính chất chung nào đó. Chẳng hạn, quan hệ nhỏ hơn xác định trên các số nguyên bao gồm tất cả các cặp có thứ tự các số nguyên, trong đó thành tố đầu tiên của cặp nhỏ hơn thành tố thứ hai. Tương tự, quan hệ bằng nhau trên các số nguyên bao gồm tất cả các cặp có thứ tự các số nguyên, trong đó thành tố thứ nhất bằng thành tố thứ hai.

b) Quan hệ trội

Chúng ta sẽ đưa ra định nghĩa sau, quan hệ trội (a dominate relation) là một quan hệ hai ngôi (a binary relation) được xác định trên tập các nhãn an toàn "labels". Khi một cặp các nhãn an toàn (a,b) là một phần tử của tập "labels", chúng ta nói rằng cặp (a,b) thuộc quan hệ trội ((a,b) $\in$ dominates) hoặc a trội so với b (a dominates b). Dễ thấy rằng, trên quan điểm trội thì, khi một nhãn an toàn trội so với một nhãn an toàn khác mà không quan trọng hơn thì chúng ta không nói "kém quan trọng" hơn vì rằng, ở đây chúng ta quy định rằng một nhãn an toàn trội so với chính nó. Đặc biệt, điều kiện mà chúng ta sẽ sử dụng để định nghĩa quan hệ trội dominates như sau :

$\forall$ x1,x2 $\in$ "labels" : x1 dominates x2 khi và chỉ khi

lev(x1) > lev(x2) và cats(x1) $\supseteq$ cats(x2)

Điều kiện trên cho rằng, một nhãn an toàn trội so với một nhãn khác khi thành phần mức an toàn của nó lớn hơn hoặc bằng thành phần mức an toàn của nhãn kia và khi tập các hạng mục an toàn của nó là tập bao của tập các hạng mục an toàn của nhãn kia. Có thể viết lại như sau:

Dominates $\in$ labels $\times$ labels sao cho

(x1,x2) $\in$ dominates khi

lev(x1) > lev(x2) và cats(x1) $\supseteq$ cats(x2)

Lưu ý rằng, mặc dù các ký hiệu dùng để mô tả quan hệ trội khá phức tạp, trên thực tế nó hoàn toàn đơn giản. Ví dụ, quan hệ bằng nhau trên các nhãn (nghĩa là, một cặp các nhãn ở trong quan hệ này nếu các thành tố của chúng bằng nhau) có thể được mô tả như sau:

$\forall$ x1,x2 $\in$ "labels" : x1 bằng x2 khi và chỉ khi

lev(x1) = lev(x2) và cats(x1) = cats(x2)

Để tiếp tục minh hoạ về khái niệm dominates, hãy giả thiết rằng, những tuyên bố sau đây tất cả đều đúng trong môi trường quân sự với các nhãn an toàn quân sự và các hạng mục an toàn a và b :

((Tuyệt mật,{ a }),(Tuyệt mật,$\varnothing$)) $\in$ dominates

((Tối mật,{a,b}),(Không phân loại,{a})) $\in$ dominates

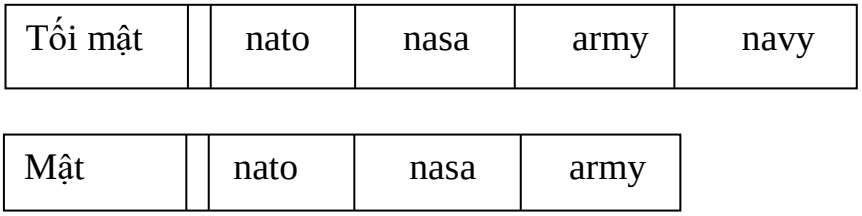
((Không phân loại,{a,b}),(Không phân loại,{a,b})) $\in$ dominates

not (((Tuyệt mật,$\varnothing$),(Không phân loại,{a})) $\in$ dominates)

not (((Tối mật,{a}),(Không phân loại,{a,b})) ∈ dominates)

not (((Tối mật,{a}),(Tối mật,{a,b})) ∈ dominates)

Như ở trên đã giả định, các tuyên bố này cũng có thể được biểu diễn ở dạng sao cho dễ đọc hơn: ví dụ, (Tuyệt mật,{a}) dominates (Tuyệt mật,{∅}). Cũng còn cách khác để miêu tả quan hệ trội bằng giản đồ như trong hình vẽ sau:



Hình 4.7 Mô tả quan hệ trội bằng giản đồ

Trong sơ đồ này, hai nhãn an toàn được vẽ ra sao cho liên hệ giữa các mức an toàn và các hạng mục an toàn dễ nhìn thấy. Trong ví dụ, mức nhãn ở trên lớn hơn mức nhãn ở dưới, còn categories của nhãn ở trên tạo thành tập bao của tập các categories của nhãn dưới. Kết quả là nhãn trên trội so với nhãn dưới.

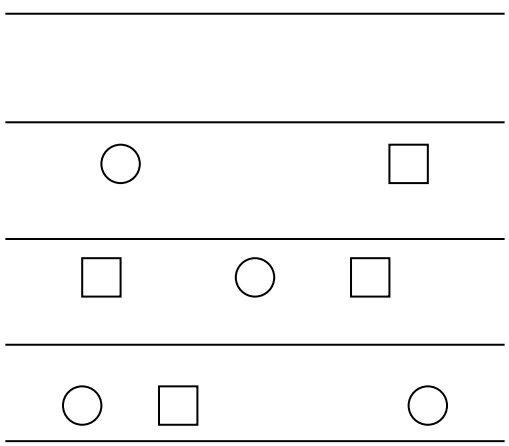
4.2.3.3. Các đồ hình mức

Chúng ta bắt đầu bằng việc mô tả kỹ thuật đồ hình mức phi hình thức. Đồ hình này dùng để mô tả mô hình Bell – Lapadula (gọi tắt là mô hình BLP) và các mô hình khác trong chương này.

Trong các thảo luận ở trước ta đã phân biệt cẩn thận giữa các mức an toàn và các nhãn an toàn (chúng bao hàm các hạng mục an toàn phi thứ bậc).Ta cũng đã phân biệt giữa mối quan hệ trội (dominates) trên các nhãn an toàn và quan hệ > trên các mức an toàn. Tuy nhiên, trong các nghiên cứu về an toàn hệ MT, để đơn giản các thảo luận người ta thường bỏ qua cấu trúc dàn của các nhãn an toàn và thay thế chúng bằng thứ tự của các mức an toàn (tức là ta chỉ chú ý tới thành phần lev(x) của nhãn an toàn x mà thôi). Sự đơn giản hoá này cho phép đánh giá các mô hình an toàn theo thuật ngữ các mức an toàn mà không xét đến trường hợp các mức an toàn không so sánh được với nhau (như trường hợp đối với hai nhãn an toàn không có nhãn nào trội hơn nhau).Thực tế cho thấy, sự đơn giản như vậy dẫn đến sự tổng quát hoá mà

không gây ảnh hưởng gì lớn tới bản chất của các mô hình an toàn. Do vậy, chúng ta sẽ thảo luận ở đây mô hình BLP theo các mức an toàn được xếp thứ tự dựa trên quan hệ >.

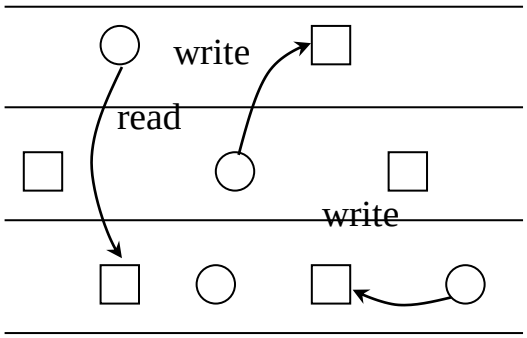
Chúng ta sẽ biểu diễn mô hình BLP bằng cái gọi là các đồ hình mức. Chúng gồm một số đường thẳng nằm ngang và một nhóm các hình tròn và hình vuông nhỏ. Các đường thẳng có thể được coi như là đường ranh giới giữa các mức an toàn khác nhau trong hệ thống đã cho (các đường nằm phía trên biểu diễn ranh giới giữa các mức an toàn cao hơn). Trong vùng giữa hai đường thẳng, các hình tròn biểu diễn các chủ thể, còn các hình vuông là các đối tượng.



Hình 4.8 Đồ hình mức

Trên đồ hình này có hai chủ thể và một đối tượng ở mức an toàn thấp nhất, có một chủ thể và hai đối tượng ở mức trung, có một chủ thể và một đối tượng nằm ở mức an toàn cao nhất.

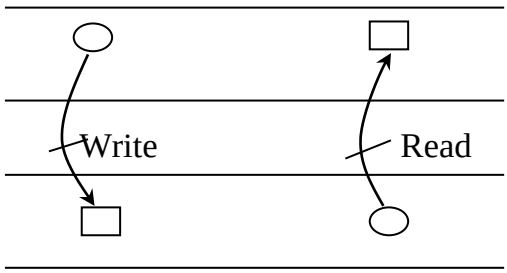
Các thao tác vẽ trên đồ hình là những cung hướng từ chủ thể đến đối tượng. Các cung hướng từ một chủ thể đến một đối tượng có ghi chữ write hoặc read chỉ thao tác ghi hoặc đọc từ chủ thể đến đối tượng. Những cung đó luôn xuất phát từ chủ thể và mũi tên chỉ hướng đến đối tượng. Hình sau là hai kiểu thao tác đọc – ghi.



Hình 4.9 Mô tả các thao tác read và write

Lưu ý rằng, hình trên vẽ một thao tác đọc từ chủ thể ở mức an toàn cao xuống một đối tượng nằm ở mức an toàn thấp nhất. Nó cũng biểu diễn một thao tác ghi từ một chủ thể ở mức trung lên một đối tượng ở mức an toàn cao nhất và một thao tác ghi của một chủ thể đến một đối tượng cùng ở mức an toàn thấp nhất.

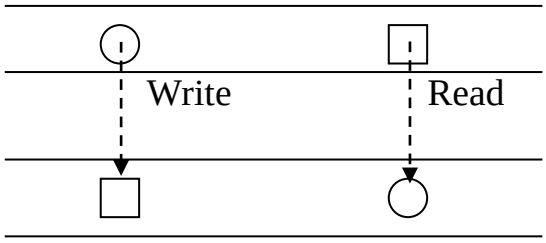
Trên đồ hình mức, các cung định hướng với đường gạch ngang chéo qua sẽ biểu diễn các thao tác không được phép. Ví dụ như trong hình biểu diễn hai thao tác như vậy.



Hình 4.10 Các thao tác đọc và ghi không được phép

Các thao tác đọc - ghi làm cho luồng thông tin di chuyển giữa chủ thể và đối tượng. Trong thao tác đọc, thông tin chảy từ đối tượng sang chủ thể, còn trong thao tác ghi, thông tin chảy từ chủ thể đến đối tượng. Để biểu diễn dòng thông tin này, ta vẽ đường chấm chấm từ các chủ thể đến các đối tượng với mũi tên chỉ hướng đi của luồng TT. Chú ý, trong thao tác đọc, cung vẽ biểu diễn thao tác read sẽ xuất phát từ chủ thể hướng tới đối tượng cần đọc, còn đường chấm hấm biểu diễn luồng TT sẽ xuất phát từ đối tượng và hướng tới chủ thể như trong hình sau.

Các dòng thông tin trong thao tác ghi chảy cùng hướng với các cung biểu diễn thao tác write (từ chủ thể hướng tới đối tượng). Lưu ý rằng, hình sau biểu diễn một hệ thống cho phép đọc lên và ghi xuống (tức là nó ngược lại với hình ở trên). Hai hình vẽ này chỉ là các ví dụ cho đồ hình mức mà thôi.



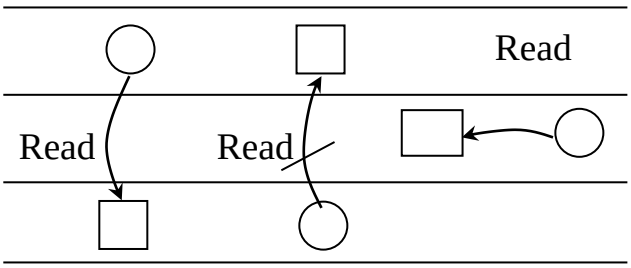
Hình 4.11 Các đường chỉ dòng thông tin.

4.2.3.4. Các quy tắc của mô hình BLP

Nhận xét cơ bản của Bell và Lapadula khi họ đưa ra mô hình của mình là: tất cả các chủ thể và các đối tượng thuộc các hệ thống MT của Chính phủ Mỹ đều được gắn với các nhãn an toàn từ loại thấp nhất như Không phân loại cho đến loại cao nhất là Tuyệt mật (giống như trong chương trước chúng ta đã bàn tới). Hơn nữa, khi làm việc cho dự án do Chính phủ Mỹ tài trợ hai ông còn phát hiện ra rằng, để ngăn cản được sự rò rỉ thông tin đến các chủ thể không uỷ quyền thì những chủ thể có nhãn an toàn thấp sẽ không được phép đọc thông tin từ các đối tượng có nhãn an toàn cao hơn. Chính điều này đã dẫn đến quy tắc thứ nhất của mô hình BLP.

a) Quy tắc không đọc lên (NRU- No read up)

Thuộc tính an toàn đơn giản hay là quy tắc không đọc lên (no read up - NRU) phát biểu rằng, một chủ thể với nhãn an toàn x_s chỉ có thể đọc thông tin từ đối tượng có nhãn an toàn xo nếu xs trội hơn so với x_0 (hay x_s dominates x_0). Điều này có nghĩa là nếu một chủ thể có độ cho phép (clearance) là Mật, cố đọc thông tin từ một đối tượng có phân lớp (classification) là Tuyệt mật trên một hệ thống tuân thủ quy tắc NRU thì yêu cầu đọc đó sẽ không được cho phép. Quy tắc NRU được minh hoạ một cách đơn giản trong hình sau.

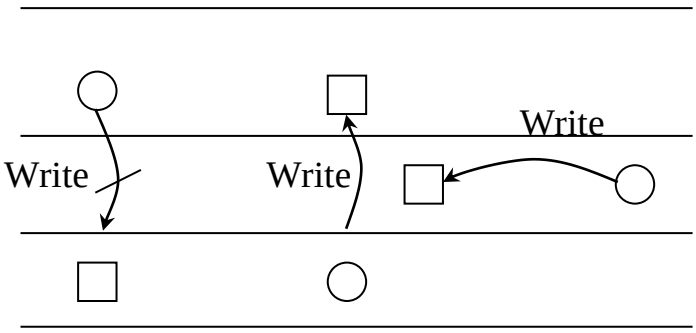


Hình 4.12 Thuộc tính an toàn đơn giản (NRU)

Trong khi xây dựng mô hình của mình Bell và Lapadula còn nhận xét thêm rằng, trong các hệ thống của Chính phủ Mỹ, người ta không cho phép các chủ thể cất giữ hoặc ghi tài liệu vào các đối tượng có nhãn an toàn thấp hơn. Ví dụ, một tài liệu Tuyệt mật mà được đặt vào một ngăn không mật thì sẽ xảy ra sự rò rỉ thông tin. Chính điều này dẫn đến quy tắc thứ hai của mô hình BLP.

b) Quy tắc không ghi xuống (NWD-No write down)

Quy tắc không ghi xuống (no write down-NWD) hay còn gọi là thuộc tính * (đọc là thuộc tính sao-Star property) phát biểu như sau: Một chủ thể có nhãn an toàn x_s chỉ có thể ghi thông tin lên một đối tượng có nhãn an toàn x_0 khi mà x_0 dominates x_s. Bởi vậy, nếu một chủ thể có độ cho phép Tuyệt mật cố ghi thông tin lên một đối tượng có phân loại Mật, trên một hệ thống tuân thủ mô hình BLP thì sẽ không được cho phép. Quy tắc này được mô tả phi chính tắc trong hình sau.



Hình 4.13 Quy tắc không ghi xuống (NWD)

Lưu ý rằng, vì các chủ thể có thể có các nhãn an toàn khác nhau nên một chủ thể có nhãn Tuyệt mật có thể ghi lên một đối tượng với nhãn Không phân loại chỉ khi chủ thể đó được gắn nhãn Không phân loại (hoặc thấp hơn).

Điều này phức tạp hơn vì nó không chỉ đòi hỏi xem xét nhãn an toàn đang có hiệu lực vào lúc đòi hỏi một thao tác, mà nó còn đòi hỏi cách thức có thể thay đổi nhãn AT đang còn hiệu lực.Ta sẽ xác định khái niệm thay đổi các nhãn an toàn trong phần thảo luận về tính ổn định của mô hình BLP dưới đây.

4.2.3.5. Tính ổn định và mô hình BLP

Ta đã thấy ở trên, các quy tắc NRU và NWD của mô hình BLP hỗ trợ một cách trực giác về cách ngăn chặn sự rò rỉ thông tin đến những nơi không được phép. Một chủ thể nào đó có độ cho phép Mật, muốn xem TT được xếp vào loại Tối mật thì quy tắc NRU sẽ ngăn chặn việc này vì TT Tuyệt mật nhạy cảm hơn TT mà chủ thể đó được phép xem. Tương tự, nếu chủ thể muốn đặt TT Tuyệt mật vào đối tượng không mật thì quy tắc NWD sẽ ngăn chặn điều này xảy ra, vì vị trí đó không phải là chỗ lưu TT nhạy cảm hơn.

Chúng ta thấy rằng, các yêu cầu đọc, ghi đều được thu xếp dựa trên các nhãn an toàn của chủ thể và đối tượng. Ngoài ra, hầu hết các yêu cầu đọc, ghi trên một hệ thống thực tế thường không phải là tự động. Nghĩa là chúng bao gồm một dãy các thao tác có hoặc không có khả năng bị ngắt bởi một hành động khác (của hệ thống). Chẳng hạn, các yêu cầu in một tập tin có thể bao gồm một dãy các lệnh gọi hệ thống và các chương trình nhân (kernel) để định vị tệp, mở nó để đọc và sau đó là khởi động quá trình in tập tin đó.

Như vậy, các quy tắc NRU và NWD ngầm đòi hỏi những thuộc tính nào đó trong tất cả các truy nhập. Đặc biệt, chúng đòi hỏi các nhãn an toàn của các chủ thể và các đối tượng trong truy nhập mong muốn nào đó sẽ không bị thay đổi trong suốt thời gian mà quá trình truy nhập vẫn còn đang xử lý theo cách thức khỏi vi phạm những chính sách an toàn. Nếu không như vậy, có thể xảy ra trường hợp sau: Một chủ thể mật đòi hỏi truy nhập đọc đến một đối tượng mật và trong khi yêu cầu đang được xử lý nhãn AT của chủ thể lại bị thay đổi (giảm xuống thấp hơn), và như vậy, chủ thể không còn xếp loại mật nữa lại được phép truy nhập đọc đến đối tượng mật. Ta thấy, tính ổn định của các nhãn an toàn ở đây có vai trò rất quan trọng.

a) Tính ổn định mạnh

Thuộc tính ổn định mạnh phát biểu rằng, các nhãn an toàn của các chủ thể và các đối tượng không bao giờ được thay đổi trong suốt thời gian hệ thống hoạt động.

Bằng cách bảo đảm điều kiện này trên hệ thống cho trước, có thể dễ dàng kết luận rằng, vấn đề vi phạm quy tắc BLP mô tả ở trên sẽ không bao giờ xuất hiện. Hạn chế hiển nhiên trong các hệ thống có tính ổn định mạnh là mức độ linh hoạt trong các thao tác bị mất đi.

b) Tính ổn định yếu

Thuộc tính ổn định yếu phát biểu rằng, các nhãn an toàn của các chủ thể và các đối tượng không bao giờ được thay đổi theo cách vi phạm đến một chính sách an toàn.

Thuộc tính này đòi hỏi các chủ thể và đối tượng kiềm chế khỏi các hành động nhất định trong khoảng thời gian khi các nhãn an toàn của chúng bị thay đổi. Ví dụ, có thể đòi hỏi để nhãn an toàn của một đối tượng không được thay đổi khi một chủ thể nào đó đang sử dụng đối tượng đó. Tuy nhiên, nếu một thao tác xen vào làm thay đổi nhãn an toàn mà không gây nên sự vi phạm quy tắc (chẳng hạn, chủ thể được nâng cấp từ Mật lên Tuyệt mật trong khi đọc một tệp Không mật) thì tính ổn định yếu này vẫn được thừa nhận.

Chú ý rằng, ta vẫn còn chưa nói gì về cách thức thay đổi thực sự các nhãn an toàn. Đó là do sự thay đổi của nhãn an toàn là một khái niệm về thao tác và được xử lý khác nhau trên hầu hết các hệ thống máy tính tuân thủ quy tắc BLP. Trong các thảo luận tiếp theo ta sẽ giả thiết rằng, các nhãn sẽ không bao giờ thay đổi trừ khi được thông báo.

4.3. CÂU HỎI

1. Trình bày các chính sách An toàn thông tin của một tổ chức.
2. Hãy xây dựng một biểu thức toán học mô tả số nhãn an toàn là một hàm của số mức và số hạng mục.
3. Hãy chỉ ra rằng quan hệ trội trên tập các nhãn an toàn quân sự có tính phản xạ, bất đối xứng và bắc cầu.
4. Hãy đưa ra các ví dụ từ các môi trường phi quân sự và phi tính toán mà hỗ trợ hai quy tắc của mô hình BLP.

5. Tạo ra một ví dụ về bối cảnh trong một môi trường phát triển phần mềm hỗ trợ hai quy tắc BLP.

6. Biểu diễn mô hình BLP (cả 2 quy tắc) theo quy tắc dòng thông tin định hướng đơn giản. Chỉ ra rằng, quy tắc mới này gửi được phần chủ đạo của cả hai quy tắc BLP.

7. Hãy giải thích cách giải quyết của các quy tắc BLP với các truy nhập đọc,ghi của một chủ thể lên một đối tượng mà phân loại của nó không liên quan với sự phân cấp của chủ thể gọi đến.

8. Hãy nhận xét về phạm vi của các hệ thống tuân thủ mô hình BLP đối với trường hợp các chủ thể ở mức thấp thay đổi hoặc phá hoại các đối tượng ở mức cao.

9. Bạn hãy mở rộng kiểu quy tắc (nó có thể ràng buộc các kiểu thay đổi nhãn an toàn) trong hệ thống có tính ổn định yếu.

10. Hãy trình bày vắn tắt mô hình ma trận quyền HRU và phân tích vấn đề chuyển quyền trong mô hình đó. Mô hình HRU có an toàn không?

11. Trình bày những vấn đề tương tự như câu 9 đối với mô hình Take-Grant.

12. Phân tích sự khác nhau cơ bản giữa mô hình BLP và các mô hình HRU, Take-Grant.

CHƯƠNG 5. CÁC TIÊU CHÍ ĐÁNH GIÁ VÀ CHUẨN AN TOÀN THÔNG TIN

Hiện nay, trên thế giới đã hình thành một hệ thống tiêu chuẩn An toàn thông tin tương đối đầy đủ, bao quát được hầu hết các khía cạnh của lĩnh vực an toàn thông tin và đáp ứng mọi đối tượng cần tiêu chuẩn hóa (sản phẩm, dịch vụ, quy trình). Hệ thống tiêu chuẩn này có thể phân thành ba loại gồm: tiêu chuẩn đánh giá, tiêu chuẩn đặc tả và tiêu chuẩn về quản lý.

Tuân thủ tiêu chuẩn an toàn thông tin (ATTT) là yếu tố quan trọng đảm bảo cho sự hoạt động ổn định và tin cậy của hạ tầng kỹ thuật, sự an toàn của hệ thống thông tin và dữ liệu của tổ chức, cá nhân. Đối với các nhà thiết kế và sản xuất, tiêu chuẩn sẽ hỗ trợ để họ có thể cung cấp cho thị trường những sản phẩm chất lượng cao và phù hợp với các đối tượng sử dụng.

Đến nay, hầu hết các khía cạnh của lĩnh vực ATTT đã được tiêu chuẩn hóa (sản phẩm, dịch vụ, quy trình). Hệ thống tiêu chuẩn này có thể phân thành ba loại như sau:

- *Các tiêu chuẩn đánh giá*: là các tiêu chuẩn dùng để đánh giá, phân loại các hệ thống thông tin và các phương tiện bảo vệ thông tin.

- *Các tiêu chuẩn đặc tả:* là các tiêu chuẩn mang đặc tính kỹ thuật, chúng xác lập các phương diện khác nhau trong việc thực thi và sử dụng các phương tiện bảo vệ thông tin.

- *Các tiêu chuẩn về quản lý:* Các tiêu chuẩn này xác định yêu cầu đối với công tác tổ chức và quản lý ATTT, quản lý rủi ro và hướng dẫn về ATTT.

Hệ thống tiêu chuẩn về ATTT hiện tại trên thế giới bao gồm Tiêu chuẩn quốc tế (do Tổ chức tiêu chuẩn hóa quốc tế ISO và Ban kỹ thuật điện quốc tế IEC tổ chức xây dựng và công bố), các Tiêu chuẩn quốc gia (do Chính phủ các nước công bố) và các Tiêu chuẩn của các tổ chức chuyên ngành (tương

ứng ở nước ta gọi là tiêu chuẩn cơ sở). Tại các quốc gia phụ thuộc vào công nghệ của phương Tây, tiêu chuẩn quốc gia và tiêu chuẩn chuyên ngành phần lớn được xây dựng theo hướng sao chép toàn bộ hoặc căn bản dựa trên tiêu chuẩn ở các nước phát triển, như là tiêu chuẩn của NIST, ANSI, BS và đặc biệt của ISO. Các nước thuộc hệ thống Xã hội chủ nghĩa trước đây thường sử dụng hệ thống tiêu chuẩn riêng chủ yếu dựa trên hệ thống tiêu chuẩn của Liên Xô. Song những năm gần đây, trong xu thế toàn cầu hóa, các nước này đang từng bước hòa nhập vào hệ thống tiêu chuẩn quốc tế.

Dưới đây sẽ giới thiệu đến hệ thống tiêu chuẩn trong lĩnh vực ATTT trên thế giới nhưng do số lượng tiêu chuẩn là rất lớn, nên sẽ chỉ phân tích những nét khái quát và tập trung vào các tiêu chuẩn được sử dụng rộng rãi nhất.

