



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÀI GIẢNG MÔN HỌC CƠ SỞ AN TOÀN THÔNG TIN CHƯƠNG 1 – TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Giảng viên:

E-mail:

Khoa:

PGS.TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

An toàn thông tin

TÀI LIỆU THAM KHẢO

1. Hoàng Xuân Dậu, *Giáo trình Cơ sở an toàn thông tin*, Học viện Công nghệ BC-VT, 2020.
2. David Kim, Michael G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlettlearning, 2012.
3. Michael E. Whitman, Herbert J. Mattord, *Principles of information security*, 4th edition, Course Technology, Cengage Learning, 2012.
4. Matt Bishop, *Introduction to Computer Security*, Prentice Hall, 2004.
5. William Stallings, *Cryptography and Network Security*, Prentice Hall, 2010.
6. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996.

ĐÁNH GIÁ MÔN HỌC

- ❖ Các điểm thành phần:
 - Chuyên cần: 10%
 - Kiểm tra: 10%
 - Bài tập/thảo luận: 20%
 - Thi cuối kỳ: 60%

NỘI DUNG MÔN HỌC

1. Tổng quan về an toàn thông tin
2. Lỗi hỏng bảo mật và các điểm yếu hệ thống
3. Các dạng tấn công và phần mềm độc hại
4. Đảm bảo an toàn thông tin dựa trên mã hóa
5. Các kỹ thuật và công nghệ đảm bảo an toàn thông tin
6. Quản lý, chính sách, pháp luật và đạo đức an toàn thông tin

NỘI DUNG CHƯƠNG 1

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

1.1 Khái quát về an toàn thông tin

Tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

1.1 Khái quát về an toàn thông tin

- ❖ Do chúng ta sống trong “thế giới kết nối” với mức độ ngày càng “sâu”
- ❖ Ngày càng có nhiều nguy cơ, đe dọa mất an toàn thông tin, hệ thống, mạng.

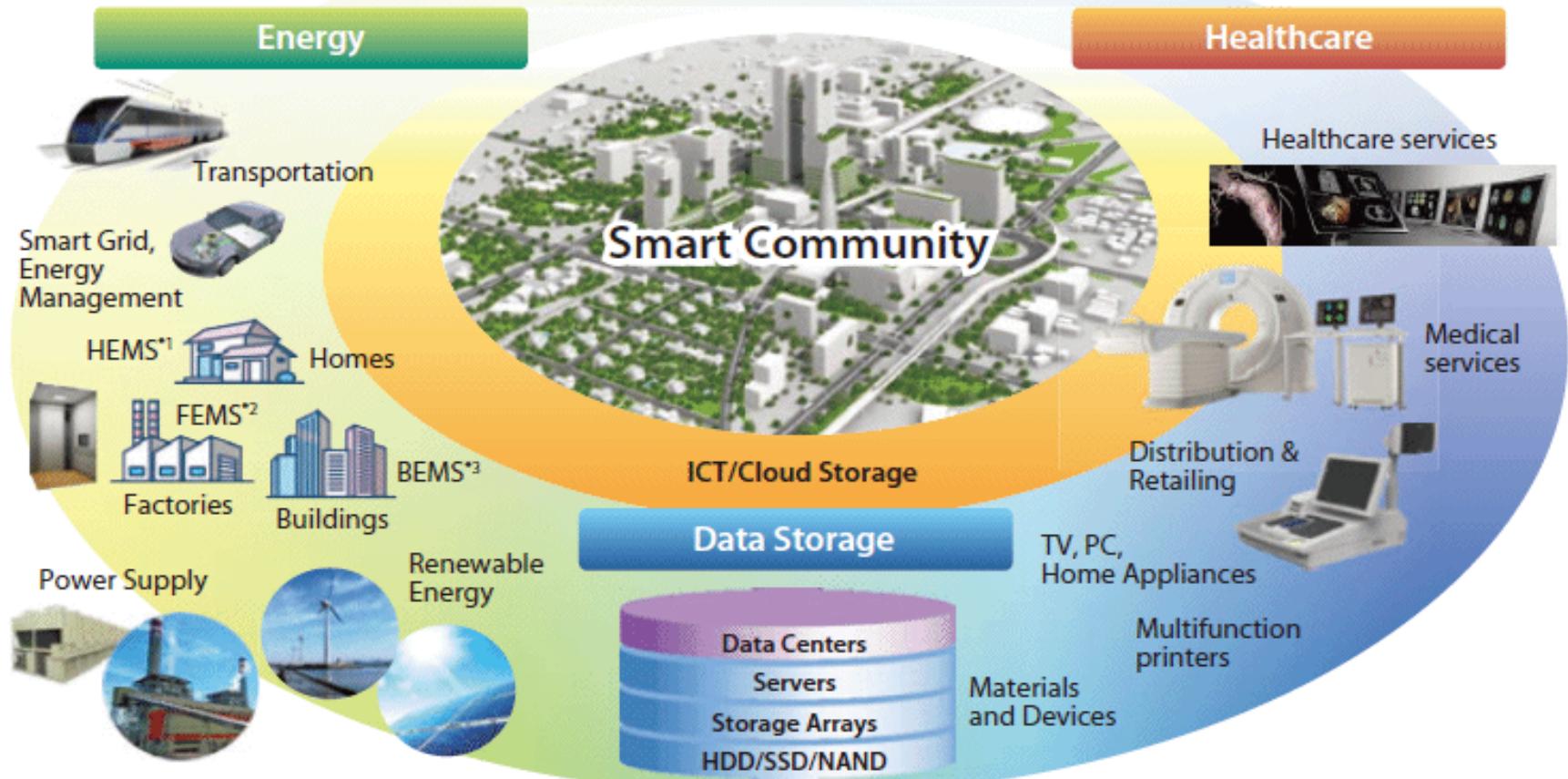
1.1 Khái quát về an toàn thông tin

❖ Do chúng ta sống trong “thế giới kết nối”:

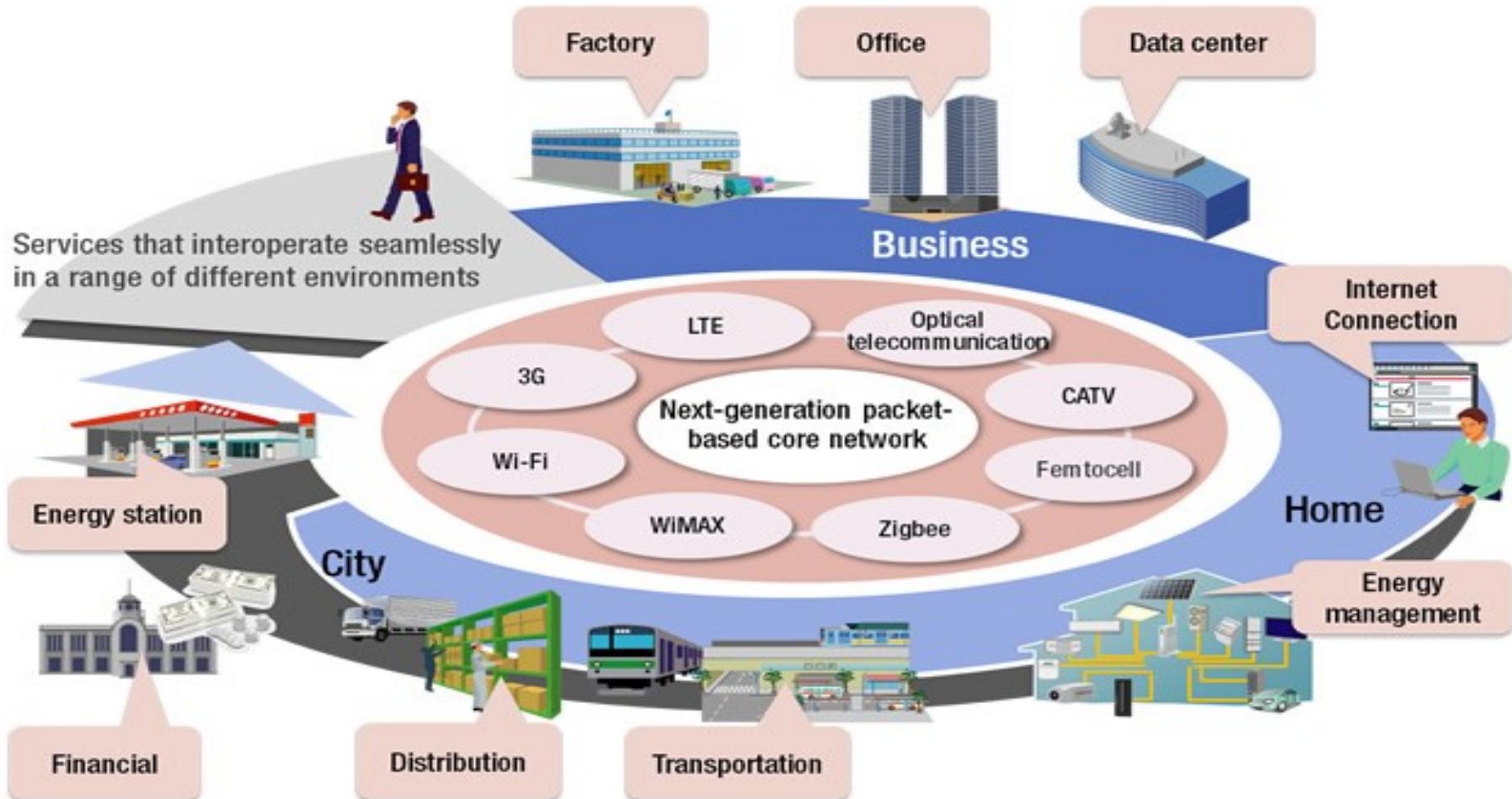
- Mọi thiết bị tính toán & truyền thông đều có kết nối Internet;
- Các hệ thống kết nối “sâu và rộng” ngày càng phổ biến:
 - Smart community (cộng đồng thông minh)
 - Smart city (thành phố thông minh)
 - Smart home (ngôi nhà thông minh),...
- Các khái niệm kết nối mọi vật, kết nối tất cả trở nên ‘nóng’:
 - IoT: Internet of Things
 - IoE: Internet of Everything.
- Các hệ thống không có kết nối khả năng sử dụng hạn chế.

1.1 Khái quát về an toàn thông tin

Three major pillars for the creation of Smart Communities



1.1 Khái quát về an toàn thông tin

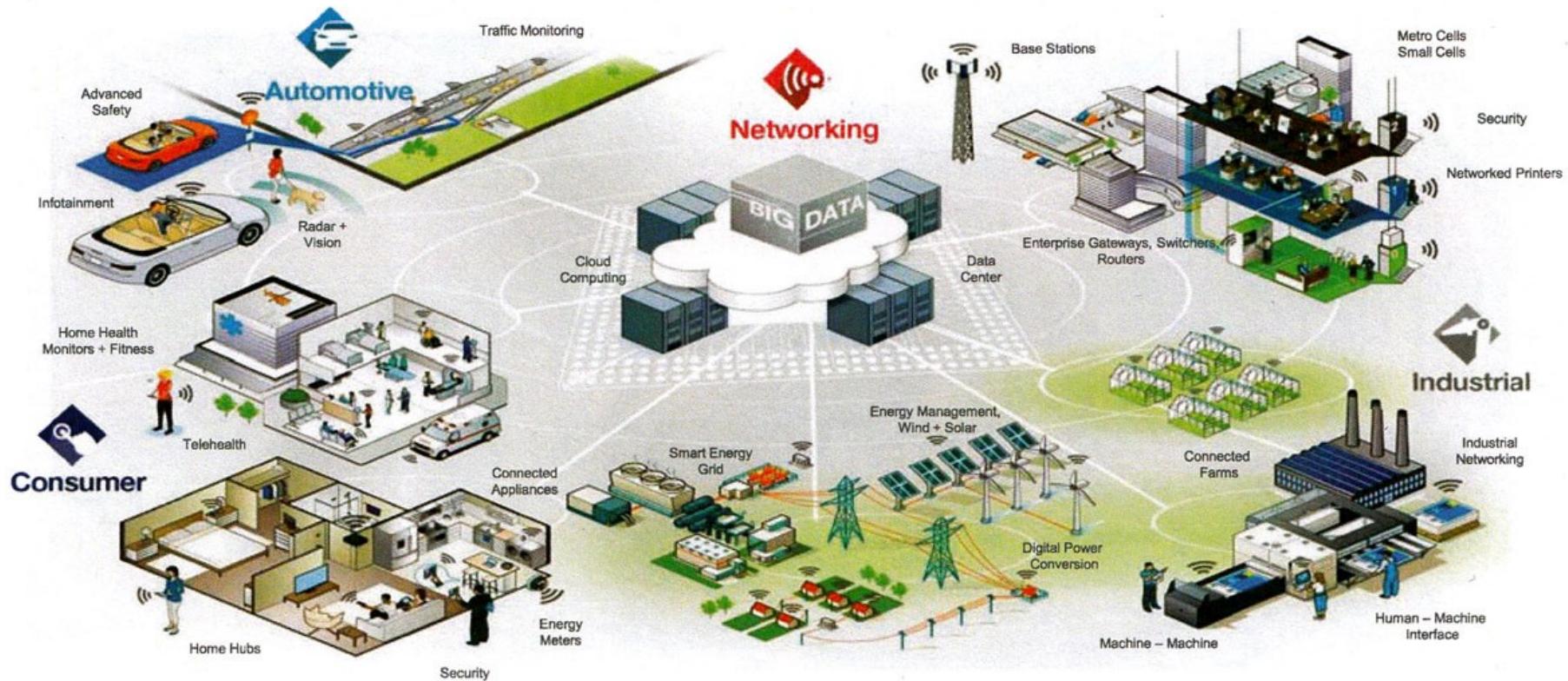


1.1 Khái quát về an toàn thông tin

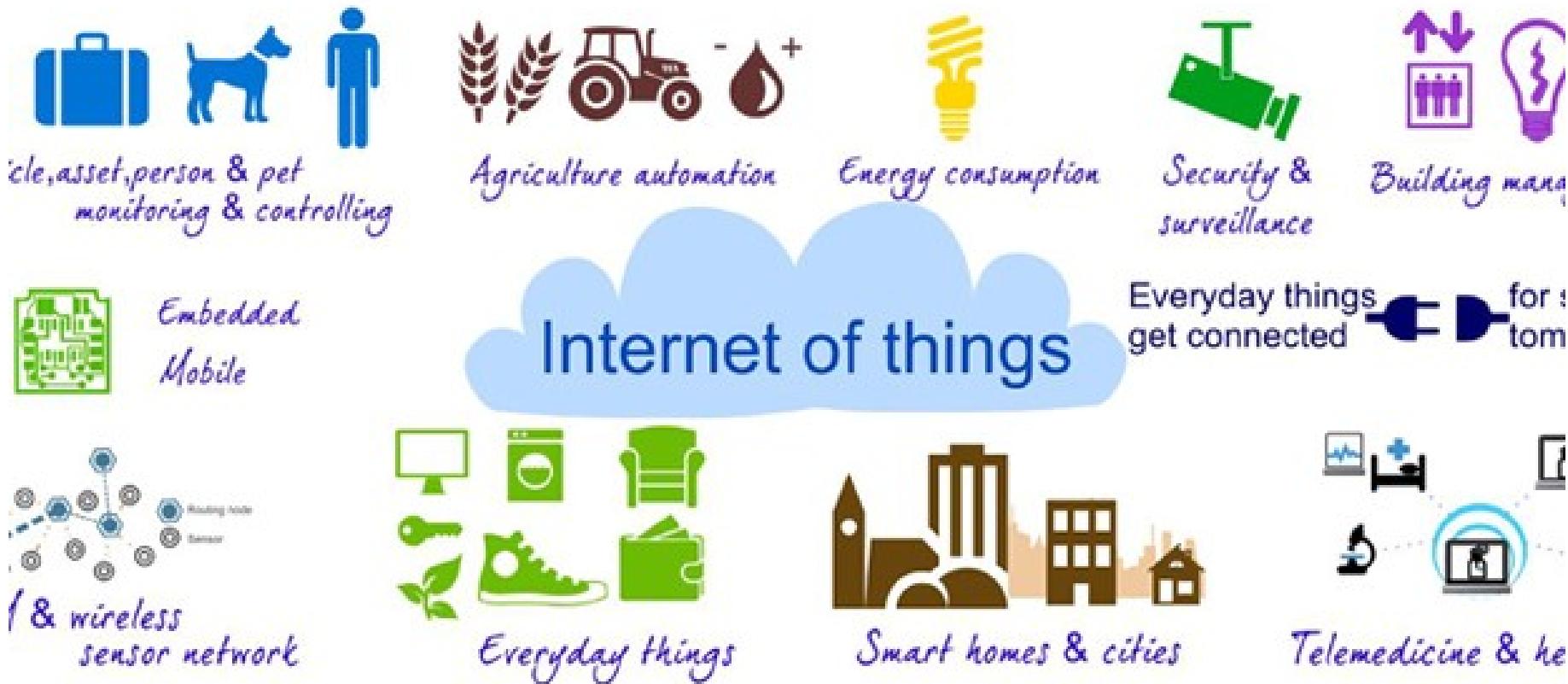


1.1 Khái quát về an toàn thông tin

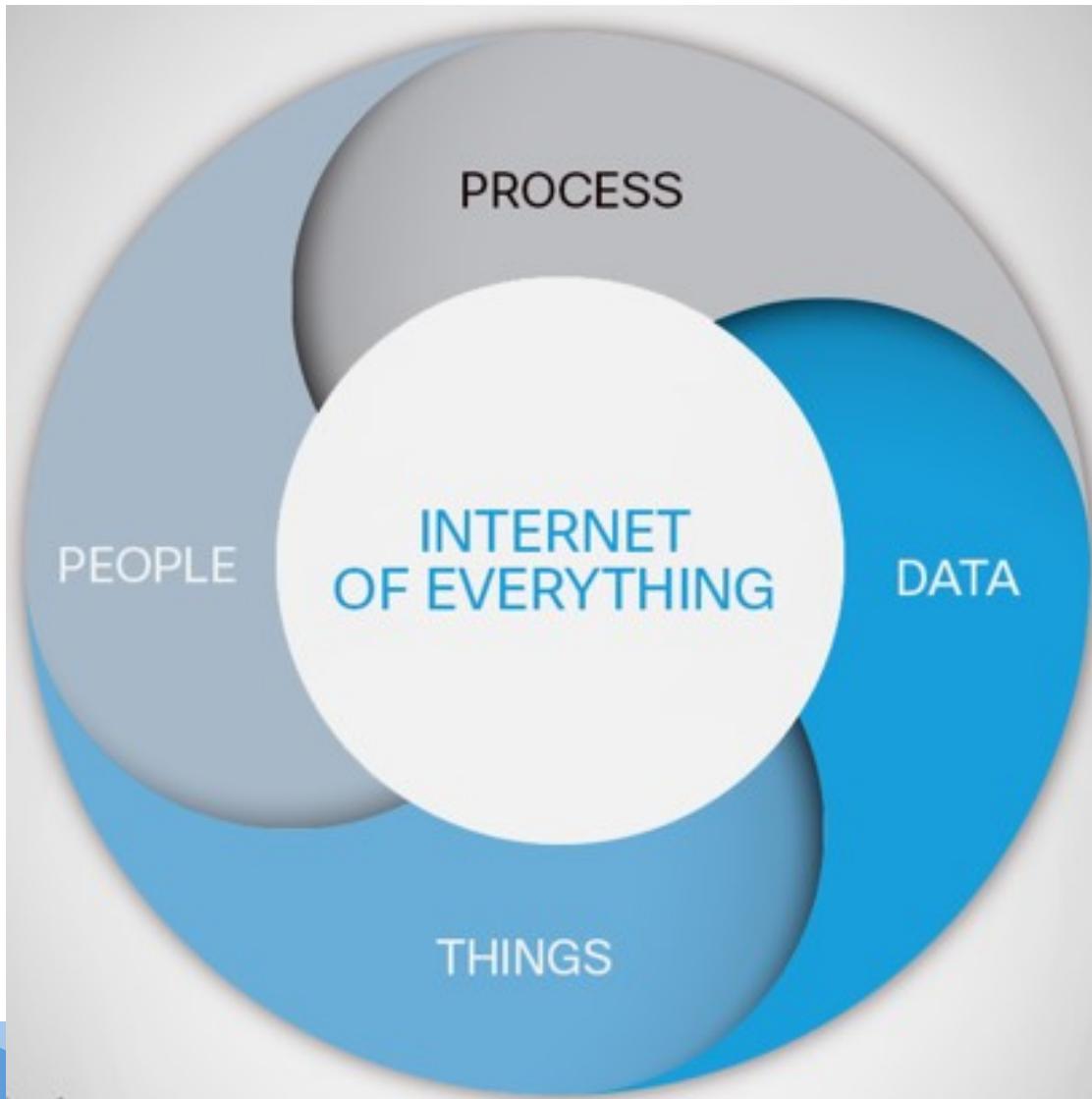
The Internet of Things



1.1 Khái quát về an toàn thông tin



1.1 Khái quát về an toàn thông tin



1.1 Khái quát về an toàn thông tin

From Internet of Things (IoT) to
The Internet of Everything (IoE)

Networked Connection of People,
Process, Data, Things

People
Connecting People in
More Relevant,
Valuable Ways



Process
Delivering the Right
Information to the Right
Person (or Machine)
at the Right Time



Data
Leveraging Data into
More Useful
Information for
Decision Making



Things
Physical Devices and
Objects Connected to the
Internet and Each Other
for Intelligent Decision
Making

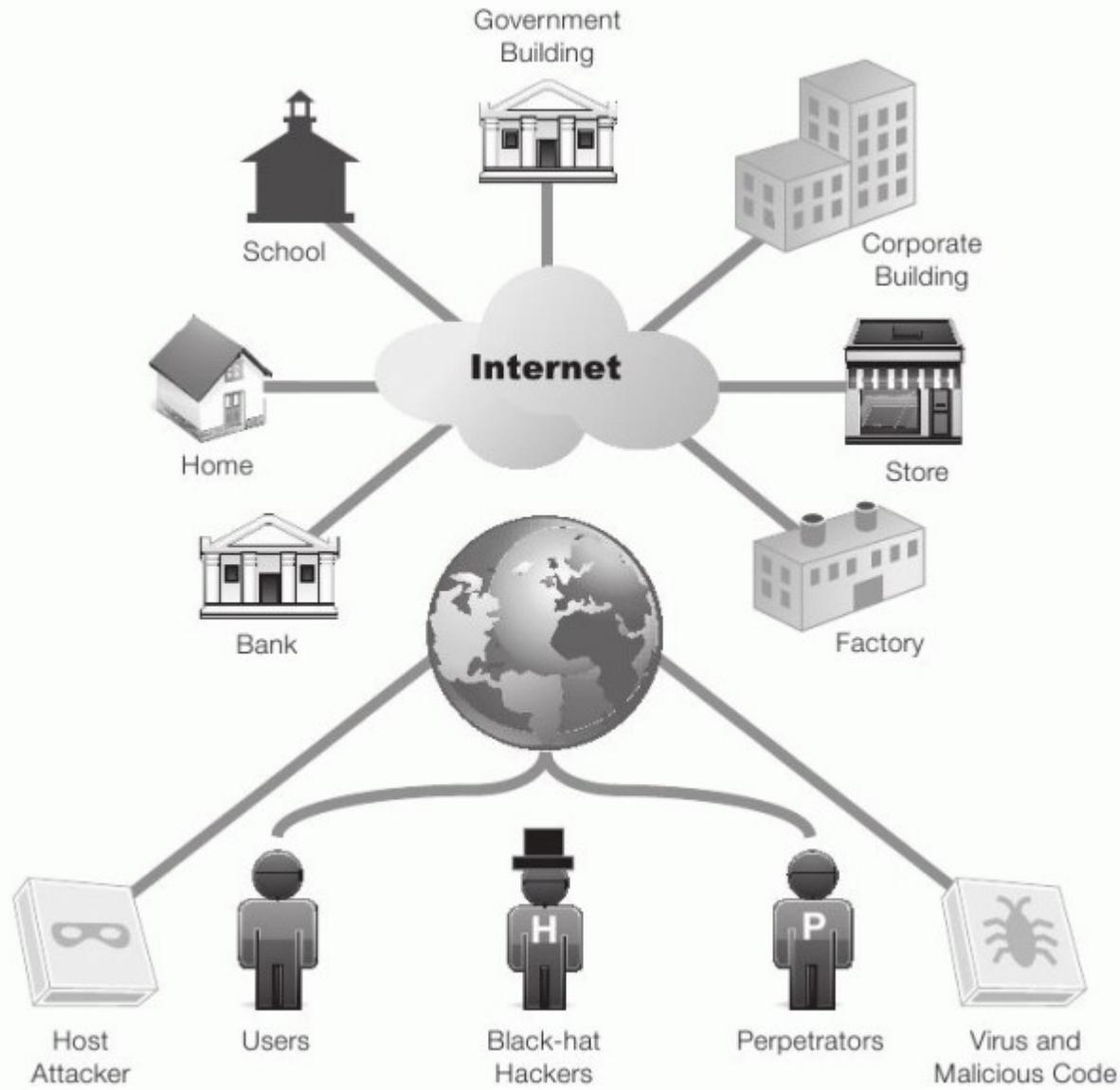


1.1 Khái quát về an toàn thông tin

- ❖ Ngày càng có 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 (vi rút, sâu,...)
 - Nguy cơ bị nghe trộm, đánh cắp và sửa đổi thông tin
 - Lỗi hoặc các khiếm khuyết phần cứng, phần mềm.

