TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

AN TOÀN THÔNG TIN INFORMATION SECURITY

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Giảng viên: TS. Trần Thế Vinh

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

TRẬN ĐÁNH WATERLOO

18 tháng 6 năm 1815 (11:35 - 20:00)
140 000 binh lính
11,5 giờ

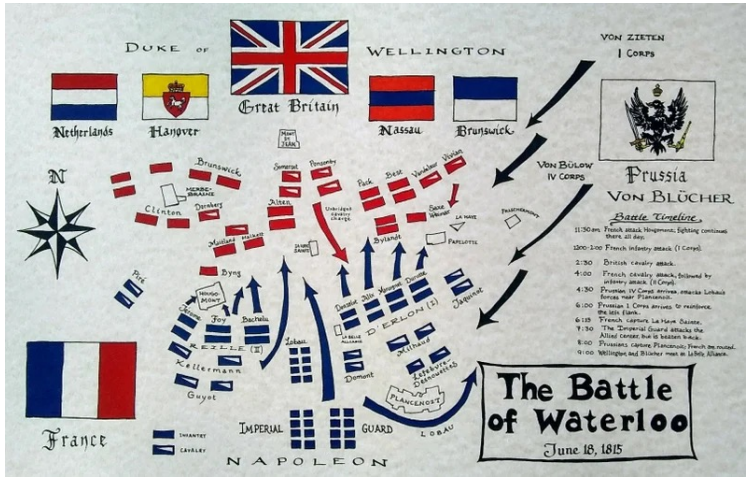
Napoleon Bonaparte

Thống chế Công tước Wellington

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

Nathan Rothschild (1777 — 1836)

Khi bắt đầu trận chiến, lợi thế nghiêng về phía Napoléon, và các nhà quan sát ở London nói rằng ông sẽ giành chiến thắng. Nhưng quân đoàn Phổ của Blücher đã đến viện trợ cho quân Anh dưới sự lãnh đạo của Wellington. Đồng minh đã thắng. Napoléon chạy trốn đến Brussels. Rothschild là người duy nhất nhận được thông tin về việc này.



Mọi người đều tin rằng Wellington đã thua trận. Sau đó, Rothschild ngay lập tức bắt đầu bán trái phiếu của mình trên sàn chứng khoán. Mọi người bắt đầu bán theo anh ta. Kết quả là giá cổ phiếu giảm xuống gần như bằng không. Tại thời điểm này, các đại lý của Rothschild đã mua lại cổ phiếu với giá rẻ. Vào ngày 21 tháng 6, lúc 11 giờ tối, phụ tá của Wellington là Thiếu tá Henry Percy chuyển báo cáo của thống chế cho chính phủ: "Napoléon đã bị đánh bại.“

Như vậy, Nathan Rothschild đã kiếm được 40 triệu bảng nhờ tin tức này. Thông tin thực, nhận được trước những người khác, cho phép Rothschilds tiến hành một trò chơi đôi bên cùng có lợi trên sàn giao dịch chứng khoán với khối lượng lớn chưa từng có.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

«Ai sở hữu thông tin
- Người đó sở hữu cả thế giới»

Nathan Rothschild

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

TẠI SAO NHIỆM VỤ BẢO VỆ THÔNG TIN LẠI TRỞ THÀNH NHIỆM VỤ CẤP THIẾT HIỆN NAY?

Một số loại thông tin đã được bảo vệ từ thời cổ đại:

-Bí mật quân sự (quân đội),

-Bí mật nhà nước (ngoại giao).

Đầu những năm 1990 Internet trên thế giới xuất hiện.

Đến cuối những năm 1990, "An Toàn Thông Tin"(Information Security) bắt đầu được nghiên cứu chuyên sâu tại các trường đại học hàng đầu thế giới.

– An ninh mạng và bảo mật thông tin

Tại sao?

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

CÁC PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

1. Bảo vệ vật lý:

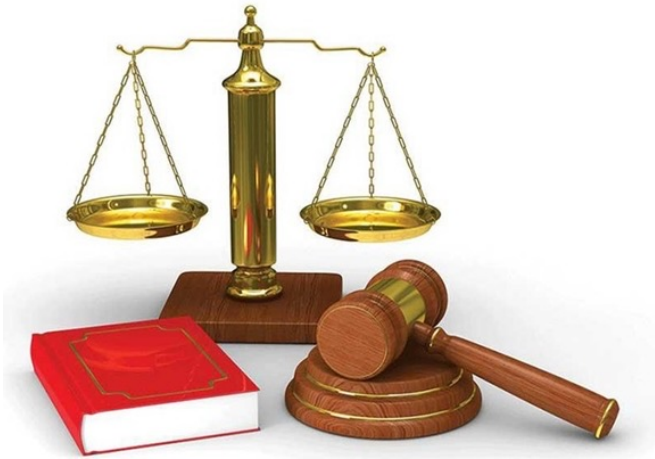
Bảo vệ thông tin vật lý. Bảo vệ thông tin bằng cách áp dụng các biện pháp của tổ chức và một tập hợp các phương tiện can thiệp vào sự xâm nhập hoặc truy cập trái phép của các cá nhân vào đối tượng được bảo vệ.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

CÁC PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

2. Bảo vệ thông qua tổ chức và luật pháp.

Đây là hoạt động bảo vệ thông tin bằng các phương pháp pháp lý, bao gồm việc xây dựng các văn bản pháp luật lập pháp và điều chỉnh (các hành vi), điều chỉnh các mối quan hệ của các chủ thể được bảo vệ thông tin, việc áp dụng các tài liệu (hành vi) này, cũng như giám sát và kiểm soát việc thực hiện chúng.



KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

CÁC PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

3. Bảo vệ bằng các thiết bị công nghệ.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

CÁC PHƯƠNG PHÁP BẢO VỆ THÔNG TIN

4. Phương pháp mật mã và kỹ thuật dấu tin

là phương pháp mã hóa thông tin và che giấu thực tế truyền thông tin

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

CÂU CHUYỆN CÁI ĐẦU CỦA NÔ LỆ

Khái niệm về steganography (giấu tin) có từ thời Alexander Đại đế. Truyền thuyết đã mang đến cho chúng ta phương pháp được sử dụng để truyền những bí mật quân sự: một nô lệ được chọn để đưa ra thông điệp, anh ta bị cạo trọc đầu và xăm chữ. Sau khi tóc mọc trở lại, người nô lệ được đưa lên đường. Người nhận tin nhắn lại cắt tóc đầu nô lệ và đọc tin nhắn.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

LỊCH SỬ NGẮN GỌN VỀ MẬT MÃ

Lịch sử của mật mã là khoảng 4 nghìn năm tuổi. Lịch sử của mật mã có thể được chia thành 4 giai đoạn.