5.1. GIỚI THIỆU BỘ TIÊU CHUẨN ISO/IEC 27000

5.1.1. Giới thiệu chung

Bộ tiêu chuẩn ISO/IEC 27000 được xây dựng dựa trên các tiêu chuẩn về quản lý an toàn thông tin BS 7799 của Viện Tiêu chuẩn Anh (British Standards Institute - BSI). Tháng 12 năm 2000, tiêu chuẩn BS 7799-1 được Tổ chức Tiêu chuẩn hoá quốc tế (ISO) chính thức chấp nhận và ban hành thành tiêu chuẩn quốc tế ISO/IEC 17799:2000. Năm 2005, tiêu chuẩn này được ban hành thành tiêu chuẩn ISO/IEC 27001:2005 Công nghệ thông tin – Hệ thống quản lý an toàn thông tin – Các yêu cầu.

Bộ tiêu chuẩn ISO/IEC 27000 là bộ sản phẩm an toàn đồng nhất giúp các tổ chức có được một công cụ cần thiết áp dụng các quy phạm an toàn thông tin tốt nhất vào hoạt động kinh doanh hàng ngày. Cho dù là một công ty lớn hay nhỏ, thì bộ tiêu chuẩn này cũng đều có thể đưa ra một phạm vi thông tin toàn diện nhất nhằm đảm bảo an toàn cho thông tin.

Bộ tiêu chuẩn ISO/IEC 27000 được xây dựng dựa trên kinh nghiệm phong phú của các chuyên gia cao cấp trong lĩnh vực an toàn thông tin từ nhiều ngành khác nhau, những người mà bản thân họ đã điều hành các dự án an toàn hệ thống kinh doanh một cách thành công trên thế giới. tiêu chuẩn ISO/IEC 27000 đưa ra một phạm vi rộng lớn về Khung Chính sách mà có thể

thay đổi và áp dụng theo nhu cầu riêng của từng tổ chức và từ đó có thể xây dựng Văn hóa An ninh Thông tin một cách toàn diện.

Bộ tiêu chuẩn ISO/IEC 27000 là tập hợp các tài liệu và tiêu chuẩn giúp doanh nghiệp đạt được mục đích bảo toàn an ninh thông tin của mình. Nội dung của bộ tiêu chuẩn này bao gồm:

- Phiên bản mới nhất ISO/IEC 27002 (ISO 17799) và ISO/IEC 27001 (trước đây là BS 7799-2).
- Bộ chính sách đầy đủ về an toàn thông tin phù hợp với ISO 27002.
- Phần giới thiệu về ISO 17799/ISO/IEC 27001/ISO 27002 dưới dạng PowerPoint
- Công cụ lập kế hoạch khôi phục dữ liệu (ISO 27002 phần 11).
- Sơ đồ chứng nhận.
- Công cụ kiểm tra (bản danh sách các mục cần kiểm tra, v.v...) dùng cho hệ thống mạng lưới hiện đại (phần 12).
- Danh sách đầy đủ các thuật ngữ chuyên môn về máy tính và an toàn thông tin.
- Bảng câu hỏi phân tích tác động đối với kinh doanh.

ISO/IEC 27001: Công nghệ thông tin - Kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

ISO 27002: Công nghệ thông tin - Kỹ thuật an toàn - Qui phạm thực hành về quản lý an toàn thông tin (ISO/IEC 17799:2005)

Đây là một bộ tổng hợp gồm hàng trăm chính sách an toàn thông tin theo ISO 27002/17799. Các chính sách đều đã được thử nghiệm, kiểm tra và đã được sử dụng trên 20 nước. Ngoài ra còn có các ghi chú giải thích cùng với các vấn đề chủ chốt để cân nhắc khi nào áp dụng từng chính sách. Các chính sách còn được tham chiếu chéo với mục tương ứng trong ISO 27002, cung cấp đường liên kết cần thiết để đối chiếu ngược với tiêu chuẩn.

5.1.2. Lợi ích của việc áp dụng

Việc áp dụng các tiêu chuẩn về ATTT theo bộ ISO/IEC 27000 làm tăng nhận thức cho đội ngũ cán bộ nhân viên về ATTT. Xây dựng một môi trường an toàn, có khả năng miễn dịch trước các rủi ro, giảm thiểu các nguy cơ do con người gây ra. Bộ tiêu chuẩn ISO/IEC 27000 đề ra những nguyên tắc

chung trong quá trình thiết kế, xây dựng hệ thống thông tin một cách khoa học, giúp cho việc quản lý hệ thống trở nên sáng sủa, an toàn, minh bạch hơn. Chúng ta xây dựng một "bức tường con người an toàn" (Secure People Wall) trong tổ chức. Một môi trường thông tin an toàn, trong sạch sẽ có tác động không nhỏ đến việc giảm thiểu chi phí vật chất đầu tư cho ATTT vốn dĩ rất tốn kém. Về lâu dài, việc nhận được chứng chỉ ISO/IEC 27001 là một lời khẳng định thuyết phục với các đối tác, các khách hàng về một môi trường thông tin an toàn và trong sạch. Tạo điều kiện thuận lợi cho sự hội nhập một môi trường thông tin lành mạnh. Điều này sẽ tác động mạnh đến ưu thế cạnh tranh của tổ chức.

Tóm lại, khi áp dụng bộ chuẩn này sẽ:

1. Chứng tỏ sự cam kết đảm bảo sự an toàn về thông tin ở mọi mức độ
2. Đảm bảo tính sẵn sàng và tin cậy của phần cứng và các cơ sở dữ liệu
3. Bảo mật thông tin, tạo niềm tin cho đối tác, khách hàng
4. Giảm giá thành và các chi phí bảo hiểm
5. Nâng cao nhận thức và trách nhiệm của nhân viên về an ninh thông tin

5.2. CÁC TIÊU CHÍ ĐÁNH GIÁ AN TOÀN THÔNG TIN

5.2.1. Các khái niệm cơ bản

Trước khi nghiên cứu nội dung của các tiêu chuẩn ATTT chúng ta cần làm quen với một số thuật ngữ và định nghĩa.

- Chính sách an toàn (Security Policy): Tập hợp các điều luật, các quy định bảo đảm sự bảo vệ có hiệu quả các hệ thống xử lý TT chống lại các hiểm họa ATTT.
- Mô hình an toàn (Security Model): Đó là các biểu diễn hình thức của chính sách an toàn.
- Kiểm soát truy nhập tuỳ chọn (Discretionary Access Control – DAC): Đó là sự điều khiển truy nhập dựa trên tập các điều luật cho phép truy nhập được xác định trước bởi nhà quản trị. Ví dụ, dưới dạng ma trận quyền (chủ thể, đối tượng, truy nhập).

• Kiểm soát truy nhập bắt buộc (chuẩn) (Mandatory Access Control – MAC): Đó là điều khiển truy nhập dựa trên các điều luật cho phép truy nhập, được xác định nhờ tập các nhãn an toàn của các chủ thể và các đối tượng, ví dụ, phụ thuộc vào độ mật của TT và mức cho phép của khách hàng.

• Nhân an toàn hay cơ sở tính toán tin cậy (Trusted Computing Base – TCB): Đó là tập hợp các thành tố máy móc, thiết bị, chương trình thực hiện sự bảo vệ và bảo đảm an toàn hệ thống.

• Nhận dạng (Indentification): Quá trình nhận biết các thực thể bằng cách gán cho chúng các dấu hiệu riêng (các đặc chỉ).

• Xác thực (Authentification): Quá trình kiểm tra tính chân thực của các đặc chỉ của các thực thể bằng các phương pháp khác nhau (chủ yếu là bằng mật mã).

• Tính đảm bảo (Assurance – phù hợp). Đó là chỉ số mức độ an toàn được đảm bảo trên thực tế, nó phản ánh tính hiệu quả và độ tin cậy của các sản phẩm bảo vệ được cài đặt và sự đáp ứng của chúng với các nhiệm vụ đặt ra (trong đa số trường hợp đây là nhiệm vụ thực hiện các CSAT).

• Phân tích đánh giá, đánh giá mức độ an toàn, đánh giá ATTT (Information Security Evaluation). Đó là sự phân tích một hệ thống TT – VT với mục đích xác định mức độ an toàn (độ bảo vệ) và mức độ đáp ứng của nó đối với các đòi hỏi ATTT trên cơ sở các tiêu chí của một chuẩn ATTT cụ thể. Đó là quá trình kiểm chuẩn một hệ thống. Đánh giá mức độ ATTT là khâu cuối của chu trình công nghệ thiết lập hệ thống ATTT, hoàn tất các thủ tục kiểm chuẩn và nó kết thúc bằng việc gán cho hệ thống một lớp AT này hoặc lớp AT kia hay mức AT này hoặc mức AT khác. Các chuyên gia làm việc trong lĩnh vực phân tích đánh giá ATTT gọi là các chuyên gia kiểm chuẩn ATTT.

• Phân loại học – Phép phân loại (Taxonomy). Môn khoa học về sự hệ thống hoá và phân loại các đối tượng phức tạp về tổ chức và các hiện tượng có cấu trúc thứ bậc.

• Đường dẫn tin cậy (Trusted Path). Đó là nguyên tắc tổ chức tương tác thông tin (giữa khách hàng và hệ thống) bảo đảm rằng TT được trao đổi không bị mất trên đường hoặc không bị xuyên tạc.

• Sản phẩm CNTT (Information Technology Product) là một sự kết hợp phần cứng, phần mềm và phần sụn cung cấp một chức năng được thiết kế để sử dụng hay kết hợp sử dụng trong hệ thống CNTT.

Sản phẩm CNTT có thể là một sản phẩm đơn hay nhiều sản phẩm được cấu hình lại như một hệ thống CNTT, mạng máy tính hay một giải pháp nhằm thoả mãn những yêu cầu của người sử dụng.

Chính vì vậy mà việc kiểm định xảy ra trong phương tiện kiểm định hay tại phía người sử dụng trong những điều kiện của các phòng thí nghiệm chứ tuyệt nhiên không phải xảy ra trong môi trường vận hành thực tế. Đánh giá ATTT của sản phẩm CNTT phải tính đến việc kiểm định sản phẩm CNTT trong môi trường vận hành thực tế của sản phẩm.

• Các tiêu chí đánh giá an toàn CNTT (Information Technology Security Evaluation Criteria – ITSEC). Đó là những yêu cầu an toàn của sản phẩm CNTT dưới hai phạm trù cụ thể là những yêu cầu chức năng và những yêu cầu đảm bảo. Những yêu cầu chức năng xác định hành vi an toàn mong muốn. Những yêu cầu đảm bảo là cơ sở cho việc đạt được sự tin chắc rằng những độ đo an toàn tuyên bố có hiệu lực và được cài đặt đúng đắn.

• Mức đảm bảo đánh giá (Evaluation Assurance Level – EAL) là một tập hợp các thành phần chức năng hoặc đảm bảo được kết hợp lại để thoả mã một tập hợp con các mục tiêu an toàn xác định. Mức đảm bảo đánh giá thường được gán cho sản phẩm CNTT sau quá trình đánh giá ATTT. Người sử dụng sẽ dựa vào các mức đảm bảo đánh giá này để biết sản phẩm CNTT mà mình đem sử dụng an toàn đến mức độ nào.

• Hồ sơ bảo vệ (Protection Profile – PP) của một chủng loại sản phẩm CNTT là tài liệu hình thức được xác định trong hệ thống tiêu chí đánh giá ATTT phản ánh một tập hợp không phụ thuộc vào cài đặt của những yêu cầu an toàn đối với sản phẩm CNTT đáp ứng những yêu cầu cụ thể của người sử dụng hoặc những tổ hợp hoàn chỉnh của những mục tiêu an toàn và những yêu cầu chức năng và đảm bảo với cơ sở hợp lý được kết hợp.

• Đối tượng đánh giá (Target of Evaluation – TOE) gồm có chính bản thân sản phẩm CNTT và tài liệu hướng dẫn người sử dụng và người quản trị gắn kết với nó phục vụ cho việc đánh giá.

• Đối tượng an toàn (Security Target – ST) là tổ hợp hoàn chỉnh của những mục tiêu an toàn, những yêu cầu chức năng và đảm bảo, những đặc tả vắn tắt và cơ sở hợp lý được sử dụng làm cơ sở để đánh giá đối tượng đã được chỉ ra (ST gắn phải gắn liền với một TOE cụ thể).

5.2.2. Sự cần thiết của các tiêu chí an toàn thông tin

Để hiểu được vấn đề, trước tiên chúng ta phải biết đánh giá ATTT là Đánh giá ATTT hiểu theo nghĩa rộng nhất là quá trình đánh giá mức độ an toàn của thông tin cần được bảo vệ dưới 03 yêu cầu chính là: (i) Tính bí mật; (ii) Tính toàn vẹn và (iii) Tính sẵn sàng hoạt động.

ATTT luôn được gắn với các phương tiện xử lý, lưu giữ và truyền tin. Trước kia các phương tiện như vậy thường đơn giản, thô sơ và không được tự động hoá hoạt động. Chính vì vậy mà đánh giá ATTT thường ít phụ thuộc vào các phương tiện xử lý thông tin mà chủ yếu phụ thuộc vào cơ chế xử lý thông tin.

Ngày nay các phương tiện như vậy chủ yếu là các phương tiện CNTT. Các phương tiện CNTT được phát triển ngày càng nhiều về số lượng, đa dạng và phức tạp về chức năng hoạt động. Những phương tiện như vậy có thể là phần mềm, phần cứng hay mềm cứng kết hợp hoặc những cơ chế bảo vệ kiểm soát hoạt động thông tin nào đó.

Khi người ta sử dụng các phương tiện CNTT trong các hoạt động thông tin của mình thì ngoài việc các phương tiện CNTT cần đảm bảo các chức năng của mình, chúng còn được yêu cầu đảm bảo các chức năng về ATTT đặt ra cho chúng.

Người sử dụng hay người sản xuất ra các phương tiện CNTT chắc chắn cần phải tự đặt ra cho mình là phương tiện hay sản phẩm CNTT mà mình chế tạo hay sử dụng có an toàn thực sự hay không? Nếu sản phẩm không đảm bảo được mức độ ATTT thì khi đem sử dụng sẽ có thể mang lại những tổn thất vô tình hay hữu ý lớn không gì bù đắp nổi cho thông tin lưu hành trong chúng.

Muốn biết sản phẩm CNTT có đảm bảo mức độ ATTT mong muốn hay không thì phải thông qua đánh giá ATTT. Không có đánh giá ATTT thì không có cách nào khác ước lượng chính xác mức độ ATTT của sản phẩm CNTT đem sử dụng.

Chúng ta sẽ thấy tính cấp thiết của đánh giá ATTT vì những thực tế sau đây:

(i) Quá trình toàn cầu hoá kéo theo việc sử dụng CNTT và Internet cũng phát triển trên phạm vi toàn cầu do vậy mà ATTT không chỉ là nhiệm vụ của mỗi quốc gia mà là nhiệm vụ chung;

(ii) Từ khi máy tính ra đời và nhất là từ khi mạng máy tính ra đời và đi vào hoạt động thì chúng phát triển với tốc độ vũ bão kéo theo các sản phẩm CNTT tăng lên gấp bội và phức tạp hoá cao về chức năng làm cho đảm bảo ATTT trở nên khó khăn gấp bội và càng khó khăn hơn cho đánh giá ATTT;

(iii) Trong xã hội CNTT được sử dụng rộng khắp và trong nhiều lĩnh vực hoạt động nên đe doạ ATTT ngày càng tăng về số lượng và mức độ tinh vi các vô tình và hữu ý có thể gây ra những thiệt hại lớn hơn rất nhiều so với trước đây làm cho nhiệm vụ ATTT trở nên quan trọng sống còn hơn bao giờ hết;

(iv) Đã đến lúc người ta không thể chấp nhận sản phẩm CNTT đem ra sử dụng mà không được đảm bảo ATTT ngay từ khâu thiết kế chế tạo như trước đây nữa. ATTT phải được đặt ngay khi thiết kế sản phẩm CNTT và phải được duy trì kiểm soát trong suốt quãng đời hoạt động của sản phẩm cho tới khi chúng không còn được lưu hành sử dụng nữa mới thôi.

Đánh giá ATTT chính vì vậy mà gắn liền với phân tích, thiết kế sản phẩm CNTT và pháp luật ATTT tạo thành một bộ ba tổng thể ATTT nhằm bảo vệ thông tin từ mức độ cao nhất có thể được.

Một dự án thiết lập hệ thống nào đó hoặc một thiết kế hệ thống an toàn nhất định chỉ có thể đi tới thành công khi mà các thành viên tham gia của nó hiểu rõ ràng họ muốn thu được những gì ở kết quả cuối cùng. Chỉ có sự nắm vững mục đích mới cho phép chọn được con đường tốt nhất để đạt được nó. Cho nên trước khi bắt tay vào thiết lập một hệ thống ATTT (hệ AT – HAT) cần phải trả lời rõ ràng câu hỏi: Thế nào là một hệ an toàn? Cần phải có một định nghĩa có tính cấu trúc khái niệm này, để trên cơ sở đó đưa ra các nguyên lý về hoạt động của HAT và tìm được công nghệ thiết lập nó.

Như chúng ta đã thấy ở các chương trước, an toàn là một đặc trưng định tính của HT, không thể đo nó theo các đơn vị nào đó, thậm chí khó có thể so sánh với kết quả duy nhất an toàn của hai hệ khác nhau, mà một hệ BVTT tốt

hơn trong trường hợp này, còn hệ BVTT kia – trong trường hợp khác. Mặt khác, ngày nay CNTT phát triển rất nhanh chóng. Các sản phẩm CNTT rất đa dạng, rất phổ biến, nhiều chủng loại làm tăng khả năng lựa chọn cho các nhà thiết kế, các chuyên gia trong lĩnh vực ATTT. Các sản phẩm khác nhau, các lựa chọn khác nhau và do đó các quan điểm về ATTT cũng rất khác nhau. Tất nhiên, ý kiến nào cũng có quyền tồn tại và phát triển, nhưng để tập trung nỗ lực của tất cả các chuyên gia vào một hướng trong thiết lập HAT thì rất cần phải thống nhất định nghĩa, mục đích để cùng nhau chọn con đường đạt được các mục tiêu đã đề ra.

Để trả lời cho các câu hỏi đó và để đồng thuận và đi tới thống nhất tất cả các quan điểm về vấn đề thiết lập các HAT, người ta đã soạn thảo và tiếp tục đưa ra các chuẩn (standards) về ATTT. Các chuẩn ATTT là các tài liệu quy chế hoá các khái niệm cơ bản và các quan niệm về ATTT ở pham vi quốc gia và quốc tế. Chính các chuẩn này xác định khái niệm "hệ an toàn" nhờ tiêu chuẩn hoá các đòi hỏi và các tiêu chí an toàn. Các tiêu chí an toàn này tạo thành thang đánh giá mức độ an toàn của hệ thống.

Như vậy bây giờ có thể trả lời cho câu hỏi nêu trên như sau: Hệ xử lý TT an toàn - đó là hệ đáp ứng được các tiêu chuẩn về ATTT. Tất nhiên không hẳn là đơn giản như vậy. Đó là đặc trưng tương đối, nó phụ thuộc vào các tiêu chí và các đòi hỏi, theo đó mà an toàn của hệ thống được đánh giá, nhưng ở đây có một điều quan trọng là tính khách quan. Các tiêu chuẩn là khách quan, và nó cho phép so sánh mức độ ATTT của các hệ khác nhau đối với một tiêu chuẩn đã được chấp nhận.

5.2.3. Vai trò của các chuẩn an toàn thông tin

5.2.3.1. Vai trò phối hợp hành động

Vai trò cơ bản của các chuẩn ATTT là tạo lập cơ sở cho sự phối hợp hành động giữa các nhà sản xuất, các khách hàng (nhà tiêu dùng) và các chuyên gia kiểm chuẩn trong quá trình xây dựng các hệ thống CNTT an toàn từ các sản phẩm của CNTT. Mỗi nhóm người này đều có cách xem xét của mình về vấn đề ATTT.

Về phía khách hàng, trước tiên họ quan tâm đến phương pháp cho phép lựa chọn đúng sản phẩm đáp ứng nhu cầu của họ và giải quyết tốt vấn đề mà

họ đặt ra. Để làm điều đó họ cần một thang đánh giá về ATTT. Thứ hai, họ cần phải có một công cụ mà nhờ nó họ có thể phát biểu các yêu cầu của mình đối với nhà sản xuất. Ở đây họ chỉ quan tâm cơ bản đến các đại lượng và tính chất kỹ thuật của sản phẩm cuối cùng (chứ không phải là các phương pháp để đạt được điều đó). Từ góc độ đó thì thang đánh giá an toàn lý tưởng cho họ có thể, ví dụ là:

Mức 1: Hệ thống xử lý TT với độ mật không cao hơn "mật"

Mức 2: Hệ thống xử lý TT với độ mật không cao hơn "tối mật"

…

Còn các yêu cầu thì khách hàng mong muốn phát biểu ở dạng dễ hiểu nhất, ví dụ như: "chúng tôi muốn rằng, khi xử lý các thông tin tối mật thì tất cả phải được bảo vệ an toàn…". Dù đây là một tiếp cận "không cấu trúc" nhưng lại là tự nhiên, vì khách hàng không hiểu rằng, các yêu cầu về ATTT thường mâu thuẫn với các yêu cầu chức năng của một hệ thống (như thuận tiện sử dụng, hiệu suất và thời gian…), và chúng thường hạn chế các nhà sản xuất rất nhiều vì phải từ bỏ lựa chọn các sản phẩm thông dụng nhất (như chương trình ứng dụng chẳng hạn)

Các nhà sản xuất cũng cần phải có các tiêu chuẩn. Đó là phương tiện để so sánh các khả năng của các sản phẩm của họ. Đó cũng là để sau này áp dụng trong quá trình kiểm chuẩn như một cơ chế đánh giá khách quan các sản phẩm đó. Các nhà sản xuất cũng cần tiêu chuẩn ATTT cho chính việc tiêu chuẩn hoá một nhóm nhất định các yêu cầu an toàn với mỗi loại sản phẩm cụ thể để giúp cho các khách hàng dễ tìm được (và hiểu được) các sản phẩm phù hợp với họ. Từ góc độ của nhà sản xuất, thì các yêu cầu về ATTT phải được cụ thể hoá tối đa và phải quy định rõ việc ứng dụng các thiết bị, các cơ chế, các thuật toán…Nhưng đây là điều không phải lúc nào cũng làm được và càng ngày càng khó thực hiện vì sự phát triển nhanh chóng của CNTT và nhu cầu về bảo vệ ATTT ngày càng đa dạng và cấp bách.

Các chuyên gia về đánh giá và kiểm chuẩn coi các chuẩn ATTT là một công cụ cho phép họ có thể định giá mức an toàn được bảo đảm bởi các sản phẩm CNTT; cũng nhờ đó họ có thể cung cấp cho các khách hàng khả năng lựa chọn có cơ sở sản phẩm mà họ mong muốn. Nhà sản xuất khi đã có kết quả đánh giá mức an toàn (loại an toàn) nhận được từ các chuyên gia kiểm

chuẩn một đánh giá khách quan về các khả năng của sản phẩm của họ. Từ góc độ của mình, các chuyên gia kiểm chuẩn ở vào vị trí khá đặc biệt: một mặt, giống như nhà sản xuất, họ cần có các tiêu chí rõ ràng và đơn giản để áp dụng vào các sản phẩm cụ thể (đơn giản hơn cả là ở dạng các câu trả lời No/Yes); mặt khác, họ phải đáp ứng một cách có cơ sở (chu đáo) các câu hỏi của khách hàng rằng sản phẩm này có thoả mãn nhu cầu hay không. Suy cho cùng, chính họ (các chuyên gia kiểm chuẩn) là người chịu trách nhiệm về sự an toàn của một sản phẩm đã nhận được đánh giá (mức ATTT) và đã đi qua được sự kiểm chuẩn.

5.2.3.2. Các yêu cầu, các tiêu chí và phân loại an toàn

Mỗi bộ tiêu chuẩn ATTT (của mỗi nước) thường có cấu trúc cơ bản như sau:

- Bộ tiêu chuẩn gồm nhiều luận điểm lớn.
- Các luận điểm chứa các yêu cầu cơ bản. Các yêu cầu thường gồm:

  + Các yêu cầu về chức năng đối với hoạt động hoặc cơ chế bảo vệ của HT

  + Các yêu cầu về đảm bảo (chất lượng kỹ thuật) an toàn TT. Các yêu cầu về ATTT là cơ sở (định hướng) để đưa ra các tiêu chí cụ thể (về chất lượng, về kỹ thuật).
- Các tiêu chí ATTT tạo thành một thang hoàn chỉnh đánh giá về mức độ bảo đảm ATTT của sản phẩm. Các tiêu chí tạo thành các nhóm cơ bản (xung quanh các yêu cầu nói ở trên) phục vụ cho việc đánh giá phân loại (phân lớp) các sản phẩm về mặt đảm bảo ATTT.

Như vậy việc đánh giá ATTT chính là sự kiểm chuẩn đối với một thiết bị hay một hệ thống cụ thể. Công việc đó được kết thúc bằng gắn cho sản phẩm một loại (lớp, mức) an toàn cụ thể.

Chính các tiêu chí ATTT giữ nhiệm vụ phối hợp các quan điểm khác nhau của người sản xuất, khách hàng và các chuyên gia kiểm chuẩn trong việc thiết kế, xây dựng một hệ thống ATTT. Sự cần thiết của các tiêu chuẩn ATTT đã hình thành từ rất lâu (cùng với sự ra đời và phát triển của các sản phẩm CNTT và máy tính điện tử). Và trong lĩnh vực này đã đạt được sự tiến bộ đáng kể. Một thế hệ mới các tiêu chuẩn ATTT đã ra đời và khẳng định vị trí

của mình vào những năm 90 của thế kỷ trước. Đó là "Tiêu chí an toàn các hệ thống máy tính tin cậy của Bộ quốc phòng Mỹ"; "Các tài liệu hướng dẫn GTK của Nga"; "Các tiêu chuẩn ATTT của châu Âu"; "Các tiêu chuẩn ATTT liên bang của Mỹ"; "Các tiêu chí ATTT của Canada" và "Hệ tiêu chí ATTT chung". Chúng ta sẽ lần lượt làm quen với các tài liệu trên trong phần sau của chương.