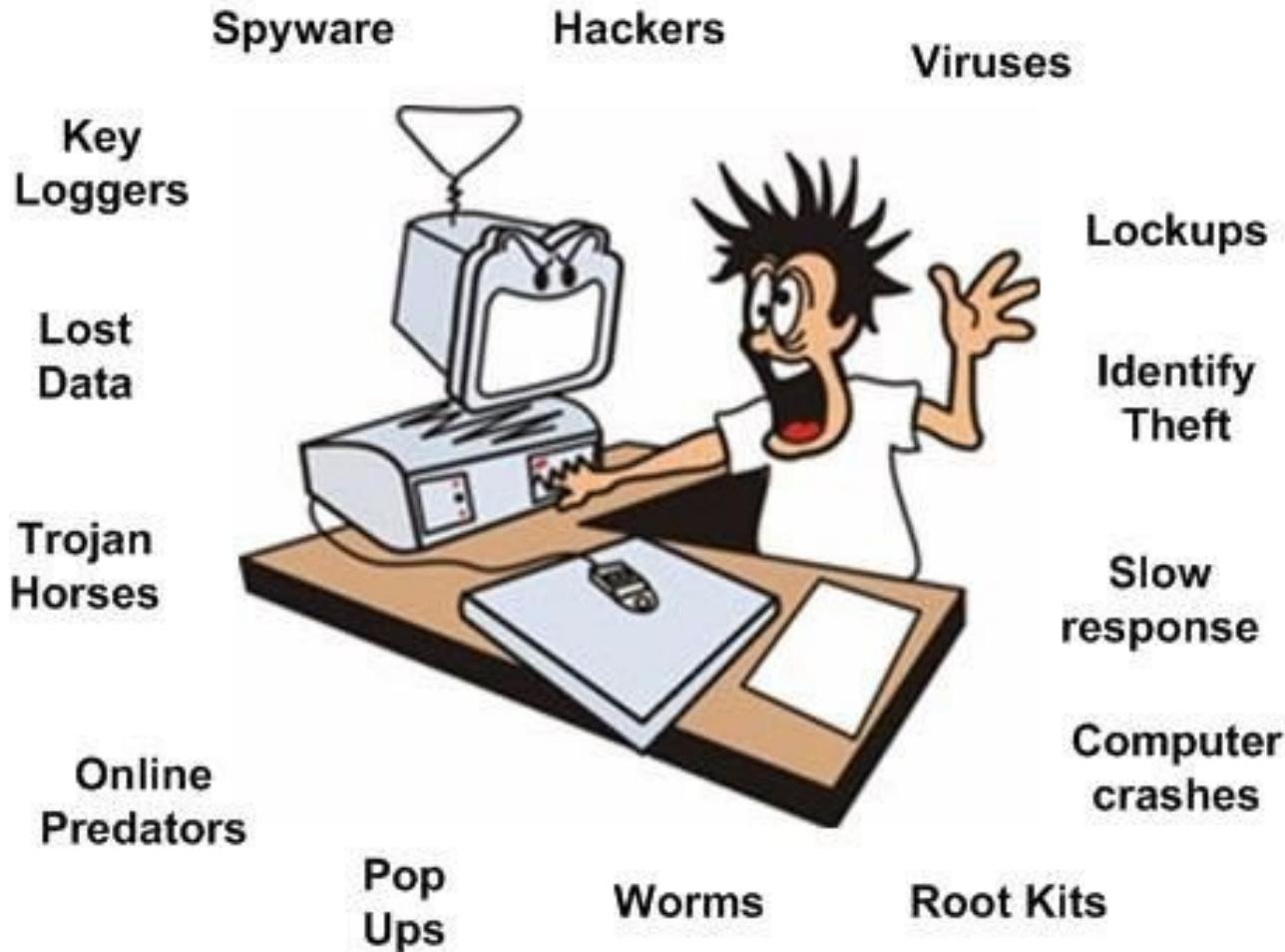
1.1 Khái quát về an toàn thông tin

Thế giới
kết nối
với nhiều
nguy cơ
và
đe dọa



1.1 Khái quát về an toàn thông tin

Các mối đe dọa và nguy cơ thường trực: tin tặc (hackers) và các phần mềm độc hại (viruses, worms, trojans)



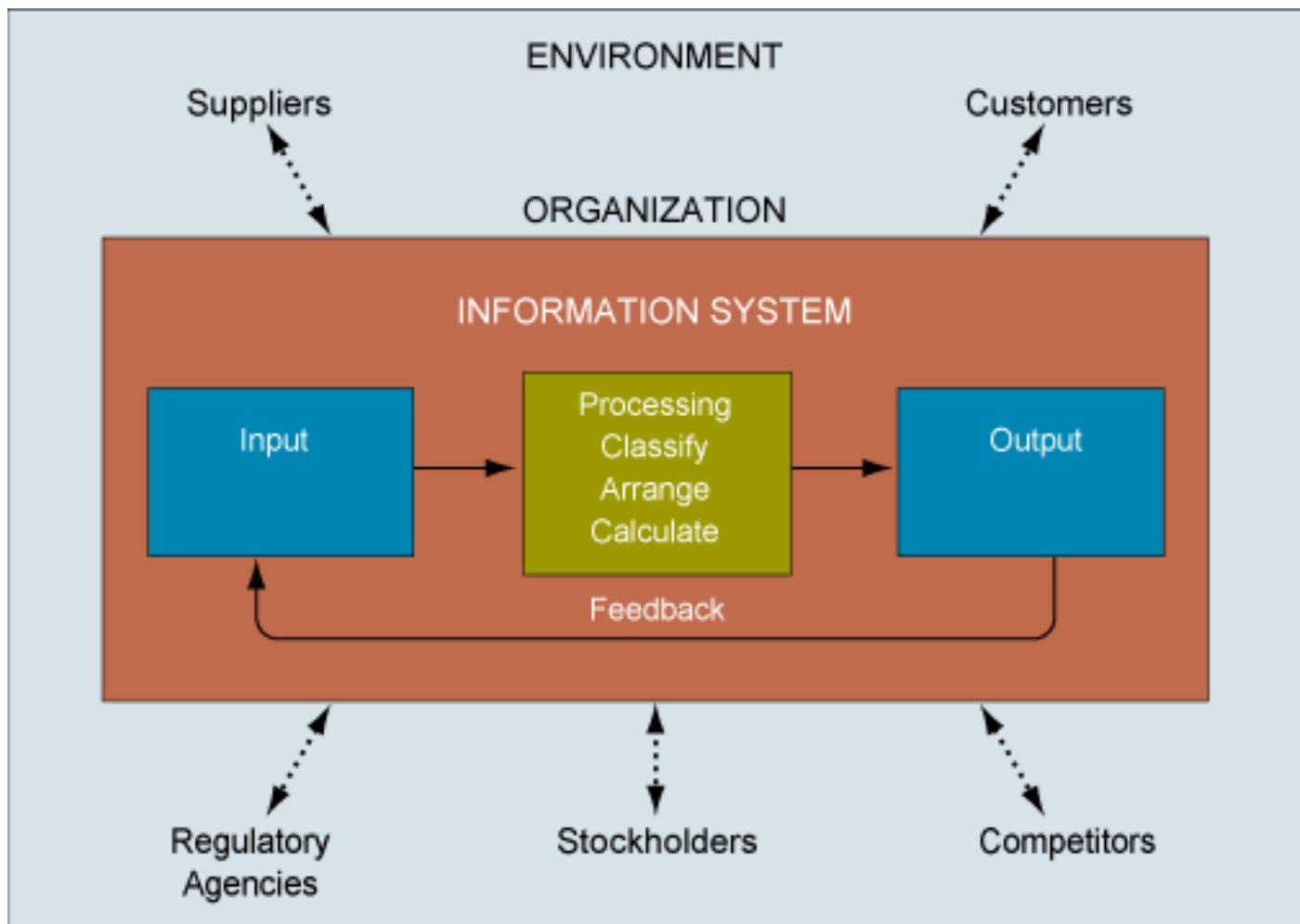
1.1 Khái quát về an toàn thông tin

❖ Hệ thống thông tin là gì?

- 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 khách hàng;
 - 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 Khái quát về an toàn thông tin

- ❖ Hệ thống thông tin là gì?

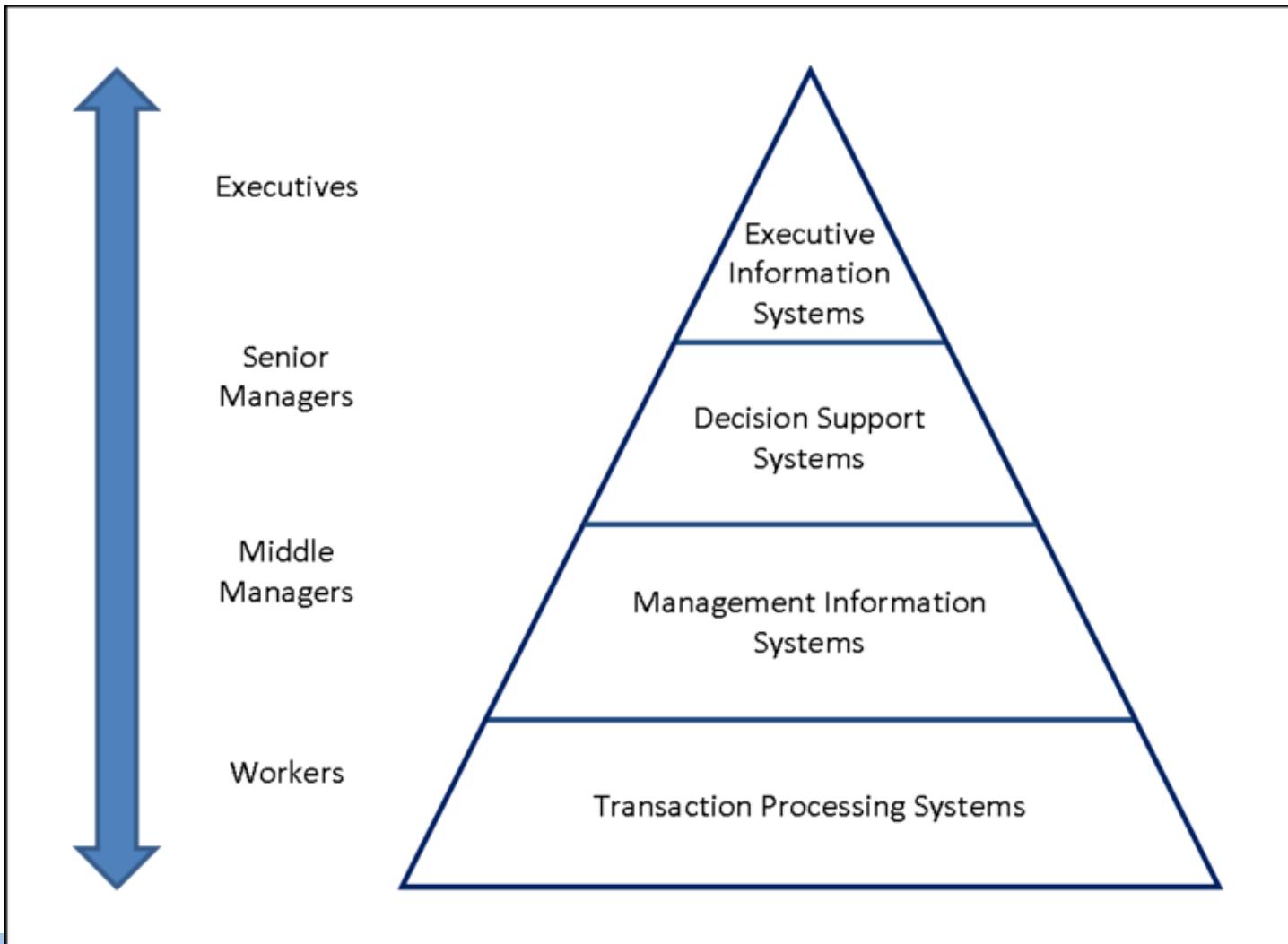


1.1 Khái quát về an toàn thông tin

- ❖ Các loại hệ thống thông tin (mô hình tháp): gồm 4 loại theo đối tượng sử dụng:
 - Hệ thống xử lý giao dịch (Transactional Processing Systems) với người sử dụng là các nhân viên (Workers);
 - Hệ thống thông tin quản lý (Management Information Systems) với người sử dụng là các quản lý bộ phận (Middle Managers);
 - Hệ thống trợ giúp ra quyết định (Decision Support Systems) với người sử dụng là các quản lý cao cấp (Senior Managers);
 - Hệ thống thông tin điều hành (Executive Information Systems) với người sử dụng là các Giám đốc điều hành (Executives).

1.1 Khái quát về an toàn thông tin

- ❖ Các loại hệ thống thông tin (mô hình tháp)



1.1 Khái quát về an toàn thông tin

❖ Một số hệ thống thông tin điển hình:

- Các kho dữ liệu (data warehouses)
- Các hệ lập kế hoạch nguồn lực doanh nghiệp (enterprise resource planning)
- Các hệ thống thông tin doanh nghiệp (enterprise systems)
- Các hệ chuyên gia (expert systems)
- Các máy tìm kiếm (search engines)
- Các hệ thống thông tin địa lý (geographic information system)
- Các hệ thống thông tin toàn cầu (global information system)
- Các hệ tự động hóa văn phòng (office automation).

1.1 Khái quát về an toàn 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, đưa ra kết quả mong muốn.

1.1 Khái quát về an toàn thông tin

❖ An toàn thông tin (Information Security) là gì?

- An toàn thông tin là việc bảo vệ chống truy nhập (access), sử dụng (use), tiết lộ (disclose), sửa đổi (modify), hoặc phá hủy (destroy) thông tin một cách trái phép (unauthorised).

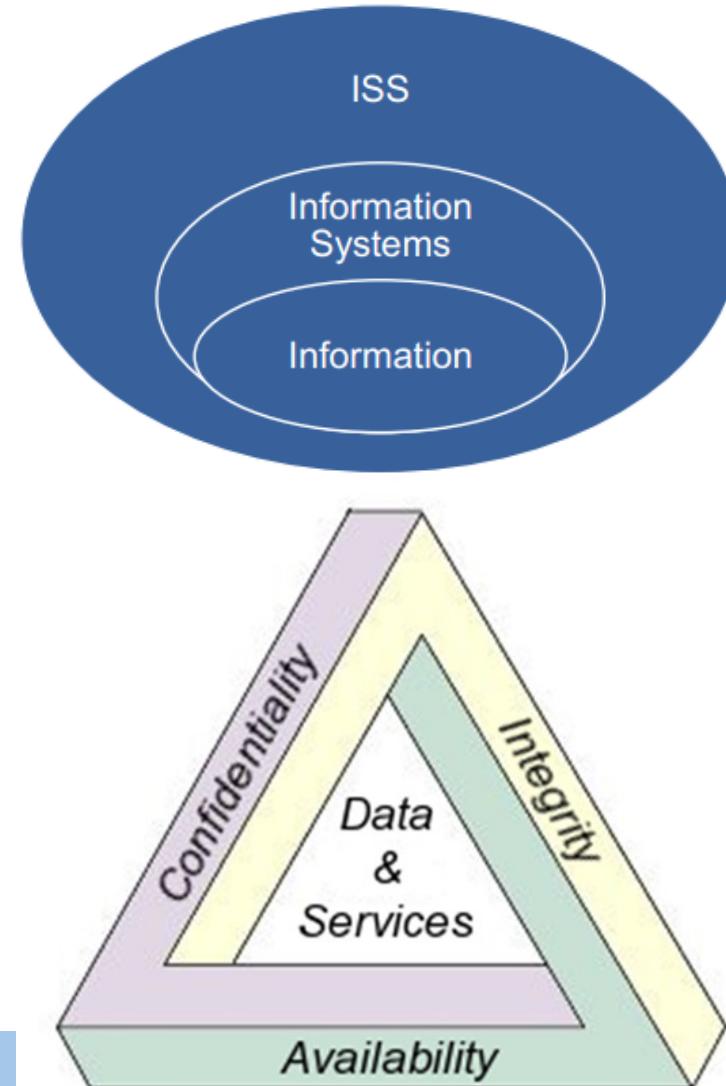
1.1 Khái quát về an toàn thông tin

❖ Hai lĩnh vực chính của an toàn thông tin (ATTT):

- 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;
 - Các hệ thống công nghệ thông tin của 1 tổ chức cần được đảm bảo an toàn khỏi các tấn công mạng.
- Đảm bảo thông tin (Information Assurance):
 - Đảm bảo thông tin không bị mất khi xảy ra các sự cố (thiên tai, hỏng hóc hệ thống, trộm cắp, phá hoại,...);
 - Thường sử dụng kỹ thuật tạo dự phòng ngoại vi (offsite backup).

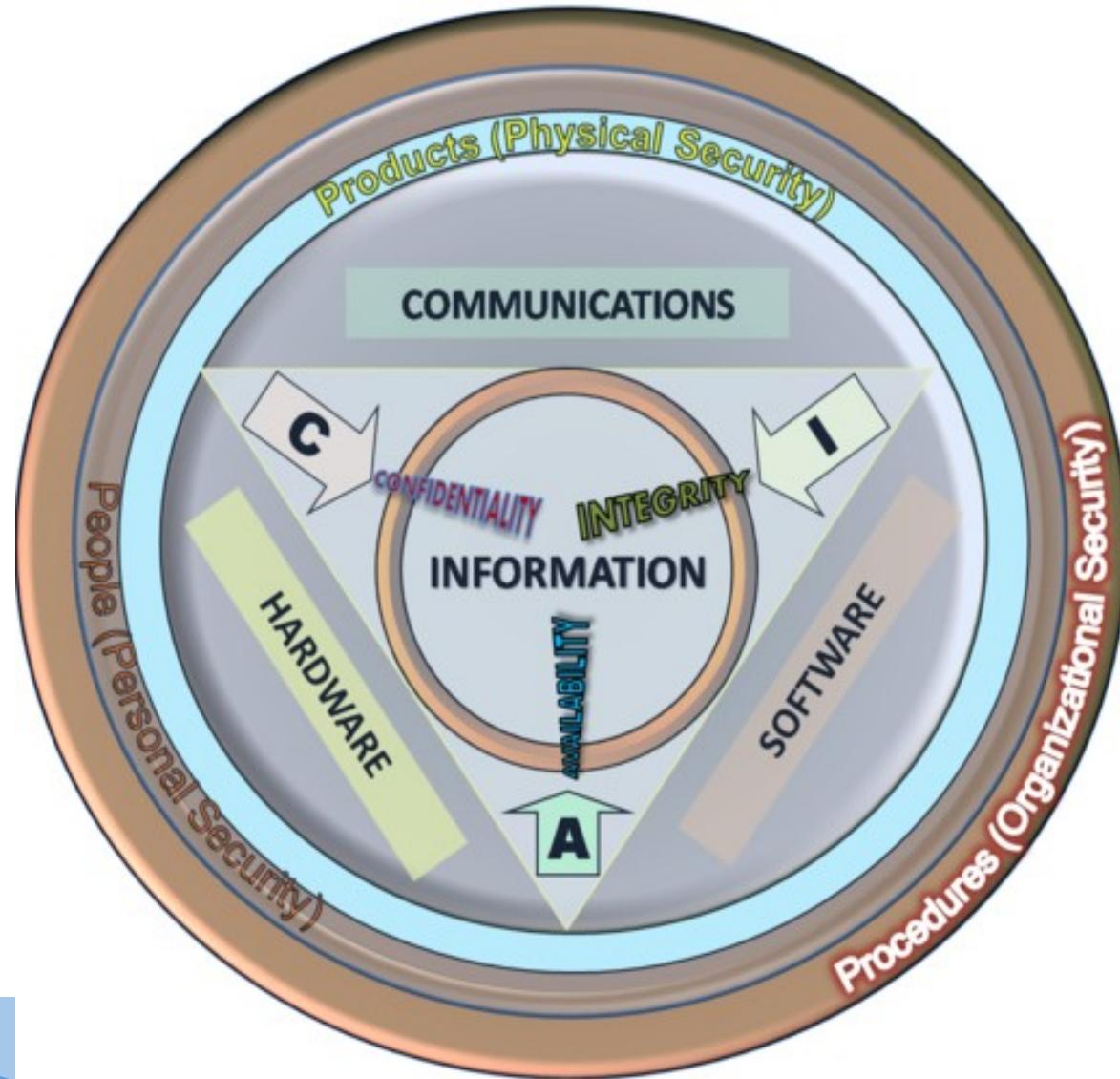
1.1 Khái quát về an toàn thông tin

- ❖ 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, bao gồm:
 - Bí mật (Confidentiality)
 - Toàn vẹn (Integrity)
 - Sẵn dùng (Availability)



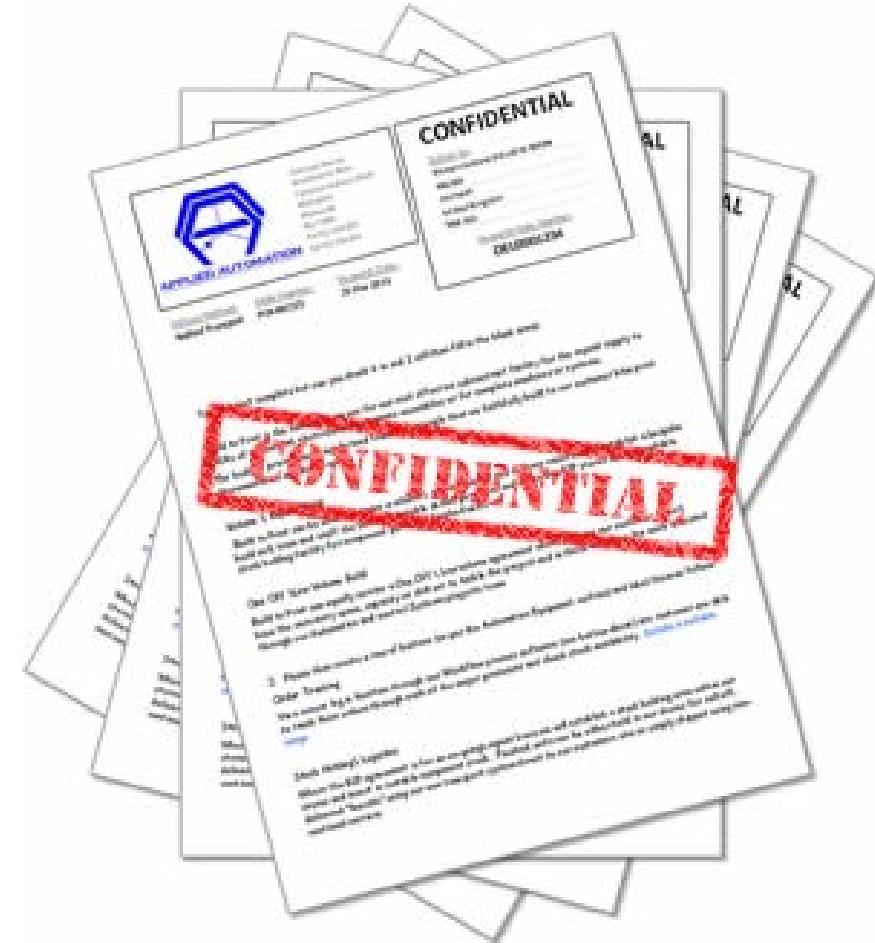
1.1 Khái quát về an toàn thông tin

- ❖ An toàn hệ thống thông tin (ISS)



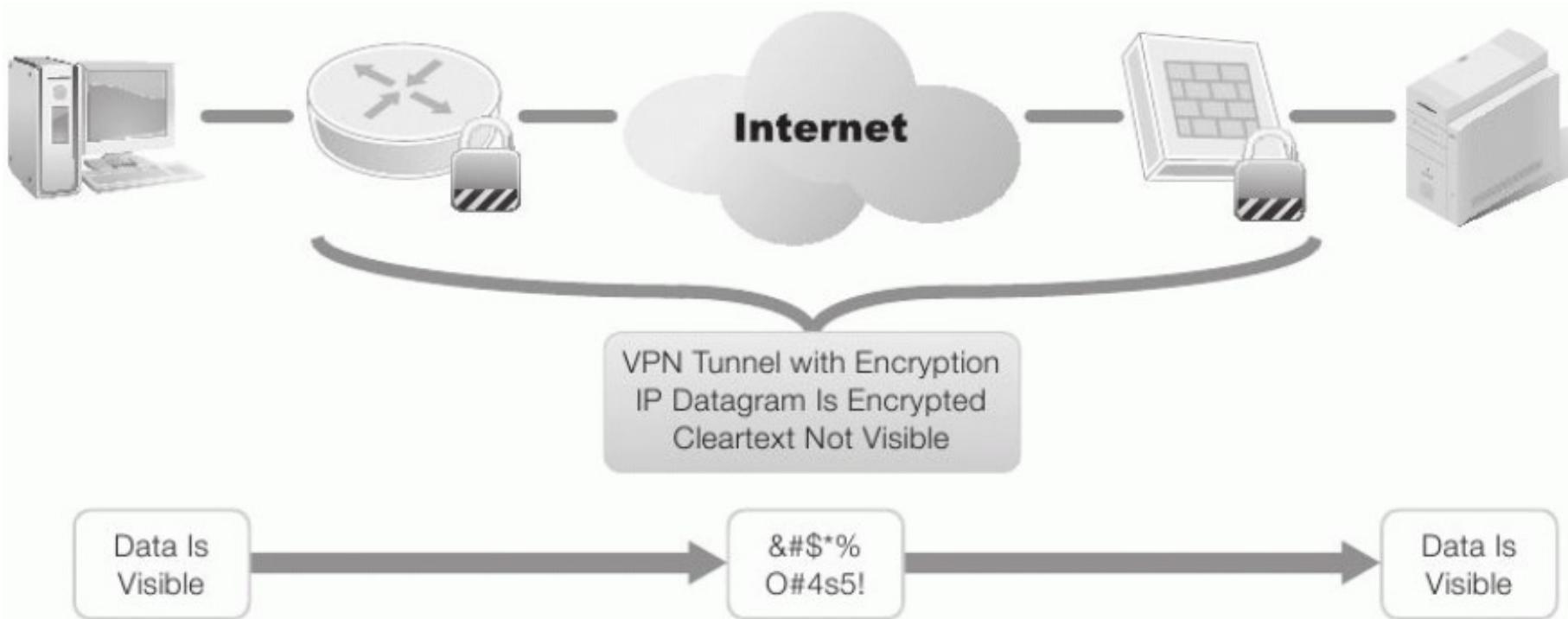
1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

- ❖ 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.



