CHƯƠNG 1

TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Bộ môn: Tin học quản lý
Khoa Thống kê – Tin học
Đại học Kinh Tế - Đại học Đà Nẵng

TÀI LIỆU THAM KHẢO

1. Slide bài giảng, 2024
2. Thái Thanh Tùng, Giáo trình Mật mã học & An toàn thông tin, Nxb Thông tin và Truyền thông, 2011.
3. Principles of Information security, Michael E. Whitman, Herbert J. Mattord, 4th Edition, 2012, Course Technology, Cengage Learning, ISBN-13: 978-1-1111-3823-3

NỘI DUNG CHƯƠNG 1

1. Khái quát về An toàn thông tin
2. Các yêu cầu đảm bảo an toàn thông tin và Hệ thống thông tin
3. Các thành phần của an toàn thông tin
4. Các mối đe dọa và nguy cơ an toàn thông tin trong các vùng hạ tầng công nghệ thông tin
5. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

1.1 Khái quát về an toàn thông tin

1. Sự cần thiết của an toàn thông tin trong đời sống hiện nay
2. Một số khái niệm trong an toàn thông tin
   - An toàn thông tin là gì?
   - Các lĩnh vực của an toàn thông tin
   - Các thành phần của an toàn thông tin
   - An toàn hệ thống thông tin
   - Mối đe dọa, điểm yếu, lỗ hổng và nguy cơ mất an toàn thông tin

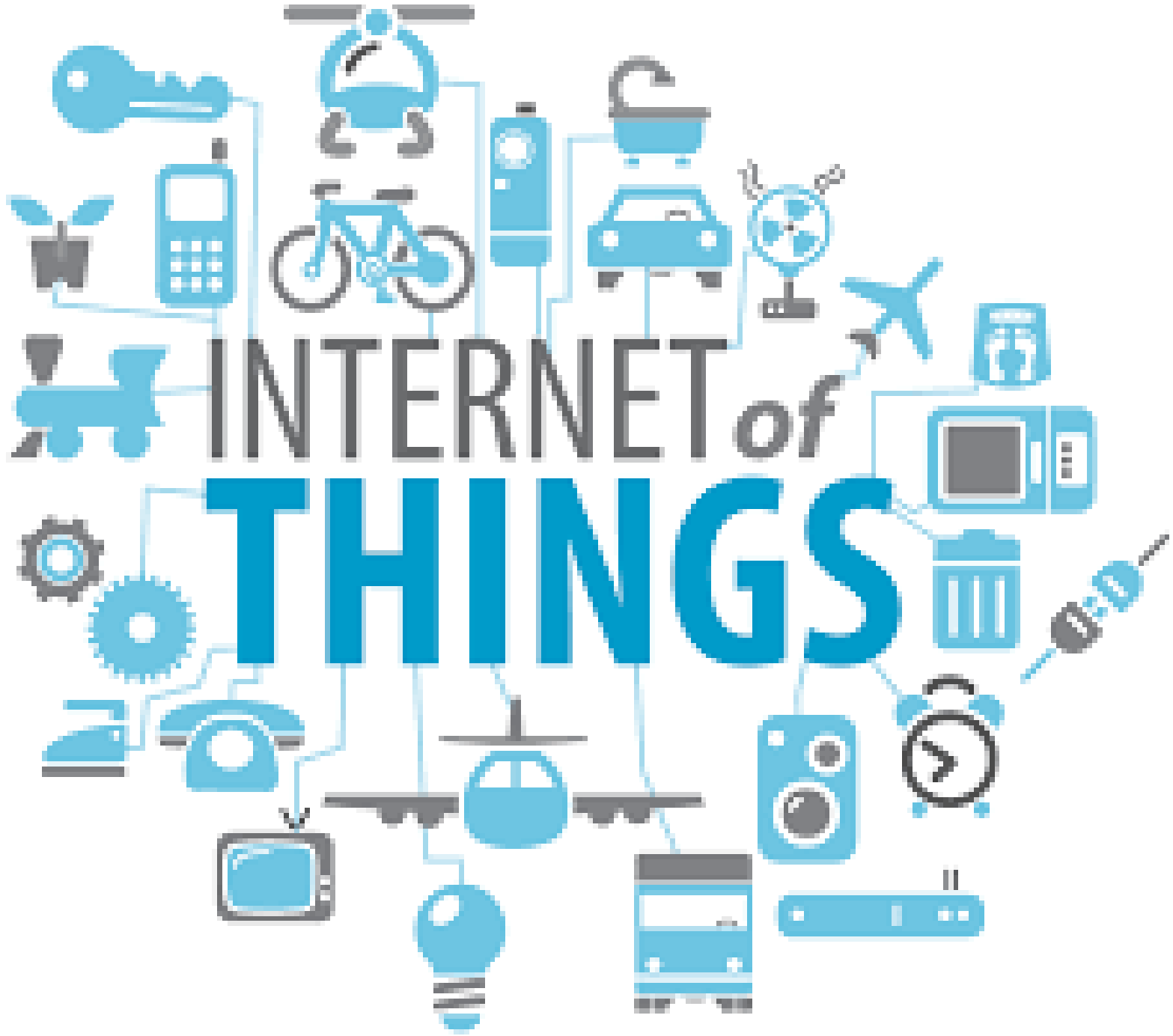
1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