1. Naive cryptography.
2. Formal cryptography
3. Scientific cryptography
4. Computer cryptography

Mật mã cổ đại (Naive cryptography) (trước đầu thế kỷ 16) được đặc trưng bởi việc sử dụng bất kỳ phương pháp nào (thường là nguyên thủy) để gây nhầm lẫn cho kẻ thù về nội dung của các văn bản được mã hóa (mật mã Caesar và Polybius).

Giai đoạn Formal cryptography (cuối thế kỷ 15 - đầu thế kỷ 20) gắn liền với sự xuất hiện của mật mã chính thức hóa và tương đối chống lại mật mã tiết lộ thủ công.

Đặc điểm phân biệt chính của mật mã khoa học (Scientific cryptography) (những năm 30 - 60 của thế kỷ XX) là sự xuất hiện của các hệ thống mật mã với sự biện minh toán học chặt chẽ về độ bền mật mã.

Mật mã máy tính (Computer cryptography) (từ những năm 70 của thế kỷ 20) nhờ sự xuất hiện của các thiết bị tính toán có hiệu suất đủ để thực hiện các hệ thống mật mã cung cấp mã hóa tốc độ cao

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên v.v đều được lưu trữ trên hệ thống máy tính.

Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh, yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của doanh nghiệp.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

HIỂM HỌA TRONG AN TOÀN THÔNG TIN

Trước hết ta xem xét các hiểm họa có trên hệ thống và phân loại chúng. Các hiểm họa đối với hệ thống có thể được phân loại thành:

- **Hiểm họa vô tình:** khi người dùng khởi động lại hệ thống ở chế độ đặc quyền, họ có thể tùy ý chỉnh sửa hệ thống. Nhưng sau khi hoàn thành công việc họ không chuyển hệ thống sang chế độ thông thường, vô tình để kẻ xấu lợi dụng.
- **Hiểm họa cố ý:** như cố tình truy cập vào hệ thống một cách trái phép.
- **Hiểm họa bị động:** là hiểm họa nhưng chưa hoặc không tác động trực tiếp lên hệ thống, như nghe trộm các gói tin trên đường truyền.
- **Hiểm họa chủ động:** là việc sửa đổi thông tin, thay đổi tình trạng hoặc hoạt động của hệ thống.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

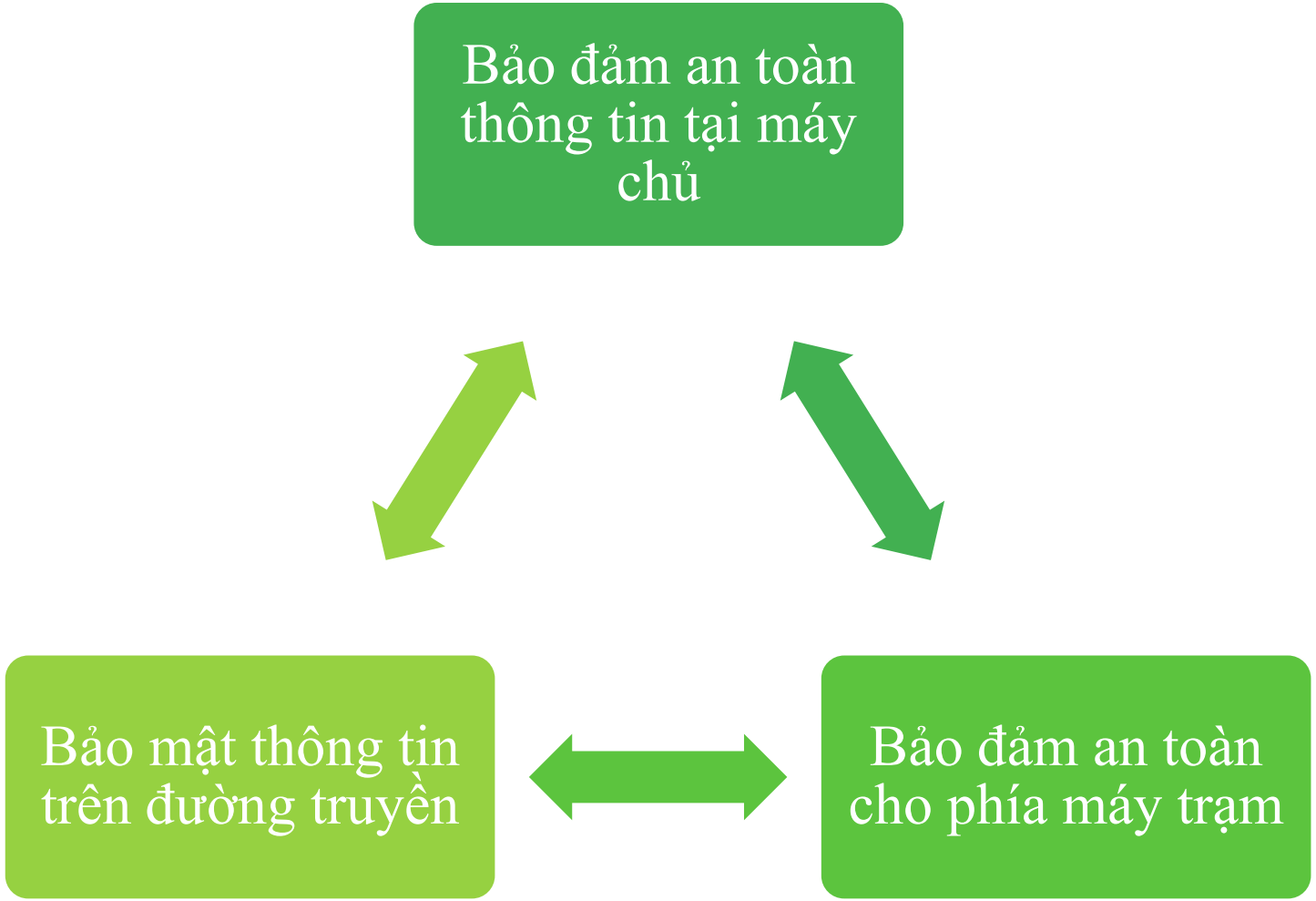
CÁC MỐI ĐE DỌA TRONG AN TOÀN THÔNG TIN

Đối với mỗi hệ thống thông tin, mối đe dọa và hậu quả tiềm ẩn là rất lớn, nó có thể xuất phát từ những nguyên nhân sau:

- **Từ phía người sử dụng:** xâm nhập bất hợp pháp, ăn cắp tài sản có giá trị.
- **Trong kiến trúc hệ thống thông tin:** tổ chức hệ thống kỹ thuật không có cấu trúc hoặc không đủ mạnh để bảo vệ thông tin.
- **Ngay trong chính sách bảo mật an toàn thông tin:** không chấp hành các chuẩn an toàn, không xác định rõ các quyền trong vận hành hệ thống.
- **Thông tin trong hệ thống máy tính** cũng sẽ dễ bị xâm nhập nếu không có công cụ quản lý, kiểm tra và điều khiển hệ thống.
- Nguy cơ hay lỗ hổng nằm ngay trong **cấu trúc phần cứng** của các thiết bị tin học và **trong phần mềm hệ thống** và **ứng dụng** do hãng sản xuất cài sẵn các loại 'rệp' điện tử theo ý đồ định trước, gọi là 'bom điện tử'.
- Nguy hiểm nhất đối với mạng máy tính là **tin tặc**, từ phía bọn tội phạm.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

NHIỆM VỤ BẢO ĐẢM AN TOÀN THÔNG TIN



KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

NHIỆM VỤ BẢO ĐẢM AN TOÀN THÔNG TIN

❖ An toàn thông tin đã thay đổi rất nhiều trong thời gian gần đây. Trước kia, hầu như chỉ có nhu cầu bảo mật thông tin, nay đòi hỏi thêm nhiều yêu cầu mới như **an ninh tại máy chủ** và **trên mạng**.

❖ Trước kia, các phương pháp truyền thống được cung cấp bởi các cơ chế hành chính và phương tiện vật lý như: nơi lưu trữ bảo vệ các tài liệu quan trọng và cung cấp giấy phép được quyền sử dụng các tài liệu mật đó.

❖ Ngày nay, máy tính đòi hỏi các phương pháp tự động để bảo vệ các tệp và các thông tin lưu trữ. Nhu cầu bảo mật rất lớn và rất đa dạng, có mặt khắp mọi nơi, mọi lúc. Do đó, **không thể không** đề ra các qui trình tự động hỗ trợ bảo đảm an toàn thông tin.

❖ Việc sử dụng mạng và truyền thông đòi hỏi phải có các phương tiện bảo vệ dữ liệu khi truyền. Trong đó có cả các phương tiện **phần mềm** và **phần cứng**, đòi hỏi có những nghiên cứu mới đáp ứng các bài toán thực tiễn đặt ra.

KIẾN THỨC CHUNG VỀ AN TOÀN THÔNG TIN

GIẢI PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

- An ninh bao gồm cả việc truyền và truyền trên mạng càng không đơn giản. Yêu cầu là bảo mật, xác thực, chống từ chối và toàn vẹn.
- Trong khi phát triển cơ chế bảo mật và thuật toán, cần phải xem xét các tấn công có thể x. Đôi khi kẻ tấn công nhìn nhận vấn đề dưới góc độ khác, nên chúng khai thác được các điểm yếu của hệ thống.
- Đã có các cơ chế an ninh rồi, còn cần phải quyết định dùng chúng ở đâu, trên giao thức nào, ở thiết bị nào và thông qua các dịch vụ gì.
- Cơ chế an ninh thông thường bao gồm nhiều **thuật toán và giao thức**, nhiều bên tham gia, ví dụ như muốn mã hóa, thì hai bên phải chia sẻ khóa mật, các thuật toán mã hóa và giải mã. Rồi việc phân phối khóa giữa người gửi và người nhận, khung thời gian cho việc truyền.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

Bảo vệ thông tin - cung cấp ba nhiệm vụ chính:

1. Đảm bảo bí mật thông tin (Confidentiality).
2. Đảm bảo tính toàn vẹn của thông tin (Integrity).
3. Đảm bảo sự sẵn sàng (Availability) của thông tin.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