1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

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

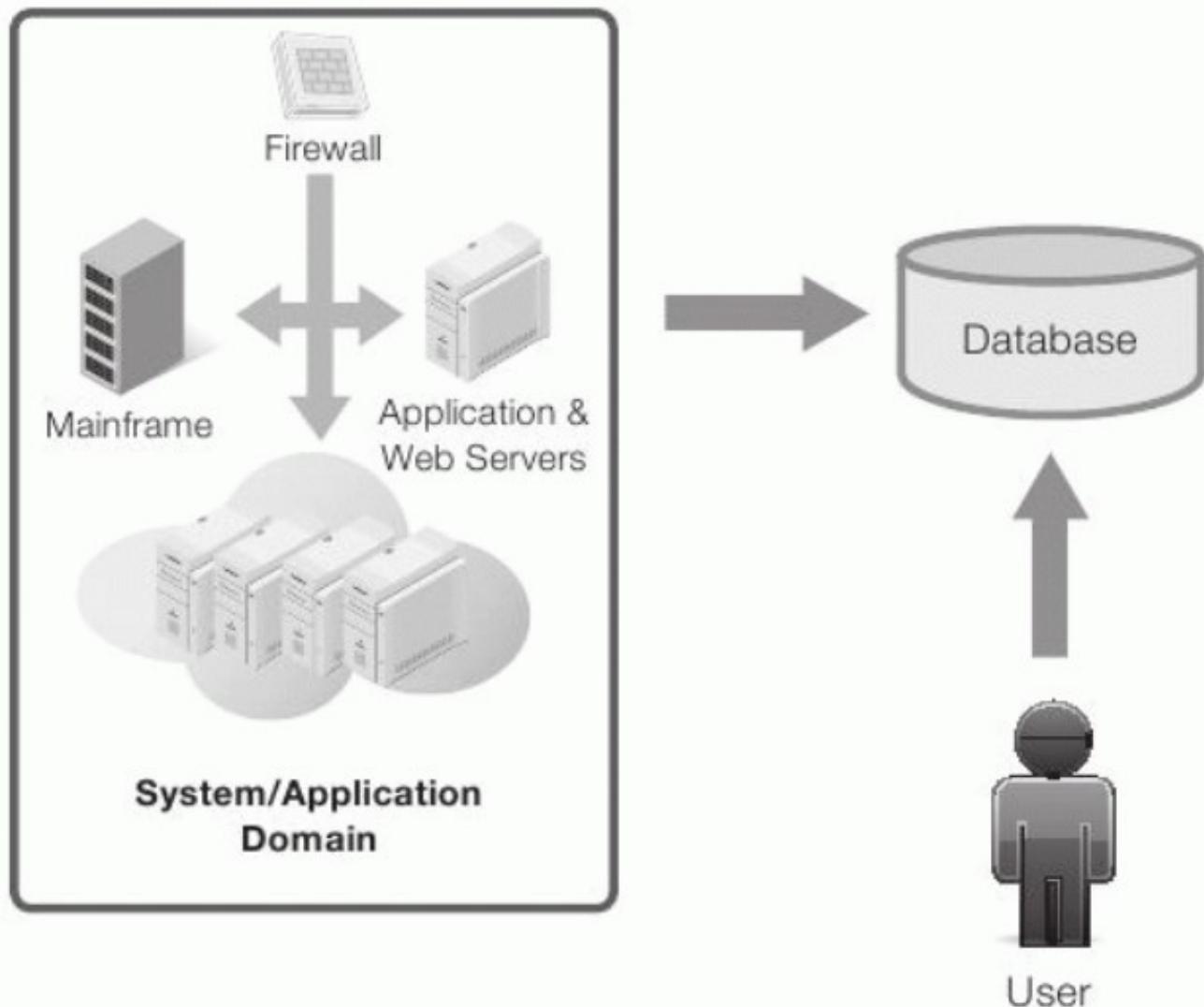


1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

- ❖ 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.

1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

- ❖ Tính toàn vẹn của hệ thống thông tin: thông tin chỉ có thể được sửa đổi bởi người dùng có thẩm quyền.

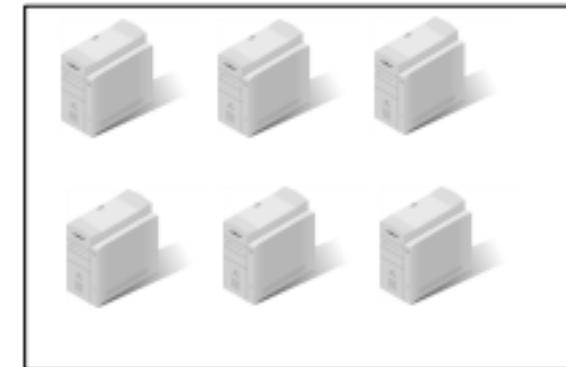
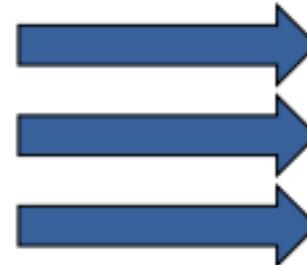
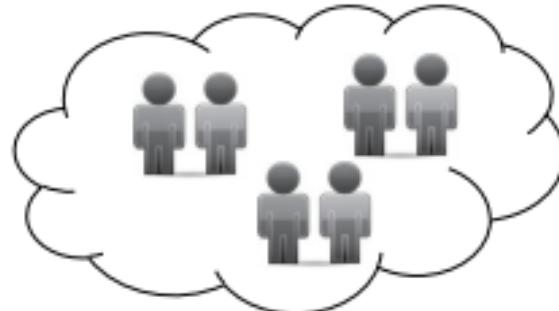
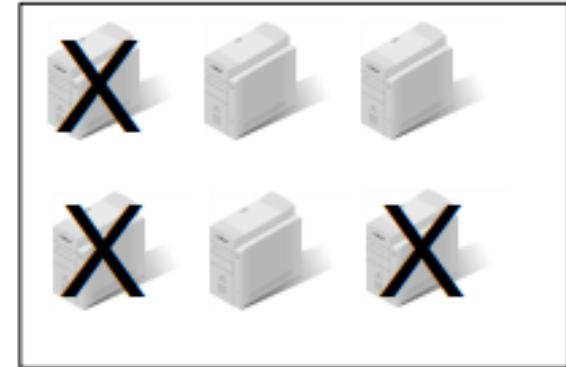
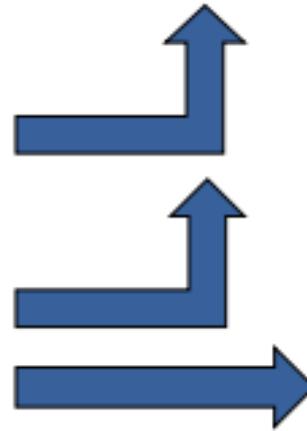
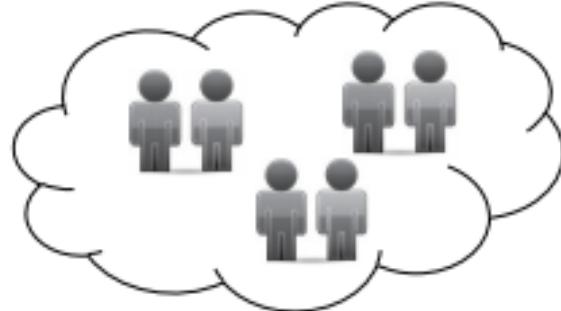


1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

- ❖ Tính sẵn dùng (Availability): thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.
- ❖ 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: $A = (\text{Uptime}) / (\text{Uptime} + \text{Downtime})$;
 - Thời gian trung bình giữa các sự cố;
 - Thời gian trung bình ngừng để sửa chữa;
 - Thời gian khôi phục sau sự cố.

1.2 Các yêu cầu đảm bảo ATTT và an toàn HTTT

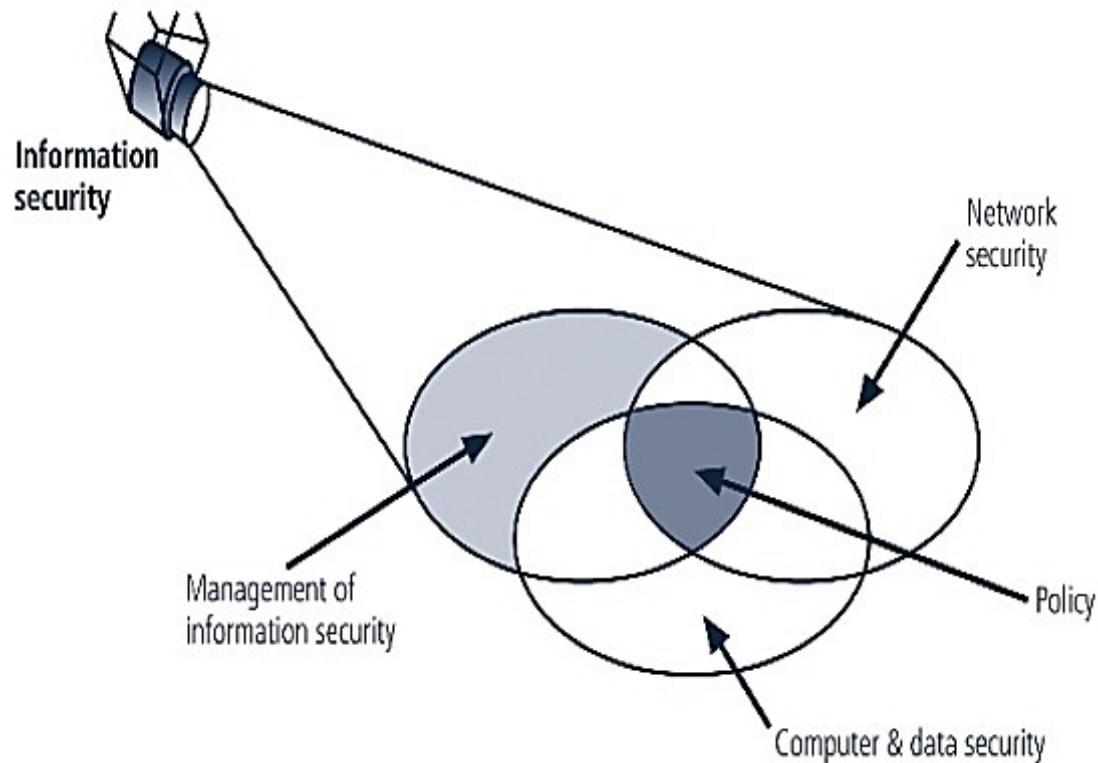
❖ Tính sẵn dùng



1.3 Các thành phần của an toàn thông tin

❖ Các thành phần của ATTT:

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



1.3 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.



1.3 Các thành phần của an toàn thông tin

❖ An ninh mạng:

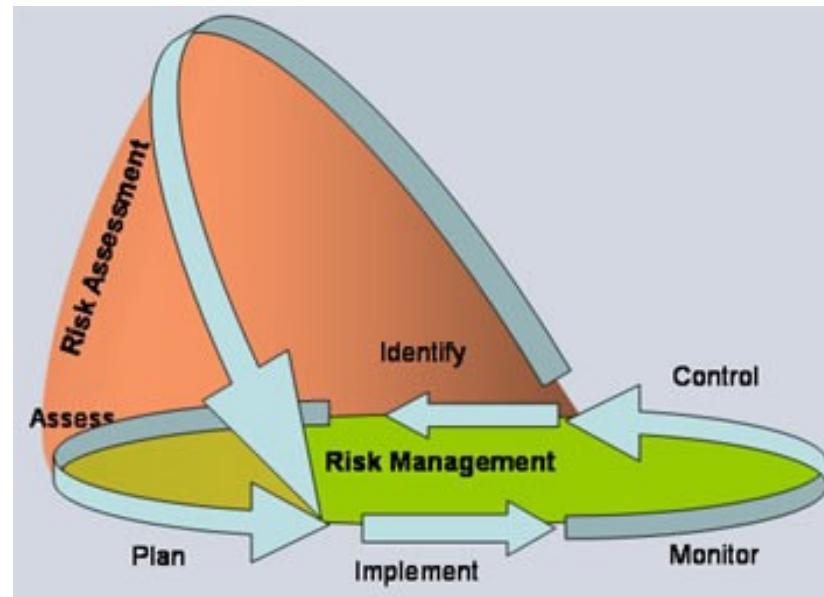
- Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập;
- Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- Vấn đề giám sát mạng.



1.3 Các thành phần của an toàn thông tin

❖ Quản lý an toàn thông tin:

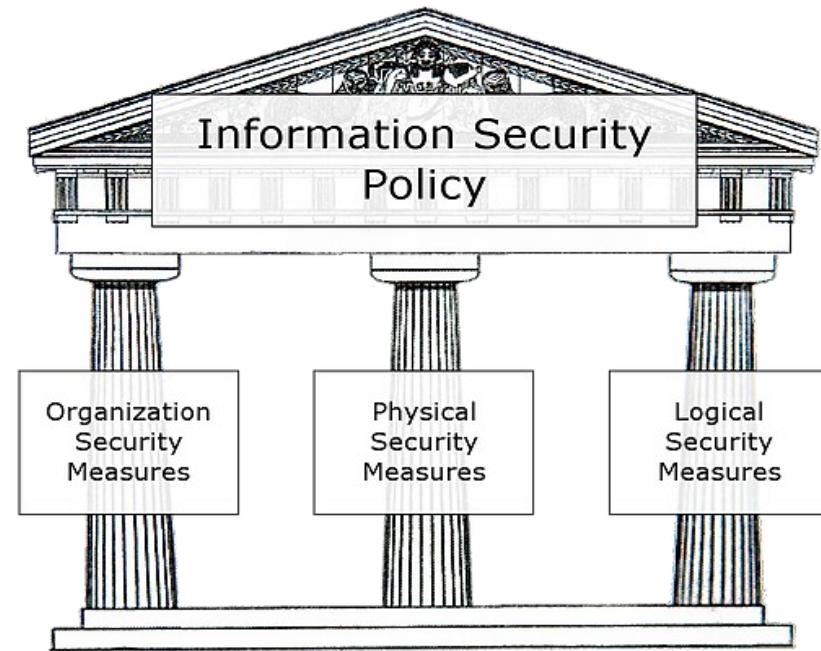
- Quản lý rủi ro
 - Nhận dạng
 - Đánh giá
- Thực thi quản lý an toàn thông tin
 - Lập kế hoạch (Plan)
 - Thực thi kế hoạch (Do/Implement)
 - Giám sát kết quả thực hiện (Monitor)
 - Thực hiện các kiểm soát (Control).



1.3 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).

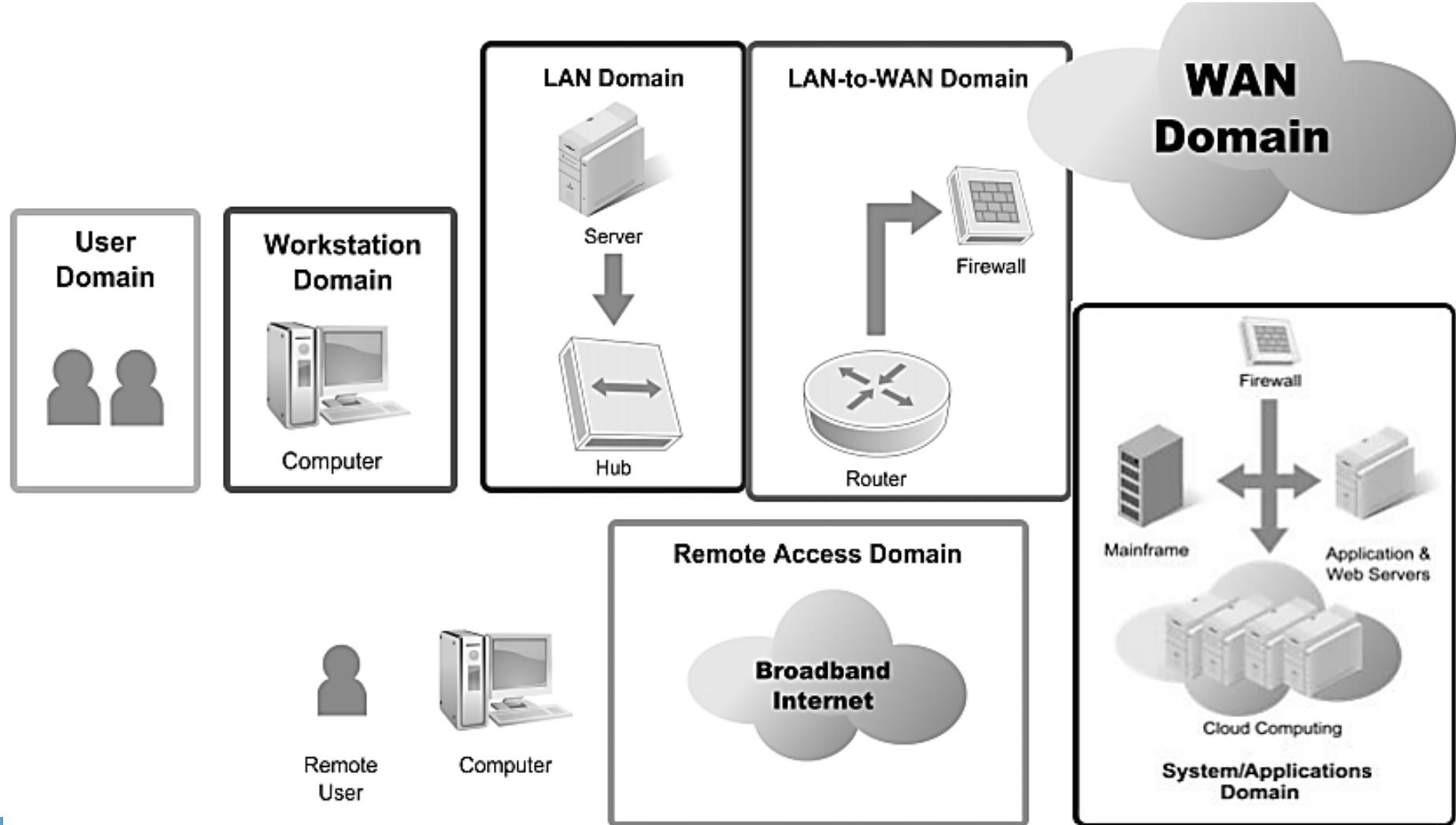


1.4 Các mối đe dọa & nguy cơ trong các vùng hạ tầng CNTT

❖ 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)

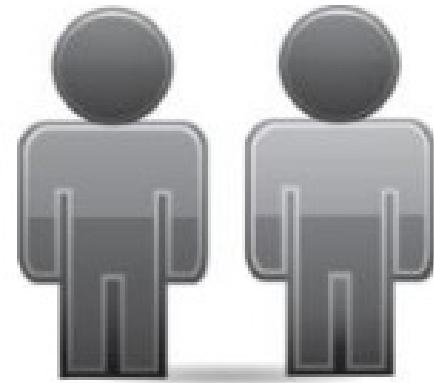
1.4 Các mối đe dọa & nguy cơ trong các vùng hạ tầng CNTT



1.4 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 thẻ tống tiền hoặc chiếm đoạt thông tin quan trọng.



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

❖ Các đe dọa (threats) với vùng máy trạm:

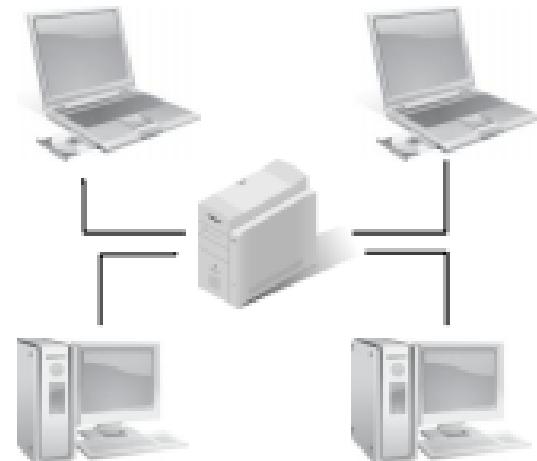
- Truy nhập trái phép vào máy trạm
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy trạm
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy trạm
- Các hiểm họa từ virus, mã độc và các phần mềm độc hại
- Người dùng đưa CD/DVD/USB với các files cá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



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

❖ Các đe dọa (threats) với vùng LAN:

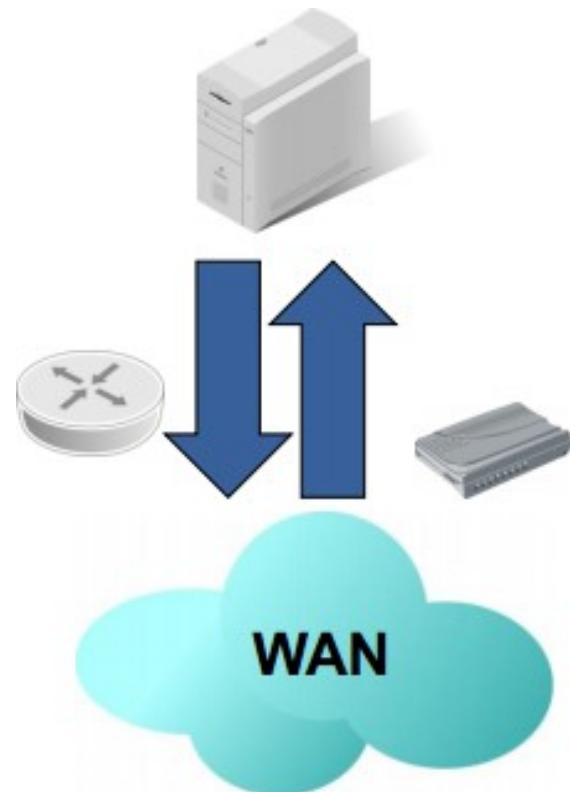
- Truy nhập trái phép vào mạng LAN vật lý
- Truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu
- Các lỗ hổng an ninh trong hệ điều hành máy chủ
- Các lỗ hổng an ninh trong các phần mềm ứng dụng máy chủ
- Nguy cơ từ người dùng giả mạo trong mạng WLAN
- Tính bí mật dữ liệu trong mạng WLAN có thể bị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



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

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

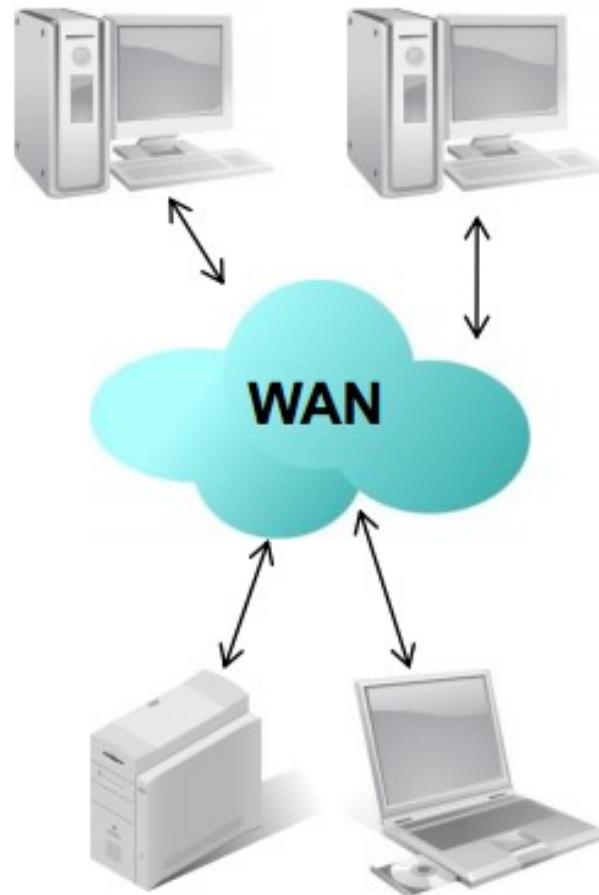
- Thăm dò và rà quét trái phép các cổng dịch vụ
- Truy nhập trái phép
- Lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác
- Người dùng cục bộ (trong LAN) có thể tải các file không xác định nội dung từ các nguồn không xác định.