- **Tại sao cần đảm bảo an toàn cho thông tin, hệ thống và mạng?**
- Do chúng ta sống trong "thế giới kết nối":
  - Mọi thiết bị tính toán & truyền thông đều có kết nối Internet;
  - Các hệ thống kết nối "sâu và rộng" ngày càng phổ biến:
    - Smart community (cộng đồng thông minh)
    - Smart city (thành phố thông minh)
    - Smart home (ngôi nhà thông minh)
  - Các khái niệm kết nối mọi vật, kết nối tất cả trở nên 'nóng'
    - IoT: Internet of Things
    - IoE: Internet of Everything
  - Các hệ thống không có kết nối khả năng sử dụng hạn chế.

1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

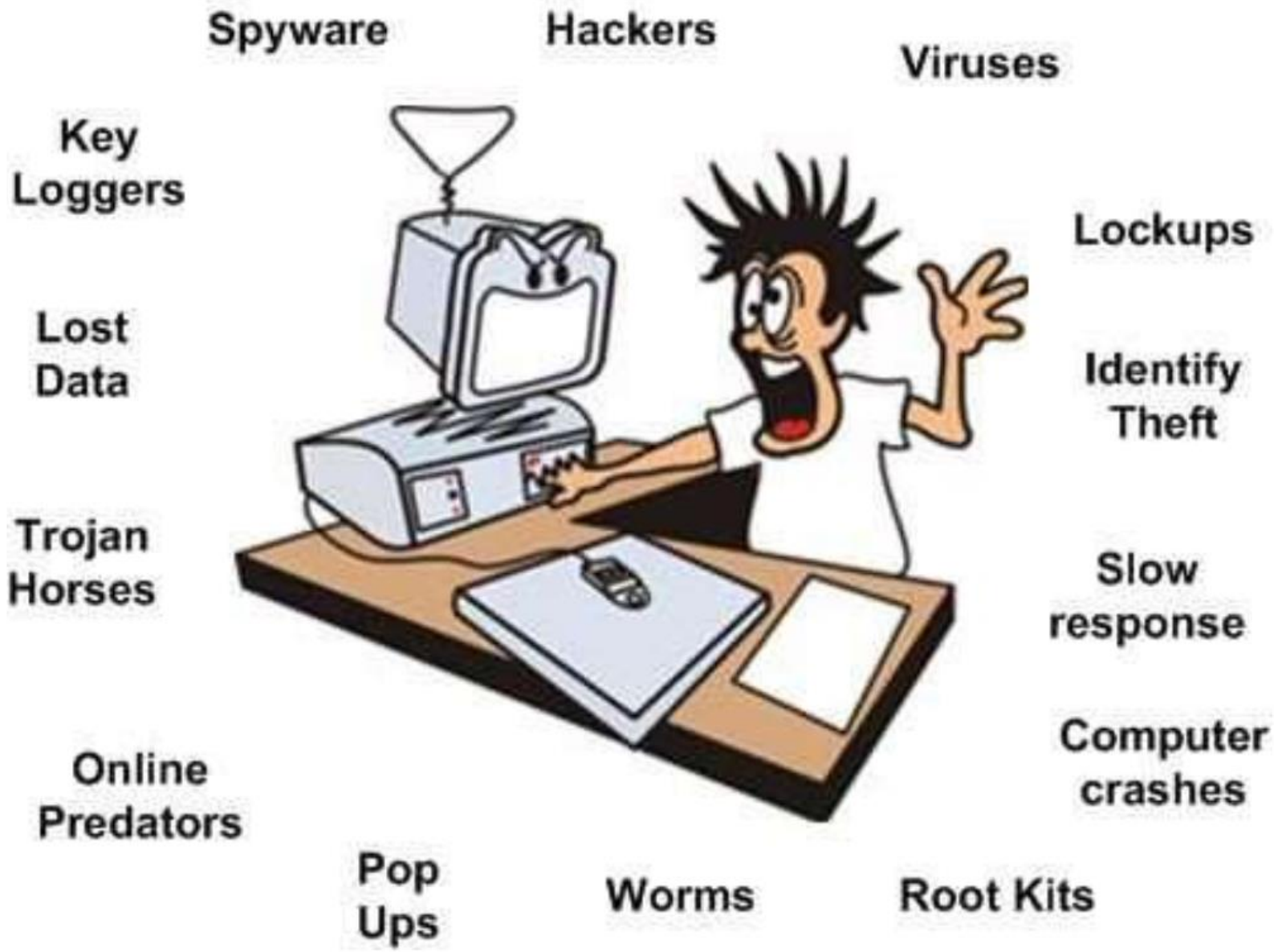


1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

- **Tại sao cần đảm bảo an toàn cho thông tin, hệ thống và mạng?**
- Nhiều nguy cơ, đe dọa mất an toàn thông tin, hệ thống mạng:
  - Bị tấn công từ tin tặc
  - Bị tấn công hoặc lạm dụng từ người dùng
  - Lây nhiễm các phần mềm độc hại (virút,...)
  - Nguy cơ bị nghe trộm, đánh cắp và sửa đổi thông tin
  - Lỗi hoặc các khiếm khuyết phần cứng, phần mềm.

1.1.1 Sự cần thiết của ATTT trong đời sống hiện nay

Các nguy cơ, đe dọa mất an toàn thông tin, hệ thống mạng



1.1.2 Một số khái niệm trong An toàn thông tin

❑ An toàn thông tin là gì?

- ➢ An toàn kỹ thuật cho các hoạt động của các cơ sở hạ tầng thông tin **bao gồm việc bảo vệ chống truy cập, sử dụng, tiết lộ, sửa đổi hoặc phá hủy thông tin một cách trái phép.**
- ➢ An toàn phần cứng và phần mềm theo các tiêu chuẩn kỹ thuật do nhà nước ban hành