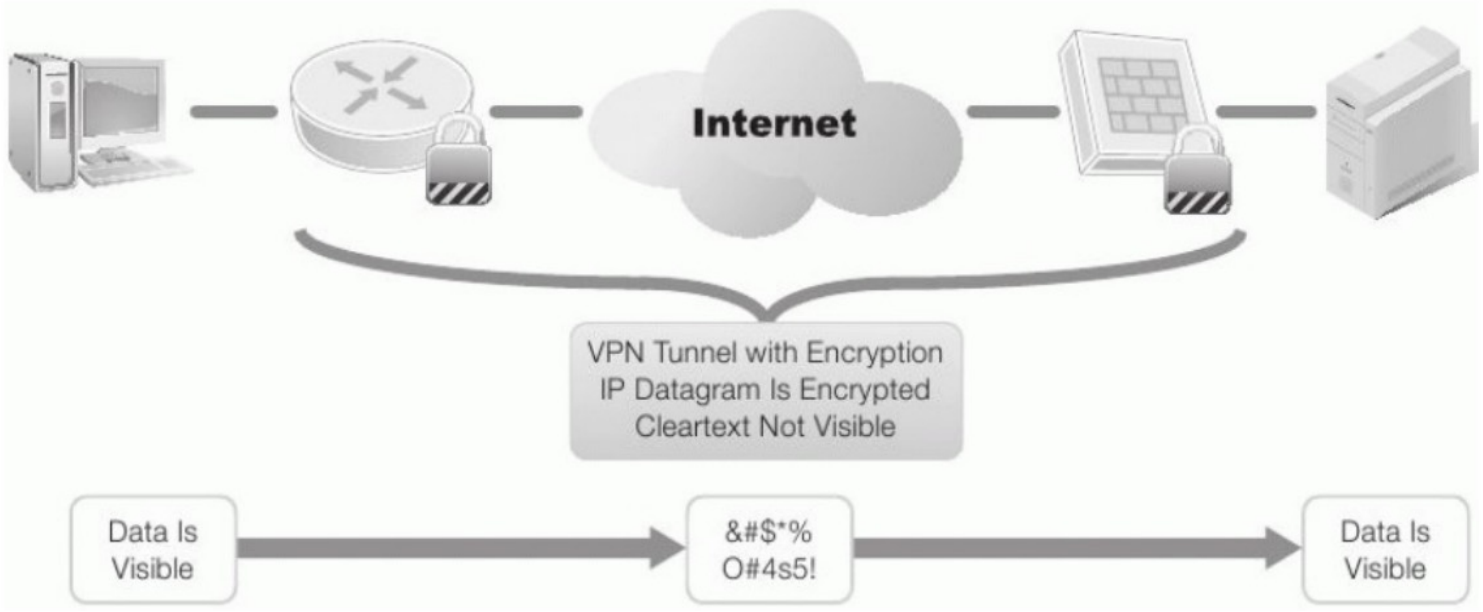
CÁC YÊU CẦU ĐẢM BẢO AN TOÀN THÔNG TIN

Tính bí mật (Confidentiality): chỉ người dùng có thẩm quyền mới được truy nhập thông tin.

Các thông tin bí mật có thể gồm:

- Dữ liệu riêng của cá nhân;
- Các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan/tổ chức;
- Các thông tin có liên quan đến an ninh quốc gia.

Tính bí mật có thể được đảm bảo bằng kênh mã hóa VPN



CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

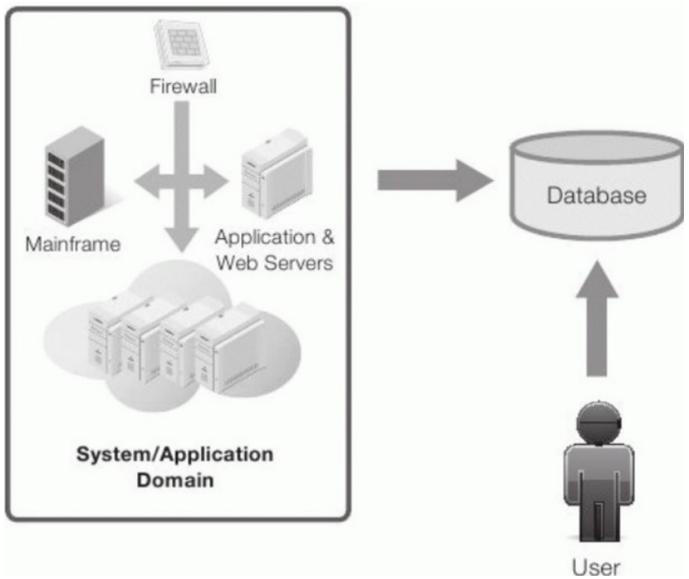
CÁC YÊU CẦU ĐẢM BẢO AN TOÀN THÔNG TIN

Tính toàn vẹn (Integrity): thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu.

- Trong nhiều tổ chức, thông tin có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế;
- Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin.

Dữ liệu là toàn vẹn nếu:

- Dữ liệu không bị thay đổi;
- Dữ liệu hợp lệ;
- Dữ liệu chính xác.



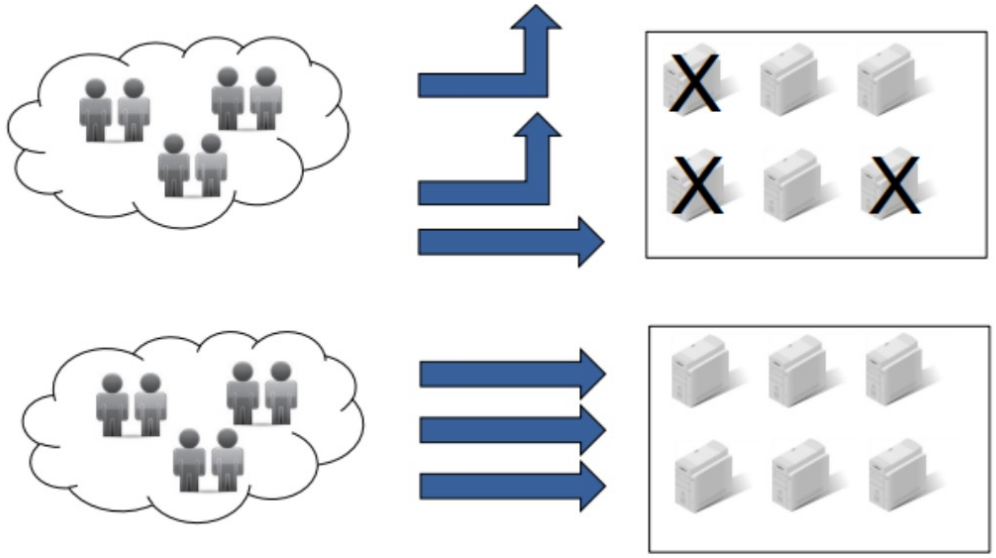
CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC YÊU CẦU ĐẢM BẢO AN TOÀN THÔNG TIN

Tính sẵn sàng (Availability): thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.

Tính sẵn có có thể được đo bằng các yếu tố:

- Thời gian cung cấp dịch vụ (Uptime);
- Thời gian ngừng cung cấp dịch vụ (Downtime);
- Tỷ lệ phục vụ: A = (Uptime)/(Uptime + Downtime);
- Thời gian trung bình giữa các sự cố;
- Thời gian trung bình ngừng để sửa chữa;
- Thời gian khôi phục sau sự cố.