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

❖ Các đe dọa (threats) với vùng WAN:

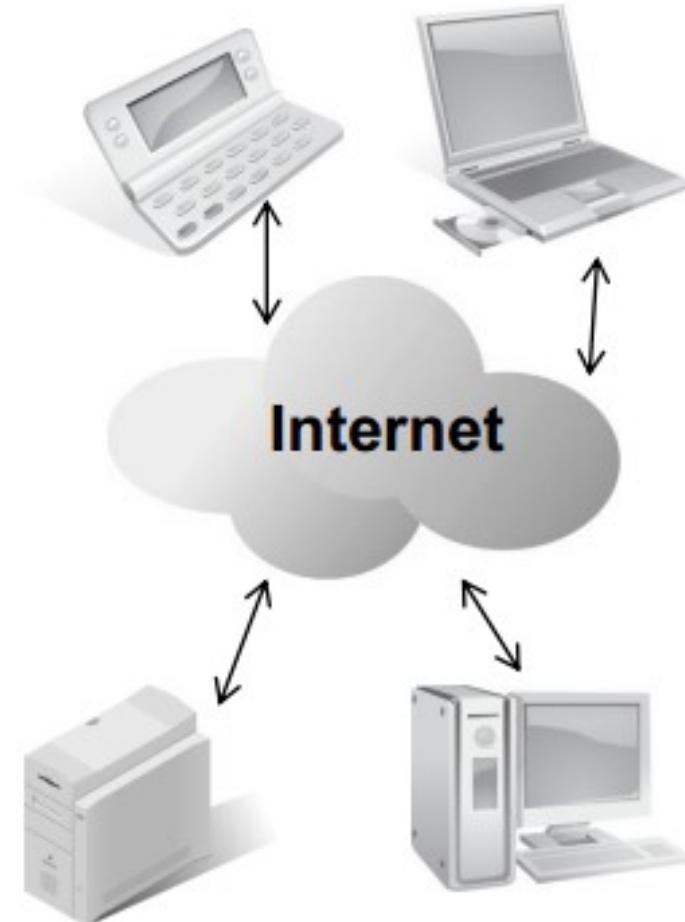
- Rủi ro từ việc dữ liệu có thể được truy nhập trong môi trường công cộng và mở
- Hầu hết dữ liệu được truyền dưới dạng rõ (cleartext/plaintext)
- Dễ bị nghe trộm
- Dễ bị tấn công phá hoại
- Dễ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS)
- Kẻ tấn công có thể tự do, dễ dàng gửi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



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

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

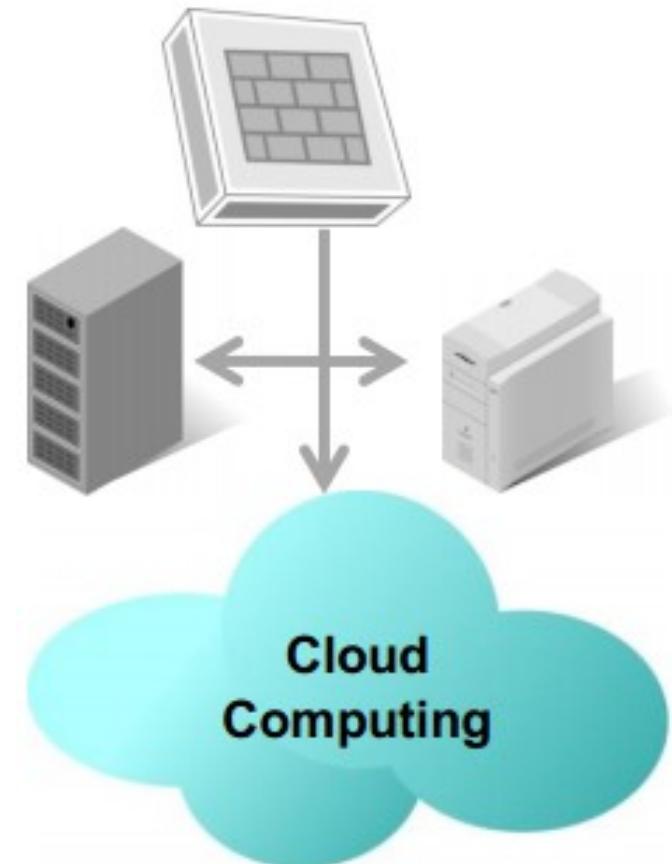
- Tấn công kiểu vét cạn (brute force) vào tên người dùng và mật khẩu
- Tấn công vào hệ thống đăng nhập và điều khiển truy cập
- Truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu
- Thông tin bí mật có thể bị đánh cắp từ xa
- Dò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.



1.4 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.



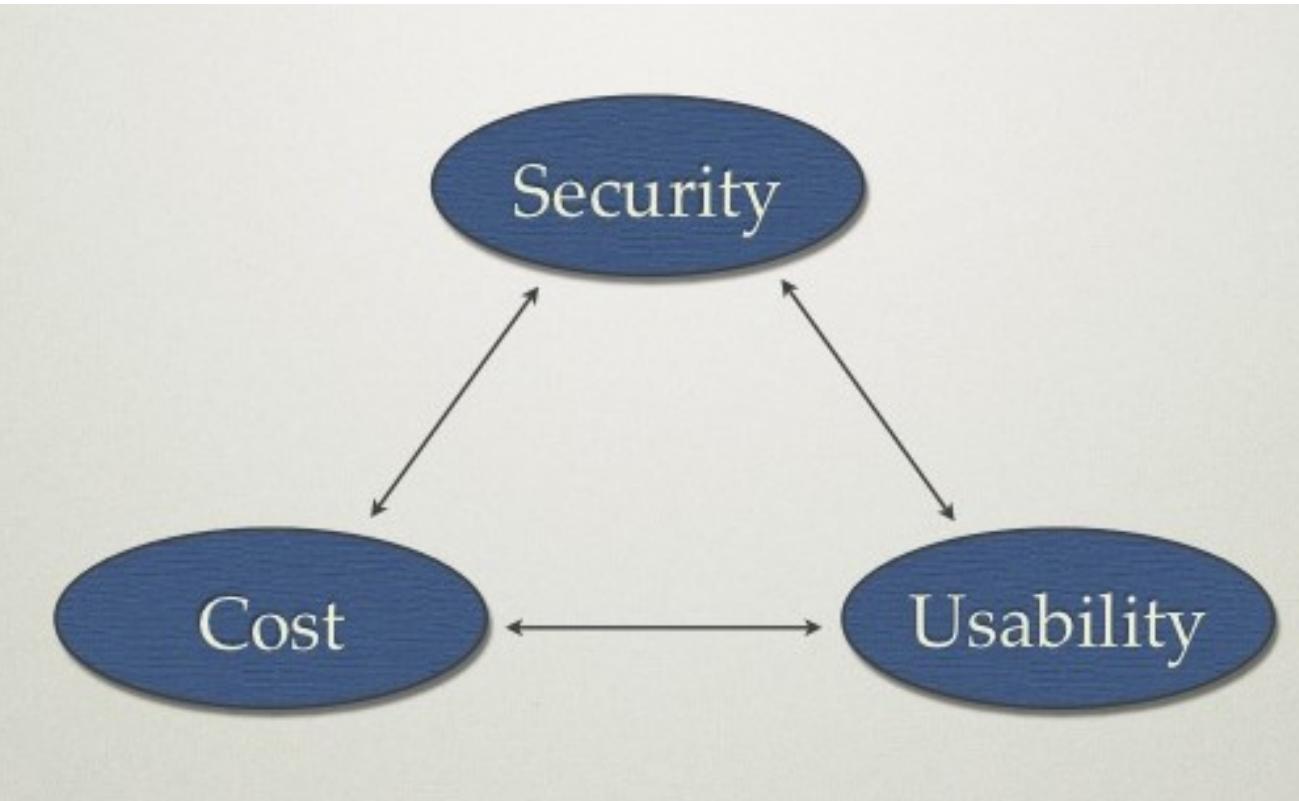
1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

❖ 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 độ an toàn, tính hữu dụng và chi phí.

1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

- ❖ Cần cân bằng giữa Usability (tính hữu dụng), Cost (chi phí) và Security (độ an toàn)



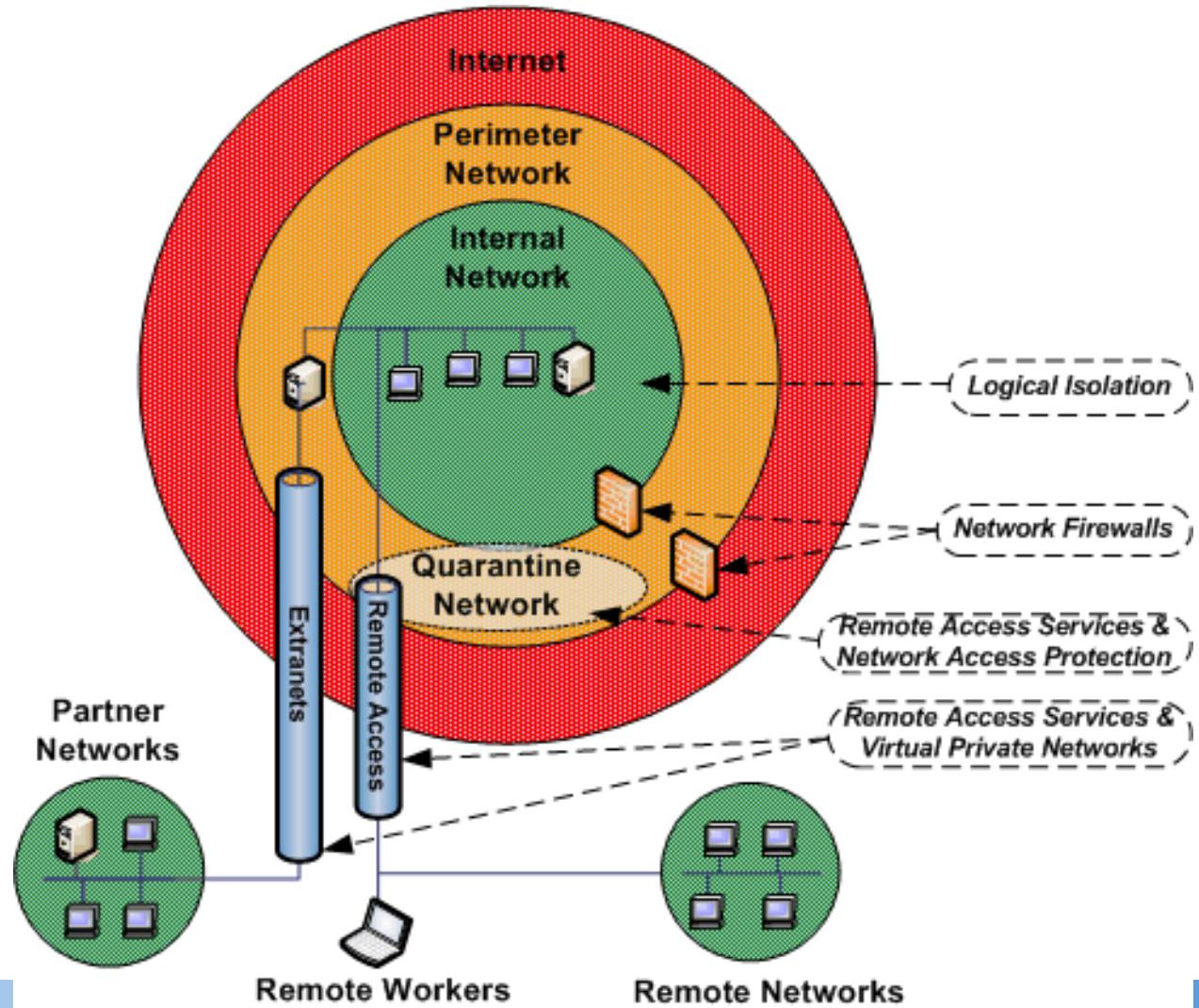
1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

- ❖ Mô hình Layered Security Model hoặc Defence in Depth



1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

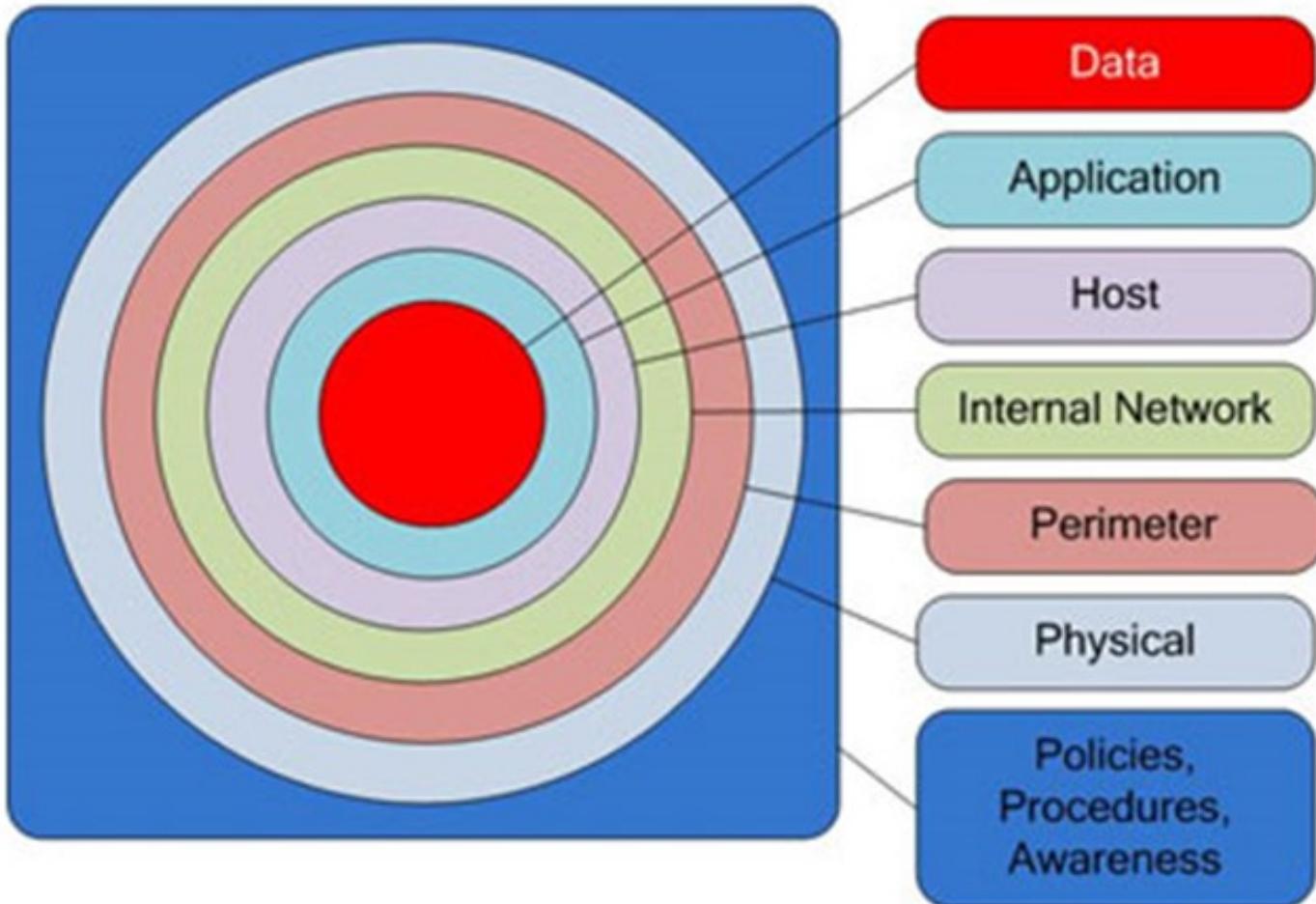
- ❖ Mô hình Layered Security Model hoặc Defence in Depth



1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

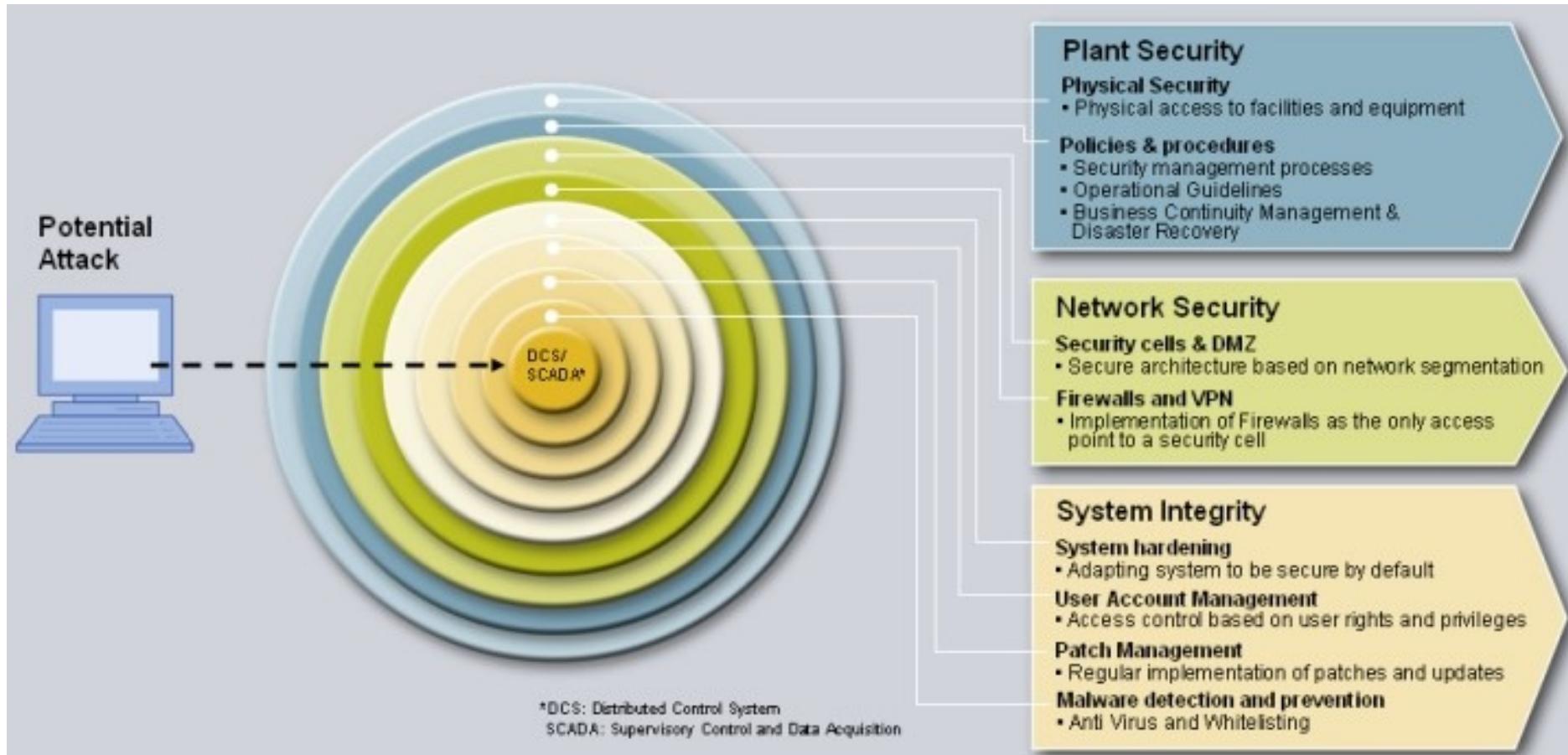
- ❖ Mô hình Layered Security Model hoặc Defence in Depth

Defense in Depth Layers



1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

❖ Mô hình Layered Security Model hoặc Defence in Depth



1.5 Mô hình tổng quát đảm bảo ATTT và an toàn HTTT

❖ Các lớp phòng vệ điển hình:

- 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 Integrity)
 - 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.



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN**

**CHƯƠNG 2 - LỖ HỒNG BẢO MẬT
VÀ ĐIỂM YẾU HỆ THỐNG**

Giảng viên:

E-mail:

Khoa:

PGS.TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

An toàn thông tin

NỘI DUNG CHƯƠNG 2

1. Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống
2. Các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng
3. Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống
4. Giới thiệu một số công cụ rà quét lỗ hổng bảo mật.

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- ❖ Các thành phần của hệ thống máy tính
- ❖ Khái niệm điểm yếu hệ thống và các lỗ hổng bảo mật
- ❖ Phân bố các lỗ hổng bảo mật:
 - Phần cứng / phần mềm
 - Các hệ điều hành phổ biến
 - Các ứng dụng phổ biến

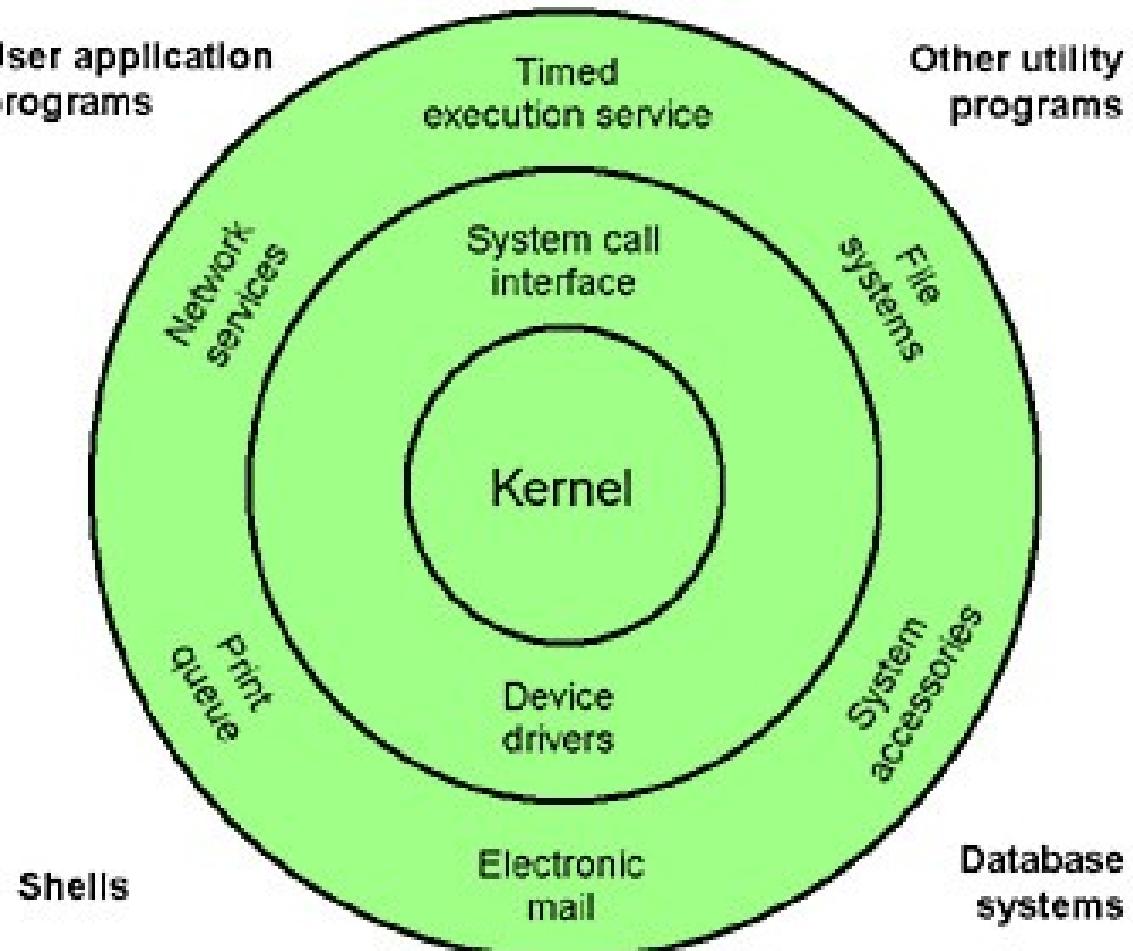
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

❖ Các thành phần của hệ thống máy tính:

- Hệ thống phần cứng
 - CPU, ROM, RAM, Bus,...
 - Các giao diện ghép nối và các thiết bị ngoại vi.
- Hệ thống phần mềm
 - Hệ điều hành
 - Nhân hệ điều hành, các trình điều khiển thiết bị
 - Các trình cung cấp dịch vụ, tiện ích,...
 - Các phần mềm ứng dụng
 - Các dịch vụ (máy chủ web, CSDL, DNS,...)
 - Trình duyệt web, các ứng dụng giao tiếp,...
 - Các bộ ứng dụng văn phòng, lập trình.

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Mô hình
hệ điều
hành
Unix/Linux,
các dịch vụ
và các ứng
dụng



2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- ❖ Các điểm yếu hệ thống (system weaknesses) là các lỗi hay các khiếm khuyết (thiết kế, cài đặt, phần cứng hoặc phần mềm) tồn tại trong hệ thống.
 - Các điểm yếu đã biết và đã được khắc phục;
 - Các điểm yếu đã biết và chưa được khắc phục;
 - Các điểm yếu chưa biết/chưa được phát hiện.

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- ❖ Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu trong một hệ thống cho phép kẻ tấn công khai thác gây tổn hại đến các thuộc tính an ninh, an toàn của hệ thống đó:
 - Toàn vẹn (integrity)
 - Bí mật (confidentiality)
 - Sẵn dùng (availability).