- ➢ Duy trì các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng (theo định nghĩa trong Nghị định 64-2007/NĐ-CP)

1.1.2 Một số khái niệm trong An toàn thông tin

❑ An toàn thông tin là gì?

- ➢ Mục tiêu hướng tới của ATTT là bảo vệ các tài sản thông tin. Tuy nhiên, các sản phẩm và hệ thống thường luôn tồn tại những điểm yếu dẫn đến những rủi ro có thể xảy ra.
- ➢ Các đối tượng tấn công (tin tặc) có chủ tâm đánh cắp, lợi dụng hoặc phá hoại tài sản của các chủ sở hữu, tìm cách khai thác các điểm yếu để tấn công, tạo ra các nguy cơ và các rủi ro cho các hệ thống thông tin

1.1.2 Một số khái niệm trong An toàn thông tin

❑ Hai lĩnh vực chính của an toàn thông tin

- An toàn công nghệ thông tin (IT Security)
  - Đôi khi còn gọi là an toàn máy tính (Computer Security) là ATTT áp dụng cho các hệ thống công nghệ thông tin;
  - Các hệ thống công nghệ thông tin của 1 tổ chức cần được đảm bảo an toàn khỏi các tấn công mạng.

1.1.2 Một số khái niệm trong An toàn thông tin

❑ Hai lĩnh vực chính của an toàn thông tin

- ➢ Đảm bảo thông tin (Information Assurance)
  - Đảm bảo an toàn cho cả phần cứng và phần mềm hoạt động theo các tiêu chuẩn kỹ thuật do nhà nước ban hành
  - Đảm bảo thông tin không bị mất khi xảy ra các sự cố (thiên tai, hỏng hóc hệ thống, trộm cắp, phá hoại,…); ngăn ngừa khả năng lợi dụng mạng và các cơ sở hạ tầng thông tin để thực hiện các hành vi trái phép;
  - Đảm bảo các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng.
  - Thường sử dụng kỹ thuật tạo dự phòng ngoại vi (offsite backup).