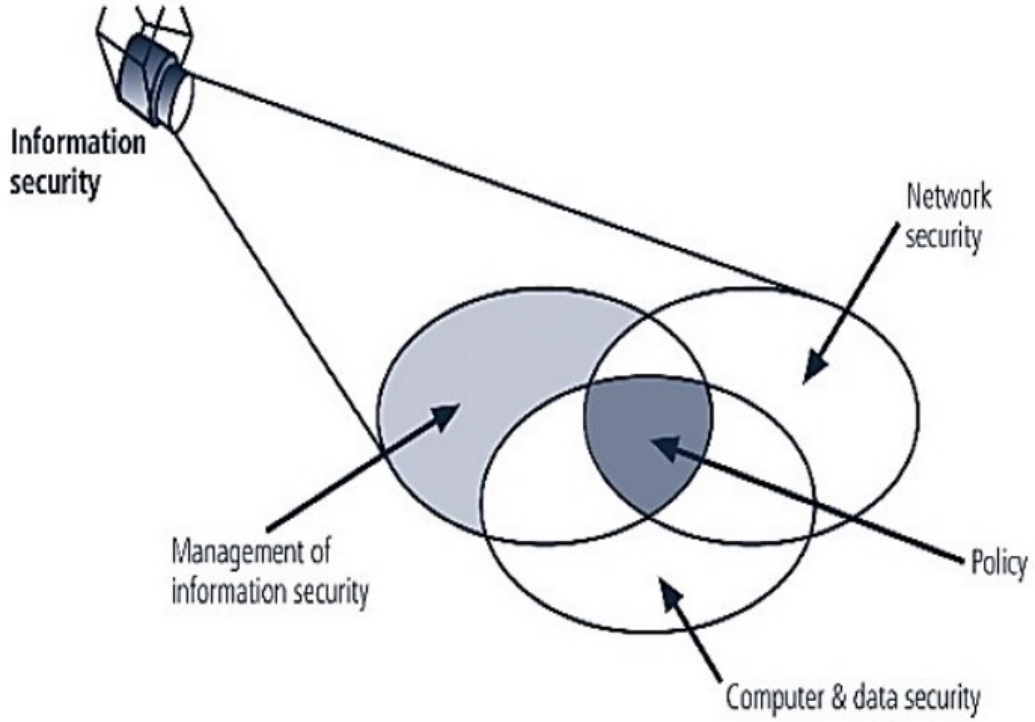


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC THÀNH PHẦN CỦA AN TOÀN THÔNG TIN

Các thành phần của AN TOÀN THÔNG TIN:

- An toàn máy tính và dữ liệu (Computer and data security)
- An ninh mạng (Network security)
- Quản lý AN TOÀN THÔNG TIN (Management of information security)
- Chính sách AN TOÀN THÔNG TIN (Policy)



CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC THÀNH PHẦN CỦA AN TOÀN THÔNG TIN

An toàn máy tính và dữ liệu:

- Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ;
- Vấn đề điều khiển truy nhập;
- Vấn đề mã hóa và bảo mật dữ liệu;
- Vấn đề phòng chống phần mềm độc hại;
- Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC THÀNH PHẦN CỦA AN TOÀN THÔNG TIN

An ninh mạng:

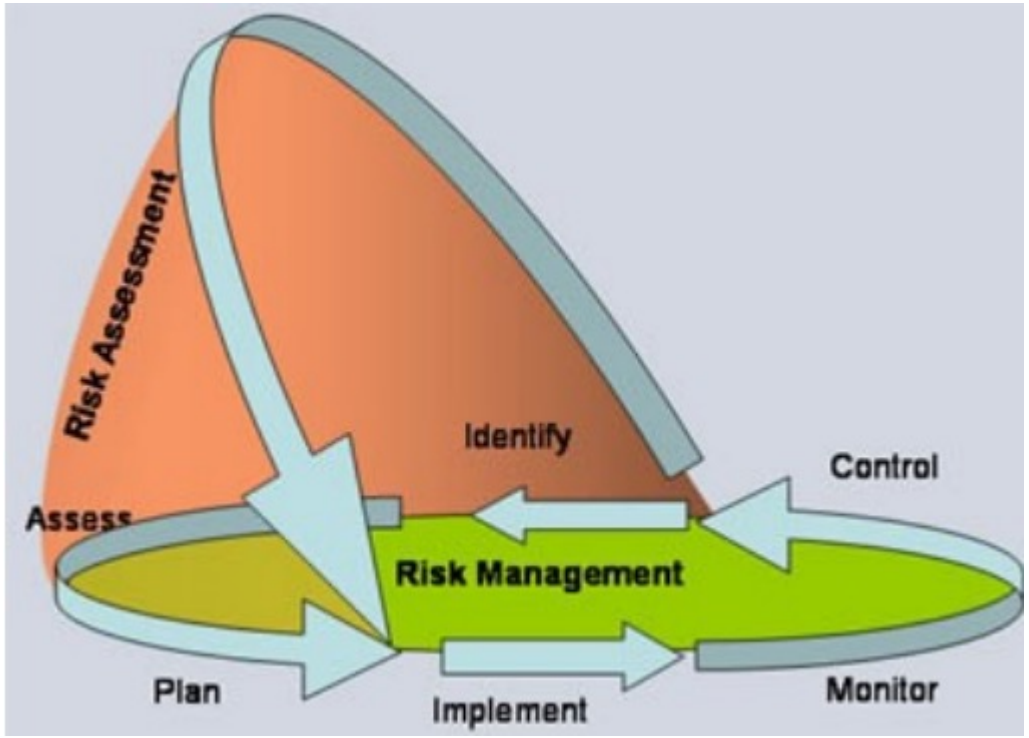
- Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập;
- Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- Vấn đề giám sát mạng.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC THÀNH PHẦN CỦA AN TOÀN THÔNG TIN

Quản lý an toàn thông tin:

- Quản lý rủi ro
- Nhận dạng
- Đánh giá
- Thực thi quản lý an toàn thông tin
- Lập kế hoạch (Plan)
- Thực thi kế hoạch (Do/Implement)
- Giám sát kết quả thực hiện (Monitor)
- Thực hiện các kiểm soát (Control).