5.2.4. Sơ lược lịch sử phát triển

Như chúng ta đã biết giai đoạn này kéo dài từ khi CNTT ra đời cho tới trước khi ra đời hệ thống tiêu chí đánh giá an toàn CNTT đầu tiên vào năm 1983. Trước đây người ta nhầm tưởng rằng an toàn máy tính và an toàn mạng là hai phần của ATTT hiện đại từ khi mạng Internet ra đời vào những năm 60 của thế kỷ trước. Nhưng thực tế an toàn máy tính hay COMPUSEC ra đời từ khi các máy tính ra đời vào năm 1946.

Trong giai đoạn này tuy có nhu cầu về đánh giá ATTT nhưng nhu cầu chỉ nhằm tới các hệ thống CNTT chứ chưa phải là các sản phẩm CNTT. Hơn nữa nhu cầu đánh giá chỉ xuất hiện chủ yếu đối với các chính phủ nhằm vào lĩnh vực quốc phòng và an ninh quốc gia chứ không phải là các hãng hay các tổ chức và cá nhân nhằm vào lĩnh vực thông tin kinh tế xã hội.

Giai đoạn này cũng là giai đoạn manh nha xuất hiện các tài liệu hướng dẫn về an toàn máy tính, tiền thân của hệ thống tiêu chí đánh giá ATTT sau này.

Tháng 01/1973 Bộ quốc phòng Mỹ cho xuất bản Sách hướng dẫn an toàn máy tính – Các kỹ thuật và các quy trình cài đặt, khử hoạt, kiểm định và đánh giá tài nguyên chia sẻ các hệ thống xử lý số liệu động (ADP Computer Security Manual – Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resoure Sharing ADP systems).

Tháng 06/1979 Bộ quốc phòng Mỹ cho xuất bản hai sách hướng dẫn với lần chỉnh lý đầu tiên (ADP Computer Security Manual – Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resoure Sharing ADP systems, with 1st Amendent).

Đây có thể coi là những tài liệu tiền thân của các hệ thống tiêu chí đánh giá ATTT. Chúng dự báo tính cấp thiết và khả năng chín muồi của những hệ thống tiêu chí đánh giá ATTT vạn năng sẽ ra đời trong nay mai không xa.

Hệ thống tiêu chí đánh giá an toàn CNTT đầu tiên của nhân loại ra đời vào tháng 08/1983 bởi Bộ quốc phòng Mỹ với tên tiếng Anh là US Trusted Computer System Evaluation Criteria (TCSEC) hay còn gọi là Sách da cam (Orange Book) gọi theo màu của bìa ngoài cuốn sách này.

Tuy nhiên người ta quen coi Sách da cam ra đời vào tháng 12/1985 tương ứng với tái bản lần thứ hai của nó. Các tiêu chí được xác định trong TCSEC trước tiên quan tâm đến các hệ thống tin cậy xử lý dữ liệu tự động về thương mại hiện hành. Các tiêu chí đề cập các đặc tính an toàn và các biện pháp đảm bảo tối thiểu được yêu cầu gắn kết với mỗi đặc tả trong các đặc tả an toàn khác nhau. Các yêu cầu của đặc tính nhằm tới các hệ thống xử lý TT dựa trên các hệ điều hành mục đích chung. Còn các yêu cầu đặc tính an toàn cũng có thể áp dụng cho các hệ thống với môi trường đặc biệt như là các bộ xử lý hay các máy tính kiểm soát quá trình liên lạc. Riêng các yêu cầu đảm bảo được áp dụng cho tất cả các dạng các môi trường và các hệ thống tính toán.

Hệ thống tiêu chí đánh giá an toàn CNTT của Châu Âu thể hiện rõ nỗ lực của cộng đồng châu Âu ra đời vào tháng 06/1991, phiên bản 1.2 với tên tiếng Anh là Information Technology Security Evaluation Criteria (ITSEC).

Những quốc gia đóng góp chính là:

- Pháp với tài liệu Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'information (SCSSI 1989).
- Anh với 3 tài liệu chính phủ và thương mại: (i) UK Systems Security Confidence Levels (CESG 1989); (ii) DTI Commercial Computer Security Centre Evaluation Manual (DTI 1989-1); (iii) DTI Commercial Computer Security Centre Functionality Manual (DTI 1989-2).
- Đức với tài liệu IT Security Criteria (ZSIEC) (GISA 1989)
- Hà Lan cũng có đóng góp cho ITSEC.

Tiền thân của ITSEC phải kể đến TCSEC. TCSEC đã ảnh hưởng tới tất cả các tài liệu đã nêu trên đây.

ITSEC nhằm đến nhu cầu cần thiết của cả các sản phẩm an toàn thương mại và an toàn chính phủ. ITSEC nhằm đến sự mở rộng của TCSEC với những mức đánh giá chuyển đổi được sang các mức đánh giá của TCSEC.

Hệ thống tiêu chí an toàn CNTT của riêng Canada ra đời vào tháng 01/1993 phiên bản 3.0 với tên tiếng Anh là The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).

CTCPEC đánh giá tính hiệu quả của các dịch vụ an toàn của sản phẩm. Các tiêu chí này được thiết kế cho chính phủ sử dụng mà không nhằm đến định hướng lớn mạnh của các sản phẩm thương mại.

Các tiêu chí liên bang là sự cập nhật của TCSEC ra đời vào tháng 12/1992 với tên tiếng Anh là The Federal Criteria for Information Technology (FC) nhằm trở thành chuẩn an toàn quốc gia của Mỹ bảo vệ sự đầu tư hiện hành trong công nghệ an toàn, cải tiến quá trình đánh giá an toàn đang tồn tại, dự kiến đối với những cần thiết thay đổi của khách hàng và thúc đẩy sự hoà hợp quốc tế trong đánh giá an toàn CNTT. Mặc dù vậy nó vẫn có những lỗi xảy ra. Sau một số lần sửa đổi từ sự xuất bản đầu tiên của FC đã được chấp nhận bởi cộng đồng an toàn.

Trong năm 1992 Uỷ ban kỹ thuật nhà nước (GTK) trực thuộc tổng thống Liên bang Nga đã xuất bản 5 tài liệu hướng dẫn dành cho các vấn đề bảo vệ chống truy cập trái phép tới thông tin. Đây chính là những tài liệu chuẩn an toàn CNTT của Liên bang Nga.

Ngoài châu Âu, Bắc Mỹ ra, chuẩn an toàn CNTT còn phát triển tại Nam Thái Bình Dương (Australia và New Zealand) năm 1994 và Đông á (Nhật Bản năm 1992 và Hàn Quốc năm 1998)

Nhu cầu về một hệ thống tiêu chí thống nhất và tiên tiến đã đến. Quá trình này bắt đầu từ năm 1993 mà vào tháng 05/1995 vẫn đang còn trong giai đoạn phát triển. Tháng 01/1996 phiên bản dự thảo 1.0 được phát hành. Từ đó đến tháng 10/1997 phê bình góp ý công khai và đánh giá thử. Tháng 10/1997 phiên bản dự thảo Beta 2.0 được phát hành. Tháng 05/1998 phiên bản 2.0 được phát hành. Và cho đến tháng 12/1999 thì CC chính thức phát hành với tên gọi là ISO/IEC 15408 với tên đầy đủ tiếng Anh là Information Technology – Security Techniques – Evaluation Criteria for IT Security.

Từ đó đến nay xu hướng thống nhất và hoàn thiện hệ thống tiêu chí đánh giá ATTT là xu hướng tất yếu và nhiều nỗ lực phát triển đã được tập trung rất hiệu quả. Tuy nhiên sự hoàn thiện và đầy đủ vẫn còn là cái đích cần phấn đấu chứ chưa phải là mục tiêu đã hoàn thành.

5.2.5. Giới thiệu các tiêu chí đánh giá

5.2.5.1. Sách Da cam của bộ quốc phòng Mỹ (TCSEC – 1983)

a) Mục đích ban hành

"Các tiêu chí an toàn hệ thống máy tính" (Trusted Computer System Evaluation Criteria), còn có tên gọi nổi tiếng là "sách Da cam" được công bố vào năm 1983 bởi Bộ quốc phòng Mỹ. Mục đích của nó là xác định các yêu cầu an toàn đối với các thiết bị và bảo đảm chương trình (phần mềm) của các hệ thống máy tính; và đưa ra phương pháp và công nghệ tương ứng cho việc phân tích đánh giá mức độ đảm bảo chính sách an toàn trong hệ thống máy tính của Bộ quốc phòng Mỹ.

Trong tài liệu này, lần đầu tiên đưa ra các khái niệm như "chính sách an toàn", "môi trường tính toán tin cậy" (trusted computing base – TCB)… Theo sách Da cam, Hệ máy tính an toàn (HAT) là hệ thống duy trì sự quản lý tiếp cận tới các TT được xử lý trong đó sao cho, chỉ có các khách hàng có uỷ quyền (thông qua xác thực và nhận dạng) hoặc các quá trình thay mặt họ mới có thể có khả năng đọc, ghi, cập nhật và lấy TT ra. Chính trong sách Da cam này, các thuật ngữ và các quan niệm về bảo vệ, tập hợp các yêu cầu về chức năng lần đầu tiên được đưa ra. Chúng là cơ sở để hình thành tất cả các tiêu chuẩn ATTT sau này.

b) Phân loại các yêu cầu và các tiêu chí của sách Da cam

Trong sách Da cam đưa ra 3 loại yêu cầu an toàn lớn: chính sách an toàn, kiểm toán (audit) và tính đảm bảo (assurance). Trong khuôn khổ 3 yêu cầu lớn này hình thành 6 yêu cầu an toàn cơ bản. 4 yêu cầu đầu tiên trực tiếp hướng tới việc đảm bảo ATTT, còn 2 yêu cầu sau nói về chất lượng của chính các thiết bị bảo vệ. Chúng ta xem xét chi tiết hơn các yêu cầu đó.

i) Yêu cầu lớn về CSAT (Security Policy)

CSAT gồm 2 yêu cầu cơ bản.

- Yêu cầu 1: CSAT. Hệ thống phải duy trì chính xác một CSAT nhất định. Khả năng các chủ thể truy nhập tới các đối tượng phải được quyết định trên cơ sở nhận dạng và tập hợp các điều luật quản lý truy nhập. Ở những chỗ cần thiết phải sử dụng chính sách MAC, cho phép kiểm soát có hiệu quả tiếp cận tới các TT nhạy cảm (dạng tối mật, tuyệt mật …).

- Yêu cầu 2: Nhãn (Labels). Các nhãn an toàn phải được gán cho các đối tượng, và phải được sử dụng như các dấu hiệu cho kiểm soát truy nhập. Để thực hiện MAC hệ thống phải đảm bảo khả năng gán cho mỗi đối tượng một nhãn hoặc nhóm các dấu hiệu xác định độ mật của đối tượng và/hoặc chế độ truy nhập tới đối tượng đó.

ii) Yêu cầu lớn về kiểm toán (Audit)

Audit gồm 2 yêu cầu cơ bản.

- Yêu cầu 3: Nhận dạng và xác thực (Indentification and Authentification). Tất cả các chủ thể đều phải có các đặc chỉ riêng (indentification). Việc kiểm soát truy nhập phải được thực hiện trên cơ sở nhận dạng và xác thực các chủ thể và đối tượng truy nhập và các điều luật kiểm soát truy nhập. Các dữ liệu dùng cho xác thực và nhận dạng phải được bảo vệ khỏi các tiếp cận trái phép, các xuyên tạc và huỷ hoại và chúng phải được gắn với tất cả các thành tố tích cực của hệ thống máy tính mà hoạt động của các thành tố này có tính tới hạn từ góc độ an toàn.

- Yêu cầu 4: Đăng ký và kiểm toán (Registration & Audit). Để xác định mức độ trách nhiệm của các khách hàng về hành động của họ trong HT, tất cả các sự kiện diễn ra trong hệ thống mà có ý nghĩa từ góc độ an toàn đều phải được theo dõi và đăng ký vào trong một sổ sách được bảo vệ (gọi là vết kiểm toán). Hệ thống đăng ký phải thực hiện việc phân tích từ luồng các sự kiện chọn tách ra những sự kiện có ảnh hưởng đến an toàn để giảm bớt kích thước sổ ghi (bản ghi kiểm toán). Bản ghi kiểm toán cần phải được bảo vệ chống tiếp cận trái phép, xuyên tạc và huỷ hoại.

iii) Yêu cầu lớn về tính đảm bảo (Assurance)

Tính đảm bảo assurance gồm 2 yêu cầu cơ bản.

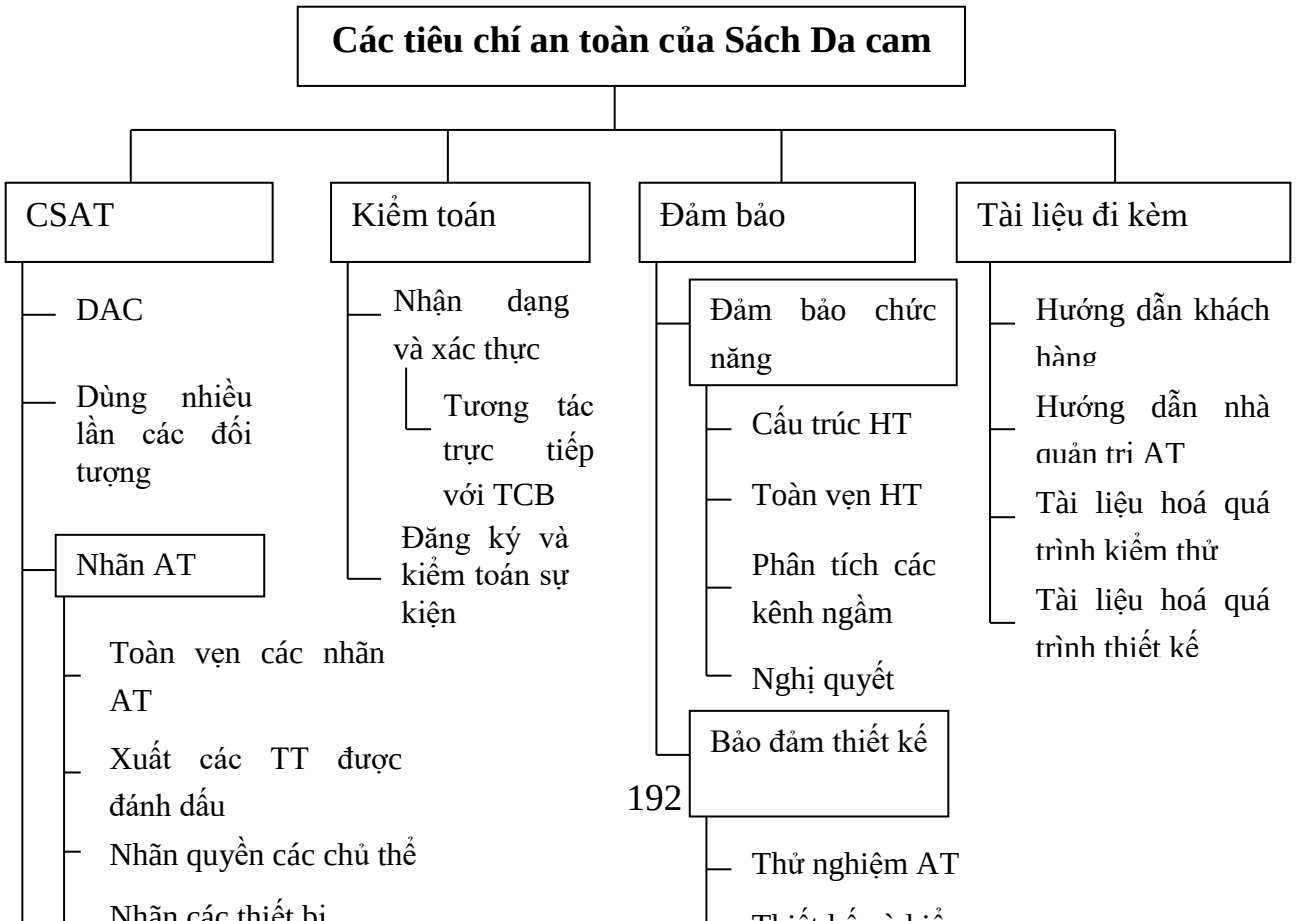
- Yêu cầu 5: Kiểm soát sự đảm bảo cho hoạt động của các thiết bị bảo vệ. Các thiết bị bảo vệ phải chứa các phần cứng hoặc phần mềm độc lập, bảo đảm cho khả năng làm việc của chức năng bảo vệ. Điều này có nghĩa là, tất cả

các thiết bị bảo vệ, bảo đảm CSAT, quản lý nhãn an toàn, nhận dạng và xác thực, đăng ký và kiểm toán đều phải được đặt dưới sự kiểm soát của các thiết bị kiểm tra sự hoạt động chính xác của chúng. Nguyên tắc kiểm soát sự đảm bảo là ở chỗ các thiết bị kiểm soát phải hoàn toàn độc lập với các thiết bị bảo vệ.

- Yêu cầu 6: Bảo vệ liên tục. Tất cả các thiết bị bảo vệ (kể cả các thiết bị thực hiện yêu cầu này) đều phải được bảo vệ chống sự can thiệp bất hợp pháp và hoặc ngắt dừng. Sự bảo vệ này phải là thường xuyên và liên tục trong mọi chế độ hoạt động của hệ bảo vệ và hệ thống máy tính nói chung. Yêu cầu này được áp dụng cho toàn bộ chu kỳ sống của hệ thống. Ngoài ra, việc thực hiện yêu cầu này là một trong những yếu tố then chốt chứng minh cho sự an toàn của hệ thống.

iv) Phân loại các tiêu chí an toàn

Các tiêu chí trong Sách Da cam là sự cụ thể hoá của 6 yêu cầu cơ bản và tổng quát nêu trên. Các tiêu chí làm thành một thang thống nhất đánh giá sự an toàn của hệ thống máy tính. Chúng được chia thành 4 nhóm với độ an toàn khác nhau: từ độ an toàn cực tiểu (nhóm D) đến độ an toàn chứng minh hình thức được (nhóm A). Mỗi nhóm lại được phân chia mịn hơn thành các lớp (7 lớp). Mỗi lớp chứa 4 nhóm tiêu chí như trong hình 5.1:



Hình 5.1 Các tiêu chí an toàn của Sách Da cam

c) Các lớp an toàn của Hệ thống máy tính

Như đã nói ở trên, Sách Da cam đưa ra 4 nhóm tiêu chí tương ứng với các mức độ an toàn từ thấp nhất (D) đến cao nhất (A). Mỗi nhóm (A, B, C, D) bao gồm một hoặc vài lớp. Các nhóm D và A chứa mỗi nhóm chứa một lớp (lớp D và lớp A tương ứng); nhóm C có 2 lớp (lớp C1 và lớp C2), còn nhóm B có 3 lớp (B1, B2, B3) đặc trưng bởi tập hợp các tiêu chí an toàn khác nhau. Độ an toàn tăng dần theo chiều từ nhóm D đến nhóm A, còng trong mỗi nhóm – tăng theo số thứ tự của các lớp.

Nhóm D: Bảo vệ cực tiểu.

- Lớp D: Bảo vệ cực tiểu. Tất cả các hệ thống không đáp ứng được các yêu cầu của các lớp khác đều thuộc lớp này. Có thể nói, các hệ thống thuộc lớp D là không an toàn.

Nhóm C: Bảo vệ tuỳ chọn (Discretionary Security – DS).

Đặc trưng của nhóm C là cơ chế DAC và đăng ký hành động của các chủ thể.

- Lớp C1: Bảo vệ tuỳ chọn. Các hệ thống thuộc lớp C1 thỏa mãn yêu cầu bảo đảm phân tách các khách hàng và thông tin và bao gồm cả các thiết bị kiểm soát truy nhập, cho phép đặt ra các hạn chế với mỗi khách hàng riêng biệt; điều này cung cấp cho họ khả năng bảo vệ các TT riêng của mình khỏi các khách hàng khác. Lớp C1 gồm các hệ thống đa khách hàng, trong đó thực hiện việc cùng xử lý các TT (dữ liệu) cung một độ mật.

- Lớp C2: Kiểm soát truy nhập. Các hệ thống thuộc lớp này thực hiện kiểm soát truy nhập có lựa chọn hơn lớp C1, nhờ áp dụng các thiết bị giám

sát cá nhân đối với hành động của các khách hàng bằng đăng ký, kiểm toán sự kiện và phân chia các tài nguyên.

Nhóm B: Bảo vệ bắt buộc (Mandatory Security – MS).

Các đòi hỏi chính của nhóm này là điều khiển truy nhập chuẩn nhờ sử dụng các nhãn AT, duy trì mô hình và CSAT, và cả tồn tại các đặc tả về chức năngTCB. Đối với các hệ thống thuộc nhóm B monitor reference (ghi nhận tham chiếu) phải kiểm soát tất cả các sự kiện trong hệ thống.

- Lớp B1: Bảo vệ với áp dụng các nhãn AT. Các hệ thống của lớp này phải thỏa mãn tất cả các yêu cầu của lớp C2, và ngoài ra chúng phải duy trì một cách phi hình thức một mô hình AT, mã hoá dữ liệu và MAC. Khi xuất TT khỏi hệ thống thì TT phải được mã hoá. Các lỗi được phát hiện trong quá trình kiểm thử phải được loại trừ.

- Lớp B2: Bảo vệ cấu trúc. Để tương ứng với lớp B2 TCB của hệ thống phải duy trì một mô hình AT được thuyết minh bằng tài liệu rõ ràng và được xác định hình thức hoá. Mô hình này phải dùng được cả hai cơ chế DAC và MAC; và các cơ chế kiểm soát truy nhập phải được áp dụng cho tất cả các chủ thể (so với các hệ thống của lớp B1). Ngoài ra, phải thực hiện sự kiểm soát các kênh ngầm rò rỉ TT. Trong cấu trúc TCB phải tách riêng được các yếu tố tới hạn từ góc độ an toàn. Giao diện TCB phải được xác định rõ ràng, còn cấu trúc của TCB và sự thực hiện nó phải tính tới khả năng tiến hành các thử nghiệm kiểm tra (kiểm thử). So với lớp B1, cần phải tăng cường các thiết bị xác thực. Quản lý an toàn phải do các nhà quản trị hệ thống thực hiện. Cần phải có các thiết bị kiểm soát cấu hình.

- Lớp B3: Các miền an toàn (Secure Domains – SD). Để tương ứng lớp B3, TCB của hệ thống phải duy trì Reference Monitor kiểm soát tất cả các loại truy nhập của các chủ thể tới các đối tượng. Ngoài ra, TCB phải được thiết kế với mục đích đưa ra khỏi nó các tiểu hệ không chịu trách nhiệm thực hiện các chức năng bảo vệ và phải đủ chặt chẽ để kiểm thử và phân tích có hiệu quả. Trong quá trình thiết kế và thực hiện TCB cần áp dụng các phương pháp và các thiết bị sao cho cực tiểu hoá sự phức tạp của nó. Các thiết bị kiểm toán (Audit) phải bao gồm các cơ chế thông báo của nhà quản trị khi xuất hiện các sự kiện về an toàn của hệ thống. Yêu cầu phải có các thiết bị khôi phục khả năng làm việc của hệ thống.

Nhóm A: Bảo vệ có kiểm chuẩn.

Đây là nhóm đặc trưng bởi việc áp dụng các phương pháp hình thức của kiểm chuẩn tính đảm bảo làm việc của các cơ chế kiểm soát truy nhập (DAC và MAC). Đòi hỏi thêm các tài liệu chứng minh rằng, cấu trúc và sự thực hiện của TCB đáp ứng các yêu cầu an toàn.

- Lớp A1: Kiểm chuẩn hình thức. Các hệ thống thuộc lớp A1 tương đương với các hệ thống lớp B3 về mặt chức năng, và với chúng không có yêu cầu chức năng nào thêm. Khác với các hệ thống lớp B3 là ở chỗ, trong quá trình thiết kế cần phải áp dụng các phương pháp kiểm chuẩn hình thức, nó cho phép thu được sự thực hiện đúng đắn các chức năng bảo vệ (với độ tin cậy cao). Quá trình chứng minh sự phù hợp của việc thực hiện được bắt đầu ngay từ thời kỳ đầu tiên của thiết kế với việc thiết lập mô hình an toàn và các đặc tả mức cao. Để bảo đảm các phương pháp kiểm chuẩn, các hệ thống lớp A1 cần phải có các thiết bị mạnh về quản lý cấu hình và các thủ tục bảo vệ phân tán.

d) Các thuyết minh và sự phát triển cúa Sách Da cam

Việc công bố Sách Da cam đã trở thành một giai đoạn quan trọng và giữ một vai trò đáng kể trong sự phát triển các công nghệ bảo đảm an toàn của các hệ thống máy tính. Tuy nhiên, trong quá trình áp dụng các luận điểm của nó đã thấy rằng, có một số vấn đề thực tế quan trọng không được đề cập tới trong bộ chuẩn này, và ngoài ra với sự phát triển có nhiều luận điểm của nó đã trở thành lỗi thời đòi hỏi phải xem xét lại. Một loạt các vấn đề về an toàn mạng máy tính và CSDL đã được đề cập trong các tài liệu riêng do Trung tâm an toàn máy tính quốc gia (NCSC) của Mỹ công bố như là các bổ sung cho sách Da cam dưới dạng các thuyết minh (Interpretations): Thuyết minh cho các mạng tin cậy (Trusted Network Interpretation); Thuyết minh cho các Hệ quản trị CSDL tin cậy (Trusted Database Management System Interpretation). Các tài liệu này chứa đựng sự minh hoạ các luận điểm cơ bản của Sách Da cam áp dụng vào các hệ thống xử lý TT tương ứng.