1.1.2 Một số khái niệm trong An toàn thông tin

❑ Hệ thống thông tin

- ➢ Hệ thống thông tin (IS – Information System) là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số;
- ➢ Các doanh nghiệp và các tổ chức sử dụng các hệ thống thông tin (HTTT) để thực hiện và quản lý các hoạt động:
  - Tương tác với khác khàng;
  - Tương tác với các nhà cung cấp;
  - Tương tác với các cơ quan chính quyền;
  - Quảng bá thương hiệu và sản phẩm;
  - Cạnh tranh với các đối thủ trên thị trường.

1.1.2 Một số khái niệm trong An toàn thông tin

❑ Hệ thống thông tin

- ➢ Một hệ thống thông tin dựa trên máy tính (Computer-Based Information System) là một hệ thống thông tin sử dụng công nghệ máy tính để thực thi các nhiệm vụ.
- ➢ Các thành phần của hệ thống thông tin dựa trên máy tính:
  - Hardware: phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu
  - Software: các phần mềm chạy trên phần cứng để xử lý dữ liệu
  - Databases: lưu trữ dữ liệu
  - Networks: hệ thống truyền dẫn thông tin/dữ liệu
  - Procedures: tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu

1.1.2 Một số khái niệm trong An toàn thông tin

- **Mối đe dọa/ nguy cơ (threat):** Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…).
- **Điểm yếu (weakness):** là những khiếm khuyết hoặc lỗi tồn tại trọng hệ thống:
  - Điểm yếu phần cứng
  - Điểm yếu phần mềm (Hệ điều hành và ứng dụng)
- **Lỗ hổng (vulnerability):** là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

1.1.2 Một số khái niệm trong An toàn thông tin

- **Rủi ro (risk):** là tiềm năng một mối đe dọa có thể khai khác một lỗ hổng để tấn công hoặc gây nguy hiểm cho hệ thống. Nguy cơ xuất hiện khi có mối đe dọa và lỗ hổng bảo mật.
- **Quan hệ giữa Mối đe dọa và Lỗ hổng:**
  - Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại;
  - Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực;
  - Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

1.1.2 Một số khái niệm trong An toàn thông tin

- **An toàn Hệ thống thông tin (ISS – Information Systems Security)**
  - Là việc đảm bảo các thuộc tính an ninh an toàn của hệ thống thông tin:
    - Bí mật (Confidentiality)
    - Toàn vẹn (Integrity)
    - Sẵn sàng (Availability)

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính bí mật (Confidentiality):**
  - Thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính) được cấp phép
  - Giới hạn truy cập về cả mặt vật lý, như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng.
  - Một số cách:
    - Khóa kín và niêm phong thiết bị
    - Yêu cầu đối tượng cung cấp credential (user + password) hay đặc điểm về sinh trắc để xác thực
    - Sử dụng firewall hoặc ACL để ngăn chặn truy cập trái phép
    - Mã hóa thông tin sử dụng các giao thức và thuật toán,v..v.

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính bí mật (Confidentiality):**
  - 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.
  - Một giải pháp đảm bảo an toàn là xác định quyền được truy cập đối với thông tin đang tìm kiếm, đối với một số lượng người sử dụng nhất định và một số lượng thông tin là tài sản nhất định. Trong trường hợp kiểm soát truy cập, nhóm người truy cập sẽ được kiểm soát xem họ đã truy cập những dữ liệu nào.

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính toàn vẹn (Integrity):**
  - Thông tin chỉ được xóa/ sửa bởi đối tượng được phép và đảm bảo tính chính xác thông tin khi lưu trữ hay truyền
  - 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.

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính toàn vẹn (Integrity):**
  - Giải pháp "data integrity" bao gồm xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến tư một nguồn đáng tin cậy và ta gọi đó là tính "authenticity" của thông tin.
  - Tính toàn vẹn của thông tin bị phá vỡ khi:
    - Thay đổi giao diện trang chủ của một website
    - Chặn đứng và thay đổi gói tin được gửi qua mạng
    - Chỉnh sửa trái phép các file được lưu trữ trên máy tính
    - Do có sự cố trên đường truyền mà tín hiệu bị nhiễu hoặc suy hao dẫn đến thông tin bị sai lệch

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính sẵn dùng/ khả dụng (Availability):**
  - Tính sẵn dùng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và mạng.
  - Tính sẵn dùng đảm bảo độ ổn định đáng tin cậy của thông tin, cũng như đảm nhiệm chức năng là thước đo, xác định phạm vi tới hạn an toàn của một HTTT.
  - Thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.
  - Một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên 1 năm thì độ sẵn dùng của nó là 99,999%.