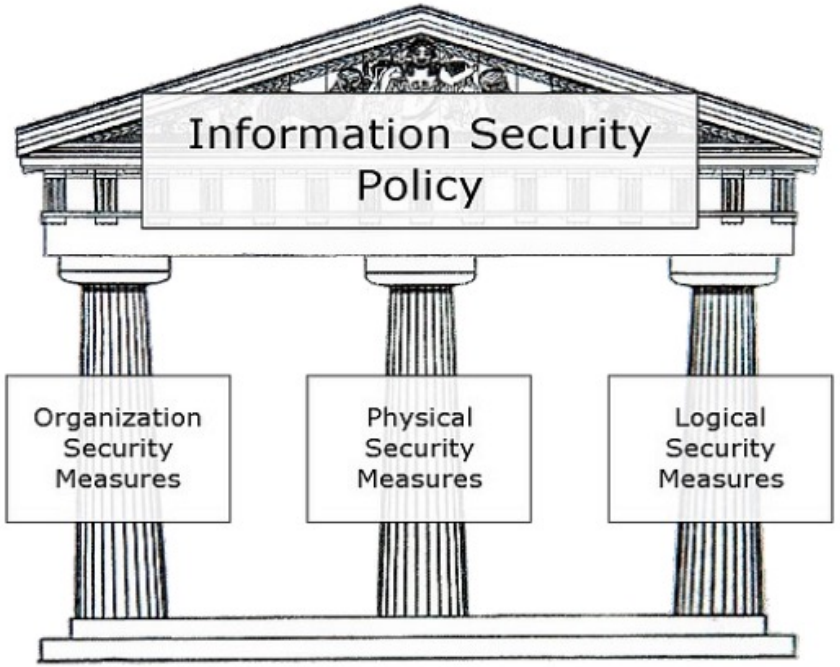


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC THÀNH PHẦN CỦA AN TOÀN THÔNG TIN

Chính sách an toàn thông tin:

- Chính sách an toàn ở mức vật lý (Physical security policy)
- Chính sách an toàn ở mức tổ chức (Organizational security policy)
- Chính sách an toàn ở mức logic (Logical security policy).

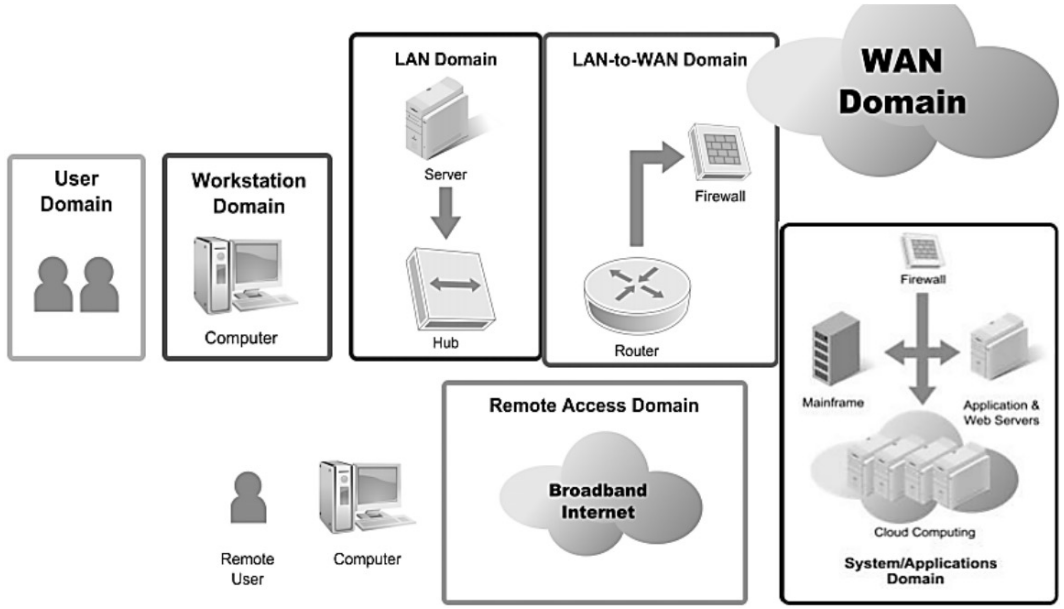


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các vùng trong hạ tầng CNTT:

- Vùng người dùng (User domain)
- Vùng máy trạm (Workstation domain)
- Vùng mạng LAN (LAN domain)
- Vùng LAN-to-WAN (LAN-to-WAN domain)
- Vùng WAN (WAN domain)
- Vùng truy nhập từ xa (Remote Access domain)
- Vùng hệ thống/ứng dụng (Systems/Applications domain)



CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng người dùng:

- Thiếu ý thức về vấn đề an ninh an toàn
- Coi nhẹ các chính sách an ninh an toàn
- Vi phạm chính sách an ninh an toàn
- Đưa CD/DVD/USB với các files cá nhân vào hệ thống
- Tải ảnh, âm nhạc, video
- Phá hoại dữ liệu, ứng dụng và hệ thống
- Tấn công phá hoại từ các nhân viên bất mãn
- Nhân viên có thể tống tiền hoặc chiếm đoạt thông tin quan trọng.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng máy trạm:

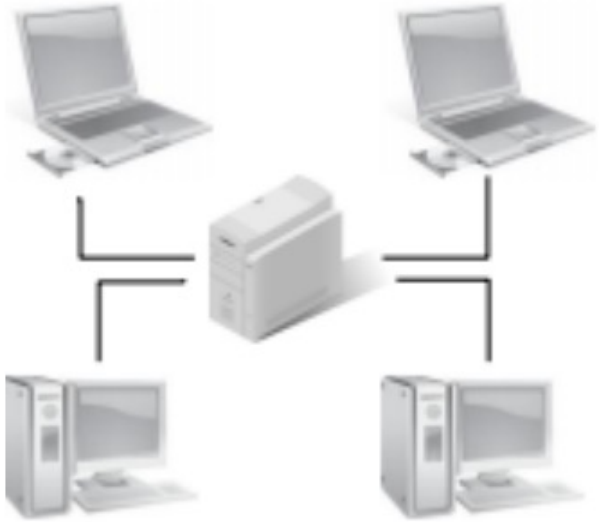
- Truy nhập trái phép vào máy trạm
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy trạm
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy trạm
- Các hiểm họa từ virus, mã độc và các phần mềm độc hại
- Người dùng đưa CD/DVD/USB với các files cá nhân vào hệ thống
- Người dùng tải ảnh, âm nhạc, video.

CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng LAN:

- Truy nhập trái phép vào mạng LAN vật lý
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy chủ
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy chủ
- Nguy cơ từ người dùng giả mạo trong mạng WLAN
- Tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa
- Các hướng dẫn và chuẩn cấu hình cho máy chủ LAN chưa được tuân thủ.