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- **Toàn vẹn (integrity):**
 - Mọi sửa đổi đến thông tin/hệ thống chỉ được thực hiện bởi các bên có đủ thẩm quyền;
 - Kẻ tấn công có thể lợi dụng điểm yếu an ninh để lăng lẽ sửa đổi thông tin/hệ thống → phá vỡ tính toàn vẹn;
 - Ví dụ:
 - Thông thường trong hệ thống kiểm soát truy nhập, chỉ người quản trị có quyền thay đổi quyền truy nhập đến mọi file;
 - Một điểm yếu trong hệ thống có thể cho phép một người dùng bình thường thay đổi quyền truy nhập đến mọi file tương tự người quản trị.

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

■ Bí mật (confidentiality):

- Chỉ những người có thẩm được phép truy nhập đến thông tin/hệ thống;
- Kẻ tấn công có thể lợi dụng điểm yếu an ninh để truy nhập trái phép → phá vỡ tính bí mật;
- Ví dụ:
 - Một điểm yếu an ninh cho phép người dùng web thường đọc được nội dung một file mà lẽ ra người đó không được quyền đọc;
 - Một điểm yếu trong hệ thống kiểm soát truy nhập cho phép một nhân viên bình thường đọc được các báo cáo “mật” của công ty mà chỉ Ban Giám đốc được phép đọc.

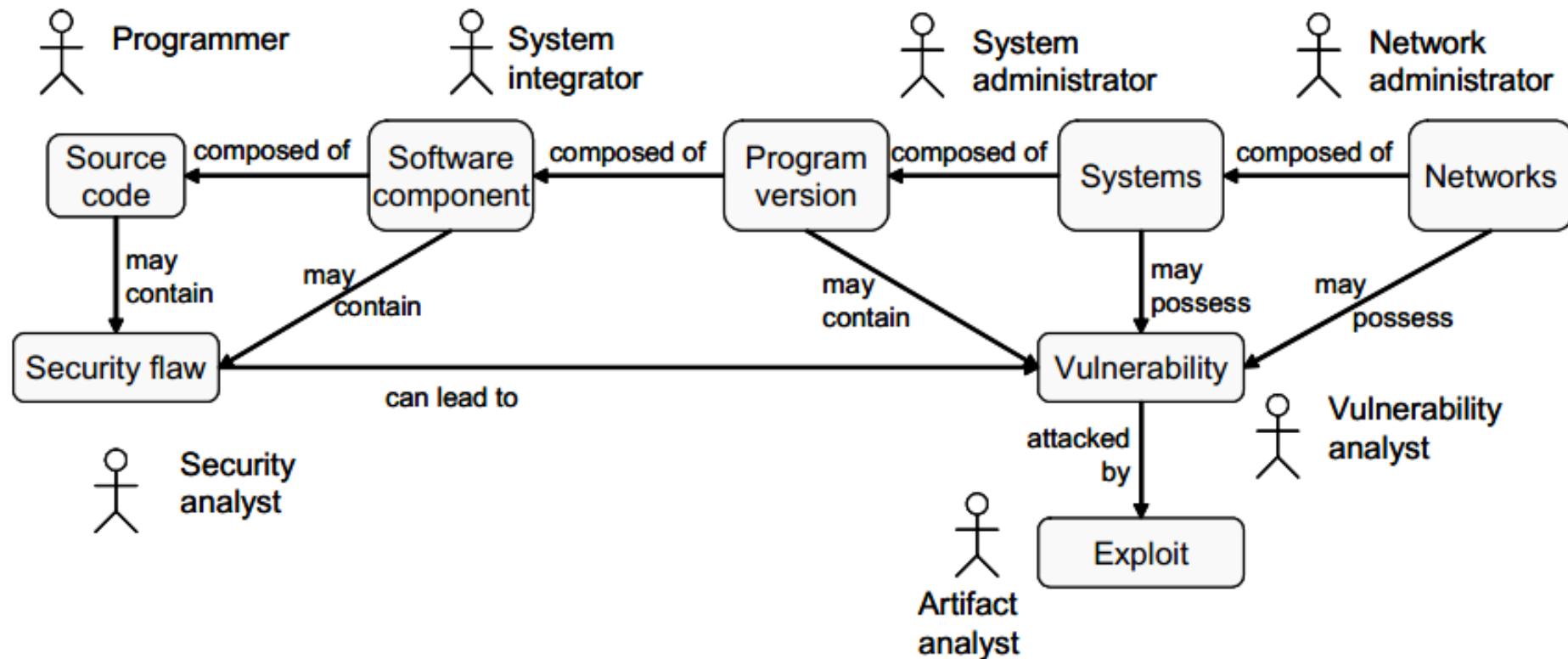
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

■ Sẵn dùng (availability):

- Đảm bảo khả năng truy nhập đến thông tin/hệ thống cho người dùng hợp pháp;
- Kẻ tấn công có thể lợi dụng điểm yếu an ninh để ngăn chặn hoặc gây khó khăn cho người dùng hợp pháp truy nhập vào thông tin/hệ thống;
- Ví dụ:
 - Một điểm yếu an ninh có thể cho phép kẻ tấn công làm máy chủ ngừng hoạt động → không thể cung cấp dịch vụ cho người dùng hợp pháp → phá vỡ tính sẵn dùng;
 - Kẻ tấn công cũng có thể gửi một lượng lớn yêu cầu giả mạo đến máy chủ gây cạn kiệt tài nguyên hoặc tắc nghẽn đường truyền → người dùng hợp pháp không thể truy cập → phá vỡ tính sẵn dùng.

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Mô hình các quan hệ giữa các đối tượng và vai trò trong hệ thống



2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- Source code: mã nguồn
- Software component: thành phần phần mềm
- Program version: phiên bản chương trình
- Systems: các hệ thống
- Networks: các mạng
- Security flaw: khiếm khuyết an ninh
- Vulnerability: lỗ hổng an ninh
- Exploit: khai thác lỗ hổng an ninh
- Programmer: lập trình viên
- System integrator: nhân viên tích hợp hệ thống
- System administrator: nhân viên quản trị hệ thống
- Network administrator: nhân viên quản trị mạng
- Security analyst: nhân viên phân tích an ninh
- Vulnerability analyst: nhân viên phân tích lỗ hổng an ninh
- Artifact analyst: nhân viên phân tích hiện vật.

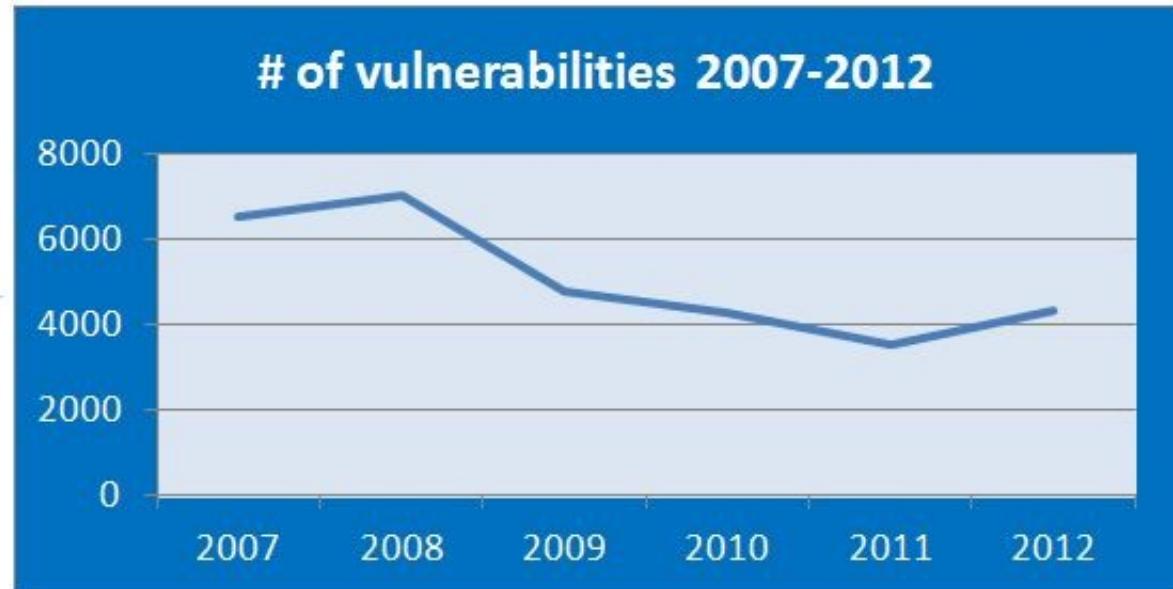
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

- Mức độ nghiêm trọng của lỗ hổng bảo mật:
 - 4 mức độ nghiêm trọng theo Microsoft:
 - Nguy hiểm (Critical)
 - Quan trọng (Important)
 - Trung bình (Moderate)
 - Thấp (Low).
 - 3 mức độ nghiêm trọng theo một số tổ chức khác:
 - Cao (High)
 - Trung bình (Medium)
 - Thấp (Low).

2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

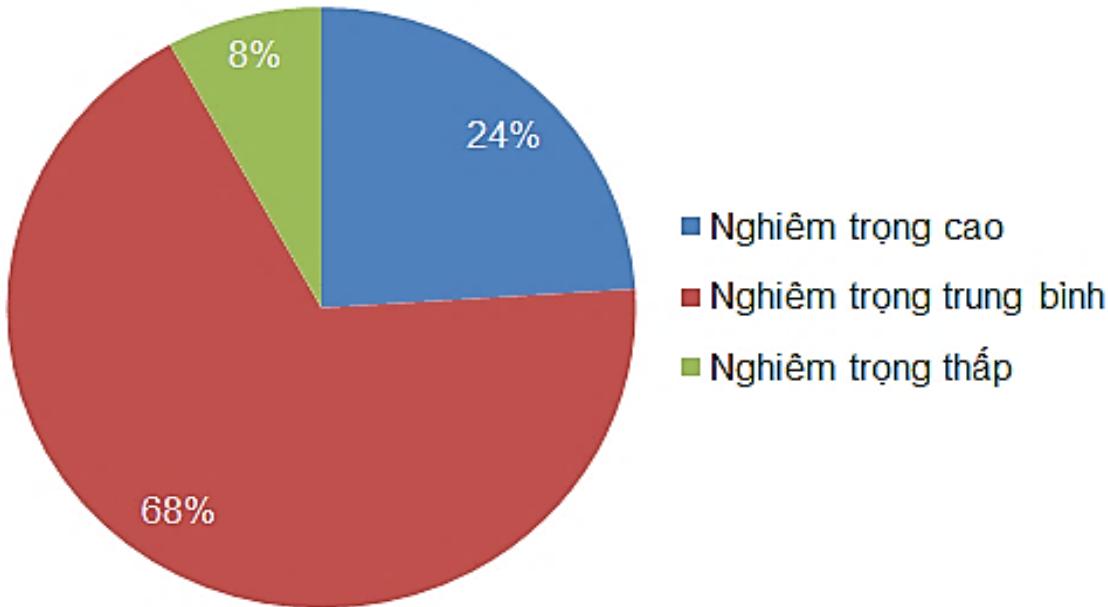
Số lượng các lỗ hổng bảo mật được phát hiện trong giai đoạn 2007-2012 (US National Vulnerability Database)

Year	# of vulnerabilities
2007	6496
2008	6992
2009	4783
2010	4258
2011	3532
2012	4347



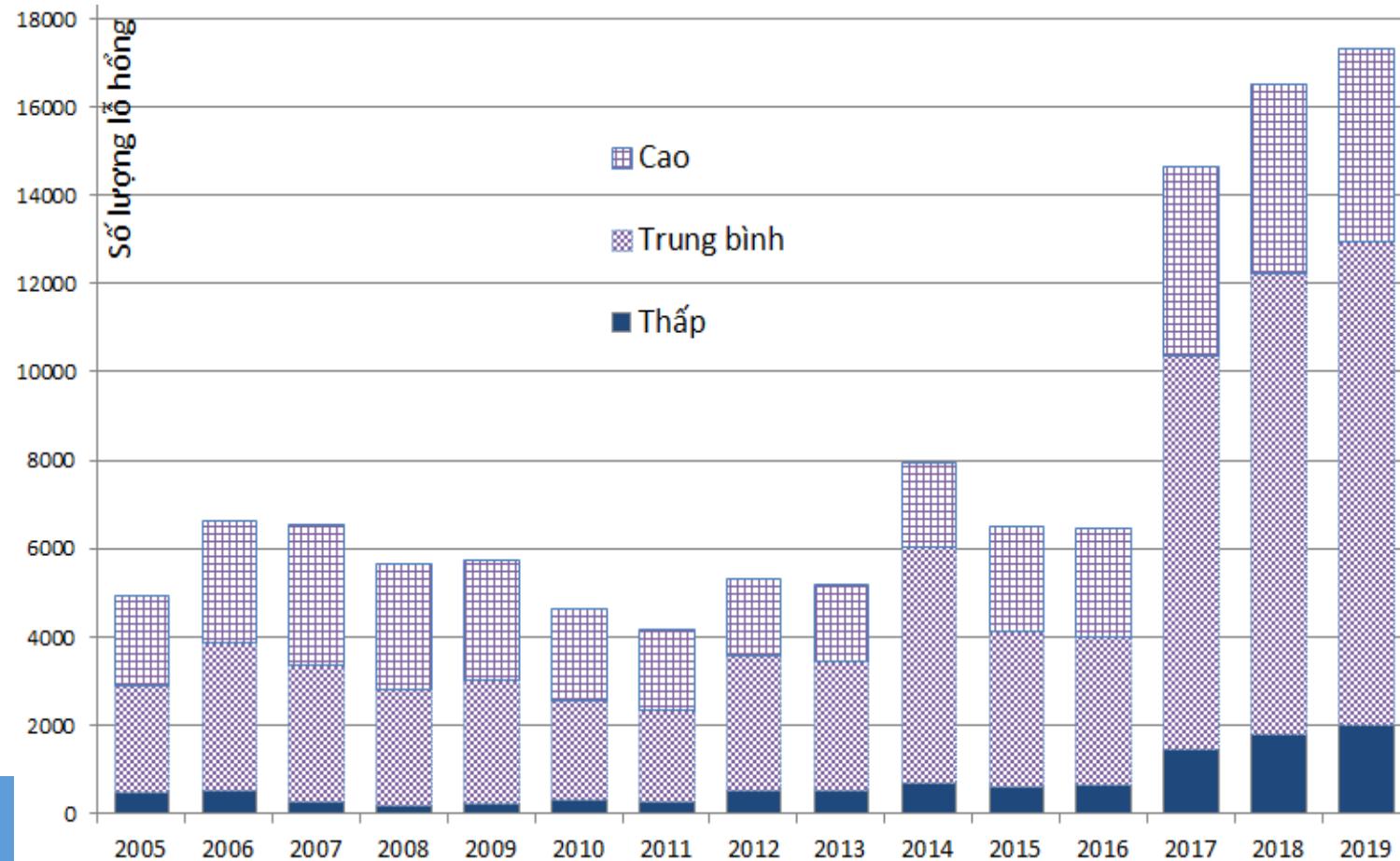
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Phân bố các lỗ hổng bảo mật phát hiện trong năm 2014
theo mức độ nghiêm trọng



2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Số lượng các lỗ hổng bảo mật nghiêm trọng phát hiện trong giai đoạn 2005-2019

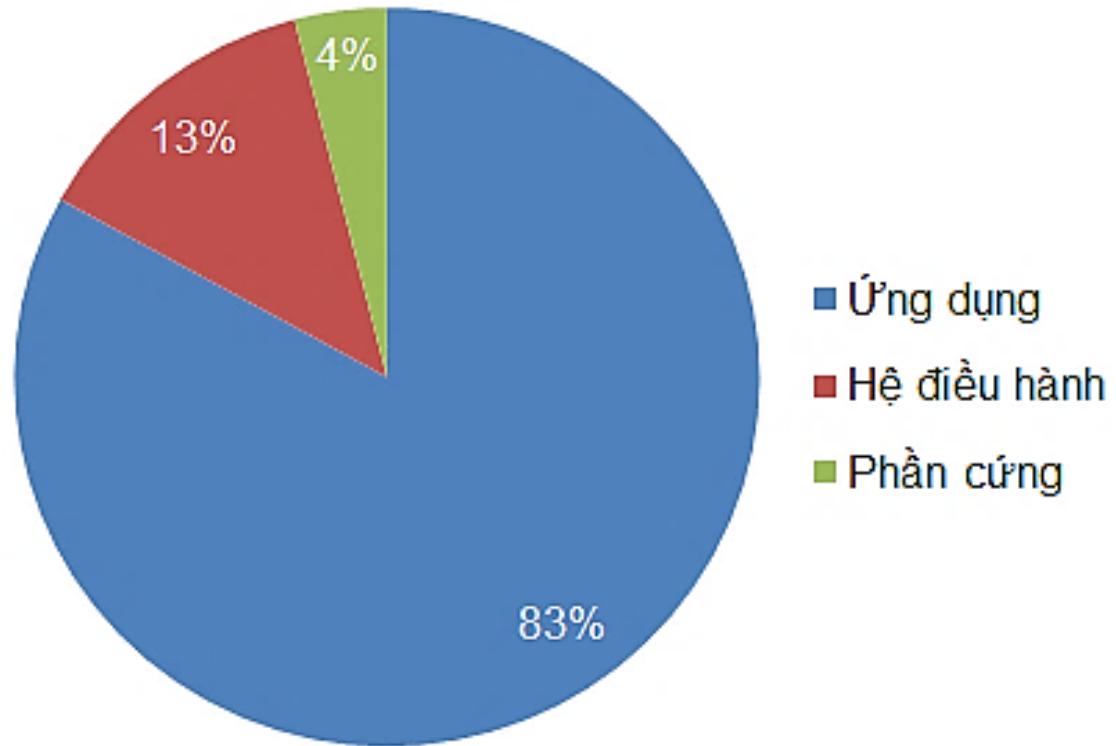


2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Vendor	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2012	2011	2012	2011	2012	2011	2012	2011
Oracle	↑ 424	262	↑ 76	46	↑ 238	163	↑ 110	53
Apple	↑ 270	246	↑ 141	139	↑ 115	89	↓ 14	18
Mozilla	↑ 195	110	↑ 118	65	↑ 72	42	↑ 5	3
Microsoft	↓ 169	244	↓ 117	195	↑ 48	46	↑ 4	3
IBM	↑ 154	143	↓ 42	50	↑ 94	82	↑ 18	11
Google	↓ 150	299	↓ 79	173	↓ 66	125	↑ 5	1
Adobe	↓ 137	189	↓ 127	153	↓ 10	36	● 0	0
Cisco	↓ 134	135	↓ 85	109	↑ 45	24	↑ 4	2
HP	↓ 74	144	↓ 38	79	↓ 31	60	● 5	5
Apache	↑ 55	44	↑ 10	3	↑ 41	37	● 4	4

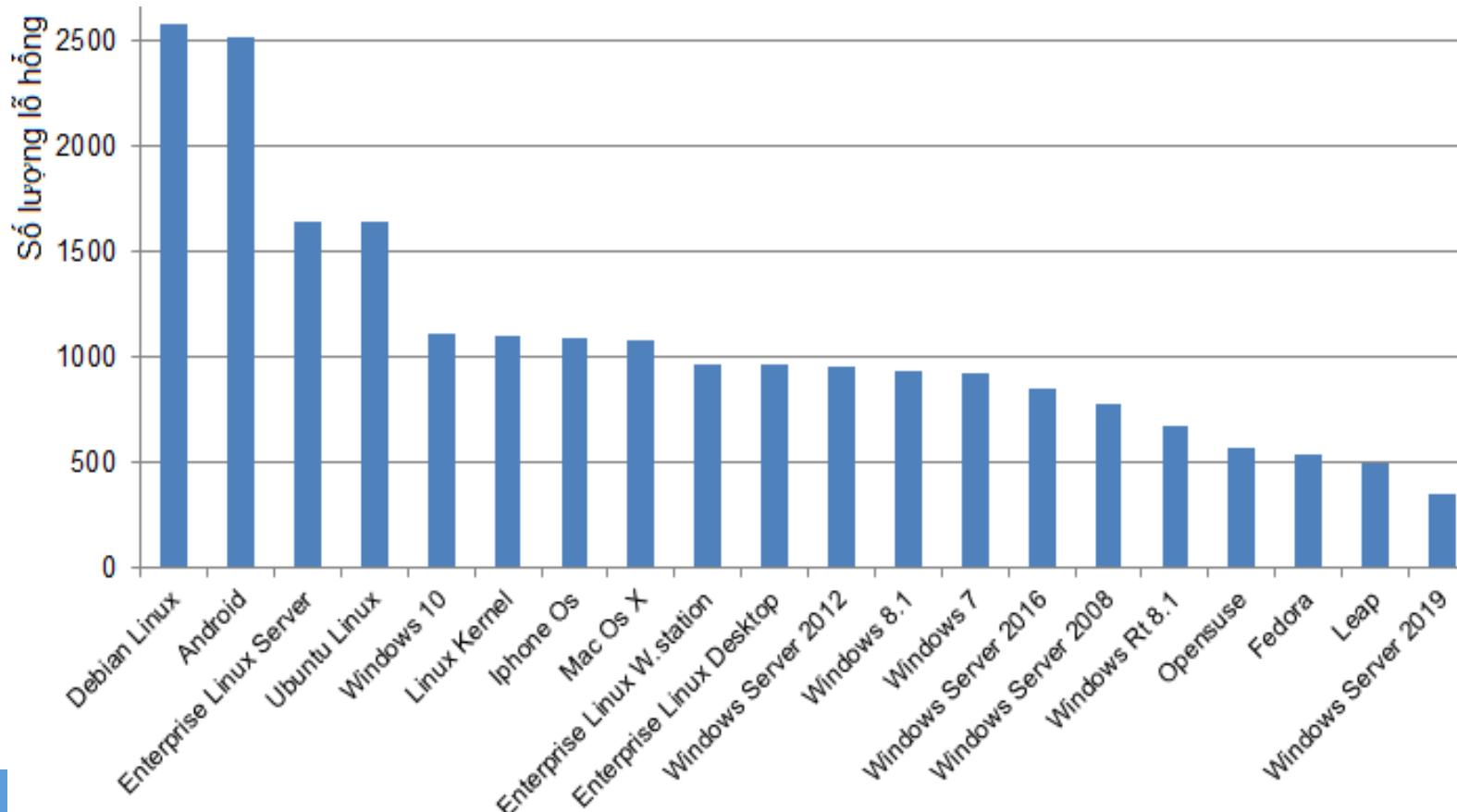
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Phân bố các lỗ hổng bảo mật phát hiện trong năm 2014 trên các thành phần của hệ thống



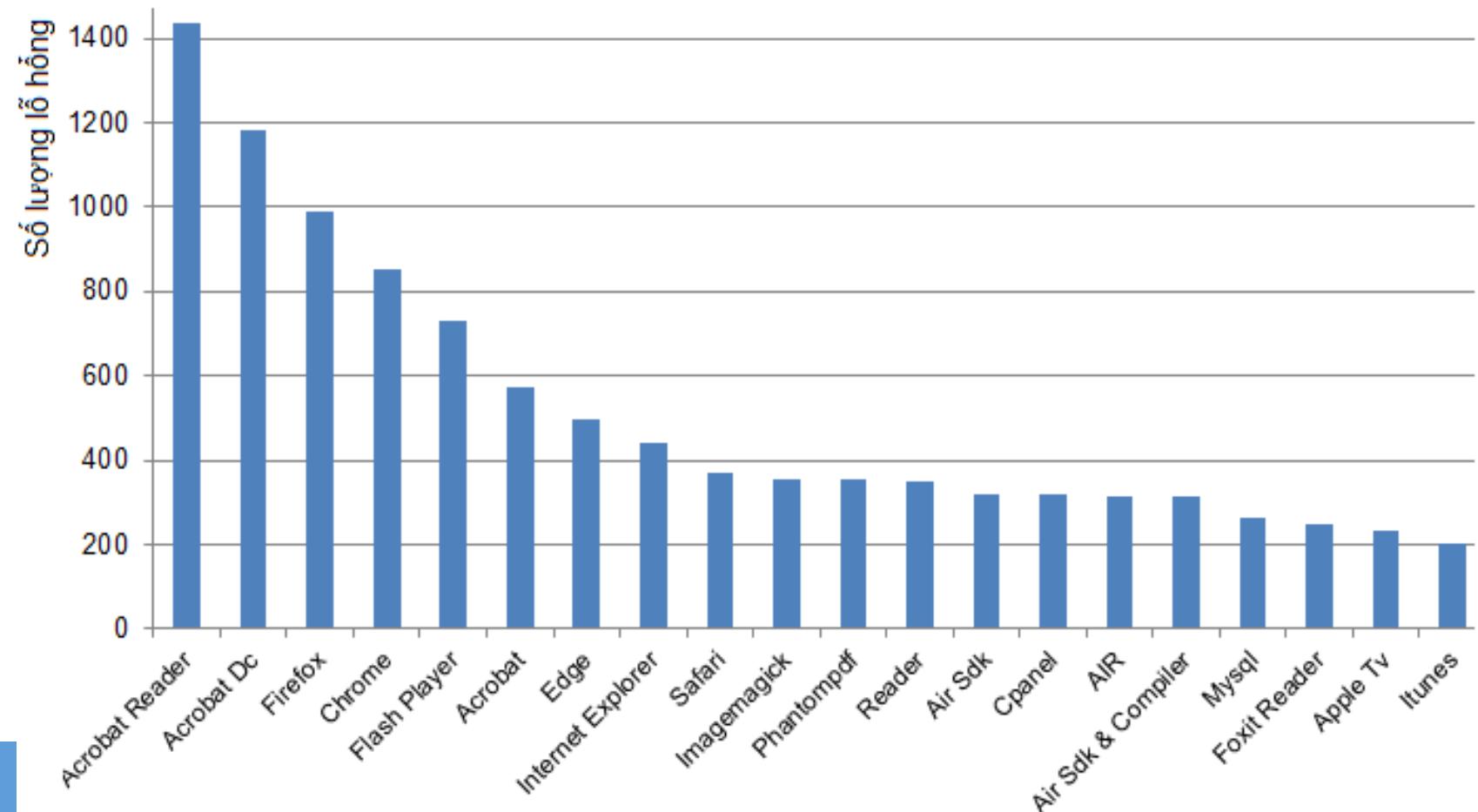
2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Top 20 hệ điều hành có nhiều lỗ hổng được phát hiện từ 2015-2019