1.2 Các yêu cầu đảm bảo ATTT và HTTT

- **Tính sẵn dùng (Availability):**
  - Tính sẵn dùng 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.

1.3 Các thành phần của An toàn thông tin

1. An toàn máy tính và dữ liệu(Computer and data security)
2. An ninh mạng (Network security)
3. Quản lý ATTT (Management of information security)
4. Chính sách ATTT (Policy)

1.3.1 An toàn máy tính và dữ liệu

- Đảm bảo an toàn hệ điều hành, ứng dụng/dịch vụ
- Vấn đề Điều khiển truy cập
- Vấn đề Mã hóa/bảo mật dữ liệu
- Vấn đề Phòng chống phần mềm độc hại
- Sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố

1.3.2 An ninh mạng

- Tưởng lửa (Firewall)
  - Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập
- Mạng riêng ảo (VPN)
- Bảo mật dữ liệu truyền (SSL/TLS, PGP)
- Các kỹ thuật và hệ thống phát hiện/ngăn chặn tấn công, xâm nhập (IPS/IDS)
- Giám sát mạng

1.3.3 Quản lý an toàn thông tin

- Quản lý rủi ro (risk)
  - Nhận dạng
  - Đánh giá
- Thực thi quản lý an toàn thông tin
  - Lập kế hoạch
  - Thực thi kế hoạch
  - Giám sát kết quả
  - Thực hiện các kiểm soát
- Chính sách ATTT
- Đào tạo người dùng

1.3.4 Chính sách an toàn thông tin

- Chính sách ATTT ở mức vật lý (Physical security policy)
- Chính sách ATTT ở mức tổ chức (Orgranisational security policy)
- Chính sách ATTT ở mức logic (Logical security policy)
- Áp dụng chính sách xác thực ‘mạnh’ sử dụng đặc điểm sinh trắc (Biometric) thay cho mật khẩu truyền thống

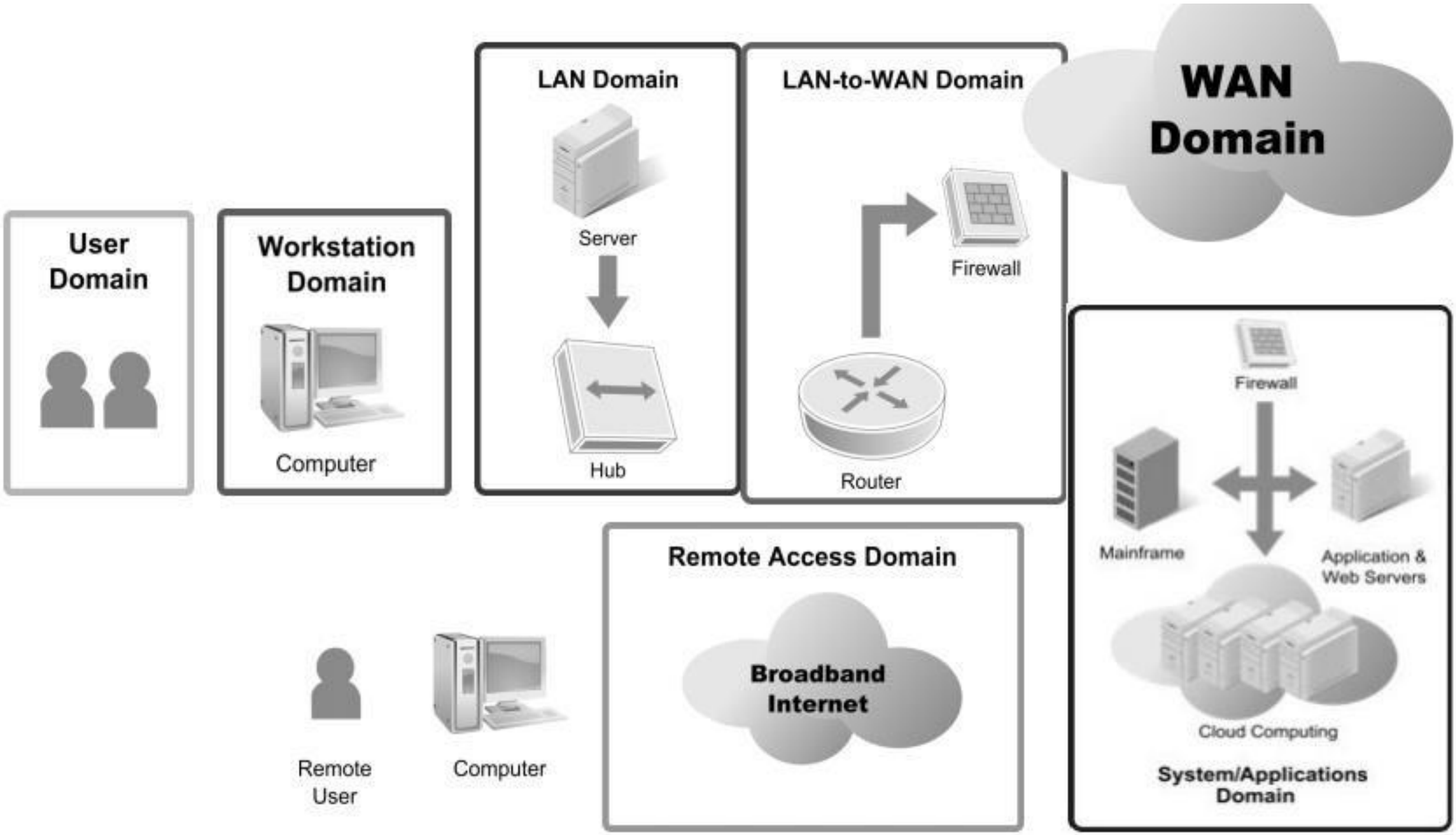
1.4 Các mối đe dọa và nguy cơ ATTT trong các vùng hạ tầng CNTT