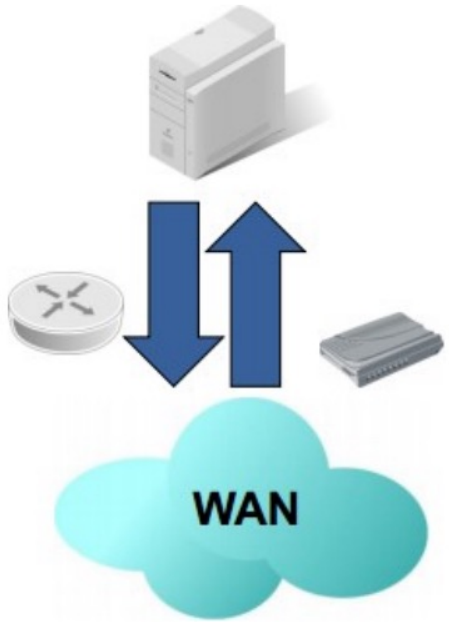


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng LAN-to-WAN:

- Thăm dò và rà quét trái phép các cổng dịch vụ
- Truy nhập trái phép
- Lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác
- Người dụng cục bộ (trong LAN) có thể tải các file không xác định nội dung từ các nguồn không xác định.

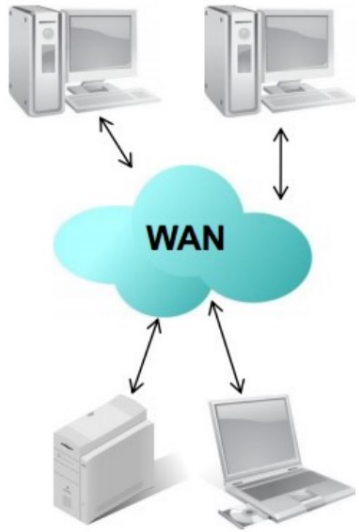


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng WAN:

- Rủi ro từ việc dữ liệu có thể được truy nhập trong môi trường công cộng và mở
- Hầu hết dữ liệu được truyền dưới dạng rõ (cleartext/plaintext)
- Dễ bị nghe trộm
- Dễ bị tấn công phá hoại
- Dễ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)
- Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm virus, sâu và các phần mềm độc hại.

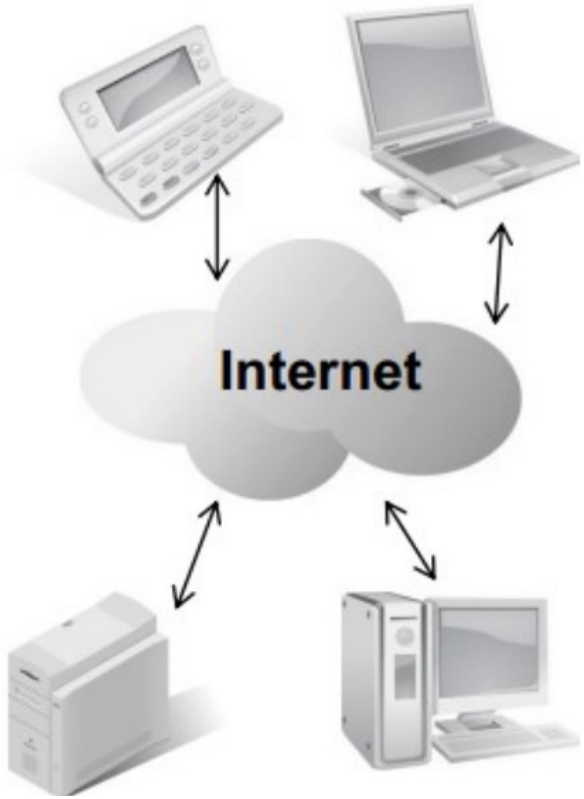


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng truy nhập từ xa:

- Tấn công kiểu vét cạn (brute force) vào tên người dùng và mật khẩu
- Tấn công vào hệ thống đăng nhập và điều khiển truy cập
- Truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu
- Thông tin bí mật có thể bị đánh cắp từ xa
- Dò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.

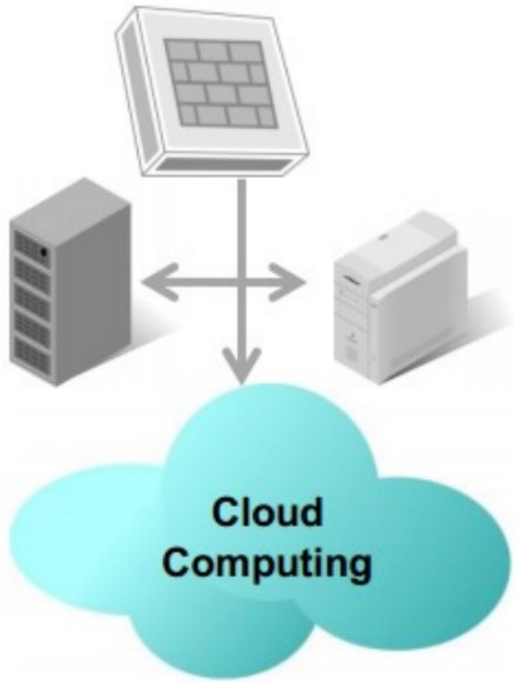


CÁC ĐẶC TRƯNG VỀ KỸ THUẬT AN TOÀN THÔNG TIN

CÁC MỐI ĐE DỌA & NGUY CƠ TRONG CÁC VÙNG HẠ TẦNG CNTT

Các đe dọa (threats) với vùng hệ thống/ứng dụng:

- Truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp
- Khó khăn trong quản lý các máy chủ yêu cầu tính sẵn dùng cao
- Lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ
- Các vấn đề an ninh trong các môi trường ảo của điện toán đám mây
- Vấn đề hỏng hóc hoặc mất dữ liệu.



BỘ TIÊU CHUẨN AN TOÀN THÔNG TIN

ISO = International Organization for Standardization – Tổ chức tiêu chuẩn hoá quốc tế
ISO 27001 là một tiêu chuẩn được công nhận trên toàn thế giới. Trên thực tế, tiêu chuẩn toàn cầu đối với hệ thống quản lý an toàn thông tin (ISMS).
ISO 27001 đảm bảo rằng một công ty hoặc tổ chức phi lợi nhuận hiểu được điểm mạnh và điểm yếu của mình nằm ở đâu.