Sự lạc hậu của loạt các luận điểm trong Sách Da cam trước tiên là do sự phát triển nhanh chóng của CNTT, việc chuyển từ các máy tính lớn (mainframe) sang các máy trạm làm việc và các PC có hiệu suất cao trong mô hình tính toán trên mạng. Để cho các luận điểm cơ bản của Sách Da cam thích ứng với nhu cầu hiện tại, người ta đã tiến hành khối lượng lớn các công việc

về thuyết minh và phát triển các luận điểm của bộ chuẩn này. Kết quả là đã ra đời một loạt các tài liệu đi kèm Sách Da cam, rất nhiều trong số đó đã trở thành phần không thể tách rời của nó. Đó là:

- Chỉ dẫn về DAC trong các hệ thống tin cậy (A guide to understanding discretionary access control in trusted systems)
- Chỉ dẫn về quản lý mật khẩu (Password management guide-line)
- Chỉ dẫn về áp dụng các tiêu chí an toàn hệ thống máy tính trong các môi trương đặc biệt (Guidance for applying the Department of Defence Trusted Computer System Evaluation Criteria in specific environment)
- Chỉ dẫn về kiểm toán trong các hệ an toàn (A guide to understanding Audit in trusted systems)
- Chỉ dẫn về quản lý cấu hình trong các hệ an toàn (A guide to understanding configuration management in trusted systems)

Số lượng các tài liệu như vậy cùng với các bình luận, các thuyến minh ngày càng tăng và đã lớn hơn cả bản thân Sách Da cam rất nhiều. Cho nên đến năm 1995 NCSC của Mỹ đã tập hợp tất cả các bổ sung, thuyến minh lại và cho công bố thành một tài liệu có tên là " Thuyết minh các tiêu chí an toàn hệ thống máy tính " (The Interpreted Trusted Computer System Evaluation Criteria Requirements). Tài liệu này đã ghi nhận tất cả các bổ sung, thay đổi đối với Sách Da cam, và thực sự đổi mới nó, đã cho phép nó được áp dụng trong các điều kiện hiện tại.

Trong bảng dưới đây sẽ thể hiện sự phân bố các yêu cầu an toàn của Sách Da cam theo các lớp như đã nói ở trên. Lưu ý rằng, các tiêu chí an toàn chính là các yêu cầu tạo thành (có thể một yêu cầu tương ứng với một tiêu chí, cũng có thể vài yêu cầu cho ta một tiêu chí)

Khi xem bảng phân bố này cần lưu ý các ký hiệu với chú giải sau:

" – " – Không có yêu cầu với lớp này

" + " – Yêu cầu mới hoặc yêu cầu bổ sung

" = " – Yêu cầu trùng với yêu cầu lớp trước đó

Đây là cách trình bày thường gặp trong các Tiêu chuẩn ATTT.

Bảng 5.1 Sự phân bố các yêu cầu an toàn của Sách Da cam theo các lớp

Các yêu cầu cơ bản của Sách Da cam	Các lớp an toàn					
	C1	C2	B1	B2	B3	A1
Chính sánh an toàn						
1. CSAT tuỳ chọn (D)	+	+	+	=	=	=
2. CSAT bắt buộc (M)	–	–	+	+	=	=
3. Các nhãn bí mật	–	–	+	+	=	=
4. Toàn vẹn các nhãn	–	–	+	=	=	=
5. Nhãn công tác	–	–	–	+	=	=
6. Dùng lại nhãn	–	–	+	=	=	=
7. Giải phóng tài nguyên khi dùng lại các đối tượng	–	+	=	+	=	=
8. Cách ly các Môđun	–	+	=	=	=	=
9. Đánh dấu các thiết bị vào/ra	–	–	+	=	=	=
10.Đánh dấu sự đọc ra	–	–	+	=	=	=
Kiểm toán (Audit)						
11. Nhận dạng và xác thực	+	+	=	=	=	=
12. Audit	–	+	+	+	+	=
13. Tuyết tin cậy (Trusted path)	–	–	–	+	=	=
Đảm bảo (Assurance)						
14. Đặc tả và kiểm chuẩn thiết kế	–	–	+	+	+	+
15. Cấu trúc hệ thống (nhiều tầng)	+	=	=	+	+	=

16. Toàn vẹn hệ thống	+	=	=	=	=	=
17. Kiểm thử hệ thống an toàn	+	+	+	+	+	=
18. Sự phục hồi tin cậy sau sự cố	–	–	–	–	+	=
19. Quản lý cấu hình hệ thống	–	–	–	+	+	+
20. Thông báo trước về hệ thống	–	–	–	+	+	=
21. Lan truyền tin cậy	–	–	–	–	+	=
22. Phân tích các kênh nguồn	–	–	–	+	+	+
Tài liệu hoá						
23.Chỉ dẫn khách hàng	+	=	=	=	=	=
24. Chỉ dẫn về cấu hình bảo vệ	+	+	+	+	+	=
25. Tài liệu về kiểm thử	+	=	=	=	=	+
26. Tài liệu thiết kế	+	=	+	+	=	+

5.2.5.2. Tiêu chí an toàn công nghệ thông tin châu Âu

Các vấn đề về ATTT đặt ra cấp thiết không chỉ với nước Mỹ. Ngay sau khi ra đời Sách Da cam của Bộ quốc phòng Mỹ, các nước châu Âu cũng đã soạn thảo và cho ra đời "Các tiêu chí đánh giá an toàn CNTT" (Information Technology Security Evaluation Criteria), sau đây sẽ gọi là "Các tiêu chí châu Âu". Ở đây chúng tôi tóm lược tài liệu này dựa trên phiên bản 1.2 được công bố tháng 6/1991 bởi các cơ quan có thẩm quyền của 4 nước: Pháp, Đức, Hà Lan và Anh quốc.

a) Các khái niệm cơ bản

Các tiêu chí châu Âu xem xét các nhiệm vụ cơ bản của các thiết bị ATTT như sau:

- Bảo vệ TT chống các truy nhập trái phép nhằm bảo đảm tính bí mật.

• Bảo đảm toàn vẹn TT bằng cách bảo vệ chống lại sự bóp méo hoặc huỷ hoại bất hợp pháp.

• Bảo đảm khả năng làm việc của hệ thống bằng việc chống lại các hiểm họa khước từ dịch vụ.

Để thoả mãn các yêu cầu về bí mật, toàn vẹn và sẵn sàng dịch vụ, cần phải thực hiện một tập hợp tương ứng các chức năng an toàn: như nhận dạng và xác thực, kiểm soát truy nhập, khôi phục sau sự cố… Để cho các thiết bị bảo vệ có thể được coi là có hiệu quả, đòi hỏi phải có một mức độ nhất định tin cậy trong sự chọn lựa đúng các thiết bị và trong hoạt động chính xác của chúng. Để giải quyết vấn đề này, trong các tiêu chí châu Âu lần đầu tiên đưa ra khái niệm về tính đảm bảo (tính phù hợp) của các thiết bị bảo vệ (assurance).

Yêu cầu đảm bảo bao gồm hai khía cạnh: Tính hiệu quả phản ánh sự tương ứng của các thiết bị bảo vệ với các nhiệm vụ đặt ra, và tính chính xác đặc trưng cho quá trình thiết kế và hoạt động (thực tế) của chúng. Tính hiệu quả xác định bởi sự tương ứng giữa các nhiệm vụ đặt ra trước các thiết bị an toàn và tập hợp thực hiện các chức năng bảo vệ – tính đầy đủ và đồng bộ, đơn giản sử dụng, có tính tới các hậu quả tiềm năng nếu kẻ xấu lợi dụng các điểm xung yếu của bảo vệ. Tính chính xác ở đây được hiểu là sự đúng đắn và tin cậy trong hiện thực hoá các chức năng an toàn.

Đánh giá chung về mức độ an toàn của hệ thống được gộp lại từ khả năng về chức năng hoạt động của các thiết bị bảo vệ và mức độ đảm bảo của sự hiện thực hoá các chức năng đó.

b) Các tiêu chí chức năng

Trong các tiêu chí châu Âu, các thiết bị ATTT được xem xét ở trên 3 mức chi tiết. Ở mức đầu tiên, xem xét các mục tiêu mà sự an toàn đặt ra; mức thứ hai chứa các đặc tả chức năng bảo vệ; mức thứ ba – các cơ chế thực hiện chúng.

Các đặc tả chức năng bảo vệ được xem xét từ góc độ các yêu cầu sau đây:

• Nhận dạng và xác thực

• Kiểm soát truy nhập

- Kiểm toán
- Dùng lại các đối tượng
- Toàn vẹn thông tin
- Tin cậy dịch vụ
- An toàn trao đổi các dữ liệu

Đa số các yêu cầu nêu trên trùng với các yêu cầu tương tự của "Sách Da cam". Chúng ta xem xét một số nét đặc trưng cho "Các tiêu chí châu Âu".

Các yêu cầu về an toàn trao đổi dữ liệu, quy định công tác của các thiết bị bảo đảm an toàn các dữ liệu được truyền theo các kênh liên lạc, bao gồm các yêu cầu như sau:

- Xác thực
- Kiểm soát truy nhập
- Bí mật dữ liệu
- Toàn ven dữ liệu
- Chống chối bỏ

Tập hợp các chức năng an toàn có thể phân loại nhờ sử dụng các lớp đã xác định trong Sách Da cam (có thể chuyển đổi được). Có 5 lớp như vậy, đó là các lớp F - C1, F - C2, F – B1, F – B2, F – B3. Còn 5 lớp không chuyển đổi về Sách Da cam được.. Chúng ta xem xét 5 lớp này kỹ hơn vì chúng phản ánh quan điểm riêng của "Châu Âu" về vấn đề ATTT:

- Lớp F- IN dùng cho các hệ thống có nhu cầu cao về bảo đảm tính toàn vẹn (INtergrity) mà điển hình là các hệ quản trị CSDL. Có thể miêu tả nó trên cơ sở khái niệm "các vai trò", tương ứng với các hoạt động của khách hàng, và trên cơ sở cho phép một truy nhập tới các đối tượng xác định chỉ thông qua các trình uỷ quyền. Cần phải phân biệt các dạng truy nhập sau đây: đọc, ghi, xoá, tạo lập, đổi tên và thực thi (read, write, add, delete, creat, rename, execute)

- Lớp F – AV. Đặc trưng bởi các yêu cầu tăng cường về bảo đảm khả năng làm việc (tăng tính khả dụng – AVailable). Điều này quan trọng cho các hệ thống kiểm soát các quá trình công nghệ. Trong các yêu cầu của lớp này chỉ ra rằng. hệ thống cần phải được khôi phục sau mỗi ngừng trệ của một thành phần riêng biệt nào đó, sao cho tất cả các chức năng tới hạn quan trọng

đều vẫn được liên tục sẵn sàng cho các truy nhập. Sự thay thế các bộ phận, chi tiết cũng phải được duy trì trong chế độ như vậy. Không phụ thuộc vào tải trọng ra sao, cần phải bảo đảm một thời gian nhất định cho phản ứng của hệ thống trước các sự kiện bên ngoài.

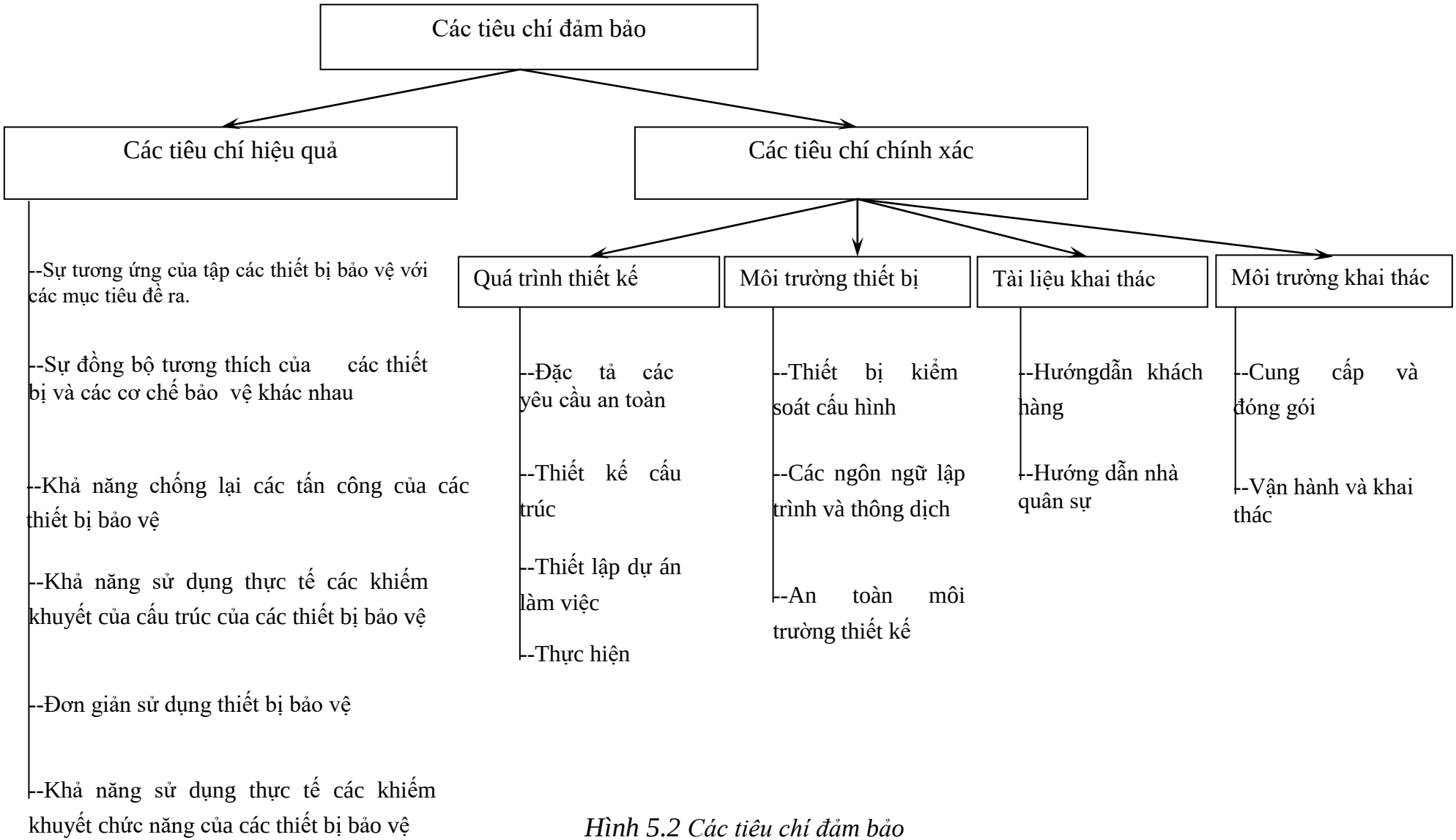
• Lớp F – DI hướng tới các hệ thống phân tán (DIstribution). Trước khi bắt đầu trao đổi và trong khi thu nhận các dữ liệu, các bên cần phải có khả năng tiến hành nhận dạng các thành viên tham gia tương tác và xác thực chúng. Cần phải sử dụng các thiết bị kiểm soát lỗi và sửa sai. Đặc biệt trong việc truyền dữ liệu, cần phải phát hiện được tất cả các sai lệch ngẫu nhiên hoặc cố ý của TT địa chỉ và TT khách hàng. Cần phát hiện các ý đồ phát lại các bản tin đã được truyền.

• Lớp F – DC dành quan tâm đặc biệt cho các yêu cầu về tính bí mật của TT được truyền nhận. TT theo các kênh liên lạc phải được truyền đi ở dạng mã hoá. Các khoá mã phải được bảo vệ chống các tiếp cận trái phép.

• Lớp F – DX áp đặt các yêu cầu tăng cường tới cả tính toàn vẹn và tính bí mật của TT. Có thể coi F – DX là tích hợp của các lớp F – DI và F – DC với các khả năng tăng cường thêm về mã hoá và bảo vệ chống phân tích lưu lượng. Cần phải giới hạn tiếp cận tới TT đã được truyền trước đó vì TT này về nguyên tắc có thể hậu thuẫn cho mã thám (phân tích mã)

c) Các tiêu chí bảo đảm (Assurance)

Các tiêu chí châu Âu dành cho tính bảo đảm sự quan tâm lớn hơn các yêu cầu chức năng. Mức đảm bảo có 2 thành phần – tính hiệu quả và tính chính xác làm việc của các thiết bị bảo vệ. Để đánh giá mức độ đảm bảo người ta sử dụng các tiêu chí sau đây:



Hình 5.2 Các tiêu chí đảm bảo

Các tiêu chí châu Âu xác định 7 mức đảm bảo – từ E0 đến E6 (theo thứ tự tăng dần). Mức E0 đánh dấu mức bảo đảm thấp nhất (tương tự lớp D của Sách Da cam). Trong kiểm tra tính đảm bảo người ta phân tích toàn bộ chu kỳ sống của hệ thống – từ pha đầu tiên của thiết kế cho đến khai thác và bảo dưỡng. Các mức đảm bảo từ E1 đến E6 được xây dựng theo thứ tự tăng dần sự cẩn trọng trong kiểm soát . Chẳng hạn, ở mức E1 chỉ phân tích cấu trúc chung của HT, còn tính đảm bảo của các thiết bị bảo vệ (TBBV) được khẳng định bằng kiểm thử chức năng. Ở mức E3, việc phân tích tiến hành với các bản nguồn của các chương trình và sơ đồ cài đặt thiết bị. Ở mức E6 đòi hỏi miêu tả hình thức các chức năng an toàn, cấu trúc chung và cả chính sách an toàn.

Độ an toàn của hệ thống được xác định bởi cơ chế yếu nhất trong các cơ chế bảo vệ tới hạn quan trọng. Trong các tiêu chí châu Âu có 3 mức an toàn: Cơ sở, trung bình và cao.

Mức an toàn cơ sở nếu các TBBV có khả năng chống lại các tấn công ngẫu nhiên riêng biệt.

Mức an toàn là trung bình nếu các TBBV có khả năng chống lại kẻ xấu, có trong tay lượng tài nguyên hạn chế và khả năng chuyên môn hạn chế.

Cuối cùng, mức an toàn có thể coi là cao, nếu có sự chắc chắn rằng, các TBBV chỉ có thể bị vô hiệu hoá bởi kẻ xấu có trình độ chuyên môn cao và có một tập hợp các khả năng về tài nguyên vô biên (không giới hạn).

d) Kết luận

" Các tiêu chí an toàn CNTT châu Âu", xuất hiện ngay sau Sách Da cam đã có ảnh hưởng đáng kể tới các tiêu chuẩn ATTT và phương pháp luận kiểm chuẩn.

Thành tựu chính của tài liệu này là đưa ra khái niệm đảm bảo (assurance) của các TBBV và xác định được một thang đánh giá riêng cho các tiêu chí đảm bảo. Như đã nói, Các tiêu chí châu Âu coi tính đảm bảo của các TBBV có ý nghĩa lớn hơn là các chức năng của chúng. Lối tiếp cận này được sử dụng trong nhiều bộ Tiêu chuẩn ATTT xuất hiện sau đó.

Cần lưu ý rằng, Các tiêu chí châu Âu gắn liền với Sách Da cam của Mỹ, điều đó làm cho nó không hoàn toàn là một tài liệu độc lập.

Thoạt nhìn, cảm thấy ngạc nhiên rằng, Các tiêu chí châu Âu thừa nhận khả năng tồn tại các khiếm khuyết trong các hệ thống đã qua kiểm chuẩn (các tiêu chí về khả năng sử dụng các khiếm khuyết của bảo vệ). Tuy nhiên thực ra điều đó chỉ thể hiện một quan điểm thực dụng trong cách nhìn hiện trạng và thừa nhận điều rõ ràng là: các hệ thống đang tồn tại còn rất chưa hoàn thiện, còn xa mới tới được mức hoàn hảo.

5.2.5.3. Hệ tiêu chí an toàn của Liên Bang Nga

a) Các luận điểm cơ bản

Năm 1992, Uỷ ban kỹ thuật nhà nước (GTK) trực thuộc tổng thống Liên Bang Nga đã công bố năm (5) tài liệu về các vấn đề bảo vệ TT chống lại các tiếp cận trái phép (TCTP). Quan trọng nhất là các tài liệu sau đây:

- Phương hướng bảo vệ các thiết bị tính toán (CBT) chống các TCTP tới TT.
- CBT bảo vệ chống TCTP. và các chỉ số bảo vệ chống TCTP tới TT.
- Các hệ thống tự động hoá (AC) bảo vệ chống các TCTP và Phân loại các AC và các yêu cầu về bảo vệ TT.

Tư tưởng chỉ đạo cho các tài liệu nằm ở tài liệu chính là "Phương hướng bảo vệ CBT chống các TCTP tới TT". Ở đây chứa đựng các quan điểm của GTK về vấn đề ATTT và các nguyên lý cơ bản bảo vệ các hệ thống máy tính. Theo các quan điểm này thì: nhiệm vụ cơ bản của các thiết bị an toàn là bảo vệ chống lại các TCTP tới TT. Nếu như các thiết bị kiểm soát toàn vẹn còn được nói đến ít nhiều, thì việc duy trì sự sẵn sàng phục vụ của hệ thống xử lý TT nói chung không được nói tới. Sự thiên lệch về phía bảo đảm tính bí mật được giải thích là vì các tài liệu này được soạn thảo với mục đích áp dụng cho các hệ thống thông tin của Bộ quốc phòng và các lực lượng an ninh Liên Bang Nga (hay còn gọi là các cơ cấu sức mạnh).

b) Phân loại các tiêu chí và các yêu cầu an toàn

Các tài liệu chỉ dẫn GTK đưa ra 2 nhóm tiêu chí an toàn: các chỉ số bảo vệ của các thiết bị tính toán chống các TCTP và các tiêu chí bảo vệ của các hệ thống tự động hoá xử lý dữ liệu. Nhóm đầu tiên cho phép đánh giá mức độ bảo vệ của các thành tố riêng rẽ của hệ thống tính toán, còn nhóm thứ hai dành cho các hệ thống đầy đủ xử lý các dữ liệu.

* Chỉ số bảo vệ của CBT chống các TCTP. Tài liệu GTK xác định phân loại CBT theo mức độ bảo vệ TT (chống các TCTP) trên cơ sở liệt kê các chỉ số bảo vệ và tập hợp các yêu cầu miêu tả chúng. ở đây CBT được hiểu là tập hợp các phần mềm (chương trình) và các yếu tố kỹ thuật của các hệ thống xử lý dữ liệu, có khả năng hoạt động độc lập hoặc hoạt động trong thành phần của các hệ thống khác.

Chỉ số này chứa các yêu cầu bảo vệ CBT chống các TCTP tới TT và được áp dụng cho các chương trình hệ thống chung và các hệ điều hành (tính tới cấu trúc của MTĐT). Các liệt kê cụ thể của các chỉ số xác định các lớp bảo vệ CBT và được mô tả bằng một tập hợp các yêu cầu. Tập hợp tất cả các TBBV tạo thành tổ hợp các TBBV (KCZ). Các tài liệu GTK xác định 7 lớp bảo vệ CBT chống TCTP, thấp nhất là lớp 7 cao nhất là lớp 1.

Các chỉ số bảo vệ và các yêu cầu tới các lớp được dẫn ra trong bảng dưới đây.

Các ký hiệu có ý nghĩa như sau:

"–" Không có yêu cầu tới lớp này.

"+" Các yêu cầu mới hoặc bổ sung vào.