1. Bảy vùng trong cơ sở hạ tầng CNTT
2. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

1.4.1 Bảy vùng trong cơ sở hạ tầng CNTT

- Bảy vùng trong cơ sở 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)

1.4.1 Bảy vùng trong cơ sở hạ tầng CNTT



1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

- **Các đe dọa/nguy cơ 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 trái phép
  - 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 nhạy cảm, hoặc quan trọng.

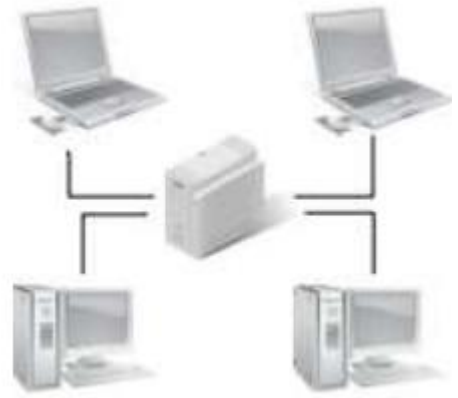
1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

- **Các đe dọa/nguy cơ 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 trái phép.

1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

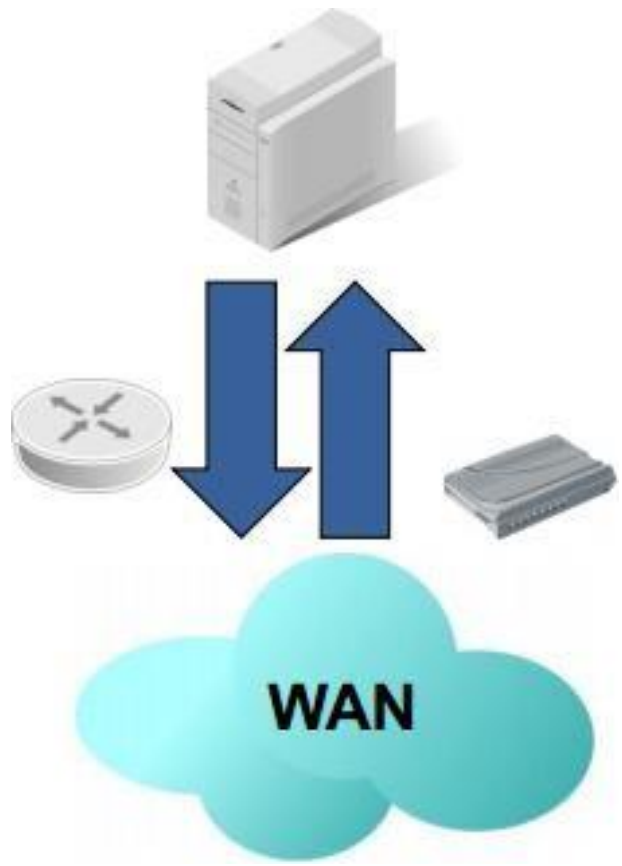
❑ Các đe dọa/nguy cơ với vùng LAN:

- ➢ 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.