AN TOÀN THÔNG TIN CÁ NHÂN

MỘT SỐ KỸ THUẬT AN TOÀN VÀ BẢO MẬT THÔNG TIN

Mã hóa thông tin

Trong khoa học mật mã là việc sử dụng các kỹ thuật thích hợp để biến đổi một bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau giữa người gửi và người nhận mà người ngoài cuộc có thể có được sự hiện hữu của dãy mã ngẫu nhiên đó nhưng khó có thể chuyển thành bản thông điệp ban đầu nếu không có "khóa" để giải mã của thông điệp.

Mã hóa và giải mã gồm:

- Bản rõ (plaintext or cleartext): Chứa các xâu ký tự gốc, thông tin trong bản rõ là thông tin cần mã hoá để giữ bí mật.
- Bản mã (ciphertext): Chứa các ký tự sau khi đã được mã hoá, mà nội dung của nó được giữ bí mật.
- Mật mã học (Crytography) Là nghệ thuật và khoa học để giữ thông tin được an toàn.
- Sự mã hoá (Encryption): Quá trình che dấu thông tin bằng phương pháp nào đó để làm ẩn nội dung bên trong gọi là sự mã hoá.
- Sự giải mã (Decryption): Quá trình biến đổi trả lại bản mã bản thành bản rõ gọi là giải mã.

AN TOÀN THÔNG TIN CÁ NHÂN

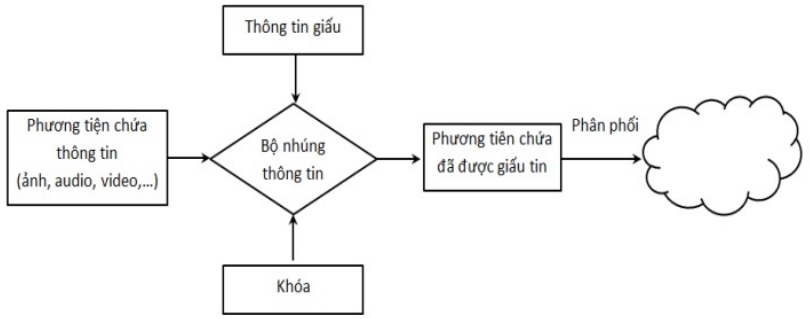
MỘT SỐ KỸ THUẬT AN TOÀN VÀ BẢO MẬT THÔNG TIN

Giấu tin

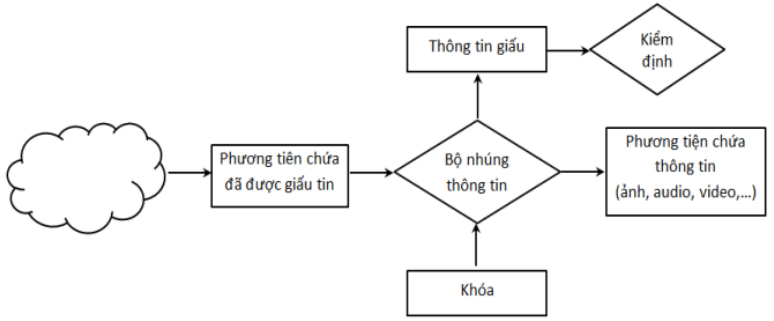
Giấu tin là kỹ thuật nhúng một lượng thông tin số (ảnh, audio, video) vào trong một đối tượng dữ liệu số khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu, đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Mục đích của giấu tin là làm cho thông tin đã giấu không thể nghe thấy hoặc nhìn thấy được, người ngoài cuộc không thể nhận thấy được sự tồn tại của thông tin đã giấu.

Kỹ thuật giấu tin gồm 2 phần là thuật toán giấu tin và thuật toán tách thông tin đã giấu trong ra khỏi phương tiện mang tin đã giấu.

Giấu tin khác với mật mã ở chỗ trong khi kỹ thuật giấu tin mật là tìm cách ẩn giấu thông điệp vào một phương tiện số như hình ảnh, audio, video mà người ngoài cuộc khó có thể phát hiện được sự hiện hữu của thông điệp trong phương tiện số đó mặc dù người ngoài cuộc có thể có nó trong tay. Còn trong khoa học mật mã người ta tìm cách để biến đổi bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau trên mạng công cộng mà người ngoài cuộc có thể có được sự hiện hữu của dãy mã ngẫu nhiên đó nhưng khó có thể chuyển thành bản thông điệp ban đầu nếu không có "khóa" để giải mã của thông điệp.



Quá trình giấu tin



Quá trình tách (lấy ra) thông tin đã giấu

AN TOÀN THÔNG TIN CÁ NHÂN

MỘT SỐ KỸ THUẬT AN TOÀN VÀ BẢO MẬT THÔNG TIN

Chữ ký số

Ngày nay, với sự phát triển bùng nổ của công nghệ thông tin nói chung và Internet nói riêng, công việc kinh doanh của các doanh nghiệp trở nên thuận lợi hơn, tiết kiệm được rất nhiều thời gian cũng như các thủ tục hành chính. Tuy nhiên, Internet cũng mang lại nhiều rủi ro cho các tổ chức, cá nhân, mà một trong những vấn đề lớn nhất và vấn đề gian lận vì vậy chữ ký số đã được ra đời để đảm bảo sự an toàn trong việc giao dịch số.

Chữ ký điện số là thông tin đi kèm theo dữ liệu (văn bản, âm thanh,hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện số là chuỗi thông tin cho phép xác định nguồn gốc, xuất xứ, thực thể đã tạo ra 1 thông điệp.

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật, qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật.

Khóa công khai thường được phân phối thông qua chứng thực khóa công khai. Quá trình sử dụng chữ ký số bao gồm 2 phần: tạo chữ ký và kiểm tra chữ ký. Mỗi người cần 1 cặp khóa gồm khóa công khai và khóa bí mật.

Khóa bí mật dùng để tạo chữ ký số (CKS) và khóa công khai dùng để thẩm định chữ ký số (xác thực)

Thẩm định chữ ký số: Quá trình thẩm định chữ ký số là quá trình xác thực được người gửi, chống chối bỏ, xác thực sự toàn vẹn của thông tin