"=" Các yêu cầu trùng với yêu cầu của lớp trước đó

"KCZ" Tổ hợp các thiết bị bảo vệ

(Xem kỹ bảng này và hãy so sánh với sự phân loại tương tự của Sách Da cam của Bộ quốc phòng Mỹ ở phần trên)

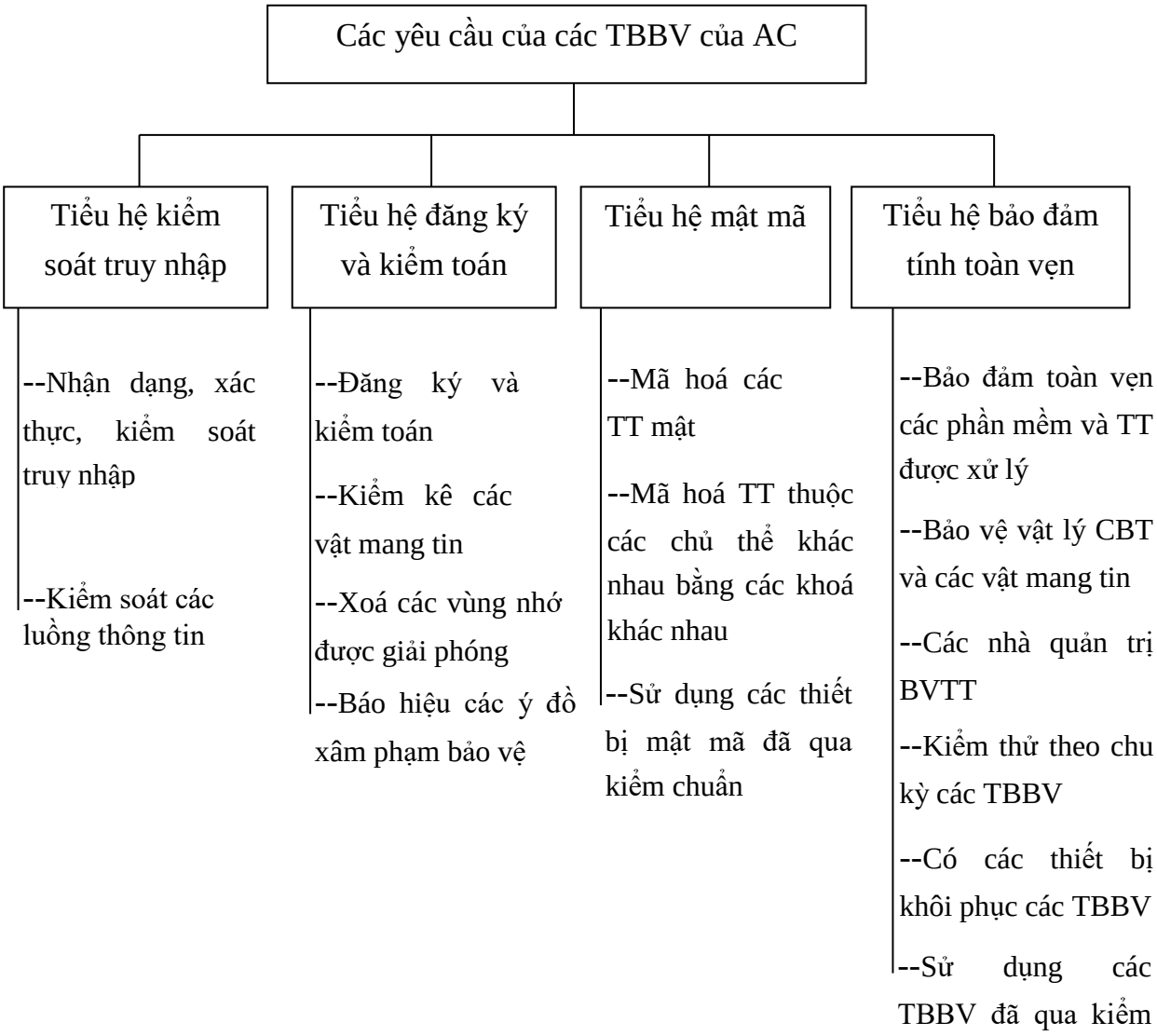
Bảng 5.2 Các chỉ số bảo vệ và các yêu cầu tới các lớp

Tên gọi các chỉ số	Các lớp bảo vệ					
	6	5	4	3	2	1
Kiểm soát truy nhập tuỳ chọn (DAC)	+	+	+	=	+	=
Kiểm soát truy nhập bắt buộc (MAC)	–	–	+	=	=	=
Xoá sạch bộ nhớ	–	+	+	+	=	=
Cách ly các mô đun	–	–	+	=	+	=
Nguỵ trang (mã hoá) các tài liệu	–	–	+	=	=	=

Bảo vệ vào/ra tránh các vật mang TT lạ	−	−	+	=	=	=
Gắn khách hàng với thiết bị	−	−	+	=	=	=
Nhận dạng và xác thực	+	=	+	=	=	=
Bảo hiểm thiết kế	−	+	+	+	+	+
Đăng ký	−	+	+	+	=	=
Tương tác khách hàng với KCZ	−	−	−	+	=	=
Khôi phục tin cậy	−	−	−	+	=	=
Toàn vẹn KCZ	−	+	+	+	=	=
Kiểm soát sự thay đổi	−	−	−	−	+	=
Kiểm soát sự phân tán	−	−	−	−	+	=
Bảo hiểm cấu trúc	−	−	−	−	−	+
Kiểm thử	+	+	+	+	+	=
Chỉ dẫn khách hàng	+	=	=	=	=	=
Chỉ dẫn về KCZ	+	+	=	+	+	=
Tài liệu bằng văn bản	+	+	+	+	+	=
Tài liệu thiết kế	+	+	+	+	+	+

* Các yêu cầu bảo vệ của các hệ thống tự động hoá

Các yêu cầu này là một thành phần của các tiêu chí bảo vệ của các hệ thống tự động hoá xử lý dữ liệu. Các yêu cầu tạo thành các nhóm xung quanh các tiểu hệ thực hiện chúng. Không có những yêu cầu về tính sẵn sàng phục vụ của HT, nhưng lại có các mục dành cho các thiết bị mật mã. Trong nhiều bộ tiêu chuẩn ATTT không hề nói tới mật mã, vì ở đó người ta xem nó chỉ như một cơ chế bảo vệ thực hiện các yêu cầu về xác thực, kiểm toán toàn vẹn…Loại trừ chỉ có "Các tiêu chí chung" (Common Criteria – CC), tuy nhiên trong đó yêu cầu của mục mật mã chỉ nói về quản lý khoá mà thôi. Phân loại các yêu cầu về các TBBV của AC dẫn ra trong bảng sau:



Hình 5.3 Các yêu cầu của các TBBV của AC

c) Các lớp bảo vệ của các hệ thống tự động hoá (AC)

Các tài liệu GTK xác định 9 lớp bảo vệ của AC chống các TCTP, mỗi lớp được đặc trưng bởi một tập các yêu cầu đối với các TBBV. Các lớp chia thành 3 nhóm, phân biệt bởi đặc tính xử lý TT trong AC. Các nhóm của AC được xác định trên cơ sở các dấu hiệu sau:

- Tồn tại trong AC các TT với các độ mật khác nhau.
- Mức quyền của các khách hàng AC truy nhập tới các TT mật.
- Chế độ xử lý TT trong AC (tập thể hay cá nhân).

Trong mỗi nhóm có một trật tự các lớp bảo vệ AC. Lớp có độ bảo vệ cao nhất trong một nhóm được ký hiệu là NA, ở đây N – số thứ tự của nhóm (từ 1 đến 3). Lớp tiếp theo là NB...

Nhóm thứ ba bao gồm các AC, trong đó chỉ có một khách hàng làm việc được tiếp cận tất cả các TT chứa trong các vật mang cùng một cường độ mật. Nhóm này có 2 lớp – 3B và 3A.

Nhóm thứ hai bao gồm các AC, trong đó các khách hàng có cùng các quyền truy nhập tới tất cả các TT được xử lý và/hoặc lưu giữ trong AC trên các vật mang có độ mật khác nhau. Nhóm này có 2 lớp - 2B và 2A.

Nhóm thứ nhất bao gồm các AC nhiều người dùng, trong đó đồng thời cùng xử lý và/hoặc lưu giữ TT có độ mật khác nhau. Không phải tất cả các khách hàng đều có quyền tiếp cận như nhau. Nhóm này có 5 lớp – 1E, 1D, 1C, 1B và 1A.

d) Kết luận

Việc soạn thảo các tài liệu GTK là kết quả của sự phát triển mạnh mẽ quá trình áp dụng CNTT tại nước Nga. Trước những năm 90 (TK 20) sự cần thiết của các tài liệu như vậy chưa xuất hiện. Vì rằng, đa số các trường hợp xử lý và lưu trữ TT mật được thực hiện không có áp dụng máy tính. Cho nên các tài liệu GTK là giai đoạn đầu của việc hình thành các tiêu chuẩn ATTT của nước Nga.

Việc soạn thảo các tài liệu đã chịu ảnh hưởng to lớn của Sách Da cam. Chúng có nhiều nét giống nhau: cùng hướng tới các hệ thống áp dụng cho quân đội, cùng sử dụng một thang tổng quát để đánh giá độ bảo vệ…

5.2.5.4. Hệ tiêu chí chung đánh giá ATTT

a) Mục đích ban hành

"Hệ tiêu chí an toàn CNTT chung" (Common Criteria for Information Technology Security Evaluation thường gọi là Các tiêu chí chung - Common Criteria) là kết quả của nỗ lực tập thể của các tác giả "Các tiêu chí an toàn CNTT châu Âu", "Các tiêu chí liên bang của Mỹ", "Các tiêu chí an toàn các hệ thống máy tính của Canada", nhằm hướng tới sự kết hợp (tích hợp) các luận điểm cơ bản của các tài liệu này và để đưa ra một chuẩn quốc tế thống nhất về an toàn CNTT. Công việc của một đề án to lớn nhất trong lịch sử các tiêu chuẩn ATTT được tiến hành bắt đầu vào tháng 6 năm 1993 (chỉ 10 năm sau khi công bố Sách Da cam). Phiên bản 2.1 của chuẩn này đã được Tổ chức

tiêu chuẩn quốc tế ISO phê chuẩn vào năm 1999 như là một chuẩn ATTT quốc tế ISO/IEC 15408.

Phiên bản đầu tiên của "Tiêu chí chung" được công bố vào 31/01/1996. Các tác giả của nó là Viện các tiêu chuẩn và công nghệ quốc gia và Cục an ninh quốc gia của Mỹ, các cơ quan tương tự của Anh, Canada, Pháp và Hà Lan. Phiên bản thứ 2 ra đời vào 5/1998. Ở đây chúng ta làm quen với phiên bản 2.1 của nó như đã nói ở trên.

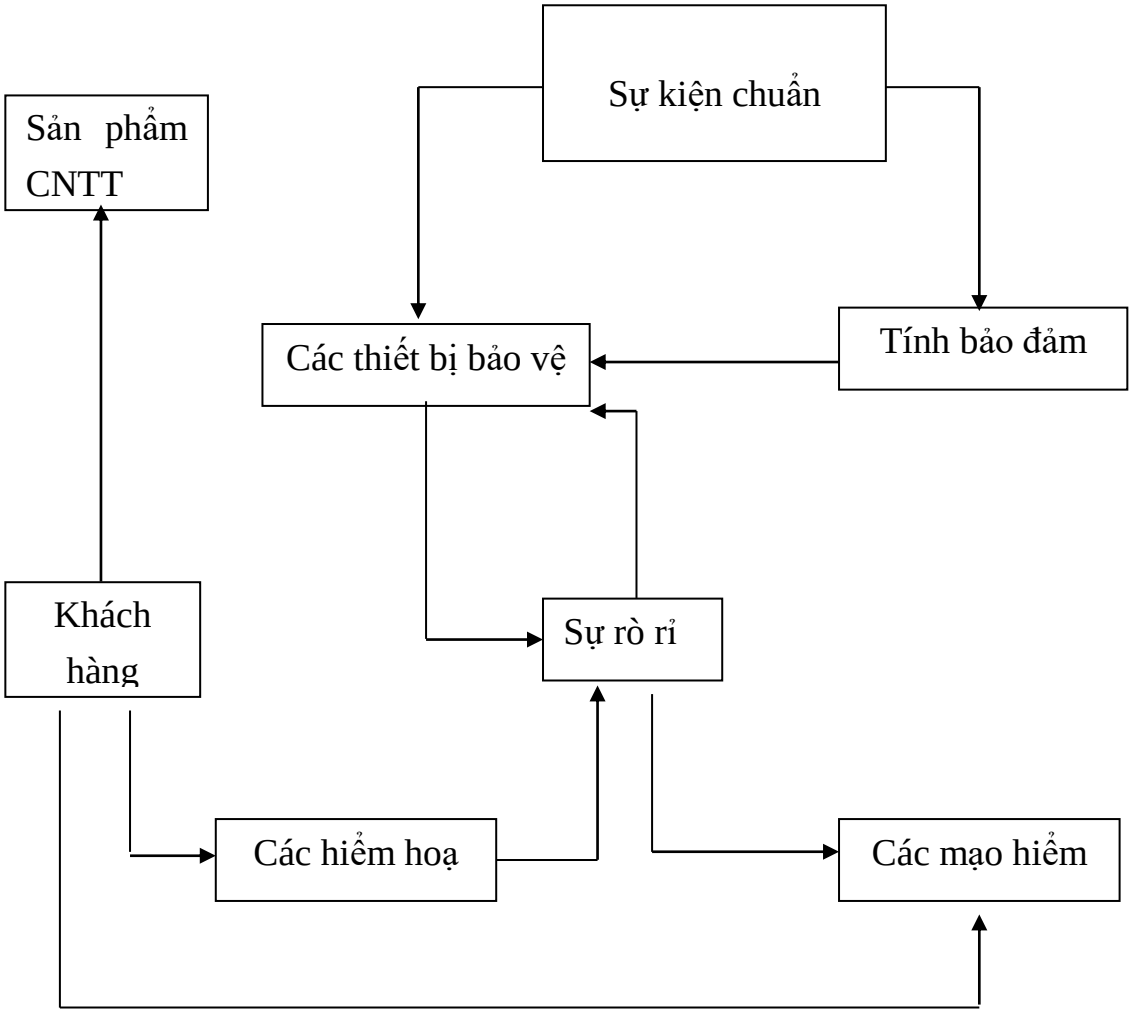
"Các tiêu chí chung" giữ được những trùng lặp cùng các tiêu chuẩn đang tồn tại và phát triển chúng lên bằng cách đưa vào các khái niệm, các hướng mới tương ứng với mức độ phát triển của CNTT hiện đại và sự tích hợp (liên kết) của các hệ thống thông tin của quốc gia vào một không gian TT thống nhất toàn thế giới. Tài liệu này được xây dựng trên cơ sở các thành tựu của hàng loạt các nghiên cứu trong lĩnh vực an toàn CNTT những năm 90 và trên kết quả phân tích kinh nghiệm áp dụng các tiêu chuẩn đã kết tinh vào các thành tựu đó. Các tiêu chí chung đưa ra một số khái niệm mới (mà chúng ta đã biết ở phần đầu như: Sản phẩm CNTT (IT-product), Hồ sơ bảo vệ (Protection Profile-PP). CC được soạn thảo nhằm đáp ứng nhu cầu của 3 nhóm người: Các nhà sản xuất, các nhà tiêu dùng các sản phẩm CNTT và các chuyên gia đánh giá độ an toàn của các sản phẩm đó.

Như vậy, CC bảo đảm các điều kiện chuẩn cho quá trình lựa chọn các sản phẩm CNTT, mà đối với chúng sẽ đặt ra các yêu cầu về chức năng hoạt động trong môi trường có các hiểm họa nhất định. CC là tài liệu chỉ dẫn cho các nhà thiết kế các hệ thống an toàn và nó cũng quy chế hoá công nghệ thiết lập các hệ thống như vậy cùng các thủ tục đánh giá mức độ bảo đảm an toàn của chúng.

CC xem xét ATTT, trước tiên là tính bí mật và toàn vẹn của TT được xử lý bởi các sản phẩm CNTT và cả tính sẵn sàng phục vụ của các tài nguyên HT; và thứ hai là nó đặt ra cho các TBBV nhiệm vụ chống lại các hiểm họa cơ bản tồn tại trong môi trường khai thác các sản phẩm này và nhiệm vụ thực hiện chính sách an toàn đã được chấp nhận trong môi trường khai thác đó.

Vì thế trong CC có tất cả các khía cạnh của quá trình thiết kế, sản xuất và khai thác của các sản phẩm CNTT dùng để làm việc trong các điều kiện tác

động của các hiểm họa ATTT. Các mối liên hệ nhân-quả giữa các khái niệm cơ bản của CC được dẫn ra trong sơ đồ sau:



Hình 5.4 Các mối liên hệ nhân-quả giữa các khái niệm cơ bản của CC

Các khách hàng của các sản phẩm CNTT lo ngại về tồn tại các hiểm họa ATTT, sẽ dẫn tới sự mạo hiểm nhất định cho các TT được xử lý. Để chống lại các hiểm họa này sản phẩm CNTT phải gồm có cả các TBBV cho phép khẳng định tính đảm bảo trước các hiểm họa và các mạo hiểm.

b) Các luận điểm cơ bản

Trước tiên chúng ta làm quen với một số khái niệm – thuật ngữ của CC:

- Vấn đề an toàn – Khái niệm cơ bản của CC, biểu diễn nhu cầu của các khách hàng của sản phẩm CNTT trong việc chống lại tập hợp các hiểm họa an toàn hoặc trong sự cần thiết thực hiện một chính sách an toàn.

• Hồ sơ bảo vệ - Đó là một tài liệu chuẩn đặc biệt, chứa đựng các vấn đề an toàn, các yêu cầu chức năng, các yêu cầu đảm bảo, các đặc trưng của TBBV và cơ sở luận chứng của chúng. Nó là tài liệu hướng dẫn cho các nhà sản xuất, thiết kế sản phẩm CNTT trong quá trình thiết lập đích an toàn.

• Đích an toàn – là tài liệu chuẩn đặc biệt, chứa đựng các vấn đề an toàn, các yêu cầu chức năng, các yêu cầu đảm bảo, các đặc trưng của TBBV và cơ sở luận chứng của chúng. Trong quá trình phân tích, đánh giá nó sẽ là sự mô tả sản phẩm CNTT.

Theo CC, an toàn CNTT có thể đặt được bằng cách áp dụng công nghệ thiết kế, kiểm chuẩn và khai thác các sản phẩm CNTT do các tác giả đề xuất trong hệ tiêu chí này.

Trên quan điểm của CC, điều quan trọng nhất trong các yêu cầu an toàn mà các nhà thiết kế định hướng theo, đó là các sản phẩm CNTT phải đáp ứng các nhu cầu của khách hàng. Chỉ có bảo đảm điều này mới có thể đạt được mục đích đề ra – bảo đảm an toàn CNTT trong môi trường tác động của các hiểm họa an toàn.

CC xác định khá nhiều các yêu cầu điển hình (các mẫu yêu cầu), mà cùng với cơ chế hồ sơ bảo vệ chúng cho phép các khách hàng lựa chọn được các yêu cầu riêng phù hợp với nhu cầu an toàn của họ. Các nhà thiết kế có thể sử dụng hồ sơ bảo vệ như là một cơ sở để đưa ra các đặc tả các sản phẩm của mình. Hồ sơ bảo vệ và các đặc tả TBBV tạo thành cái gọi là đề án bảo vệ. Chính đề án bảo vệ là đại diện của sản phẩm CNTT trong quá trình phân tích đánh giá.

Sự phân tích đánh giá có thể được tiến hành song song với thiết kế sản phẩm CNTT hoặc sau khi kết thúc thiết kế. Để tiến hành được phân tích đánh giá, nhà thiết kế sản phẩm phải trình ra các tài liệu sau đây:

- Hồ sơ bảo vệ (Protection Profile): mô tả vai trò của sản phẩm và chỉ ra đặc trưng của môi trường khai thác nó, và cũng xác lập trong đó các Nhiệm vụ bảo vệ và các yêu cầu mà sản phẩm phải đáp ứng.
- Đối tượng an toàn (Security Target - ST): bao gồm các đặc tả các TBBV; luận chứng của sự tương ứng của sản phẩm với các nhiệm vụ bảo vệ từ Hồ sơ bảo vệ, và với các yêu cầu của CC đã nêu ra trong đó (Tức Hồ sơ bảo vệ)

- Các luận cứ khác nhau và các khẳng định các tính chất và khả năng của sản phẩm, do các nhà thiết kế thu được.
- Chính sản phẩm CNTT.
- Các cứ liệu phụ thu được bằng cách tiến hành các thu thập độc lập khác nhau.

Quá trình phân tích đánh giá gồm 3 giai đoạn:

1. Phân tích hồ sơ bảo vệ về các mặt: tính đầy đủ, không mâu thuẫn, tính khả thi và khả năng được sử dụng như tập hợp các yêu cầu cho sản phẩm được thiết kế
2. Phân tích đích an toàn về các mặt: sự tương ứng với các yêu cầu của Hồ sơ bảo vệ, tính đầy đủ, không mâu thuẫn, tính khả thi và khả năng được sử dụng như một mẫu trong phân tích sản phẩm CNTT.
3. Phân tích sản phẩm CNTT về sự tương ứng với đích an toàn.

Kết quả của phân tích đánh giá là kết luận rằng sản phẩm CNTT đã được đánh giá tương ứng với Đối tượng an toàn được giới thiệu. Bản kết luận bao gồm một số báo cáo, khác nhau bởi mức độ chi tiết hoá, và chứa đựng quan điểm của các chuyên gia kiểm chuẩn về sản phẩm trên cơ sở các tiêu chí phân loại CC. Các báo cáo này có thể được sử dụng bởi các nhà sản xuất và cả các khách hàng.

Việc áp dụng phân tích đánh giá và kiểm chuẩn làm nâng cao chất lượng công việc của các nhà sản xuất trong thiết kế và sản xuất các sản phẩm. Trong các sản phẩm đã qua đánh giá độ an toàn, xác suất xuất hiện các lỗi và các điểm yếu bảo vệ và các rò rỉ nhỏ đi một cách đáng kể (so với trong các sản phẩm thông thường). Điều đó nói lên rằng, áp dụng "các tiêu chí chung" có ảnh hưởng tích cực và xây dựng tới quá trình hình thành các yêu cầu, thiết kế sản xuất sản phẩm CNTT, chính sản phẩm và sự khai thác nó. Chúng ta hãy xem xét kỹ hơn về Hồ sơ bảo vệ và Đối tượng an toàn.

i) Hồ sơ bảo vệ (Protection Profile) – HSBV

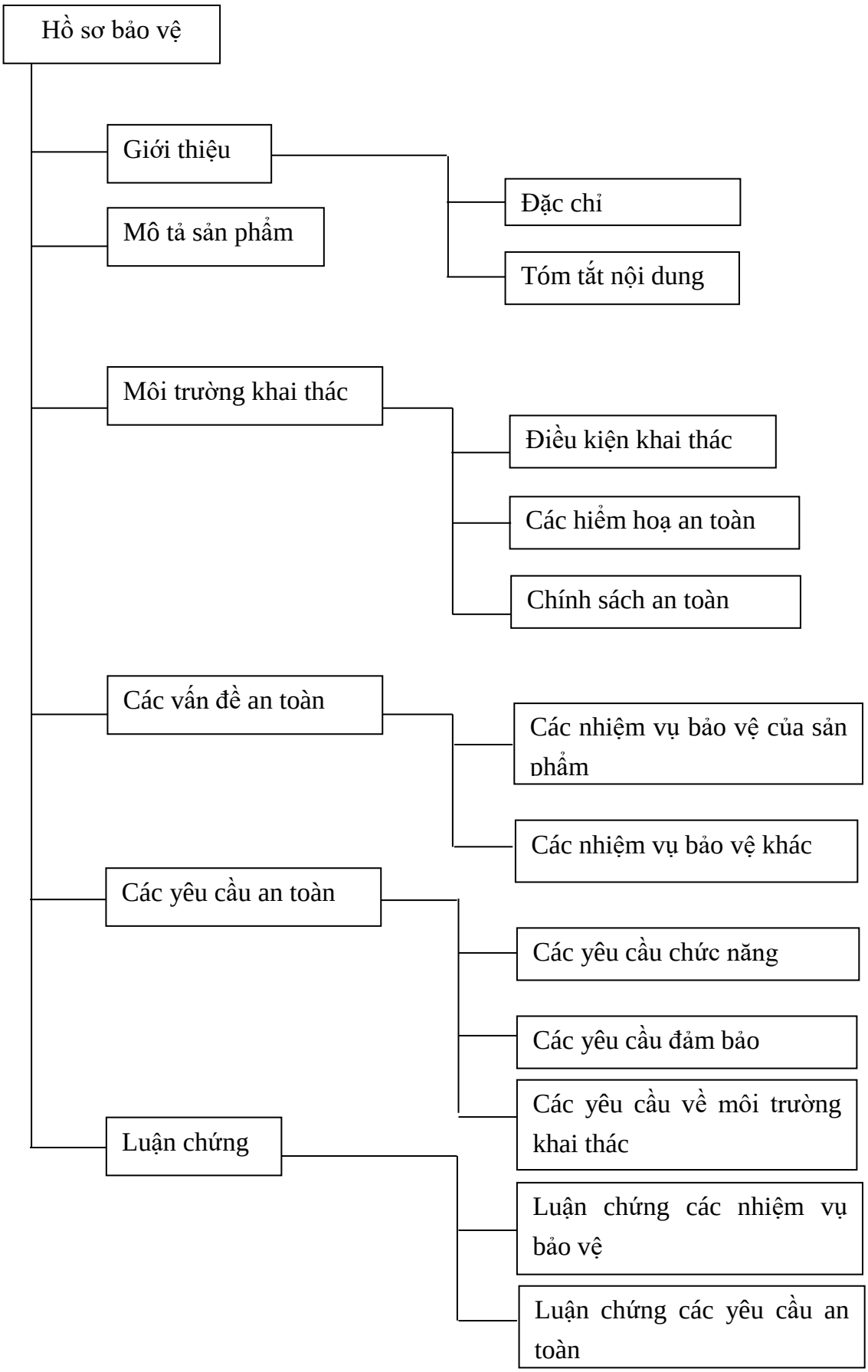
HSBV xác định các yêu cầu an toàn đối với một chủng loại nhất định các sản phẩm CNTT, không chính xác hoá các phương pháp và phương tiện thực hiện chúng. Nhờ HSBV mà các khách hàng hình thành các yêu cầu của họ tới các nhà sản xuất. Cấu trúc của HSBV như sau.

Chúng ta hãy xem xét vai trò và nội dung của các tiểu mục của HSBV.

• Giới thiệu chứa thông tin cần để cho tìm kiếm HSBV cụ thể trong thư viện các HSBV

- Đặc chỉ của HSBV là một tên đặc biệt, thích hợp cho việc tìm kiếm nó trong vô số các HSBV giống nhau và để đánh dấu khi tham khảo tới nó.
- Tóm tắt nội dung chứa những lời gắn gọn của HSB, để trên cơ sở đó khách hàng có thể đi đến kết luận về sự tương ứng của HSBV với các đòi hỏi của họ.

• Mô tả sản phẩm CNTT chứa một số đặc trưng gắn gọn của sản phẩm, nhiệm vụ chức năng, các nguyên lý làm việc, phương pháp sử dụng…Các TT này không cần phải phân tích và kiểm chuẩn, nhưng phải cung cấp cho các chuyên gia để giải thích các yêu cầu an toàn và xác định sự phù hợp của chúng với các nhiệm vụ mà các sản phẩm này giải quyết, và cũng để hiểu rõ cấu trúc và các nguyên lý làm việc của sản phẩm CNTT.



Hình 5.5 Cấu trúc của Hồ sơ bảo vệ

• Môi trường khai thác. Mục này chứa sự mô tả môi trường hoạt động của sản phẩm CNTT trên góc độ an toàn.

- Các điều kiện khai thác. Mô tả các điều kiện khai thác sản phẩm cần phải chứa đặc trưng đầy đủ môi trường khai thác trên quan điểm an toàn, kể cả các giới hạn về điều kiện áp dụng sản phẩm.
- Các hiểm họa an toàn. Mô tả các hiểm họa an toàn, tác động trong môi trường khai thác mà sự bảo vệ sản phẩm phải đối mặt.Với mỗi hiểm họa cần chỉ rõ nguồn gốc của nó, phương pháp và đối tượng tác động của hiểm họa.
- Chính sách an toàn. Mô tả CSAT cần phải xác định rõ và khi cần thiết, phải giải thích các điều luật của CSAT cần thiết phải thực hiện trong sản phẩm.

• Các nhiệm vụ bảo vệ phản ánh các nhu cầu của khách hàng trong việc chống lại các hiểm họa an toàn đã chỉ ra và/hoặc trong việc thực hiện CSAT.