1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

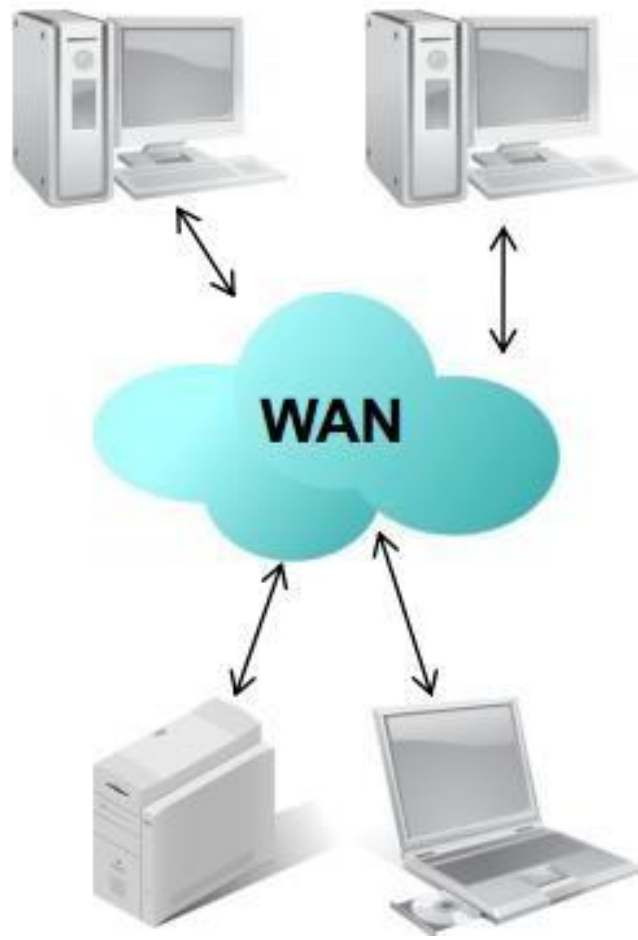
- **Các đe dọa/nguy cơ với vùng LAN-to-WAN:**
  - Thăm dò và rà quét trái phép các cổng dịch vụ
  - Truy nhập trái phép
  - Lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác
  - Người dụng cục bộ (trong LAN) có thể tải các file không xác định nội dung từ các nguồn không xác định.



1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

❑ Các đe dọa/nguy cơ 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.



1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

- **Các đe dọa/nguy cơ 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 thông CNTT, ứng dụng và dữ liệu
  - Thông tin bí mật có thể bị đánh cắp từ xa
  - Rò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.

1.4.2 Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

- **Các đe dọa/nguy cơ 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.