2.1 Tổng quan về lỗ hổng bảo mật và điểm yếu hệ thống

Top 20 ứng dụng có nhiều lỗ hổng được phát hiện từ 2015-2019



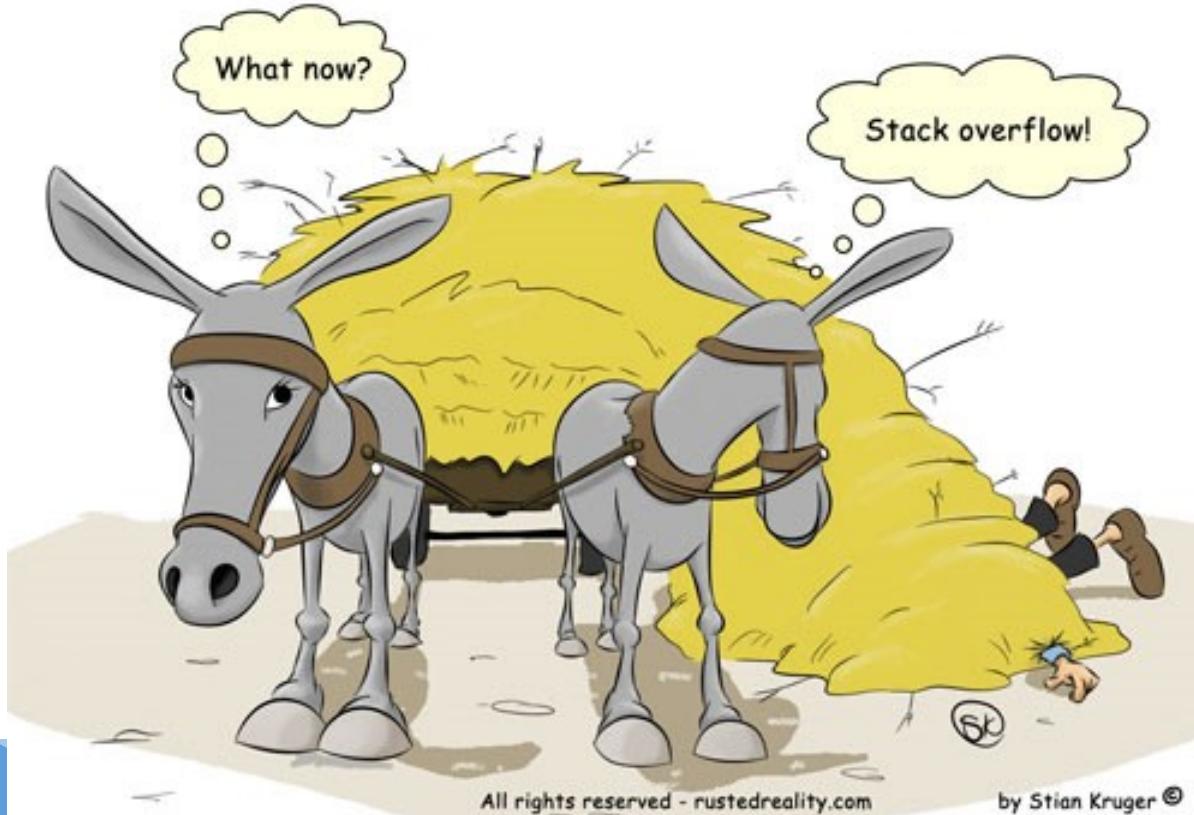
2.2 Các dạng lỗ hổng trong HĐH và phần mềm ứng dụng

❖ Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng:

- Lỗi tràn bộ đệm (buffer overflows)
- Không kiểm tra đầu vào (unvalidated input)
- Các vấn đề với điều khiển truy cập (access-control problems)
- Các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (weaknesses in authentication, authorization, or cryptographic practices)
- Các lỗ hổng bảo mật khác.

2.2.1 Các dạng lỗ hổng - Lỗi tràn bộ đệm

- ❖ Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi bộ đệm (giới hạn cuối hoặc cả giới hạn đầu của bộ đệm);



2.2.1 Các dạng lỗ hổng - Lỗi tràn bộ đệm

- ❖ Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống;
- ❖ Lỗi tràn bộ đệm là lỗi trong khâu lập trình phần mềm và nó chiếm một tỷ lệ lớn cho số các lỗi gây lỗ hổng bảo mật;
- ❖ Không phải tất cả các lỗi tràn bộ đệm có thể bị khai thác bởi kẻ tấn công.

2.2.1 Các dạng lỗ hổng - Lỗi tràn bộ đệm

❖ Các vùng nhớ chứa bộ đệm của ứng dụng:

- Ngăn xếp (Stack): vùng nhớ lưu các tham số gọi hàm, thủ tục, phương thức và dữ liệu cục bộ của chúng;
- Vùng nhớ cấp phát động (Heap): là vùng nhớ chung lưu dữ liệu cho ứng dụng.

2.2.1 Các dạng lỗ hổng - Lỗi tràn bộ đệm

❖ Giải thích cơ chế lỗi tràn bộ đệm trên bộ nhớ Stack và khả năng khai thác lỗ hổng:

- Bài trình bày “Smashing the Stack” của tác giả Mark Shancek, 2003.
 - Cơ chế hoạt động của Stack
 - Minh họa lỗi tràn bộ đệm trong Stack
 - Giải thích khả năng khai thác lỗi
 - Giải thích cơ chế hoạt động của sâu SQL Slammer và MS Blast – khai thác lỗi tràn bộ đệm.

2.2.1 Các dạng lỗ hổng - Lỗi tràn bộ đệm

❖ Các biện pháp phòng chống lỗi tràn bộ đệm:

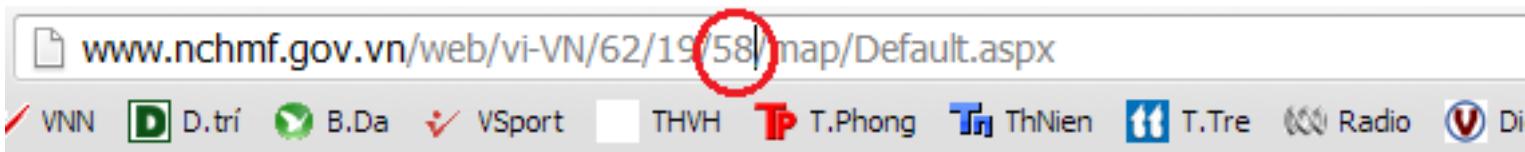
- Kiểm tra mã nguồn thủ công để tìm và khắc phục các điểm có khả năng xảy ra lỗi tràn bộ đệm;
- Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi tràn bộ đệm;
- Đặt cơ chế không cho phép thực hiện mã trong Stack (DEP – Data Execution Prevention);
- Sử dụng các cơ chế bảo vệ Stack:
 - Thêm một số ngẫu nhiên (canary) phía trước địa chỉ trả về;
 - Kiểm tra số ngẫu nhiên này trước khi trả về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trả về.
- Sử dụng các ngôn ngữ/công cụ lập trình không gây tràn (trong trường hợp có thể):
 - Các ngôn ngữ không gây tràn: Java, .Net
 - Các thư viện an toàn.

2.2.2 Các dạng lỗ hổng - Không kiểm tra đầu vào

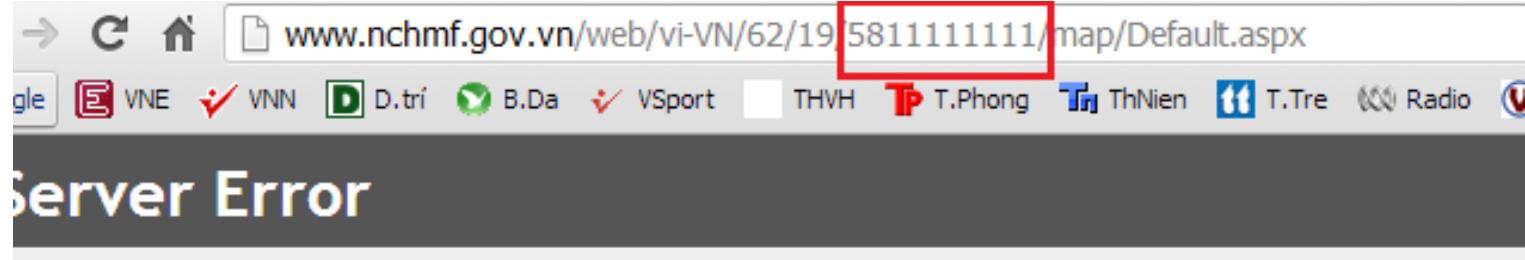
- ❖ Các dữ liệu đầu vào (input data) cần được kiểm tra để đảm bảo đạt các yêu cầu về định dạng và kích thước;
- ❖ Các dạng dữ liệu nhập hiển hình cần kiểm tra:
 - Các trường dữ liệu text
 - Các lệnh được truyền qua URL để kích hoạt chương trình
 - Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng hoặc các tiến trình khác cung cấp
 - Các đối số đầu vào trong dòng lệnh
 - Các dữ liệu từ mạng hoặc các nguồn không tin cậy
- ❖ Kẻ tấn công có thể kiểm tra các dữ liệu đầu vào và thử tất cả các khả năng có thể để khai thác.

2.2.2 Các dạng lỗ hổng - Không kiểm tra đầu vào

Trang web bị lỗi do không kiểm tra dữ liệu đầu vào từ URL



The screenshot shows a browser window with the URL www.nchmf.gov.vn/web/vi-VN/62/19/581111111111/map/Default.aspx. The part of the URL after the first slash is circled in red.



The screenshot shows a browser window displaying a "Server Error" page. The URL in the address bar is highlighted with a red box. The error message "500 - Internal server error." is displayed prominently in red, followed by the text "There is a problem with the resource you are looking for, and it cannot be displayed."

2.2.2 Các dạng lỗ hổng - Không kiểm tra đầu vào

❖ Chèn mã độc SQL vào trường text:

'Mã asp + SQL server
Dim searchString, sqlString

```
searchString = "iPhone 13"  
sqlString = "SELECT * FROM tbl_products WHERE product_name = " &  
searchString & ""  
==> SELECT * FROM tbl_products WHERE product_name = 'iPhone 13'
```

```
searchString = "iPhone 13';DELETE FROM tbl_products;--"  
sqlString = "SELECT * FROM tbl_products WHERE product_name = " &  
searchString & ""  
==> SELECT * FROM tbl_products WHERE product_name = 'iPhone 13';  
DELETE FROM tbl_products; --'
```

2.2.2 Các dạng lỗ hổng - Không kiểm tra đầu vào

- ❖ Chèn mã SQL để đăng nhập mà không cần tài khoản và mật khẩu:

'Mã asp + SQL server

```
Dim username, password, sqlString
```

```
username = "dauhoang"
```

```
password = "abc123"
```

```
sqlString = "SELECT * FROM tbl_users WHERE username = "" & username & "" AND password = "" & password & """
```

```
==> SELECT * FROM tbl_users WHERE username = 'dauhoang' AND password = 'abc123'
```

```
username = "aaaa' OR 1=1 --"
```

```
password = "aaaa"
```

```
sqlString = "SELECT * FROM tbl_users WHERE username = "" & username & "" AND password = "" & password & """
```

```
==> SELECT * FROM tbl_users WHERE username = 'aaaa' OR 1=1 --' AND password = 'aaaa'
```

2.2.2 Các dạng lỗ hổng - Không kiểm tra đầu vào

❖ Các biện pháp phòng chống:

- Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
- Kiểm tra kích thước và định dạng dữ liệu đầu vào;
- Kiểm tra sự hợp lý của nội dung dữ liệu;
- Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng:
 - Các ký tự đặc biệt: *, ', =, --
 - Các từ khóa: SELECT, INSERT, UPDATE, DELETE,

2.3.3 Các dạng lỗ hổng - Các v.đề với điều khiển truy nhập

- ❖ Điều khiển truy nhập (Access control) liên quan đến việc điều khiển ai (chủ thẻ) được truy cập đến cái gì (đối tượng)?
- ❖ Điều khiển truy nhập có thể được thiết lập bởi hệ điều hành hoặc mỗi ứng dụng, thường gồm 2 bước:
 - Xác thực (Authentication): xác thực thông tin nhận dạng của chủ thẻ;
 - Trao quyền (Authorization): cấp quyền truy nhập cho chủ thẻ sau khi thông tin nhận dạng được xác thực.
- ❖ Các chủ thẻ được cấp quyền truy nhập vào hệ thống theo các cấp độ khác nhau dựa trên chính sách an ninh của tổ chức.

2.3.3 Các dạng lỗ hổng - Các v.đề với điều khiển truy cập

- ❖ Nếu kiểm soát truy nhập bị lỗi, một người dùng bình thường có thể đoạt quyền của người quản trị và toàn quyền truy nhập vào hệ thống;
- ❖ Một kẻ tấn công có thể lợi dụng lỗ hổng bảo mật của hệ thống kiểm soát truy nhập để truy nhập vào các file trong hệ thống.
- ❖ Một ứng dụng chạy trên user quản trị có toàn quyền truy nhập vào hệ thống:
 - Nếu một kẻ tấn công chiếm được quyền điều khiển chương trình sẽ có toàn quyền truy nhập vào hệ thống.

2.3.3 Các dạng lỗ hổng - Các v.đề với điều khiển truy cập

❖ Phương pháp phòng chống:

- Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng;
- Luôn chạy các chương trình ứng dụng với quyền tối thiểu – vừa đủ để thực thi các tác vụ;
- Kiểm soát chặt chẽ người dùng, xóa bỏ hoặc cấm truy nhập với những người dùng ngầm định kiểu everyone;
- Thực thi chính sách mật khẩu an toàn;
- Cấp quyền vừa đủ cho người dùng thực thi nhiệm vụ.

2.3.4 Các dạng lỗ hổng - Các vấn đề với xác thực, trao quyền và mật mã

❖ Xác thực:

- Mật khẩu được lưu dưới dạng rõ (plain text) → nguy cơ bị lộ mật khẩu rất cao trong quá truyền thông tin xác thực;
- Sử dụng mật khẩu đơn giản, dễ đoán, hoặc dùng mật khẩu trong thời gian dài;
- Sử dụng cơ chế xác thực không đủ mạnh: ví dụ các cơ chế xác thực của giao thức HTTP.

❖ Trao quyền:

- Cơ chế thực hiện trao quyền không đủ mạnh, dễ bị vượt qua;
- Ví dụ: một trang web chỉ thực hiện ẩn các links đến các trang web mà người dùng không được truy nhập mà không thực sự kiểm tra quyền truy nhập trên từng trang. Nếu người dùng tự gõ URL của trang thì vẫn có thể truy nhập.

2.3.4 Các dạng lỗ hổng - Các vấn đề với xác thực, trao quyền và mật mã

❖ Các vấn đề với các hệ mật mã:

- Sử dụng giải thuật mã hóa/giải mã, hàm băm yếu, lạc hậu, hoặc có lỗ hổng (DES, MD4, MD5,...);
- Sử dụng khóa mã hóa/giải mã yếu;
 - Khóa có chiều dài ngắn;
 - Khóa dễ đoán.
- Các vấn đề trao đổi khóa bí mật;
- Các vấn đề xác thực người gửi/người nhận;
- Chi phí tính toán lớn (đặc biệt đối với các hệ mã hóa công khai).

2.3.5 Các dạng lỗ hổng - Các điểm yếu bảo mật khác

❖ Các thao tác không an toàn với files:

- Thực hiện đọc/ghi file lưu ở những nơi mà các người dùng khác cũng có thể ghi file đó;
- Không kiểm tra chính xác loại file, định danh thiết bị, các links hoặc các thuộc tính khác của file trước khi sử dụng;
- Không kiểm tra mã trả về sau mỗi thao tác với file;
- Giả thiết một file có đường dẫn cục bộ là file cục bộ và bỏ qua các thủ tục kiểm tra:
 - File ở xa có thể được ánh xạ vào hệ thống file cục bộ → có đường dẫn cục bộ.

2.3.5 Các dạng lỗ hổng - Các điểm yếu bảo mật khác

❖ Các điều kiện đua tranh (Race conditions):

- Một điều kiện đua tranh tồn tại khi có sự thay đổi trật tự của 2 hay một số sự kiện gây ra sự thay đổi hành vi của hệ thống;
- Đây là một dạng lỗi nếu chương trình chỉ có thể thực hiện đúng chức năng nếu các sự kiện phải xảy ra theo đúng trật tự;
- Kẻ tấn công có thể lợi dụng khoảng thời gian giữa 2 sự kiện để chèn mã độc, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống.

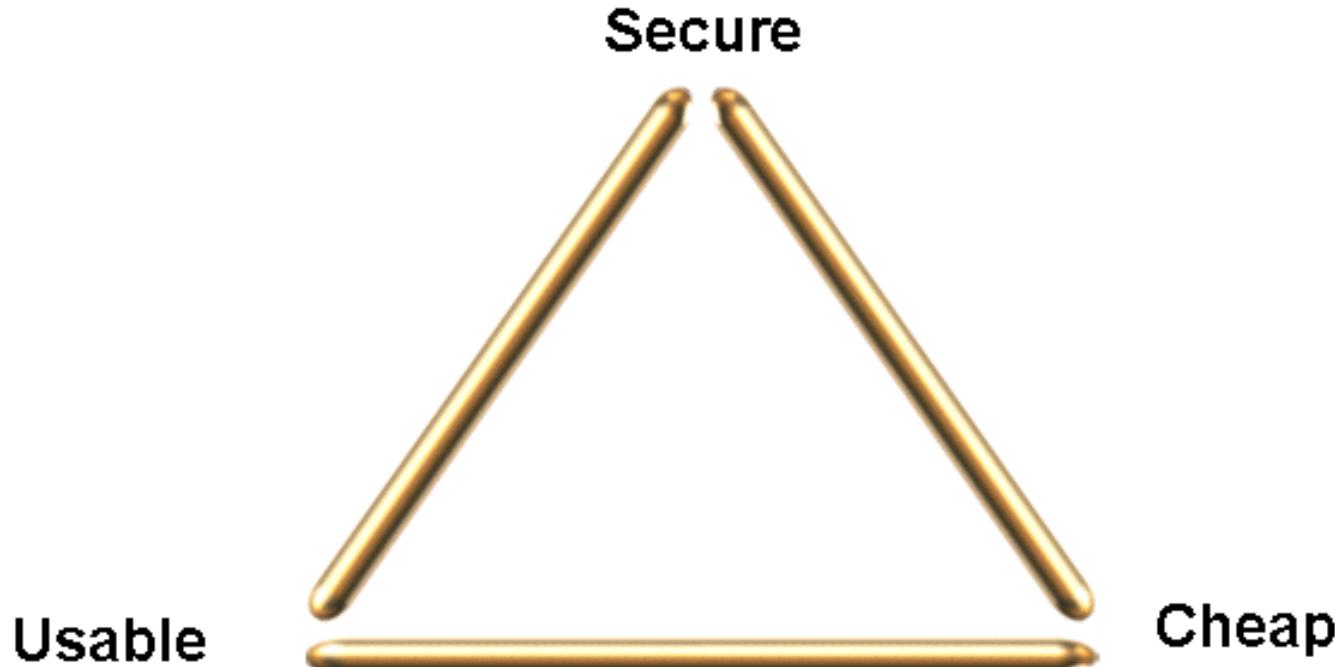
2.3.5 Các điểm yếu bảo mật khác

❖ Các điều kiện đua tranh – Ví dụ:

- Các file tạm thời (Temporary files) thường được lưu ở một thư mục chung quản lý bởi HDH. Tiến trình của nhiều người dùng cùng có thể đọc/ghi file tạm thời;
- Nếu 1 tiến trình tạo các cặp khóa bí mật và công khai, và lưu chúng vào một file tạm thời và sau đó đọc lại để lưu vào CSDL;
- Kẻ tấn công có thể tạo một race condition trong khoảng thời gian tiến trình chuyển từ ghi sang đọc các cặp khóa:
 - Thay file tạm của tiến trình bằng file chứa khóa của hắn → tiến trình sẽ đọc và lưu khóa của kẻ tấn công → mọi thông điệp mã hóa sử dụng khóa trên có thể được giải mã;
 - Đọc file tạm của tiến trình để đánh cắp các cặp khóa.

2.3 Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống

- ❖ Nguyên tắc: cân bằng giữa An toàn (Secure), Hữu dụng (Usable) và Rẻ tiền (Cheap)



2.3 Quản lý, khắc phục các lỗ hổng bảo mật (tiếp)

❖ Một số biện pháp cụ thể:

- Thường xuyên cập nhật thông tin về các điểm yếu, lỗ hổng bảo mật từ các trang web chính thức:
 - <http://cve.mitre.org/> (CVE - Common Vulnerabilities and Exposures)
 - <http://www.cvedetails.com/> (CVE Details)
 - <http://web.nvd.nist.gov> (National Vulnerability Database)
 - <https://owasp.org/www-community/vulnerabilities/>
- Định kỳ cập nhật các bản vá, nâng cấp hệ điều hành và các phần mềm ứng dụng;
 - Sử dụng các hệ thống q.lý các bản vá và tự động cập nhật định kỳ
 - Microsoft Windows Updates
 - Tiện ích Update trên Linux
 - Tính năng tự động Update của các ứng dụng (Như Google Update service)
 - Với các lỗ hổng nghiêm trọng, cần cập nhật tức thời.

2.3 Quản lý, khắc phục các lỗ hổng bảo mật (tiếp)

❖ Một số biện pháp cụ thể:

- Cần có chính sách quản trị người dùng, mật khẩu và quyền truy nhập chặt chẽ ở mức hệ điều hành và mức ứng dụng:
 - Người dùng chỉ được cấp quyền truy nhập vừa đủ để thực hiện công việc được giao.
 - Nếu được cấp nhiều quyền hơn mức cần thiết → lạm dụng.
- Sử dụng các biện pháp phòng vệ ở lớp ngoài như tường lửa, proxies:
 - Chặn các dịch vụ/cổng không thực sự cần thiết;
 - Ghi logs các hoạt động truy nhập mạng.
- Sử dụng các phần mềm rà quét lỗ hổng, rà quét các phần mềm độc hại:
 - Có thể giảm thiểu nguy cơ bị lợi dụng, khai thác lỗ hổng bảo mật.

2.4 Giới thiệu một số công cụ rà quét lỗ hổng bảo mật

❖ Công cụ quét cổng dịch vụ:

- Nmap
- Angry IP Scanner
- SuperScan

❖ Công cụ rà quét lỗ hổng bảo mật hệ thống

- Microsoft Baseline Security Analyser
- Nessus Vulnerability Scanner

❖ Công cụ rà quét lỗ hổng ứng dụng web

- Acunetix Web Vulnerability Scanner
- OWASP ZAP
- Beyond Security AVDS
- SQLMap



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN**

**CHƯƠNG 3 - CÁC DẠNG TẤN CÔNG
VÀ CÁC PHẦN MỀM ĐỘC HẠI**

Giảng viên:

E-mail:

Khoa:

PGS.TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

An toàn thông tin

NỘI DUNG CHƯƠNG 3

1. Khái quát về mối đe dọa và tấn công
2. Các công cụ hỗ trợ tấn công
3. Các dạng tấn công phá hoại
4. Các dạng phần mềm độc hại

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Mối đe dọa (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)

- Điểm yếu là một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống.
- Các hệ thống luôn tồn tại các điểm yếu.

❖ Lỗ hổng (Vulnerability)

- Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ 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.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Các mối đe dọa thường gặp:

- Phần mềm độc hại
- Hư hỏng phần cứng hoặc phần mềm
- Kẻ tấn công ở bên trong
- Kẻ tấn công ở bên ngoài
- Mất trộm các thiết bị
- Tai họa thiên nhiên
- Gián điệp công nghiệp
- Khủng bố phá hoại.

❖ Không phải tất cả các mối đe dọa là độc hại (malicious)

- Một số là cố ý
- Một số có thể là ngẫu nhiên/vô tình.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Các lỗ hổng tồn tại trong cả 7 vùng của nền tảng CNTT.