- Các nhiệm vụ bảo vệ của sản phẩm phản ánh các nhu cầu của khách hàng trong việc chống lại các hiểm họa và/ hoặc thực hiện CSAT.
- Các nhiệm vụ bảo vệ khác phản ánh sự cần thiết tham gia của các TBBV của sản phẩm CNTT trong chống lại các hiểm họa an toàn và/hoặc thực hiện CSAT cùng với các thành tố CNTT khác.

• Các yêu cầu an toàn chứa các yêu cầu an toàn cần phải đáp ứng đối với sản phẩm CNTT để giải quyết các nhiệm vụ bảo vệ.

- Các yêu cầu chức năng chỉ chứa các yêu cầu mẫu đã được đưa ra trong các mục tương ứng của "Các tiêu chí chung". Cần phải bảo đảm mức chi tiết hoá các yêu cầu sao cho nó cho phép thể hiện rõ sự tương ứng với các nhiệm vụ bảo vệ. Các yêu cầu chức năng có thể báo trước hoặc cấm sử dụng một số phương pháp và thiết bị bảo vệ.
- Các yêu cầu đảm bảo chứa các tham chiếu lên các yêu cầu mẫu của các mức đảm bảo của "Các tiêu chí chung", nhưng cho phép định nghĩa thêm các yêu cầu đảm bảo phụ.

- Các yêu cầu về môi trường khai thác. Mục này không bắt buộc phải có. Và nó có thể chứa các yêu cầu chức năng và các yêu cầu đảm bảo, mà phải đáp ứng các thành tố CNTT tạo thành môi trường khai thác của sản phẩm đang xem xét.Trong mục này, khác với các mục khác , việc sử dụng các yêu cầu mẫu của "Các tiêu chí chung" là mong muốn nhưng không bắt buộc.

• Các cứ liệu bổ sung. Đây là mục không bắt buộc, chứa bất kỳ TT bổ sung nào có ích cho thiết kế, sản xuất và phân tích đánh giá và kiểm chuẩn sản phẩm CNTT.

• Luận chứng cần phải thể hiện rõ ràng, Hồ sơ bảo vệ chứa một tập hợp đầy đủ và hệ thống các yêu cầu, và rằng sản phẩm CNTT, đáp ứng chúng sẽ chống lại một cách có hiệu quả các hiểm họa an toàn của môi trường khai thác.

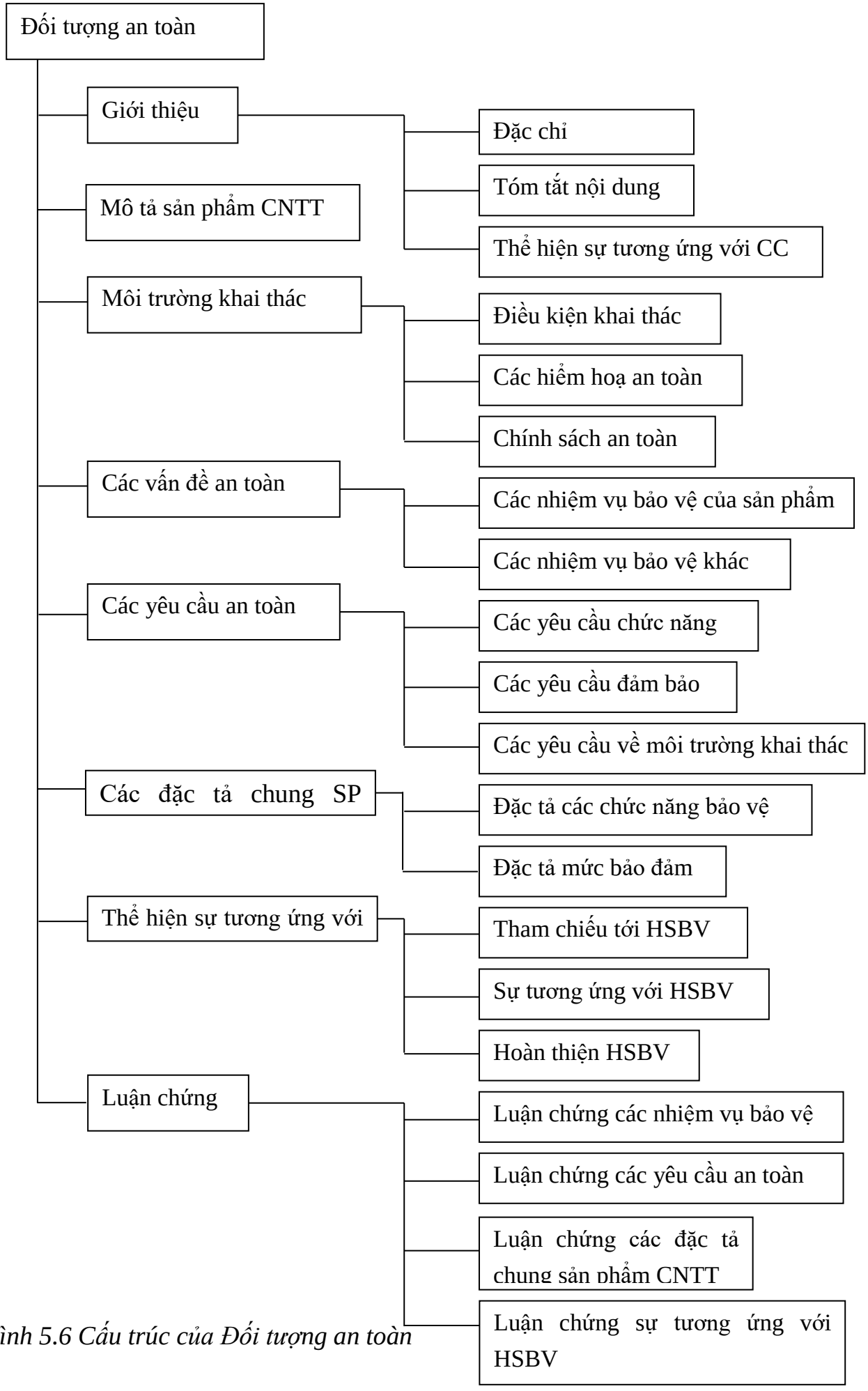
- Luận chứng các nhiệm vụ bảo vệ cần phải thể hiện rõ, rằng các nhiệm vụ bảo vệ được đưa ra trong Hồ sơ tương ứng với các tham số của môi trường khai thác, và giải quyết chúng sẽ cho phép chống lại có hiệu quả các hiểm họa an toàn và thực hiện được CSAT.
- Luận chứng các yêu cầu an toàn phải chỉ ra rằng, các yêu cầu an toàn cho phép giải quyết có hiệu quả các nhiệm vụ bảo vệ, vì các lý do:
  - Tập hợp các mục tiêu, mà các yêu cầu chức năng riêng đã theo đuổi, tương ứng với các nhiệm vụ bảo vệ đã đề ra.
  - Các yêu cầu an toàn là đồng bộ, không mâu thuẫn nhau, mà còn tăng cường nhau.
  - Lựa chọn các yêu cầu là hợp lý (đặc biệt là đối với các yêu cầu bổ sung, không có trong CC).
  - Tập hợp đã lựa chọn các yêu cầu chức năng và mức độ các yêu cầu đảm bảo phù hợp với các nhiệm vụ bảo vệ.

Hồ sơ bảo vệ là xuất phát điểm cho nhà sản xuất trong quá trình hình thành thiết lập Đề án bảo vệ, chính là các đề án kỹ thuật để sản xuất sản phẩm CNTT và là đại diện cho sản phẩm trong phân tích đánh giá an toàn.

ii) Đối tượng an toàn

Đối tượng an toàn chứa các yêu cầu và nhiệm vụ bảo vệ của sản phẩm CNTT, nó mô tả mức độ các khả năng hoạt động của các TBBV tích hợp trong sản phẩm, luận chứng và khẳng định mức độ bảo đảm của TBBV. Đối tượng an toàn vừa là điểm chỉ dẫn cho nhà thiết lập hệ thống, vừa là các mẫu của hệ thống trong quá trình phân tích đánh giá

Cấu trúc của Đối tượng an toàn được thể hiện trong hình sau:



Hình 5.6 Cấu trúc của Đối tượng an toàn

Nhiều mục của ĐTAT trùng tên với các mục của HSBV. Vì thế chúng ta dừng lại chỉ ở các mục đặc trưng cho ĐTAT và các mục có ít nhiều thay đổi gần đây:

- Giới thiệu chứa các TT cần để nhận dạng ĐTAT, xác định vị trí và tóm tắt nội dung của nó.
    - Đặc chỉ là tên riêng của ĐTAT, cần cho việc tìm kiếm và nhận dạng ĐTAT là sản phẩm CNTT tương ứng với nó.
    - Tóm tắt nội dung là chỉ dẫn khá tỷ mỷ của ĐTAT cho phép khách hàng tiềm năng xác định sự phù hợp của sản phẩm để giải quyết các nhiệm vụ của họ.
    - Thể hiện sự tương tác với CC chứa mô tả tất cả các tính chất của sản phẩm, thuộc về phân tích đánh giá trên cơ sở "Các tiêu chí chung".
- Các yêu cầu an toàn chứa các yêu cầu an toàn đối với sản phẩm, mà các nhà sản xuất định hướng theo trong quá trình thiết kế và thực hiện. Mục này của ĐTAT ít nhiều khác so với mục tương tự của HSBV.
    - Các yêu cầu chức năng đối với sản phẩm. Mục này khác với HSBV, cho phép sử dụng ngoài các yêu cầu mẫu của CC, cả các yêu cầu khác, đặc trưng cho sản phẩm cụ thể và môi trường khai thác nó. Khi miêu tả các yêu cầu đặc trưng này cần tuân thủ phong cách của CC và phải thể hiện được mức độ cụ thể vốn có của CC.
    - Các yêu cầu đảm bảo cho phép dùng các mức đảm bảo không có trong CC. Trong trường hợp này, mô tả mức đảm bảo phải rõ ràng, không mâu thuẫn và đủ cụ thể để sau này dùng cho phân tích đánh giá.
- Đặc tả chung của sản phẩm CNTT mô tả các cơ chế thực hiện các nhiệm vụ bảo vệ nhờ xác định các đặc tả ở các mức độ cao của TBVV tương ứng với các yêu cầu chức năng và các yêu cầu đảm bảo đã đưa ra.
    - Đặc tả các chức năng bảo vệ mô tả các khả năng hoạt động của các TBBV trong sản phẩm CNTT mà các nhà sản xuất coi là

để thực hiện các yêu cầu an toàn. Hình thức biểu diễn các đặc tả phải cho phép xác định được sự tương ứng giữa các chức năng bảo vệ và các yêu cầu an toàn.

- Đặc tả mức đảm bảo xác định mức đảm bảo đã nêu ra của sản phẩm và sự tương ứng của nó với các yều cầu đảm bảo, ở dạng thức đưa ra các tham số công nghệ thiết kế và thiết lập sản phẩm. Các tham số này phải được đưa ra dưới dạng sao cho có thể xác định được sự tương ứng của nó với các yêu cầu đảm bảo.

• Thể hiện sự tương ứng với HSBV. Một ĐTAT có thể đáp ứng các yêu cầu của một hoặc một vài HSBV. Mục này là không bắt buộc, và chứa các TT cần thiết cho khẳng định chấp nhận thể hiện đó. Với mỗi HSBV mà ĐTAT muốn thực hiện, mục này phải chứa các TT sau:

- Tham chiếu tới HSBV nhận dạng đơn nhất HSBV mà ĐTAT mong muốn thực hiện. Cần chỉ rõ các trường hợp mà mức bảo vệ đưa ra vượt hơn yêu cầu của Hồ sơ. Thực hiện chính xác HSBV có nghĩa là thực hiện chính xác tất cả các yêu cầu của Hồ sơ, không có một loại trừ nào.
- Sự tương ứng với HSBV xác định khả năng của sản phẩm thực hiện các nhiệm vụ bảo vệ và các yêu cầu chứa đựng trong Hồ sơ.
- Hoàn thiện HSBV phản ánh các khả năng của sản phẩm CNTT vượt ra ngoài khuôn khổ của các nhiệm vụ bảo vệ và các yêu cầu đặt ra trong Hồ sơ.

• Luận chứng phải chứng tỏ rằng, ĐTAT gồm một tập hợp đầy đủ và hệ thống của các yêu cầu, hiện thực hoá sản phẩm CNTT, sẽ chống lại có hiệu quả các hiểm họa an toàn tác động trong môi trường khai thác, và rằng, các đặc tả chung các chức năng bảo vệ tương ứng với các yêu cầu an toàn. Ngoài ra, luận chứng phải chứa khẳng định sự tương ứng với HSBV. Luận chứng gồm các tiểu mục sau:

- Luận chứng các nhiệm vụ bảo vệ phải chứng tỏ được rằng, các nhiệm vụ bảo vệ đưa ra trong ĐTAT tương ứng với các tính chất của môi trường khai thác, và việc giải quyết chúng cho phép

chống lại có hiệu quả các hiểm họa an toàn và thực hiện được CSAT đòi hỏi.

- Luận chứng các yêu cầu an toàn chỉ ra rằng, hoàn thành các yêu cầu này cho phép giải quyết các nhiệm vụ bảo vệ, vì lý do:
  - Tập hợp các yêu cầu chức năng và yêu cầu đảm bảo, và cả các điều kiện khai thác sản phẩm CNTT tương ứng với các nhiệm vụ bảo vệ.
  - Tất cả các yêu cầu an toàn là không mâu thuẫn nhau mà còn tăng cường lẫn nhau.
  - Sự lựa chọn các yêu cầu là hợp lý.
  - Mức độ các khả năng hoạt động của TBBV tương xứng với các nhiệm vụ bảo vệ.
- Luận chứng các đặc tả chung của sản phẩm phải chứng tỏ rằng, các TBBV và các phương pháp duy trì tính đảm bảo của chúng tương ứng với các yêu cầu đảm bảo đưa ra vì:
  - Tập hợp các TBBV đáp ứng các yêu cầu chức năng.
  - Mức độ an toàn đòi hỏi và mức chính xác của bảo vệ được đảm bảo bởi các thiết bị đề xuất.
  - Các biện pháp để duy trì tính đảm bảo thực hiện các yêu cầu chức năng tương xứng với các yêu cầu đảm bảo đề ra
- Luận chứng sự tương ứng với HSBV chỉ ra rằng, các yêu cầu của ĐTAT duy trì tất cả các yêu cầu của HSBV. Để như vậy, cần phải chứng tỏ rằng:
  - Tất cả sự hoàn chỉnh các nhiệm vụ bảo vệ so với HSBV được thực hiện chính xác và theo hướng phát triển và chi tiết hoá.
  - Tất cả các nhiệm vụ BV của HSBV được giải quyết thành công và tất cả các yêu cầu của HSBV đều được đáp ứng.
  - Không có yêu cầu bổ sung nào trong số đã đưa vào ĐTAT, vì các nhiệm vụ BV đặc thù và các yêu cầu an toàn, có sự mâu thuẫn với HSBV.

Như chúng ta đã thấy trong cấu trúc của HSBV và ĐTAT và qua tóm tắt nội dung của chúng, các tài liệu này trên thực tế đã quy chế hoá một các toàn

diện sự tương tác của các khách hàng, các nhà sản xuất và các chuyên gia đánh giá trong quá trình thiết lập một hệ thống an toàn (một sản phẩm CNTT). Trên thực tế, các luận điểm của 2 tài liệu này (ĐTAT và HSBV) đã xác định công nghệ thiết lập các HAT.

c) Các yêu cầu an toàn

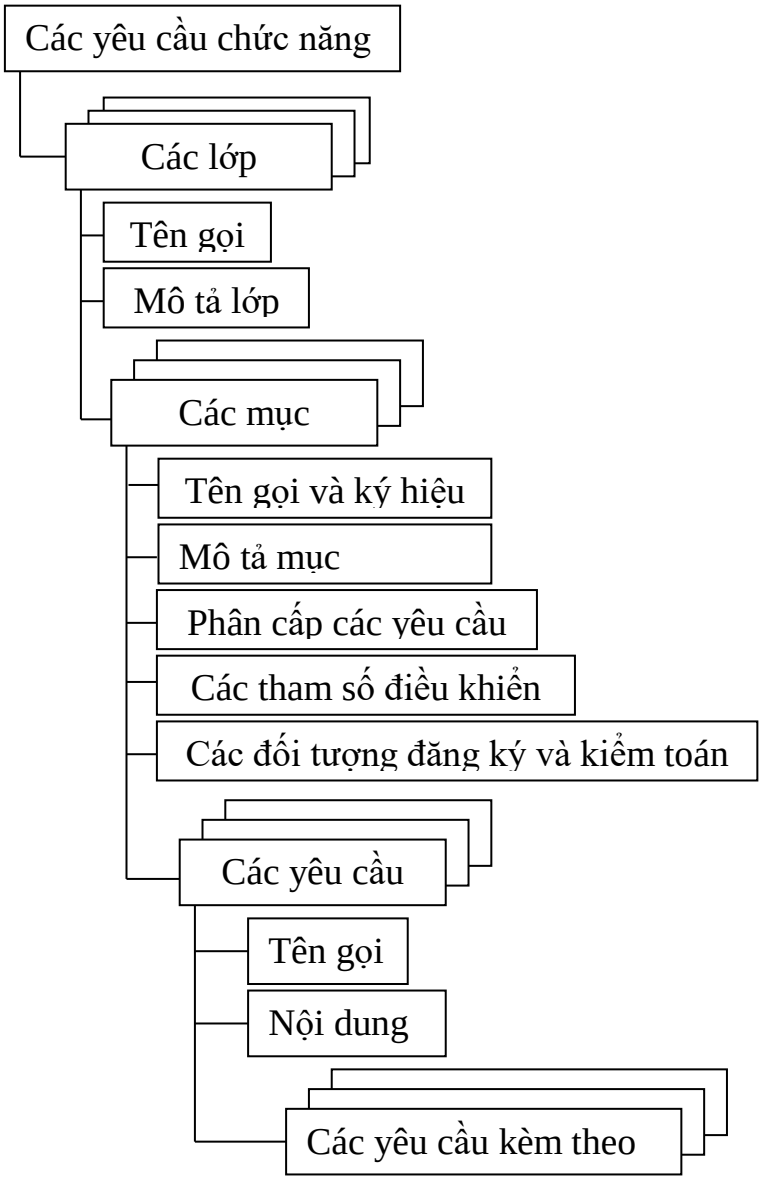
"Các tiêu chí chung" chia các yêu cầu an toàn ra là 2 loại: các yêu cầu chức năng và các yêu cầu đảm bảo.

Các yêu cầu chức năng quy định các hoạt động an toàn của các thành tố của sản phẩm CNTT và xác định các khả năng của các TBBV.

Tính bảo đảm là một đặc trưng của sản phẩm, nó chỉ ra rằng, mức độ an toàn được đảm bảo hiệu quả đến đâu, độ chính xác thực hiện của các TBBV như thế nào. Tính bảo đảm được xác định bởi các công nghệ được sử dụng trong quá trình thiết kế, xây dựng và khai thác sản phẩm. Vì vậy, các yêu cầu đảm bảo quy định công nghệ và quá trình thiết lập sản phẩm CNTT (HT), và cả sự cần thiết tiến hành phân tích các điểm yếu của bảo vệ.

i) Các yêu cầu chức năng

Các yêu cầu chức năng của CC được thể hiện dưới dạng có cấu trúc hình thức chặt chẽ, là một tổ hợp đầy đủ và rất chi tiết. Các yêu cầu được phân thành các lớp. Mỗi lớp lại có các mục (cỡ 5,6 mục), sau các mục lại đến bản thân các yêu cầu (thuộc mục và nhóm tương ứng). Mỗi yêu cầu chức năng lại được xây dựng theo sơ đồ gồm: Tên gọi, Nội dung yêu cầu và các yêu cầu đi kèm. Như vậy CC có nhiều lớp yêu cầu, mỗi lớp có nhiều mục, mỗi mục có nhiều yêu cầu, mỗi yêu cầu lại có các yêu cầu đi kèm; và như vậy CC là một tập hợp khổng lồ các yêu cầu chức năng. Cấu trúc chung của các yêu cầu chức năng của CC được chỉ ra trong hình sau:



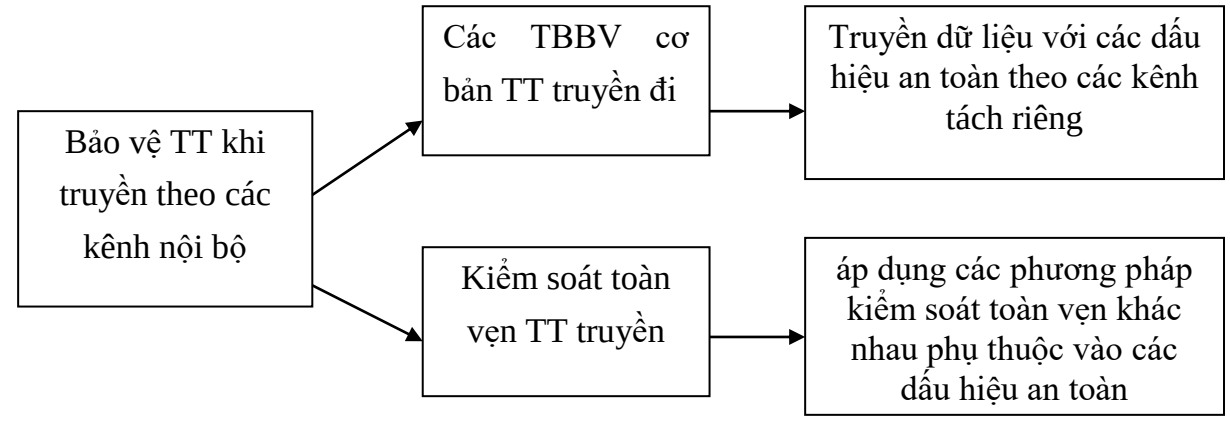
Hình 5.7 Cấu trúc chung của các yêu cầu chức năng

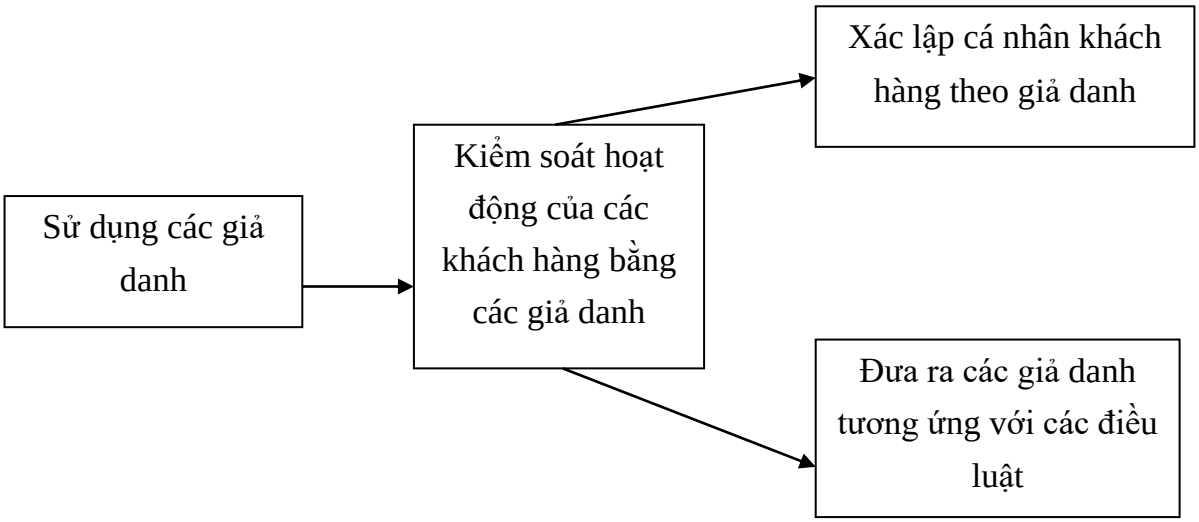
Chúng ta hãy làm quen với một vài cấu trúc tiêu biểu của CC đối với các mục trong một lớp.

- Tên gọi và ký hiệu. Mỗi mục có một tên gọi riêng và một đặc chỉ 7 ký hiệu lấy từ một tiền tố (prefix) có 3 chữ cái của đặc chỉ lớp, dấu gạch ngang và ký hiệu 3 chữ cái của mục đó. Tên gọi và ký hiệu dùng cho các tham chiếu lên mục.

- Phân cấp các yêu cầu. Sự phân cấp các yêu cầu chức năng của CC chỉ có thứ tự một phần (khác với nhiều bộ tiêu chuẩn khác thường có một trật tự thống nhất toàn bộ tạo ra một thang đánh giá duy nhất). Ví dụ điển hình ở đây

là sự phân cấp các yêu cầu bảo vệ TT khi truyền theo các kênh nội bộ và sự phân cấp các yêu cầu về sử dụng các giả danh (xem sơ đồ)





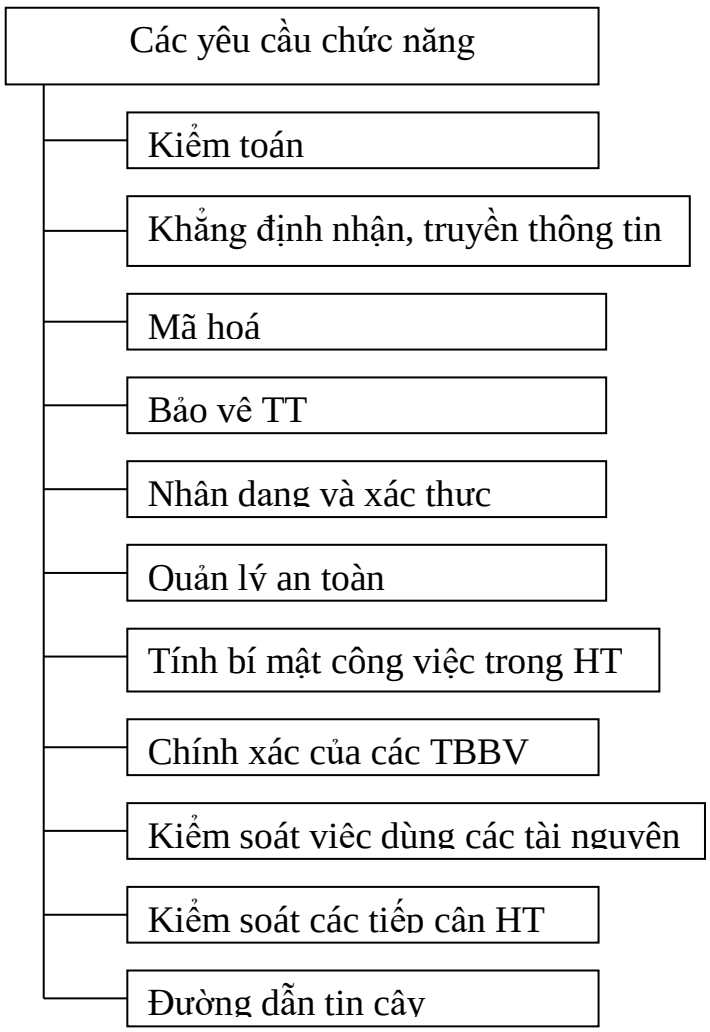
Việc thực hiện yêu cầu bảo vệ TT truyền theo các kênh nội bộ được phép tiến hành theo 2 hướng – bảo đảm an toàn khi truyền tin và kiểm soát toàn vẹn tin. Đối với mỗi hướng tồn tại 2 mức độ thực hiện các yêu cầu, phụ thuộc vào việc có hay không tính tới các dấu hiệu an toàn của TT được truyền đi. Các yêu cầu nằm ở các nhánh khác nhau là độc lập với nhau và tăng cường lẫn nhau.