1.5 Đảm bảo an toàn thông tin mạng

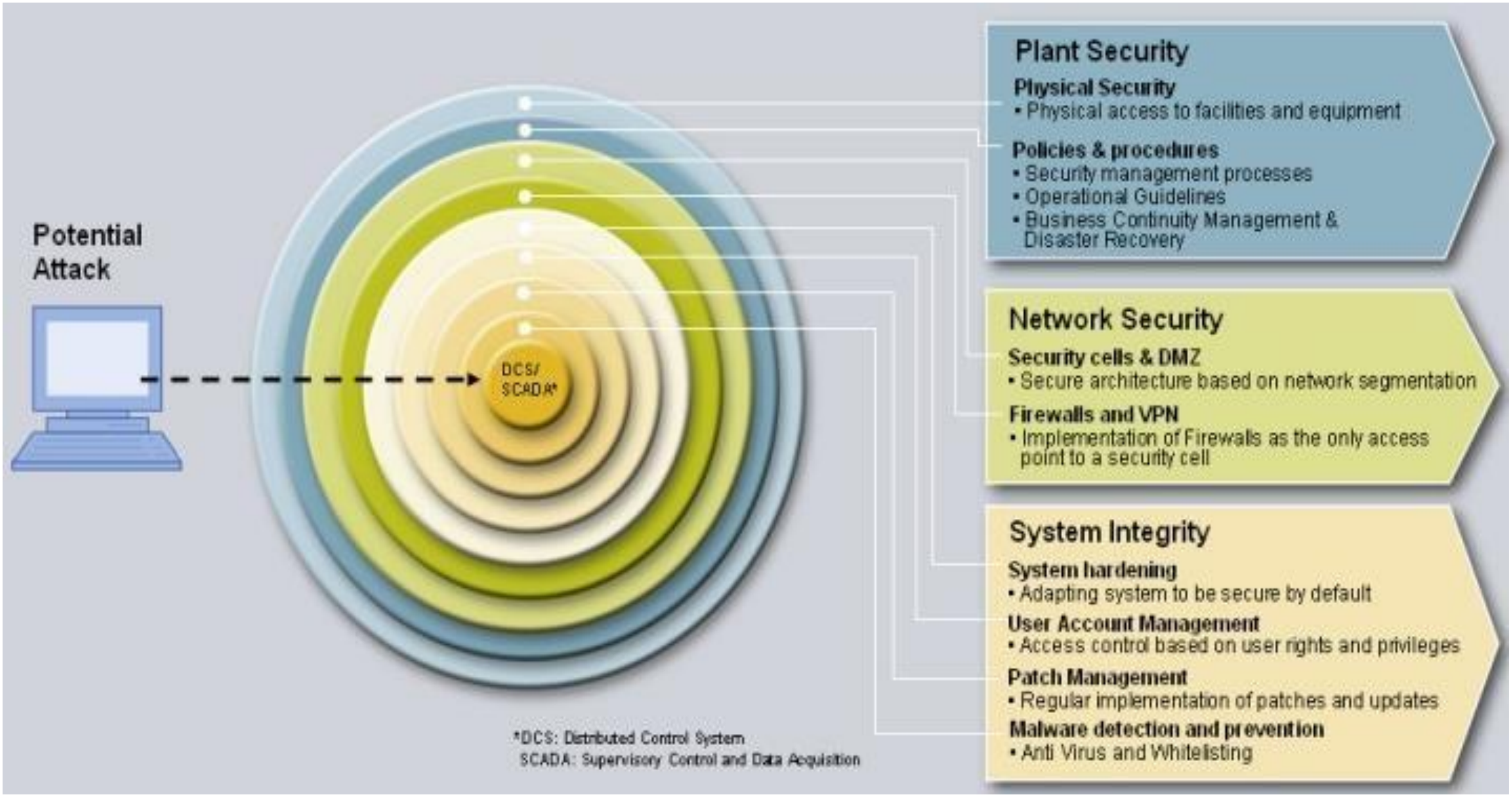
1. Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng.
2. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin
3. Xu thế tấn công mạng và giải pháp xử lý tình huống

1.5.1 Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng

- Phòng vệ nhiều lớp có chiều sâu (Defence in Depth):
  - Tạo ra nhiều lớp bảo vệ, kết hợp tính năng tác dụng của mỗi lớp để đảm bảo an toàn tối đa cho thông tin, hệ thống và mạng.
- Một lớp, một công cụ phòng vệ riêng rẽ thường không đảm bảo an toàn.
- Không tồn tại HTTT an toàn tuyệt đối
  - Thường HTTT an toàn tuyệt đối là hệ thống đóng kín và không hoặc ít có giá trị sử dụng.
  - Cần cân bằng giữa vấn đề an toàn, tính hữu dụng và chi phí đầu tư.
- Cần cân bằng giữa Usability (Tính hữu dụng), Cost (chi phí) và Security (an toàn)

1.5.2 Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

❑ Mô hình "Phòng vệ nhiều lớp":



1.5.2 Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

- **Các lớp phòng vệ điển hình trong mô hình "Phòng vệ nhiều lớp":**
  - Lớp an ninh cơ quan/tổ chức (Plant Security)
    - Lớp bảo vệ vật lý
    - Lớp chính sách & thủ tục đảm bảo ATTT
  - Lớp an ninh mạng (Network Security)
    - Lớp an ninh cho từng thành phần mạng
    - Tường lửa, mạng riêng ảo (VPN)
  - Lớp an ninh hệ thống (System Security)
    - Lớp tăng cường an ninh hệ thống
    - Lớp quản trị tài khoản và phân quyền người dùng
    - Lớp quản lý các bản vá và cập nhật phần mềm
    - Lớp phát hiện và ngăn chặn phần mềm độc hại