Phân cấp các yêu cầu về sử dụng các giả danh có cấu trúc phức tạp hơn. Mức độ tương ứng thấp nhất với yêu cầu này được đảm bảo nhờ sử dụng các giả danh, che giấu các cá nhân khách hàng làm việc với hệ thống. Tồn tại 2

hướng độc lập tăng cường yêu cầu này - Đưa ra cơ chế cho phép khi cần xác định được từng khách hàng theo giả danh của họ; và đưa ra các điều luật (khi lập các giả danh) cho phép xác lập cá nhân khách hàng. Hai yêu cầu này nằm ở 2 nhánh khác nhau và không so sánh được với nhau (và cũng không thể tăng cường nhau).

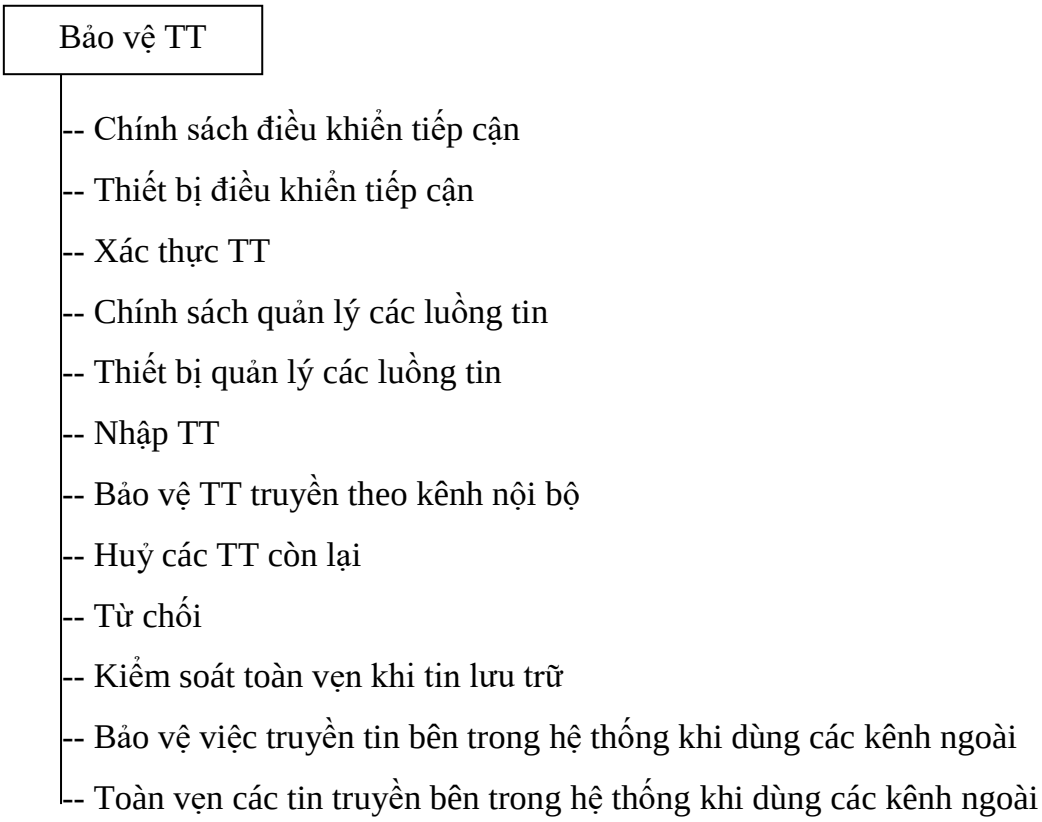
- Các tham số điều khiển. Trong tiểu mục này các tham số có thể được liệt kê, căn cứ vào các tham số này cần thực hiện quản lý các TBBV, hiện thực hoá các yêu cầu của mục đã nêu.
- Các đối tượng đăng ký và kiểm toán. Trong tiểu mục này của các yêu cầu phải liệt kê các thao tác và các sự kiện cần phải qua đăng ký và kiểm toán.

Sự phân loại các lớp của các yêu cầu chức năng của CC thể hiện trong sơ đồ dưới đây:

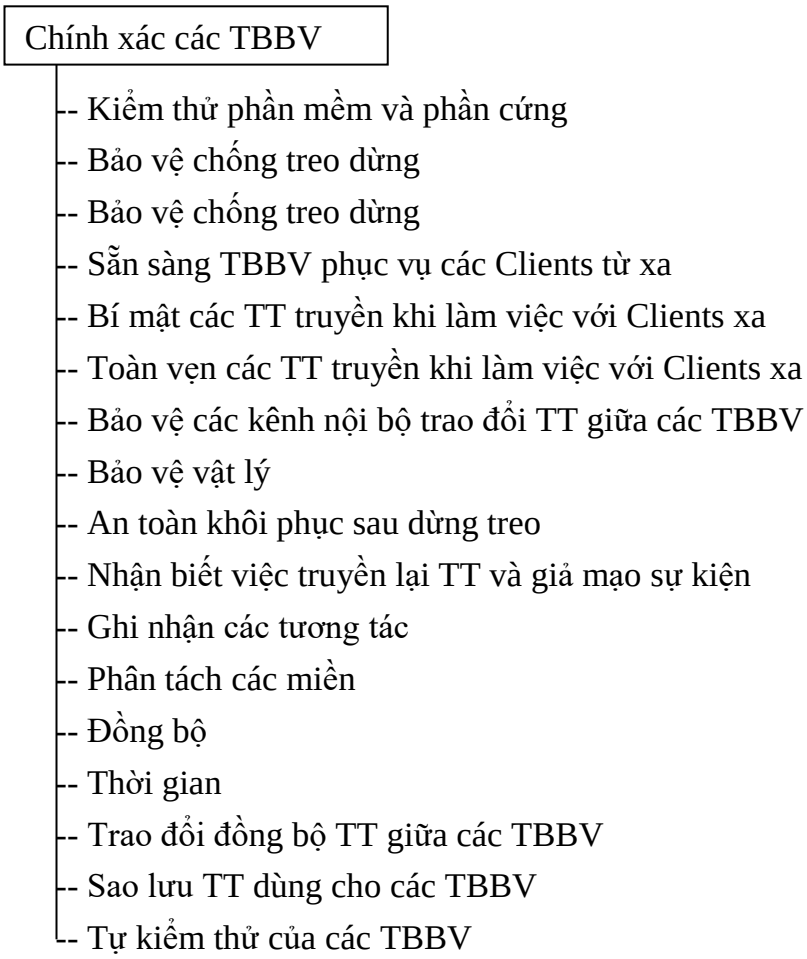


Hình 5.8 Các yêu cầu chức năng của CC

Sự phân loại các yêu cầu chức năng đối với tất cả các lớp của "Các tiêu chí chung" được chỉ ra trong loạt hình sau đây. Trước tiên là phép phân loại của 2 lớp: lớp bảo vệ TT và lớp chính xác của TBBV. Đây là 2 lớp có tính đặc thù riêng của CC.

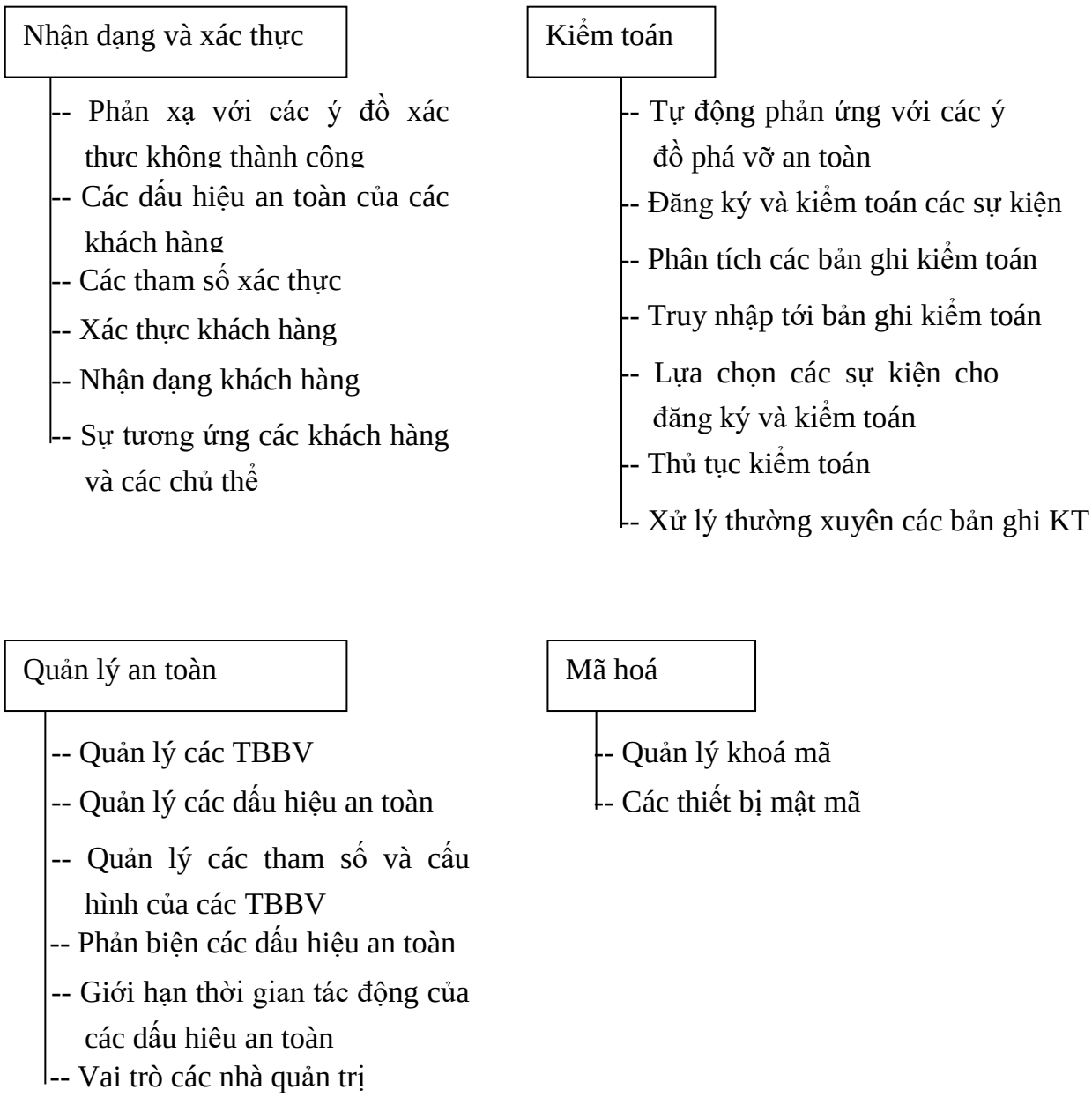


Hình 5.9 Phân loại lớp bảo vệ TT



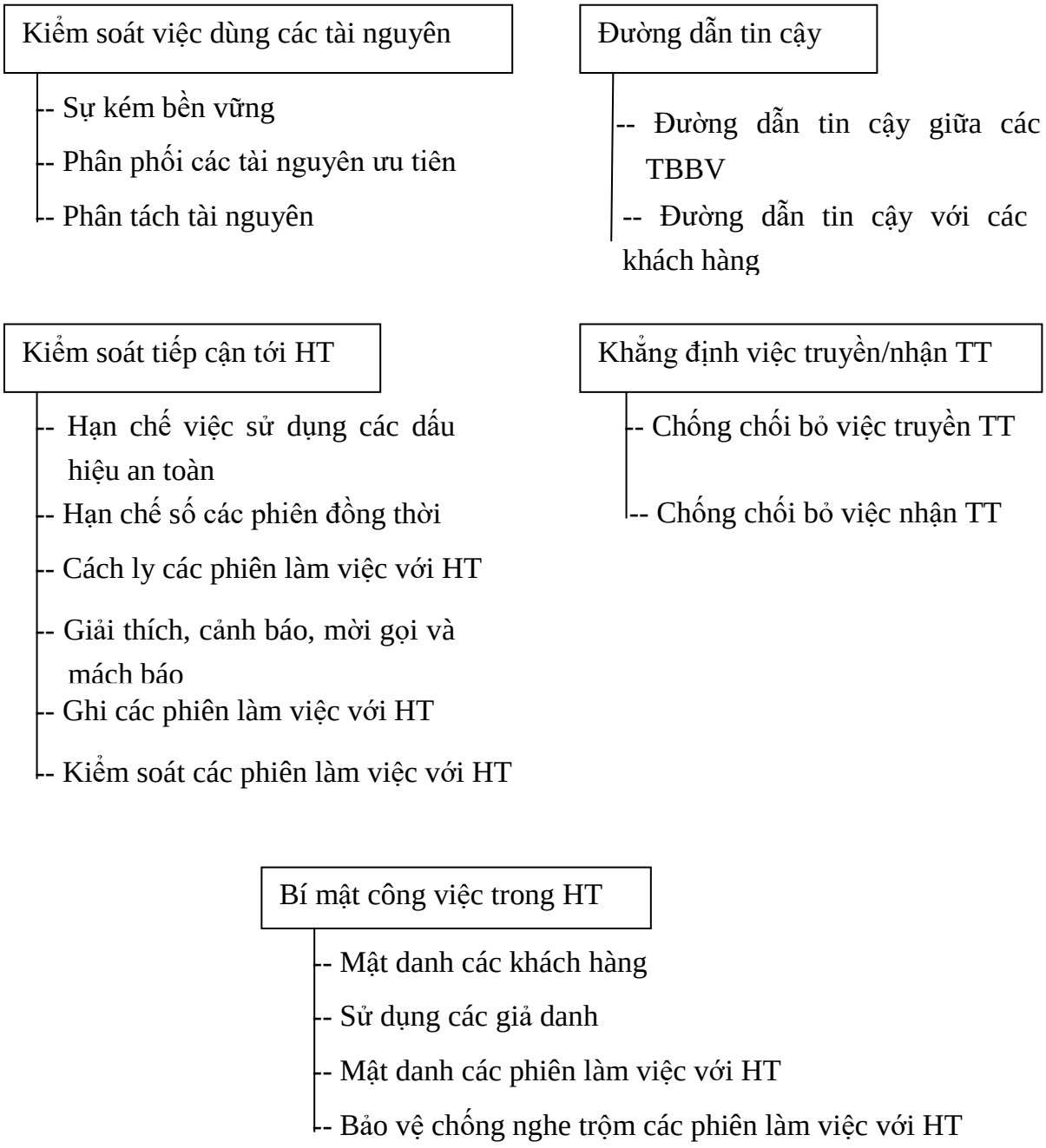
Hình 5.10 Phân loại lớp chính xác của các TBBV

Sau đây là phân loại của 4 lớp khác là: Lớp nhận dạng và xác thực; lớp kiểm toán; lớp quản lý an toàn và lớp mã hoá.



Hình 5.11 Phân loại của 4 lớp đặc thù

Tiếp theo sau đây là phân loại của 5 lớp cuối cùng:



Hình 5.12 Phân loại của 5 lớp cuối cùng

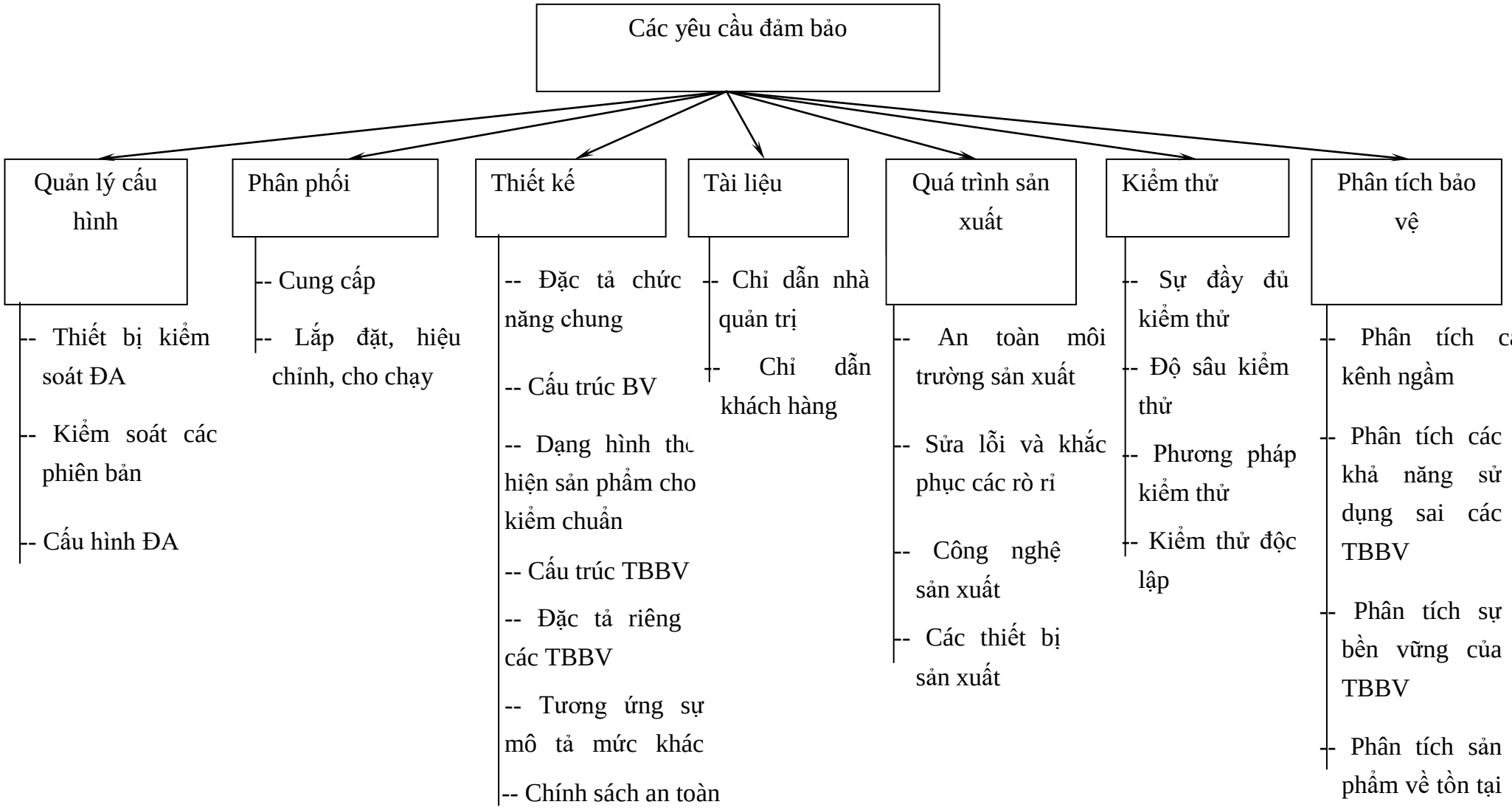
Cần lưu ý rằng, các yêu cầu về bí mật, toàn vẹn và kiểm soát truy nhập gộp vào một lớp "Bảo vệ TT" là khá hợp lý và tương ứng với các nhiệm vụ của chúng. Ở đây có sự phân tách đánh giá các yêu cầu về chính sách kiểm soát truy nhập (Các mô hình tuỳ chọn – DAC) khỏi các yêu cầu kiểm soát các

luồng TT (Các mô hình chuẩn bắt buộc – MAC). Và cũng có sự phân tách các yêu cầu về CSAT khỏi các yêu cầu thực hiện CSAT.

Lớp các yêu cầu về tính chính xác làm việc của các TBBV là có khối lượng lớn nhất. Điều đó nói lên mức độ chi tiết hoá rất cao của các yêu cầu của lớp này đối với các phương pháp và các thiết bị bảo đảm cho hoạt động bình thường của các TBBV.

ii) Các yêu cầu đảm bảo (assurance)

Các yêu cầu đảm bảo (YCĐB) của CC cấu trúc rất chặt chẽ và chúng quy chế hoá tất cả các công đoạn thiết kế, sản xuất và khai thác một sản phẩm CNTT từ góc độ duy trì tính chính xác làm việc của các TBBV và sự phù hợp của chúng với các yêu cầu chức năng, các nhiệm vụ bảo vệ và các hiểm họa, tác động trong môi trường khai thác sản phẩm.Sự phân loại các YCĐB của "Các tiêu chí chung" thể hiện trong hình sau:



Hình 5.13 Phân loại các yêu cầu đảm bảo

"Các tiêu chí chung" đưa ra 7 mức đảm bảo chuẩn, mà độ chặt chẽ của các yêu cầu đảm bảo tăng dần theo thứ tự mức 1 đến mức 7. Mỗi mức đặc trưng bằng một tập các yêu cầu đảm bảo, quy định việc áp dụng các phương pháp và công nghệ khác nhau để sản xuất, kiểm thử, quản lý và kiểm chuẩn một sản phẩm CNTT:

- Mức 1. Kiểm thử chức năng.
- Mức 2. Kiểm thử cấu trúc.
- Mức 3. Kiểm thử phương pháp và kiểm chuẩn.
- Mức 4. Thiết kế phương pháp, kiểm thử và phân tích.
- Mức 5. Các phương pháp kiểm thử và thiết kế bán hình thức.
- Mức 6. Các phương pháp kiểm chuẩn thiết kế và kiểm thử bán hình thức.
- Mức 7. Các phương pháp kiểm chuẩn thiết kế hình thức và kiểm thử.

Mỗi mức có một mô tả riêng mà ở đây chúng ta không có điều kiện phân tích chi tiết.

Sau đây là bảng phân bố các yêu cầu đảm bảo theo 7 mức an toàn đã nêu ở trên của CC.

Bảng 5.3 Phân bố các yêu cầu đảm bảo theo 7 mức an toàn của CC

Các yêu cầu đảm bảo	***Các mức đảm bảo***						
	1	2	3	4	5	6	7
1. Quản lý Đối tượng (Target)							
Các thiết bị kiểm soát Đối tượng				1	1	2	2
Kiểm soát các phiên bản (Versions)	1	2	3	4	4	5	5
Cấu hình Đối tượng			1	2	3	3	3
2. Phân phối							
Cung ứng		1	1	2	2	2	3
Lắp đặt, hiệu chỉnh, cho chạy	1	1	1	1	1	1	1
3. Thiết kế							

Các đặc tả chức năng chung	1	1	1	2	3	3	4
Cấu trúc của bảo vệ		1	2	2	3	4	5
Dạng thể hiện sản phẩm cho kiểm chuẩn				1	2	3	3
Cấu trúc của các TBBV					1	2	3
Đặc tả riêng các TBBV				1	1	2	2
Sự tương ứng mô tả các mức khác nhau	1	1	1	1	2	2	3
Chính sách an toàn				1	2	2	3
4. Tài liệu							
Chỉ dẫn nhà quản trị	1	1	1	1	1	1	1
Chỉ dẫn khách hàng	1	1	1	1	1	1	1
5. Quá trình sản xuất							
An toàn môi trường sản xuất			1	1	1	2	2
Sửa lỗi và khắc phục các rò rỉ							
Công nghệ sản xuất				1	2	2	3
Các thiết bị sản xuất				1	2	3	3
6. Kiểm thử							
Tính đầy đủ của kiểm thử		1	2	2	2	3	3
Độ sâu của kiểm thử			1	1	2	2	3
Phương pháp kiểm thử		1	1	1	1	2	2
Độc lập kiểm thử	1	1	2	2	2	2	3
7. Đánh giá rò rỉ							
Phân tích các kênh ngầm					1	2	2
Phân tích khả năng sử dụng sai các TBBV			1	2	2	3	3

Phân tích độ bền vững của các TBBV		1	1	1	1	1	1
Phân tích sản phẩm về tồn tại các rò rỉ		1	1	2	3	4	4

d) Kết luận

"Các tiêu chí chung an toàn công nghệ thông tin" là kết quả tổng hợp tất cả các thành tựu mới nhất trong lĩnh vực ATTT. Bộ tiêu chuẩn ATTT này đã nâng cao thành chuẩn chung quốc tế. Tạo khả năng thực tế cho việc xác lập một không gian ATTT chung, trong đó việc kiểm chuẩn an toàn các hệ thống sẽ được tiến hành ở mức toàn cầu, và điều này cho phép tích hợp các hệ thống thông tin quốc gia, mở ra các chân trời hoàn toàn mới cho việc ứng dụng các CNTT.

5.2.6. Phân tích và so sánh các tiêu chuẩn ATTT

5.2.6.1. Phân tích các tiêu chuẩn ATTT

a) Tính tổng quát

Đó là tính chất xác định bởi tập các HT, các thiết bị tính toán có thể áp dụng chính xác các luận điểm của một tiêu chuẩn. Ở giai đoạn mới hình thành và phát triển của các chuẩn ATTT các nhà soạn thảo cảm giác rằng vấn đề an toàn cần thiết cho chỉ một lĩnh vực hẹp các chuyên gia của chính phủ, trong an ninh quốc phòng mà thôi. Mặt khác khi đó tốc độ tin học hoá còn chậm chạp. Cho nên tính tổng quát của chuẩn ATTT không được quan tâm nhiều.

Trong chuẩn ATTT đầu tiên – Sách Da cam, các tiêu chí chỉ nhằm vào các ứng dụng quân sự, dựa trên các máy tính lớn (mainframe). Việc nâng cấp nó để cho các hệ thống phân tán, các CSDL đòi hỏi phải có các tài liệu bổ sung, các thuyết minh, các giải thích.

Sau đó ít năm, ra đời "Các tiêu chí châu Âu". Ở đây lĩnh vực áp dụng của chuẩn ATTT đã mở rộng lên rất nhiều - Đó là một tài liệu cơ sở và đã tính tới các hệ thống phân tán, các mạng, các hệ thống viễn thông… Tuy nhiên trong chuẩn châu Âu, chỉ vẫn nói về cấu trúc và nhiệm vụ của các hệ thống mà nó được áp dụng, chứ không đề cập gì đến môi trường khai thác chúng.

Tiêu chuẩn GTK của Liên bang Nga cũng có phạm vi áp dụng khá hạn chế. Đó là các PC và các hệ thống đa khách hàng (nhưng với số khách hàng hạn chế).

Cuối cùng, "Các tiêu chí chung" hoàn thiện quá trình mở rộng phạm vi ứng dụng các chuẩn ATTT bằng việc cho rằng việc sử dụng chuẩn ATTT là một thành tố không thể thiếu của công nghệ thiết lập các sản phẩm CNTT.

b) Tính mềm dẻo

Sự mềm dẻo của các luận điểm của Tiểu chuẩn xác định sự thuận tiện sử dụng nó bởi các khách hàng và các nhà sản xuất các hệ thống xử lý TT. Vì các yêu cầu của chuẩn đầu tiên (Sách Da cam) đa số là bất biến đối với các cơ chế thực hiện, cho nên chúng tỏ ra quá trừu tượng để trực tiếp có thể áp dụng trong nhiều trường hợp, do đó đòi hỏi cần có thêm các bình luận, bổ sung và mở rộng. "Các tiêu chí châu Âu" tiếp tục tiếp thu cách trình bày các yêu cầu của Sách Da cam, nhưng đi theo con đường phát triển nhanh và tích cực, có các mức và các yêu cầu đặc biệt cho các hệ thống mẫu (Hệ quản trị CSDL, hệ thống viễn thông…)

Về sự mềm dẻo thì tiêu chuẩn GTK của Nga còn thua cả Sách da cam. Nó rất cụ thể trong quy định hoá việc thực hiện các chức năng bảo vệ (Ví dụ, chỉ có GTK của Nga đưa ra yêu cầu mã hoá TT dưới dạng bắt buộc). Điều này là giảm đi sự thuận tiện trong áp dụng rất nhiều.

Cuối cùng, "Các tiêu chí chung" thực tế có một sự mềm dẻo hoàn hảo nhất, vừa có cơ chế Hồ sơ bảo vệ cho các khách hàng, vừa có cơ chế Đề án bảo vệ cho các nhà sản xuất và các chuyên gia kiểm chuẩn.

c) Tính đảm bảo

Tính đảm bảo của mức độ bảo vệ, lúc đầu được các nhà soạn thảo các tiêu chuẩn xem xét chỉ cho các mức an toàn cao nhất. Vì thế Sách Da cam coi là bắt buộc việc áp dụng các phương pháp kiểm chuẩn chính tắc (hình thức) chỉ đối với các hệ thống thuộc lớp A.

Tuy nhiên, sự cần thiết kiểm soát tính chính xác của thực hiện các yêu cầu và khẳng định hiệu quả của các TBBV cho các hệ thống thuộc mọi mức đã nhanh chóng được hiểu ra. Ngay trong "Các tiêu chí châu Âu" đã xuất hiện mục các yêu cầu đặc biệt – các yêu cầu đảm bảo, quy chế hoá công nghệ và công cụ thiết kế, sản xuất. CC xem xét tính đảm bảo thực hiện bảo vệ như là một thành tố quan trọng nhất của ATTT và nó đưa ra sự kiểm soát nhiều giai đoạn với quá trình sản xuất, cho phép khẳng định sự tương ứng của các kết

quả thu được với các mục tiêu đã đề ra, bằng cách chứng minh sự đảm bảo của các nhiệm vụ bảo vệ với các yêu cầu của khách hàng, sự đảm bảo của ĐTAT với "Các tiêu chí chung" và sự đảm bảo của sản phẩm CNTT với ĐTAT.

5.2.6.2. Xu thế phát triển của các tiêu chuẩn ATTT

Qua sự phân tích các tiêu chuẩn ATTT ở mục trên có thể chỉ ra các xu thế phát triển của các tiêu chuẩn ATTT sau đây:

1. Sự phát triển của các Tiêu chuẩn dẫn tới việc từ bỏ một thang đánh giá duy nhất phân cấp các yêu cầu và các tiêu chí, cũng dẫn đến việc thay thế chúng bằng tập các chỉ số riêng độc lập và đưa ra các thang đánh giá có trật tự từng phần.

2. Sự tăng lên không ngừng vai trò của các yêu cầu đảm bảo thực hiện bảo vệ và thực hiện CSAT chứng tỏ xu thế nghiêng về "chất" của đảm bảo an toàn hơn là "lượng" của nó.

3. Xác lập vai trò của nhà sản xuất, khách hàng và chuyên gia đánh giá sản phẩm CNTT và sự phân tách các chức năng của họ trong quá trình thiết lập các Hệ xử lý TT an toàn chứng tỏ về một sự tích hợp bình đẳng đầy đủ các tiêu chuẩn đảm bảo an toàn trong lĩnh vực CNTT.

4. Sự phân chia, đã hình thành trên cơ sở các tiêu chuẩn hiện đại về vai trò của những người tham gia vào quá trình thiết lập và khai thác các hệ thống an toàn; việc áp dụng các cơ chế và các công nghệ tương ứng đã dẫn đến một sự phân bố cân bằng trách nhiệm giữa tất cả các thành viên của quá trình.

5. Các xu thế hiện nay của quá trình tích hợp các CNTT và khát vọng vươn tới sự hình thành một không gian TT toàn cầu đã dẫn đến sự cần thiết toàn cầu hoá các tiêu chuẩn an toàn thông tin.

5.2.7. Cấu trúc

Bộ tiêu chuẩn ISO/IEC 27000 gồm các tiêu chuẩn sau:

ISO/IEC 27000 quy định các vấn đề về từ vựng và định nghĩa (thuật ngữ), các nguyên tắc cơ bản

ISO/IEC 27001:2005 các yêu cầu đối với hệ thống quản lý an toàn thông tin

ISO/IEC 27002:2007 qui phạm thực hành mô tả mục tiêu kiểm soát an toàn thông tin một các toàn diện và bảng lựa chọn kiểm soát thực hành an toàn tốt nhất

ISO/IEC 27003:2007 các hướng dẫn thực hiện hệ thống quản lý an ninh thông tin

ISO/IEC 27004:2007 đo lường và định lượng hệ thống quản lý an toàn thông tin để giúp cho việc đo lường hiệu lực của việc áp dụng ISMS

ISO/IEC 27005 quản lý rủi ro an toàn thông tin

ISO/IEC 27006 các yêu cầu đối với các cơ quan cung cấp kiểm toán và chứng nhận hệ thống quản lý an ninh thông tin

Và hiện nay bộ chuẩn này đang được xây dựng thêm. Trong số đó ta quan tâm đến chuẩn ISO/IEC 27001 nhiều hơn. Các tiêu chuẩn quốc tế ISO/IEC hiện được ứng dụng rộng rãi nhất là các tiêu chuẩn ISO/IEC 27001 và ISO/IEC 27002.

ISO/IEC 27001 là tiêu chuẩn quy định các yêu cầu đối với việc xây dựng và áp dụng hệ thống quản lý an toàn thông tin (Information Security Management System – ISMS) nhằm đảm bảo tính bảo mật (confidentiality), tính nguyên vẹn (integrity) và tính sẵn sàng (availability) đối với tài sản thông tin của các tổ chức/doanh nghiệp. Việc áp dụng một hệ thống quản lý an toàn thông tin sẽ giúp các tổ chức/doanh nghiệp ngăn ngừa, hạn chế các tổn thất trong sản xuất, kinh doanh liên quan tới việc hư hỏng, mất mát các thông tin, dữ liệu quan trọng.

ISO/IEC 27001 là một tiêu chuẩn trong bộ tiêu chuẩn ISO/IEC 27000 về quản lý an toàn thông tin. ISO/IEC 27001 cung cấp một đặc điểm kỹ thuật cho một thông tin hệ thống quản lý bảo mật (ISMS). Điều này bao gồm một số quy trình thiết kế, triển khai, duy trì và cập nhật một hệ thống ISMS. ISO/IEC 27001 có thể được dùng để chứng nhận ISMS theo tiêu chuẩn châu Âu EN45012 và hướng dẫn công nhận tiêu chuẩn ISO 27006 (trước đây EA 7/03).

ISO/IEC 27002 là một quy phạm thực hành quản lý an ninh thông tin. Nó được thiết kế để phục vụ như là một điểm tham chiếu cho việc xác định phạm vi điều khiển cần thiết cho hầu hết các trường hợp hệ thống thông tin được sử dụng. Mã thực hành này được bắt đầu như là tiêu chuẩn Anh BS

7799-1 vào năm 1995 và sau đó đã được phát hành như tiêu chuẩn quốc tế vào năm 2000 và sửa đổi năm 2005 phù hợp với các thủ tục thông thường của tiêu chuẩn ISO. Nó được đánh số lại theo tiêu chuẩn ISO/IEC 27002 trong năm 2007. Tiêu chuẩn này là tài liệu hướng dẫn và khuyến cáo cho 10 lĩnh vực an toàn: chính sách an toàn, tổ chức an toàn, quản lý tài sản, an toàn nguồn nhân lực, an toàn vật lý và môi trường, quản lý truyền thông và vận hành, quản lý truy cập, tiếp nhận, phát triển và bảo trì hệ thống thông tin, quản lý sự cố ATTT, quản lý liên tục và tuân thủ. ISO/IEC 27002 còn chỉ ra 39 bài toán quản lý và khuyến cáo nhiều biện pháp thực hành quản lý an toàn.

5.2.8. Các bước triển khai

Việc ứng dụng Công nghệ thông tin và truyền thông (ICT) vào hoạt động của các tổ chức, doanh nghiệp bắt đầu phổ biến từ những năm 90 của thế kỷ 20. Đến nay hoạt động của mỗi tổ chức không thể tách rời hệ thống thông tin dựa trên nền tảng ICT, do đó, bảo đảm an ninh cho hệ thống này đã trở nên tất yếu và cấp bách.

Xây dựng các giải pháp để đảm bảo an ninh cho hệ thống thông tin là một vấn đề phức tạp và luôn được nghiên cứu phát triển. Gần đây, cách tiếp cận bảo đảm an ninh thông tin cho tổ chức theo các hướng dẫn của bộ tiêu chuẩn ISO/IEC 27001 và ISO/IEC 27002 được xem là toàn diện và triệt để nhất. Phần này sẽ điểm qua những nội dung chính và các bước cơ bản triển khai các tiêu chuẩn này tại một tổ chức.

Trong bộ tiêu chuẩn ISO/IEC 27001/27002, khái niệm bảo đảm an ninh thông tin được hiểu là duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin. Ba tính chất này được viết tắt bằng nhóm từ tiếng Anh: CIA, trong đó C là tính bí mật (Confidentiality); I là tính toàn vẹn (Integrity); và A là tính sẵn sàng (Availability). Tính bí mật đảm bảo rằng chỉ người được phép mới có thể truy cập thông tin. Tính toàn vẹn đảm bảo sự chính xác và đầy đủ của thông tin và các phương pháp xử lý thông tin. Tính sẵn sàng đảm bảo người sử dụng được phép có thể truy cập thông tin và các tài sản tương ứng khi cần. Ba thuộc tính này luôn luôn là các tiêu chuẩn để kiểm chứng mức độ bảo đảm an ninh của thông tin và hệ thống thông tin.

Thông tin còn gắn liền với ba yếu tố là con người, quy trình nghiệp vụ và hạ tầng kỹ thuật. Trong đó hạ tầng kỹ thuật bao gồm mạng máy tính và các thiết bị lưu trữ, xử lý truyền nhận thông tin và các môi trường kỹ thuật liên quan. Quy trình nghiệp vụ là các quy trình xử lý thông tin. Yếu tố con người phải kể đến quá trình vận hành, xử lý thông tin, khai thác và sử dụng thông tin. Do vậy người ta cũng có thể hiểu hệ thống thông tin bao gồm: thông tin (dữ liệu), hạ tầng kỹ thuật, quy trình nghiệp vụ và tác động của con người. Giải pháp cho an ninh thông tin chính là các biện pháp tác động tới yếu tố con người, quy trình nghiệp vụ và hạ tầng kỹ thuật để thông tin đảm bảo được 3 thuộc tính: bảo mật, toàn vẹn và sẵn sàng.

Triển khai an ninh thông tin phải là một quá trình thường xuyên, liên tục, không chỉ thực hiện một lần là hoàn tất. Hệ thống an ninh thông tin sau khi được xây dựng và đi vào hoạt động phải được định kỳ đánh giá để phát hiện ra các điểm yếu, các mối đe dọa mới, từ đó có kế hoạch nâng cấp, hoàn thiện. Người ta thường mô tả quy trình này bằng cụm từ P.D.C.A, trong đó P: Plan - lập kế hoạch, D: Do - thực hiện, C: Check - kiểm tra đánh giá và A: Act - hiệu chỉnh, nâng cấp.

Tiêu chuẩn quốc tế ISO/IEC 27001, cung cấp mô hình chuẩn để thiết lập, triển khai, vận hành, theo dõi, đánh giá, duy trì, cải tiến hệ thống quản lý an ninh thông tin. Còn tiêu chuẩn ISO/IEC 27002 là một hệ thống các biện pháp, các khuyến cáo để đảm bảo cho an toàn thông tin, đảm bảo cho các yêu cầu đặt ra trong ISO/IEC 27001 được thực hiện.

Mô hình mà ISO/IEC 27001 đề xuất là xây dựng một Hệ thống quản lý an ninh thông tin. Hệ thống này bao gồm: một nhóm nhân sự chuyên trách vận hành quản lý các công việc liên quan đến an ninh thông tin; các chính sách, quy định, tiêu chuẩn, hướng dẫn thực hiện an ninh thông tin và các công nghệ đảm bảo an ninh thông tin. Các nội dung trên điều chỉnh cả 3 yếu tố là con người, quy trình nghiệp vụ và hạ tầng kỹ thuật.

Để xây dựng và triển khai hệ thống ISMS, sau khi xây dựng khung chính sách cho an ninh thông tin, các tổ chức phải khảo sát và liệt kê đầy đủ các "tài sản" của hệ thống thông tin trong đơn vị. Có thể hiểu tài sản bao gồm toàn bộ thông tin và các danh mục hỗ trợ liên quan (như máy móc thiết bị, thương hiệu của đơn vị, mối quan hệ và danh sách khách hàng truyền thống...)

mà nhờ đó tổ chức có thể hoạt động một cách bình thường. Các tài sản này được phân loại về tầm quan trọng, các điểm yếu trong quá trình hoạt động, các mối đe dọa có thể xảy ra đối với chúng. Phân tích các rủi ro có thể xảy ra cho các tài sản khi các mối đe dọa tác động ngay vào các điểm yếu để tạo ra các lỗi nhỏ hoặc các sự cố nghiêm trọng. Phân loại các rủi ro nhằm xây dựng các biện pháp để loại bỏ rủi ro, hoặc giảm thiểu đến mức thấp nhất các thiệt hại nếu rủi ro có thể xảy ra.

Tiêu chuẩn ISO/IEC 27001 khuyến cáo những nội dung chính của hệ thống ISMS bao gồm: Xây dựng tổ chức (nhóm chuyên trách) về an ninh thông tin; xây dựng chính sách an ninh thông tin; quản lý tài sản; quản lý nguồn nhân lực; quản lý bảo mật mức vật lý; quản lý vận hành và trao đổi thông tin; quản lý truy cập; quản lý quy trình phát triển các ứng dụng; quản lý các sự cố liên quan đến bảo mật thông tin; quản lý khắc phục các thảm họa; quản lý các vấn đề liên quan tới pháp luật. Trong đó nhóm chuyên trách về an toàn thông tin (làm việc toàn bộ thời gian) có thể mở rộng để phối hợp với các bộ phận khác nhau trong tổ chức (các thành viên mở rộng làm việc kiêm nhiệm). Hoạt động của nhóm phải diễn ra thường xuyên, liên tục để kiểm tra tính tuân thủ các quy tắc, biện pháp đã được xây dựng và cải tiến cập nhật từ mức chính sách cho đến các giải pháp công nghệ. Quy trình hoạt động tuân thủ chu trình P.D.C.A như đã giới thiệu ở trên.

Hiện nay, việc áp dụng hệ thống quản lý an toàn thông tin ISO/IEC 27001 đã được triển khai rộng khắp ở hầu hết các quốc gia trên thế giới. Tại Việt nam, thời gian qua một số tổ chức ngân hàng, tài chính,công nghệ thông tin,… cũng bắt đầu quan tâm triển khai áp dụng hệ thống này và bước đầu đã có được những kết quả nhất định.

Tiêu chuẩn ISO/IEC 27001:2005 có thể được áp dụng rộng rãi cho nhiều loại hình tổ chức (các tổ chức thương mại, cơ quan nhà nước, các tổ chức phi lợi nhuận…). Đặc biệt là các tổ chức mà các hoạt động phụ thuộc nhiều vào công nghệ thông tin, máy tính, mạng máy tính, sử dụng cơ sở dữ liệu như: ngân hàng, tài chính, viễn thông,…Một hệ thống ISMS hiệu lực, phù hợp, đầy đủ sẽ giúp bảo vệ các tài sản thông tin cũng như đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng… của tổ chức.

ISO/IEC 27001 là một phần của hệ thống quản lý chung của các tổ chức, doanh nghiệp do vậy có thể xây dựng độc lập hoặc kết hợp với các hệ thống quản lý khác như ISO 9000, ISO 14000...

Về cơ bản, các bước triển khai hệ thống ISO/IEC 27001 có nhiều điểm tương đồng với áp dụng ISO 9000 & ISO 14000… Tuy nhiên, đây là hệ thống quản lý an toàn thông tin nên có một số điểm cần chú trọng khi xây dựng như: xác định đầy đủ các tài sản thông tin, nhận biết và đánh giá mối nguy, lựa chọn các biện pháp xử lý mối nguy thích hợp…

Các bước cơ bản cần thực hiện để đạt được chứng nhận hệ thống quản lý an toàn thông tin ISO/IEC 27001:

1) Cam kết của Lãnh đạo về xây dựng hệ thống quản lý an toàn thông tin cho tổ chức

2) Phổ biến, đào tạo nhận thức về tiêu chuẩn ISO/IEC 27001 cho cán bộ

3) Thiết lập hệ thống tài liệu theo yêu cầu tiêu chuẩn ISO/IEC 27001

4) Xây dựng chính sách, mục tiêu và phạm vi của hệ thống ISMS

5) Phân tích, đánh giá các rủi ro về an toàn thông tin trong phạm vi của hệ thống

6) Thiết lập các biện pháp kiểm soát rủi ro

7) Lựa chọn mục tiêu và các biện pháp kiểm soát

8) Vận hành hệ thống ISMS đã thiết lập

9) Thực hiện các hoạt động xem xét và cải tiến hiệu lực hệ thống.

10) Đánh giá chứng nhận.

Thời gian cần thiết để xây dựng hệ thống quản lý an toàn thông tin có hiệu lực và hiệu quả cho đến khi đánh giá chính thức cần khoảng 9 ~ 18 tháng phụ thuộc vào quy mô, nhu cầu thực tế, khả năng tập trung nguồn lực của tổ chức cho quá trình xây dựng. Tổ chức cũng sẽ thuận lợi hơn nếu trước đó đã có kinh nghiệm xây dựng, vận hành một số hệ thống quản lý khác như ISO 9000, ISO 14000…

Theo đánh giá của một số chuyên gia, triển vọng áp dụng ISO/IEC 27001 tại Việt Nam là khá cao. ISO/IEC 27001 đã được các cơ quan chuyên trách của chính phủ (Tổng cục Tiêu chuẩn Đo lường chất lượng, Bộ Thông tin và Truyền thông…) khuyến cáo áp dụng rộng rãi trong cả nước. Ngoài ra, yêu

cầu về đảm bảo an ninh thông tin của khách hàng, đối tác cũng ngày một cao hơn, đòi hỏi các tổ chức, doanh nghiệp phải áp dụng ISO/IEC 27001 để tăng cường sức cạnh tranh và nâng cao thương hiệu cho chính mình.

Trong thời gian tới đây, ISO/IEC 27001 sẽ thu hút được sự quan tâm của các doanh nghiệp, tổ chức thuộc lĩnh vực tài chính (ngân hàng, chứng khoán, bảo hiểm) và các tổ chức, cơ quan Nhà nước trong lĩnh vực quốc phòng, an ninh. ISO/IEC 27001 được kỳ vọng sẽ tạo được sự quan tâm như ISO 9000 trong thập niên 90.

5.3. CÂU HỎI

1. Nêu tóm tắt lịch sử phát triển của các tiêu chuẩn ATTT?
2. Đánh giá ATTT là gì? Sản phẩm CNTT là gì?
3. Hồ sơ bảo vệ, Đề án bảo vệ là gì?
4. Nêu sự phân loại các yêu cầu và các tiêu chí của Sách Da cam của Bộ quốc phòng Mỹ.
5. Hãy nêu các yêu cầu chức năng và các tiêu chí đảm bảo của “Các tiêu chí châu Âu”.
6. Nêu các ưu điểm và nhược điểm của Hệ tiêu chí ATTT GTK của Liên bang Nga.
7. Trình bày cấu trúc của Hồ sơ bảo vệ và Đề án bảo vệ trong “Các tiêu chí chung”. Nói rõ vai trò của hai cơ chế này trong quá trình thiết kế, sản xuất và kiểm chuẩn sản phẩm CNTT.
8. Tóm tắt các yêu cầu chức năng và các yêu cầu đảm bảo của “Tiêu chí chung” .
9. Hãy phân tích về tính tổng quát và tính mềm dẻo trong các tiêu chuẩn ATTT.
10. Phân tích các xu thế phát triển của các tiêu chuẩn ATTT hiện đại.

TÀI LIỆU THAM KHẢO

[1] TS. Nguyễn Đình Vinh, *Giáo trình cơ sở an toàn thông tin*, Học viện Kỹ thuật Mật mã, (Năm 2006)

[2] TS. Nguyễn Nam Hải, *Giáo trình an toàn mạng*, Học viện Kỹ thuật Mật mã, (Năm 2006)

[3] Jason Andress, *The basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice*, ISBN 978-1-59749-653-7, 190pp, Russ Rogers, (Năm 2011)

[4] Thomas R. Peltier, Justin Peltier, John Blackley, *Information Security Fundamentals*, ISBN 0-8493-1957-9, 262pp, CRC Press LLC, (Năm 2005)

[5] Dr. Michael E.whitman, Herbert J.Mattord, CISSP, *Principles of information security, second edition*, ISBN – 13: 978 – 0 – 619 – 21625 – 2, ISBN – 10: 0 – 619 – 21625 - 5

[6] Tom Carr, *BS ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements*, ISBN 0 580 46781 3, (Năm 2005)

[7] Pascal Steichen, "*Principles and fundamentals of security: methodologies of information systems – Introduction"*, http://pst.libre.lu/m2ssic-metz/archive/2010-2011/01_intro-art.pdf

[8] "*Phòng ngự chiều sâu"*, 12/3/2013, http://vi.wikipedia.org/wiki/Ph%C3%B2ng_ng%E1%BB%B1_chi%E1%BB%81u_s%C3%A2u

[9] ThS. Trần Nguyên Vũ, "*Ứng dụng ISO 27001/27002: Cách tiếp cận toàn diện cho an ninh hệ thống thông tin"*, 05/10/2008, http://antoanthongtin.vn/Detail.aspx?CatID=5a918474-446c-47ca-8e21-a889bc2c8fd3&NewsID=358f794f-4ad9-463d-b770-dc9b56e924a8

[10] "*Giới thiệu về bộ tiêu chuẩn ISO 27000 TOOLKIT"*, 03/01/2012, Trung tâm Thông tin Tiêu chuẩn Đo lường Chất lượng, http://www.tcvninfo.org.vn/index.php?language=vi&nv=news&op=Gioi-thieu-cac-bo-tieu-chuan-moi/Gioi-thieu-ve-bo-tieu-chuan-ISO-27000-TOOLKIT-810

[11] TS. Đào Thế Long, "*An toàn thông tin – Nên bắt đầu từ đâu"*, Misoft ISTC, http://www.isystem.com.vn/News/Bao-mat-he-thong/Kinh-nghiem-bao-mat/2106/An-toan-thong-tin-Nen-bat-dau-tu-dau.aspx

[12] Nguyễn Hương Giang, "*Xây dựng hệ thống quản lý An ninh thông tin theo Tiêu chuẩn ISO/IEC 27001:2005"*, 05/04/2010, http://antoanthongtin.vn/Detail.aspx?NewsID=5d882d2e-166c-4a60-8286-1b6160dea9e2&CatID=b452f747-554b-40e6-ab3b-7af1ee3b6a3d

[13] TS. Trần Đức Lịch, "*Quá trình hình thành các tiêu chuẩn an toàn thông tin"*, Ban Cơ yếu Chính phủ, 25/06/2013, http://antoanthongtin.vn/QualityDetail.aspx?NewsID=3af39430-c66d-4726-aaea-9bc1668d59f3&CatID=ddaac893-0257-433b-9ba3-e60cdd949aa3

[14] "*Khu phi quân sự"*, http://vi.wikipedia.org/wiki/DMZ

[15] "*Information security: Physical security checklist"*, The Department for Business, Enterprise and Regulatory Reform, http://www.berr.gov.uk/files/file49964.pdf

[16] "*Information security: How to write an information security"*, The Department for Business, Enterprise and Regulatory Reform, http://www.bis.gov.uk/files/file49963.pdf