- Lỗ hổng trong vùng người dùng
- Lỗ hổng trong vùng máy trạm
- Lỗ hổng trong vùng mạng LAN
- Lỗ hổng trong vùng LAN-to-WAN
- Lỗ hổng trong vùng WAN
- Lỗ hổng trong vùng truy nhập từ xa
- Lỗ hổng trong vùng hệ thống/ứng dụng

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Các lỗ hổng tồn tại trong hệ điều hành và các phần mềm ứng dụng:

- Lỗi tràn bộ đệm (buffer overflows)
- Không kiểm tra đầu vào (unvalidated input)
- Các vấn đề với điều khiển truy cập (access-control problems)
- Các điểm yếu trong xác thực, trao quyền (weaknesses in authentication, authorization)
- Các điểm yếu trong các hệ mật mã (weaknesses in cryptographic practices).

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Tấn công độc hại/phá hoại (Malicious attacks)

- Một cuộc tấn công (attack) vào hệ thống máy tính hoặc các tài nguyên mạng được thực hiện bằng cách khai thác các lỗ hổng tồn tại trong hệ thống;
- Tấn công = Mối đe dọa + Lỗ hổng

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Các loại tấn công: 4 loại chính:

- Giả mạo (Fabrications): Giả mạo thông tin thường để đánh lừa người dùng thông thường;
- Chặn bắt (Interceptions): liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
- Gây ngắt quãng (Interruptions): gây ngắt kênh truyền thông ngăn cản việc truyền dữ liệu;
- Sửa đổi (Modifications): liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Hai kiểu tấn công:

- Tấn công chủ động (Active attacks)
 - Sửa đổi dữ liệu trên đường truyền
 - Sửa đổi dữ liệu trong file
 - Giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng
 - Tấn công chủ động là một đột nhập (intrusion) về mặt vật lý.
- Tấn công thụ động (Passive attacks)
 - Không gây ra thay đổi trên hệ thống
 - Nghe lén
 - Giám sát lưu lượng trên đường truyền.

3.1 Khái quát về mối đe dọa, lỗ hổng và tấn công

❖ Một số dạng tấn công điển hình:

- Tấn công vào mật khẩu
- Tấn công bằng mã độc
- Tấn công từ chối dịch vụ
- Tấn công giả mạo địa chỉ, nghe lén
- Tấn công kiểu phát lại và người đứng giữa
- Tấn công bằng bom thư và thư rác
- Tấn công sử dụng cửa hậu
- Tấn công kiểu Social Engineering
- Tấn công phising, pharming
- Tấn công APT.

3.2 Các công cụ hỗ trợ tấn công

- ❖ Công cụ tấn công (Attack tools) là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ giúp kẻ tấn công (attacker) tấn công vào các hệ thống máy tính hoặc các tài nguyên mạng.
- ❖ Một số công cụ và kỹ thuật hỗ trợ tấn công:
 - Công cụ quét lỗ hổng (Vulnerability scanners)
 - Công cụ quét cổng dịch vụ (Port scanners)
 - Công cụ nghe lén (Sniffers)
 - Công cụ ghi phím gõ (Keyloggers)

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ quét lỗ hổng (Vulnerability scanners)

- Thu thập các thông tin về các điểm yếu/lỗ hổng đã biết của hệ thống máy tính hoặc mạng;
- Gửi những thông điệp được tạo đặc biệt để kiểm tra điểm yếu/lỗ hổng đến hệ thống máy tính cần rà quét. Nếu hệ thống có phản hồi → điểm yếu vẫn tồn tại;
- Kẻ tấn công sử dụng kết quả rà quét điểm yếu/lỗ hổng để quyết định dạng tấn công có khả năng thành công cao nhất.

3.2 Các công cụ hỗ trợ tấn công

❖ Một số công cụ quét lỗ hổng cho người quản trị:

- Microsoft Baseline Security Analyzer:
 - Rà quét các lỗ hổng an ninh trong hệ điều hành Windows và các phần mềm của Microsoft;
 - Phân tích tình trạng lỗ hổng và có hướng dẫn khắc phục.
- Nessus vulnerability scanner:
 - Quét hệ thống hệ thống tìm lỗ hổng, điểm yếu
 - Độc lập với các nền tảng.
- Acunetix Web Vulnerability Scanner, OWASP ZAP:
 - Rà quét các ứng dụng web/trang web tìm các lỗ hổng.

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ quét cổng dịch vụ (Port scanners)

- Các cổng TCP/IP, UDP nằm trong khoảng từ 0 – 65535
 - Các cổng 0-1024 là các cổng chuẩn
 - Cổng lớn hơn 1024 là các cổng tùy gán.
- Kẻ tấn công thường sử dụng công cụ quét cổng để nhận dạng các điểm yếu trong hệ thống;

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ quét cổng dịch vụ (Port scanners)

- Công cụ quét cổng kết nối đến máy tính để xác định cổng nào được mở và có thể truy nhập vào máy tính. Từ đó xác định được dịch vụ/ứng dụng nào đang chạy trên hệ thống:
 - Cổng 80/443 mở → dịch vụ web đang chạy
 - Cổng 25 mở → dịch vụ email SMTP đang chạy
 - Cổng 1433 mở → Máy chủ CSDL MS SQL Server đang chạy
 - Cổng 53 mở → dịch vụ DNS đang chạy,...

3.2 Các công cụ hỗ trợ tấn công

❖ Nguyên tắc tối thiểu các cổng được mở:

- Đóng tất cả các cổng không sử dụng;
- Chỉ mở những cổng có dịch vụ cần thiết cho người dùng.

❖ Một số công cụ quét cổng:

- Nmap
- Portsweep
- Advanced Port Scanner (<http://www.radmin.com>)
- Angry IP Scanner
- Superscan
- NetScanTools

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ nghe lén/nghe trộm (Sniffers)

- Công cụ nghe lén cho phép bắt các gói tin khi chúng được truyền trên mạng.
- Công cụ nghe lén có thể là mô đun phần cứng, phần mềm hoặc kết hợp.
- Các thông tin nhạy cảm như mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe lén khi được truyền từ máy trạm đến máy chủ và bị lạm dụng.

3.2 Các công cụ hỗ trợ tấn công

❖ Một số công cụ cho phép bắt gói tin truyền:

- Tcpdump
- Pcap / Wincap (packet capture)
- IP Tools (<http://www.softpedia.com>)
- Wireshark

3.2 Các công cụ hỗ trợ tấn công

❖ Công cụ ghi phím gõ (Keyloggers)

- Công cụ ghi phím gõ là một dạng công cụ giám sát có thể bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào 1 file;
- Sau đó file đã ghi có thể được gửi cho kẻ tấn công theo địa chỉ chỉ định trước hoặc sao chép trực tiếp.
- Người quản lý có thể cài đặt Keylogger vào máy tính của nhân viên để theo dõi hoạt động của nhân viên;

3.2 Các công cụ hỗ trợ tấn công

❖ Cài đặt Keyloggers:

- Bằng phần cứng: thường được cài như 1 khớp nối kéo dài giữa máy tính và dây bàn phím;
- Bằng phần mềm: kẻ tấn công có thể tích hợp công cụ Keylogger vào một phần mềm thông thường và lừa người dùng cài đặt vào máy tính của mình.



3.3 Các dạng tấn công phá hoại thường gặp

- ❖ Tấn công vào mật khẩu
- ❖ Tấn công bằng mã độc
- ❖ Tấn công từ chối dịch vụ
- ❖ Tấn công giả mạo địa chỉ
- ❖ Tấn công nghe lén
- ❖ Tấn công kiểu người đứng giữa
- ❖ Tấn công bằng bom thư và thư rác
- ❖ Tấn công sử dụng cửa hậu
- ❖ Tấn công kiểu Social Engineering
- ❖ Tấn công phishing, pharming
- ❖ Tấn công APT.

3.3 Các dạng tấn công - Tấn công vào mật khẩu

- ❖ Tấn công vào mật khẩu là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản để lạm dụng;
 - Tên người dùng và mật khẩu không được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách đến máy chủ;
 - Tên người dùng và mật khẩu có thể bị đánh cắp thông qua các dạng tấn công XSS hoặc Social Engineering (lừa đảo, bẫy người dùng cung cấp thông tin);
 - Nếu kẻ tấn công có tên người dùng và mật khẩu → có thể đăng nhập vào tài khoản và thực hiện các thao tác như người dùng bình thường.

3.3 Các dạng tấn công - Tấn công vào mật khẩu

❖ Các dạng tấn công vào mật khẩu:

- Tấn công dựa trên từ điển (Dictionary attacks): người dùng có xu hướng chọn mật khẩu là các từ đơn giản có trong từ điển cho dễ nhớ → kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển.
- Tấn công vét cạn (Brute force attacks): sử dụng tổ hợp các ký tự và thử tự động.
 - Phương pháp này thường sử dụng với các mật khẩu đã được mã hóa;
 - Kẻ tấn công sử dụng tổ hợp ký tự, sau đó mã hóa với cùng thuật toán hệ thống sử dụng, và so sánh chuỗi mã hóa với chuỗi mà mật khẩu thu thập được. Nếu hai bản mã trùng nhau → tổ hợp ký tự là mật khẩu.

3.3 Các dạng tấn công - Tấn công vào mật khẩu

❖ Phòng chống:

- Chọn mật khẩu đủ mạnh: độ dài ≥ 8 ký tự gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt (?#\$...).
 - VD: Mật khẩu ‘Abc123\$5’ an toàn hơn ‘abc12345’ về mặt tính toán
- Định kỳ thay đổi mật khẩu.

❖ Một số công cụ khôi phục mật khẩu:

- Password Cracker (<http://www.softpedia.com>)
- Ophcrack
- Offline NT Password & Registry Editor
- PC Login Now
- L0phtCrack
- John the Ripper

3.3 Các dạng tấn công - Tấn công bằng mã độc

❖ Tấn công bằng mã độc có thể gồm một số dạng:

- Lợi dụng các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân;
 - Tấn công lợi dụng lỗi tràn bộ đệm (Buffer Overflow) – đã học ở chương 2
 - Tấn công lợi dụng lỗi không kiểm tra đầu vào:
 - Tấn công chèn mã SQL (SQL Injection) – một phần đã học ở chương 2
 - Tấn công script kiểu XSS, CSRF (sẽ học trong môn An toàn ứng dụng web và CSDL)
- Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại
 - Các phần mềm Adware, Spyware
 - Virus
 - Trojan

3.3 Các dạng tấn công - Tấn công bằng mã độc: Tấn công lợi dụng lỗi không kiểm tra đầu vào

- ❖ Các dữ liệu đầu vào (input data) cần được kiểm tra để đảm bảo đạt các yêu cầu về định dạng và kích thước;
- ❖ Các dạng dữ liệu nhập diễn hình cần kiểm tra:
 - Các trường dữ liệu text
 - Các lệnh được truyền qua URL để kích hoạt chương trình
 - Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng hoặc các trình duyệt khác cung cấp
 - Các đối số đầu vào trong dòng lệnh
 - Các dữ liệu từ mạng hoặc các nguồn không tin cậy
- ❖ Kẻ tấn công có thể kiểm tra các dữ liệu đầu vào và thử tất cả các khả năng để khai thác.

3.3 Các dạng tấn công - Tấn công bằng mã độc: Tấn công lợi dụng lỗi không kiểm tra đầu vào

- ❖ Một số dạng tấn công lợi dụng lỗi không kiểm tra đầu vào:
 - Cố tình nhập dữ liệu quá lớn hoặc sai định dạng gây lỗi cho ứng dụng (đã học ở chương 2)
 - Gây lỗi ứng dụng/dịch vụ, có thể làm ứng dụng ngừng hoạt động
 - Chèn mã SQL để thực hiện trên máy chủ CSDL của ứng dụng (SQL Injection)

3.3 Các dạng tấn công - Tấn công bằng mã độc: Lợi dụng lỗi không kiểm tra đầu vào - SQL Injection

- ❖ SQL Injection (chèn mã độc SQL) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và được thực hiện trên máy chủ CSDL;
- ❖ Nguyên nhân:
 - Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng;
 - Ứng dụng sử dụng các câu lệnh SQL động, trong đó dữ liệu được kết nối với mã SQL gốc để tạo câu lệnh SQL hoàn chỉnh.

3.3 Các dạng tấn công - Tấn công bằng mã độc: Lợi dụng lỗi không kiểm tra đầu vào - SQL Injection

- ❖ Tùy vào mức độ tinh vi, SQL Injection có thể cho phép kẻ tấn công:
 - Vượt qua các khâu xác thực người dùng;
 - Chèn, xóa hoặc sửa đổi dữ liệu;
 - Đánh cắp các thông tin trong CSDL;
 - Chiếm quyền điều khiển hệ thống.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

- ❖ Ví dụ: form HTML đăng nhập:

```
<form method="post" action="/test_sql.asp">
```

Tên đăng nhập: <input type=text name="username"><br \>

Mật khẩu: <input type=password name="passwd"><br \>

<input type=submit name="login" value="Log In">

```
</form>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

```
<%  
' Mã asp xử lý đăng nhập trong file test_sql.asp:  
' g.thiết đã k.nối với CSDL SQL qua đối tượng conn và bảng tbl_accounts lưu t.tin người dùng  
Dim username, passwd, sqlString, rsLogin  
' lấy dữ liệu từ form  
username = Request.Form("username")  
passwd = Request.Form("passwd")  
' tạo và thực hiện câu truy vấn sql  
sqlString = "SELECT * FROM tbl_accounts WHERE username="" &username&"" AND passwd=""  
&passwd& """  
set rsLogin = conn.execute(sqlString)  
if (NOT rsLogin.eof()) then  
    ' cho phép đăng nhập, bắt đầu phiên làm việc  
else  
    ' từ chối đăng nhập, báo lỗi  
end if  
%>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

❖ Phân tích:

- Nếu người dùng nhập admin vào trường username và abc123 vào trường passwd của form, mã xử lý hoạt động đúng:
 - Nếu tồn tại người dùng với username và password sẽ cho phép đăng nhập;
 - Nếu không tồn tại người dùng với username và password sẽ từ chối đăng nhập và báo lỗi.
- Nếu người dùng nhập **aaaa' OR 1=1--** vào trường username và một chuỗi bất kỳ vào trường passwd của form, mã xử lý hoạt động sai:
 - Chuỗi chứa câu truy vấn SQL trở thành:

```
SELECT * FROM tbl_accounts WHERE username='aaaa' OR 1=1--' AND passwd='aaaa'
```

Câu truy vấn sẽ trả về mọi bản ghi trong bảng do mệnh đề **OR 1=1** luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bởi ký hiệu **(--)**: phần lệnh sau ký hiệu **(--)** được coi là ghi chú và không được thực hiện.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

❖ Phòng chống/sửa chữa:

- Kiểm soát kích thước và định dạng của dữ liệu đầu vào, lọc bỏ các ký tự đặc biệt, các từ khóa SQL;
- Tránh sử dụng câu truy vấn trực tiếp, nên dùng:
 - Stored Procedure là dạng các câu lệnh SQL dưới dạng các thủ tục và được lưu trong CSDL;
 - Sử dụng các cơ chế truyền tham số, tạo câu truy vấn của ngôn ngữ.

❖ Chỉnh sửa form đăng nhập – thêm giới hạn kích thước dữ liệu:

```
<form method="post" action="/test_sql.asp">  
    <input type="text" name="username" value="" size=20 maxlength=15>  
    <input type="password" name="passwd" size=20 maxlength=15>  
    <input type="submit" name="login" value="Log In">  
</form>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

Chỉnh sửa mã asp xử lý đăng nhập trong file test_sql.asp:

```
<%
' giả thiết đã kết nối với CSDL SQL server qua connection conn
' và bảng tbl_accounts lưu thông tin người dùng
Dim username, passwd, sqlString, rsLogin, validInput
' lấy dữ liệu từ form, cắt bỏ các dấu trắng ở đầu và đuôi, chỉ lấy 15 ký tự
username = Trim(Left(Request.Form("username")&"", 15))
passwd = Trim(Left(Request.Form("passwd") &"", 15))
' kiểm tra đầu vào, chỉ xử lý nếu đầu vào hợp lệ
validInput = False
if (username<>"" and passwd<>"") then
    validInput = isValidUsername(username)
end if
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

' tạo và thực hiện câu truy vấn sql nếu đầu vào hợp lệ

if (isValidInput) then

```
sqlString = "SELECT * FROM tbl_accounts WHERE username=" & username & ""  
AND passwd=" & passwd & ""
```

```
set rsLogin = conn.execute(sqlString)
```

```
if (NOT rsLogin.eof()) then
```

' cho phép đăng nhập, bắt đầu phiên làm việc

```
else
```

' từ chối đăng nhập, báo lỗi

```
end if
```

```
else
```

' từ chối đăng nhập, báo lỗi

```
end if
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

' hàm kiểm tra các ký tự cho phép trong 1 chuỗi nhập vào

Function isValidUsername(inputString)

' nếu xuất hiện ký tự không cho phép → trả về False, ngược lại trả về True

End Function

%>

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

- ❖ Sử dụng Stored Procedure thay cho câu truy vấn sql trực tiếp:

```
Create Procedure sp_accountLogin
```

```
@username varchar(15),
```

```
@passwd varchar(15)
```

```
AS
```

```
SELECT * FROM tbl_accounts
```

```
WHERE (username = @username) AND (passwd = @passwd)
```

```
GO
```

- ❖ Ưu điểm:

- Stored Procedure được lưu trong CSDL nên nhanh hơn
- Hạn chế đến tối thiểu tấn công chèn mã

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Vượt qua các khâu xác thực người dùng

❖ Gọi thủ tục sp_accountLogin từ mã asp:

Dim cmd, rsLogin

' tạo đối tượng cmd, gán thủ tục, truyền tham số và thực hiện

```
set cmd = server.CreateObject("ADODB.command")
```

```
cmd.ActiveConnection = conn
```

```
cmd.CommandType = adcmdstoredproc
```

```
cmd.CommandText = " sp_accountLogin"
```

```
cmd.Parameters.Append cmd.CreateParameter("",adVarchar,adParamInput,15,username)
```

```
cmd.Parameters.Append cmd.CreateParameter("", adVarchar,adParamInput,15,passwd)
```

```
set rsLogin = cmd.execute
```

```
set cmd=nothing
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

- ❖ Ví dụ: form HTML tìm kiếm sản phẩm:

```
<form method="post" action="/test_sql.asp">  
    Nhập tên sản phẩm: <input type=text name="keyword">  
    <input type=submit name="search" value="Search">  
</form>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

Mã asp xử lý tìm kiếm trong file test_sql.asp:

```
<%
' giả thiết đã kết nối với CSDL SQL server qua connection conn
' và bảng tbl_products lưu thông tin sản phẩm
Dim keyword, sqlString, rsSearch
' lấy dữ liệu từ form
keyword = Request.Form(" keyword")
' tạo và thực hiện câu truy vấn sql
sqlString = "SELECT * FROM tbl_products WHERE product_name like '%' & keyword & '%'"
set rsSearch = conn.execute(sqlString)
if (NOT rsSearch.eof()) then
    ' hiển thị danh sách các sản phẩm
else
    ' thông báo không tìm thấy sản phẩm
end if
%>
```

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

❖ Phân tích:

- Nếu người dùng nhập **Samsung Galaxy S21** vào trường keyword của form, mã xử lý hoạt động đúng:
 - Nếu tìm thấy → hiển thị kết quả tìm kiếm;
 - Nếu không tìm thấy → thông báo không tìm thấy sản phẩm.
- Nếu người dùng nhập **Samsung Galaxy S21';DELETE FROM tbl_products;--** vào trường keyword của form, mã xử lý hoạt động sai:
 - Chuỗi chứa câu truy vấn SQL trở thành:

SELECT * FROM tbl_products WHERE keyword like '%Samsung Galaxy S21';DELETE FROM tbl_products;--%'

Câu truy vấn mới gồm 2 lệnh SQL: câu lệnh tìm kiếm sản phẩm **Samsung Galaxy S21** và câu lệnh xóa tất cả các sản phẩm trong bảng **tbl_products**. Sở dĩ kẻ tấn công có thể làm được điều này do SQL server cho phép chạy nhiều lệnh SQL và dùng dấu ; để ngăn cách các lệnh. Ký hiệu – dùng để hủy tác dụng của phần lệnh còn lại nếu có.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Sửa đổi, hoặc xóa dữ liệu

❖ Phân tích:

- Bằng thủ thuật tương tự, kẻ tấn công có thể thay lệnh DELETE bằng lệnh UPDATE hoặc INSERT để xóa hoặc chèn dữ liệu.
- Cập nhật mật khẩu của người quản trị:
`Galaxy S21';UPDATE tbl_administrators SET password=abc123 WHERE username = 'admin';--`
- Chèn thêm bản ghi:
`Galaxy S21';INSERT INTO tbl_administrators (username, password) VALUES ('attacker', 'abc12345');--`
- Xóa cả bảng dữ liệu:
`Galaxy S21';DROP TABLE tbl_products;--`

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

❖ Lỗi chèn mã SQL có thể cho phép tin tặc đánh cắp dữ liệu nhạy cảm trong CSDL thông qua 1 số bước:

- Tìm lỗi chèn mã SQL và thăm dò các thông tin về CSDL:
 - Phiên bản máy chủ CSDL: nhập các câu lệnh lỗi và kiểm tra thông báo lỗi; hoặc sử dụng @@version (MS SQL), hoặc version() (MySQL) trong UNION SELECT.
- Trích xuất thông tin về tên các bảng, trường trong CSDL
- Sử dụng lệnh UNION SELECT để ghép các thông tin định trích xuất vào câu query hiện tại của ứng dụng.

3.3 Các dạng tấn công - Tấn công bằng mã độc: **SQL Injection - Đánh cắp các thông tin trong CSDL**

- ❖ Ví dụ: form tìm kiếm sản phẩm có lỗi chèn mã SQL với câu lệnh tìm kiếm:

SELECT * FROM tbl_products

WHERE product_name like '%' + keyword + '%'

với keyword là từ khóa người dùng cung cấp từ form.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

❖ Tìm thông tin về máy chủ CSDL:

- Sử dụng lệnh UNION [ALL] SELECT để tìm số trường trong lệnh truy vấn hiện tại: gõ chuỗi tìm kiếm:
`samsung%' union all select '1', '2', '3', '4' --`
Thay đổi (tăng, giảm) danh sách cho đến khi thấy hiển thị giá trị 1, 2,...
Trên kết quả → đã tìm đúng số cột trong lệnh truy vấn hiện tại.
- Sử dụng ORDER BY <column_number> để tìm số trường:
gõ chuỗi tìm kiếm: `samsung%' ORDER BY 5 ASC | DESC`
Tăng giảm số thứ tự trường để tìm số trường. Khi kết quả hiển thị và được sắp xếp đúng → số trường tìm đã đúng.
- Sử dụng @@version hoặc version() tùy theo phiên bản máy chủ CSDL đưa vào union select để lấy thông tin về máy chủ CSDL:
`samsung%' union select @@version, '2' --`

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

❖ Trích xuất thông tin về các bảng trong CSDL MS-SQL:

- Nhập chuỗi tìm kiếm:
`samsung' union select name, object_id
from sys.objects where type='u' --`

Bảng sys.objects chứa danh sách các bảng kèm thuộc tính; 'u' là kiểu bảng do người dùng tạo; name chứa tên đối tượng (bảng) và object_id là mã số đối tượng.

Cũng có thể sử dụng bảng sys.tables để trích xuất các thông tin về các bảng người dùng tạo lập.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

❖ Trích xuất thông tin về các trường trong một bảng:

- Nhập chuỗi tìm kiếm:

```
samsung' union select name, 0  
from sys.columns where object_id = <mã số bảng> --
```

trong đó <mã số bảng> lấy từ cột object_id ở trên.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Đánh cắp các thông tin trong CSDL

❖ Trích xuất thông tin từ một bảng đã biết tên và các trường:

- Nhập chuỗi tìm kiếm:
`samsung' union select username+'-'+password, 0 from tbl_users --`
→ lấy danh sách tên truy nhập và mật khẩu của tất cả các users
- Nhập chuỗi tìm kiếm:
`samsung' union select username+'-'+password, 0
from tbl_administrators --`
→ lấy danh sách tên truy nhập và mật khẩu của tất cả các admins.
- Bằng thủ thuật tương tự, tin tặc có thể đánh cắp gần như mọi thông tin trong CSDL.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- ❖ Khả năng máy chủ cơ sở dữ liệu bị chiếm quyền điều khiển xảy ra khi website và CSDL của nó tồn tại 2 lỗ hổng:
 - Lỗ hổng cho phép tấn công chèn mã SQL;
 - Lỗ hổng thiết lập quyền truy nhập – sử dụng người dùng có quyền quản trị để truy nhập và thao tác dữ liệu website.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- ❖ Tin tức có thể chèn mã để chạy các thủ tục hệ thống cho phép can thiệp vào hệ quản trị CSDL và hệ điều hành. Ví dụ, MS SQL cung cấp các thủ tục hệ mở rộng:
 - sp_send_dbmail: cho phép gửi email từ CSDL.
 - xp_cmdshell: cho phép chạy các lệnh và chương trình cài đặt trên HĐH windows. VD:
 - EXEC xp_cmdshell 'dir *.exe'
 - EXEC xp_cmdshell 'shutdown /s /t 00' → tắt máy chủ nền chạy hệ quản trị CSDL
 - EXEC xp_cmdshell 'net stop W3SVC' → dừng hoạt động máy chủ web
 - EXEC xp_cmdshell 'net stop MSSQLSERVER' → dừng hoạt động máy chủ CSDL

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Chiếm quyền điều khiển hệ thống

- ❖ Ngoài ra, tin tặc có thể thực hiện các thao tác nguy hiểm đến CSDL nếu có quyền của người quản trị CSDL hoặc quản trị hệ thống, như:
 - Xóa cả bảng: DROP TABLE <tên bảng>
 - Xóa cả CSDL: DROP DATABASE <tên CSDL>
 - Tạo 1 tài khoản mới: sp_addlogin <username> <password>
 - Đổi mật khẩu người dùng hiện tại: sp_password <password>

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

- ❖ Các biện pháp phòng chống dựa trên kiểm tra và lọc dữ liệu đầu vào;
- ❖ Các biện pháp phòng chống dựa trên việc sử dụng thủ tục (stored procedures) trong CSDL;
- ❖ Các biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng cho phù hợp;
- ❖ Chủ động sử dụng công cụ rà quét lỗ hổng bảo mật để rà quét tìm các lỗ hổng và khắc phục.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

❖ Các biện pháp phòng chống dựa trên kiểm tra và lọc dữ liệu đầu vào:

- Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
- Kiểm tra định dạng và kích thước dữ liệu đầu vào;
- Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng:
 - Các ký tự đặc biệt: *, ', =, --
 - Các từ khóa: SELECT, INSERT, UPDATE, DELETE, DROP,....

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

- ❖ Các biện pháp phòng chống dựa trên việc sử dụng thủ tục (stored procedures) trong CSDL:
 - Đưa tất cả các câu truy vấn (SELECT) và cập nhật, sửa xóa dữ liệu (INSERT, UPDATE, DELETE) vào thủ tục; dữ liệu truyền vào thủ tục thông qua các tham số → tách dữ liệu khỏi mã, giúp hạn ngăn chặn hiệu quả tấn công chèn mã SQL.
 - Hạn chế thực hiện các câu lệnh SQL động trong thủ tục.
- ❖ Cấm hoặc vô hiệu hóa (disable) việc thực hiện các thủ tục hệ thống – các thủ tục CSDL có sẵn cho phép can thiệp vào hệ quản trị CSDL và hệ điều hành nền.
 - Các Extended/system Stored Procedures trong MS-SQL như xp_cmdshell cho phép chạy lệnh của hệ điều hành.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Phòng chống

❖ Các biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng cho phù hợp:

- Không sử dụng người dùng có quyền system admin hoặc database owner làm người dùng truy cập dữ liệu;
 - Ví dụ: không dùng user sa (MS-SQL) hoặc root (MySQL) làm user truy cập dữ liệu. Chỉ dùng các user này cho mục đích quản trị.
- Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục.
- Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp dữ liệu; Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục.

3.3 Các dạng tấn công - Tấn công bằng mã độc: SQL Injection - Công cụ kiểm tra và tấn công

- ❖ Chủ động sử dụng công cụ rà quét lỗ hổng bảo mật để rà quét tìm các lỗ hổng và khắc phục;
 - Rà quét ứng dụng web/website sử dụng công cụ Acunetix để phát hiện các lỗi chèn mã SQL;
 - Sử dụng công cụ SQLmap (có thể tải từ trang sqlmap.org) - một công cụ mã mở miễn phí viết bằng Python:
 - Cho phép kiểm tra website tìm lỗi chèn mã SQL
 - Cho phép khai thác lỗi để điều khiển máy chủ CSDL
 - Hỗ trợ hầu hết các máy chủ quản trị CSDL hiện nay: MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase và SAP MaxDB.

3.3 Các dạng tấn công - Tấn công từ chối dịch vụ

- ❖ Tấn công từ chối dịch vụ (DoS - Denial of Service Attacks) là dạng tấn công cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống;
- ❖ Hai loại tấn công DoS:
 - Tấn công logic (Logic attacks): tấn công dựa vào các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
 - Cần cài đặt các bản cập nhật thường xuyên để phòng chống.
 - Tấn công gây ngập lụt (Flooding attacks): Kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

3.3 Các dạng tấn công - Tấn công từ chối dịch vụ

❖ Các kỹ thuật tấn công DoS:

- SYN flood
- Smurf
- UDP flood
- HTTP flood
- Teardrop
- LandAttack
- Ping of death,...

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

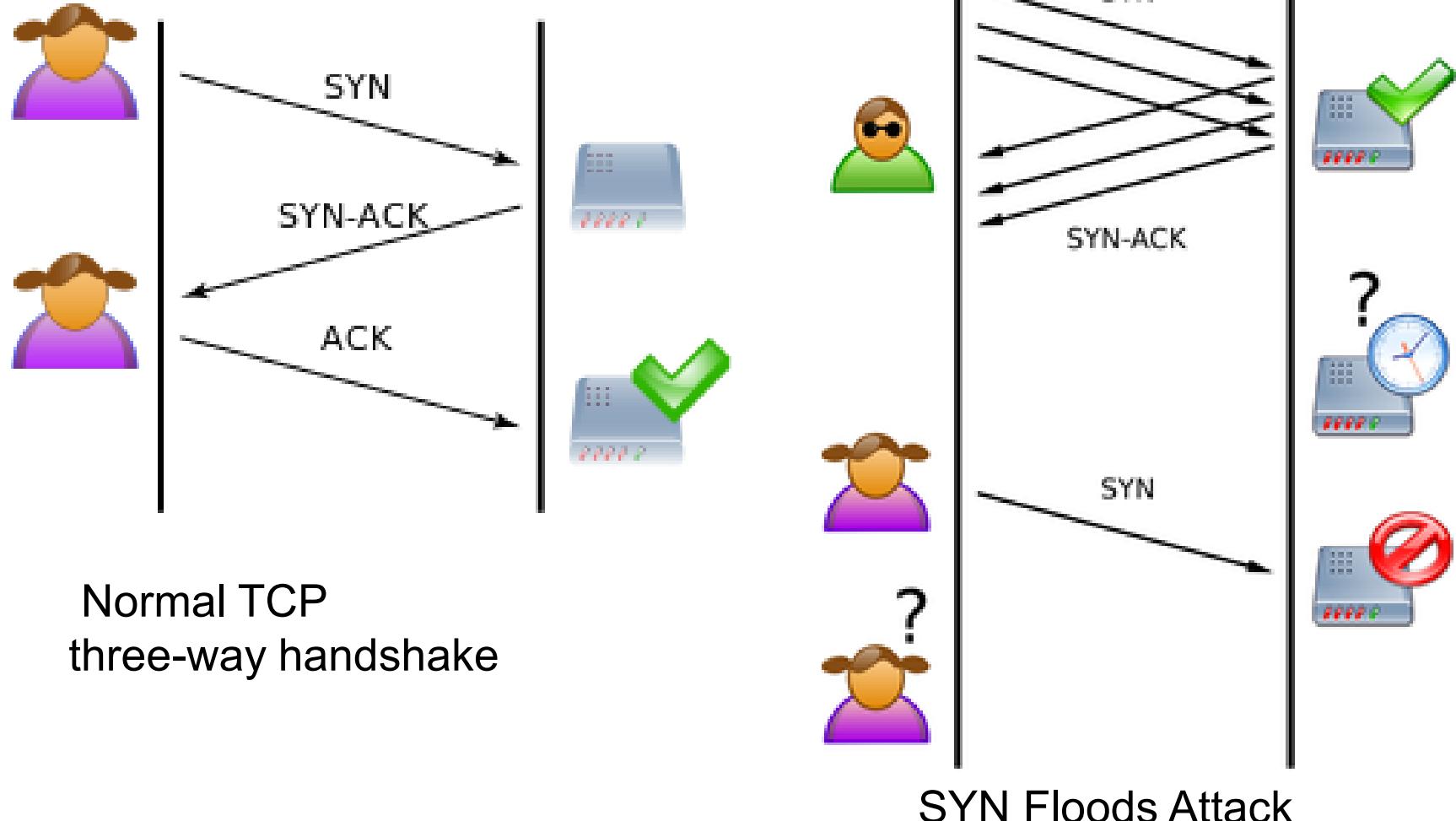
- ❖ SYN floods là kỹ thuật gây ngập lụt các gói tin mở kết nối TCP.
 - SYN là bít điều khiển của TCP dùng để đồng bộ số trình tự gói.
- ❖ SYN floods khai thác điểm yếu trong thủ tục bắt tay 3 bước khi thiết lập kết nối cho phiên truyền thông TCP/IP.
- ❖ SYN floods gây cạn kiệt tài nguyên máy chủ:
 - Có thể làm máy chủ ngừng hoạt động;
 - Hoặc không chấp nhận yêu cầu mở kết nối mới.

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

❖ Kịch bản tấn công SYN floods:

- Kẻ tấn công gửi 1 lượng lớn gói tin yêu cầu mở kết nối (SYN-REQ) đến máy tính nạn nhân;
- Máy tính nạn nhân ghi nhận yêu cầu kết nối và dành 1 chỗ trong bảng lưu kết nối trong bộ nhớ cho mỗi yêu cầu kết nối;
- Máy tính nạn nhân sau đó gửi gói tin xác nhận kết nối (SYN-ACK) đến kẻ tấn công;
- Do kẻ tấn công không bao giờ trả lời xác nhận kết nối, nên máy tính nạn nhân vẫn phải lưu tất cả các yêu cầu kết nối chưa được xác nhận trong bảng kết nối → bảng kết nối đầy và người dùng hợp pháp không thể truy nhập;
- Máy tính nạn nhân chỉ có thể xóa yêu cầu kết nối chưa được xác nhận khi nó quá hạn (timed-out).

3.3 Các dạng tấn công - Tấn công DoS - SYN floods



Normal TCP
three-way handshake

SYN Floods Attack

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

❖ Phân tích:

- Kẻ tấn công thường dùng địa chỉ IP giả mạo hoặc địa chỉ không có thực làm Source IP trong gói tin IP, nên thông điệp SYN-ACK của máy tính nạn nhân không bao giờ đến đích;
- Kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu kết nối dở dang để:
 - Các yêu cầu kết nối SYN-REQ điền đầy bảng kết nối → máy nạn nhân không thể chấp nhận yêu cầu của những người dùng khác;
 - Làm cạn kiệt tài nguyên bộ nhớ của máy nạn nhân → có thể làm máy nạn nhân ngừng hoạt động;
 - Gây nghẽn đường truyền mạng.

3.3 Các dạng tấn công - Tấn công DoS - SYN floods

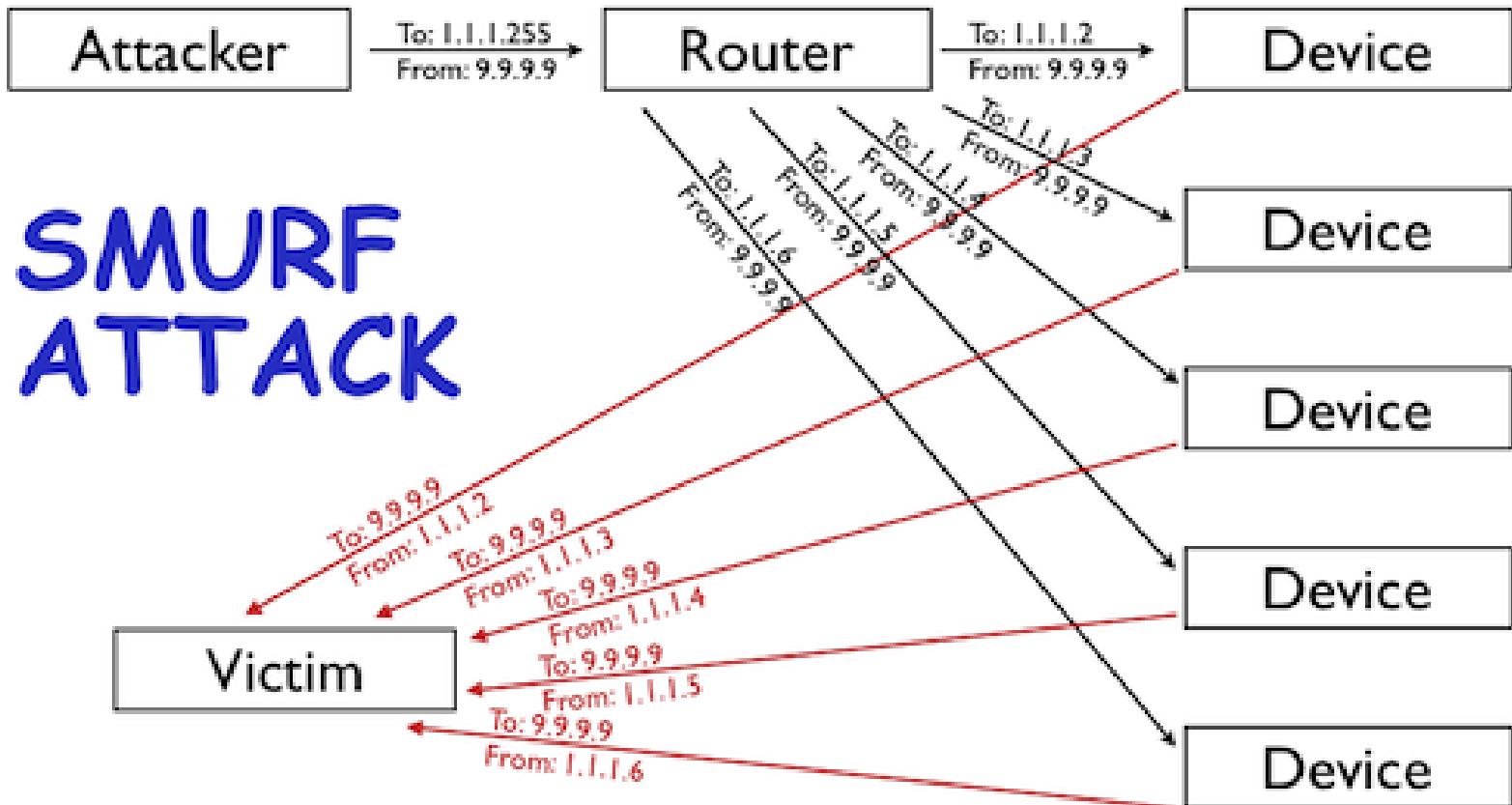
❖ Phòng chống:

- Sử dụng kỹ thuật lọc (Filtering): cần sửa đổi giao thức TCP không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước bảng kết nối (Backlog): tăng kích thước Backlog lưu các yêu cầu kết nối → tăng khả năng chấp nhận các yêu cầu;
- Giảm thời gian chờ (SYN-RECEIVED Timer): các kết nối chưa được xác nhận sẽ bị xóa khi hết thời gian chờ;
- SYN cache: yêu cầu kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng Firewalls và Proxies
 - Có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực;
 - Có khả năng tiếp nhận kết nối, chờ đến khi có xác nhận mới chuyển lại cho máy chủ đích.

3.3 Các dạng tấn công - Tấn công DoS - Smurf

- ❖ Tấn công Smurf sử dụng kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân.
- ❖ Kịch bản tấn công Smurf:
 - Kẻ tấn công gửi một lượng lớn gói tin ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một mạng sử dụng một địa chỉ quảng bá (IP Broadcast address);
 - Các máy trong mạng nhận được thông điệp ICMP sẽ gửi trả lời đến máy có địa chỉ IP là địa nguồn trong thông điệp ICMP (là máy nạn nhân);
 - Nếu lượng máy trong mạng rất lớn → máy nạn nhân sẽ bị ngập lụt đường truyền.

3.3 Các dạng tấn công - Tấn công DoS - Smurf



3.3 Các dạng tấn công - Tấn công DoS - Smurf

❖ Phòng chống:

- Cấu hình các máy và router không trả lời các yêu cầu ICMP hoặc các yêu cầu phát quảng bá;
- Cấu hình các router không chuyển tiếp yêu cầu gửi đến các địa chỉ quảng bá;
- Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.

3.3 Các dạng tấn công - Tấn công DDoS

❖ Tấn công DDoS (Distributed Denial of Service Attacks) là một loại tấn công DoS:

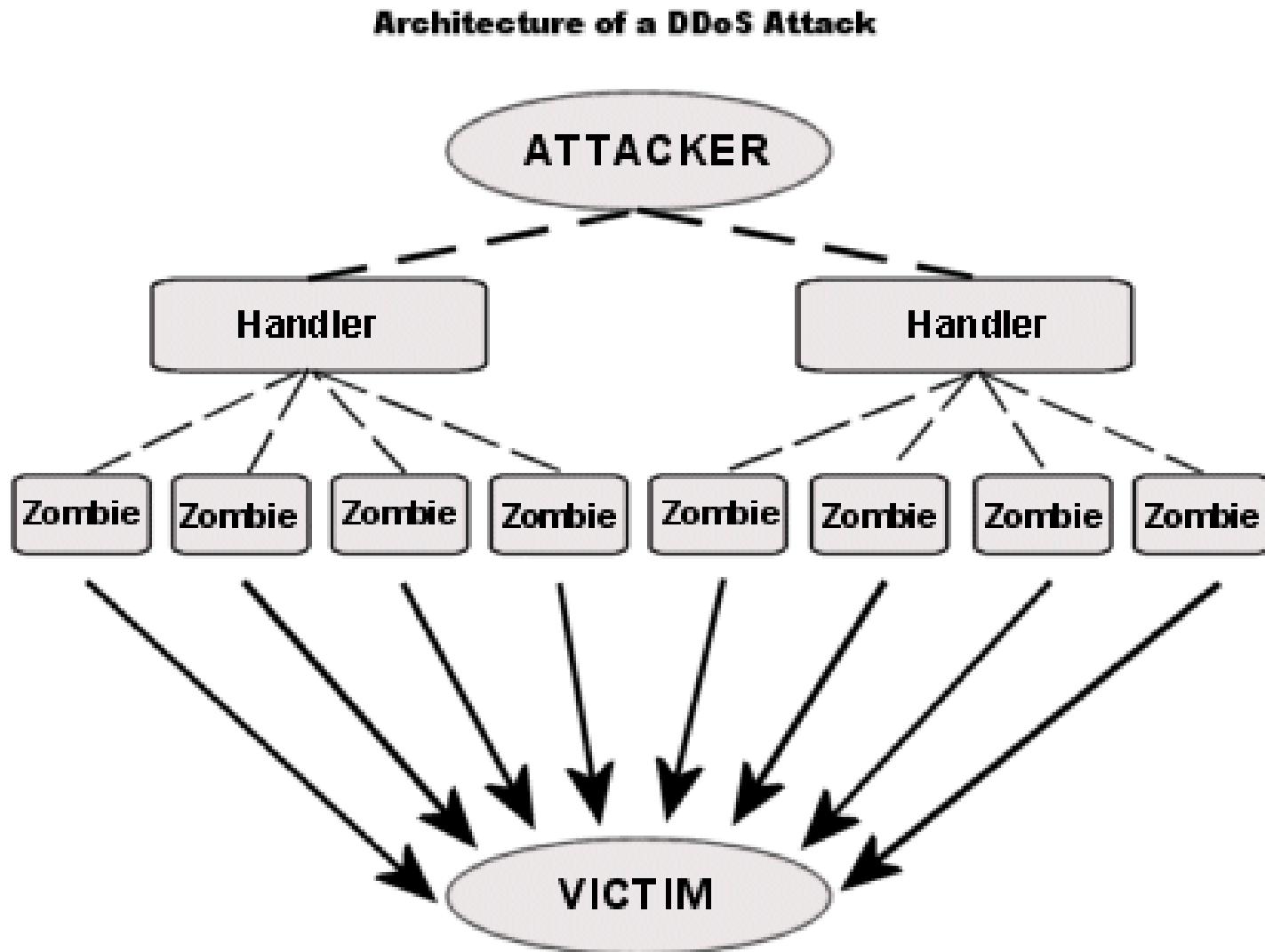
- Liên quan đến gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo;
- DDoS khác DoS ở phạm vi tấn công:
 - Số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm;
 - Số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc trăm ngàn máy, và đến từ rất nhiều vị trí địa lý khác nhau trên toàn cầu.

3.3 Các dạng tấn công - Tấn công DDoS

❖ Kịch bản tấn công DDoS:

- Kẻ tấn công chiếm quyền điều khiển hàng trăm thậm chí hàng ngàn máy tính trên mạng Internet, sau đó cài các chương trình tấn công tự động (Automated agents) lên các máy này;
 - Automated agents còn được gọi là các Bots hoặc Zombies;
 - Các máy bị chiếm quyền điều khiển hình thành mạng máy tính ma, gọi là botnet hay zombie network.
- Tiếp theo, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn khác nhau nên rất khó đối phó và lần vết để tìm ra kẻ tấn công thực sự.

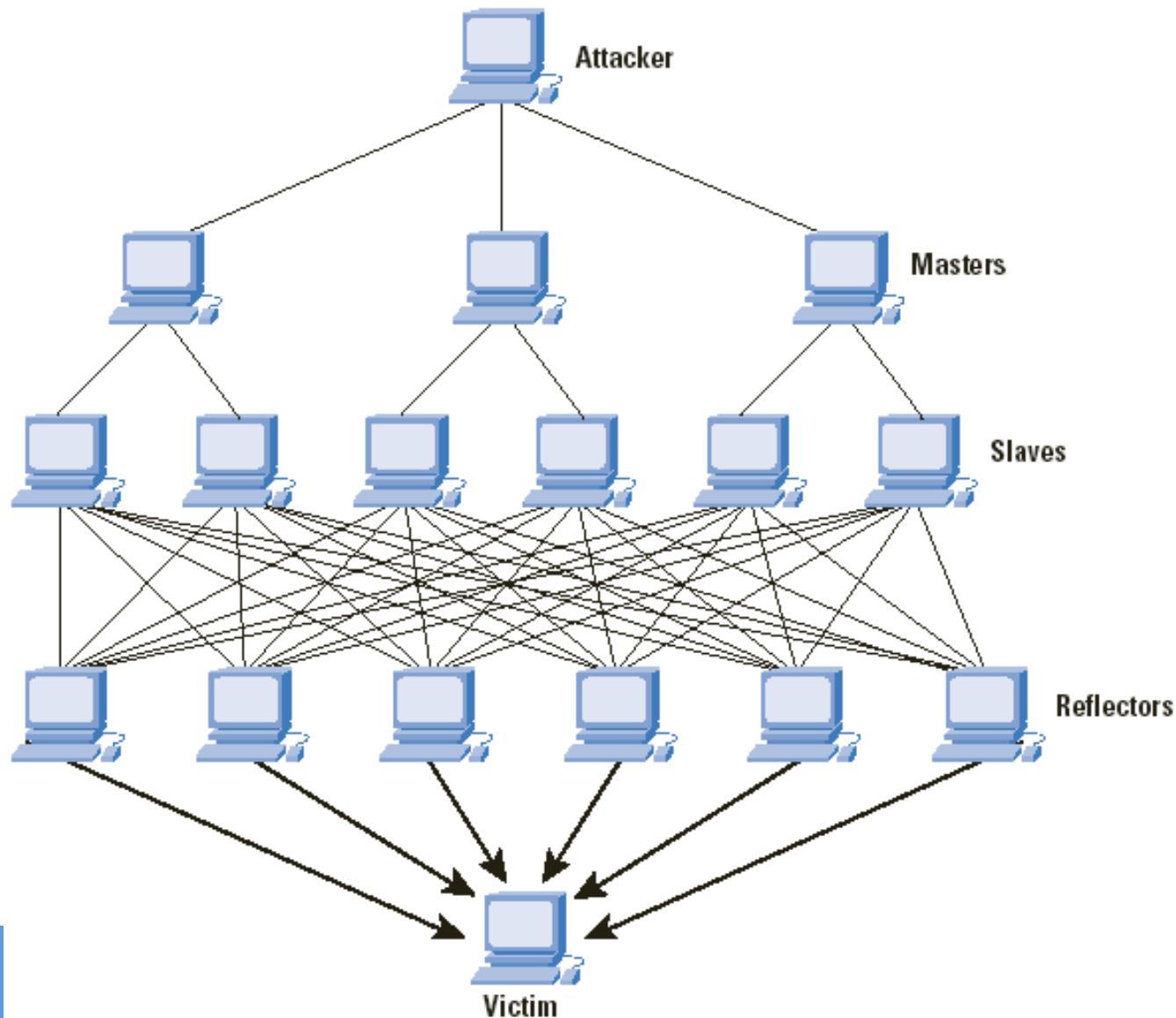
3.3 Các dạng tấn công - Tấn công DDoS



3.3 Các dạng tấn công - Tấn công Reflective DDoS

- ❖ Tấn công Reflective DDoS (DDoS phản chiếu hay gián tiếp) là một loại tấn công DDoS với một số điểm khác biệt:
 - Các máy tính do kẻ tấn công điều khiển (Slaves/Zombies) không trực tiếp tấn công máy nạn nhân;
 - Chúng gửi một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác (Reflectors) trên mạng Internet;
 - Các Reflectors gửi Reply đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;
 - Nếu các Reflectors có số lượng lớn, số Reply sẽ rất lớn và gây ngập lụt máy nạn nhân.
- ❖ Tấn công Reflective DDoS khó lẩn vết và phòng chống hơn tấn công DDoS thông thường do có thể qua nhiều cấp.

3.3 Các dạng tấn công - Tấn công Reflective DDoS



3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ

❖ Tấn công giả mạo địa chỉ IP (IP Spoofing) :

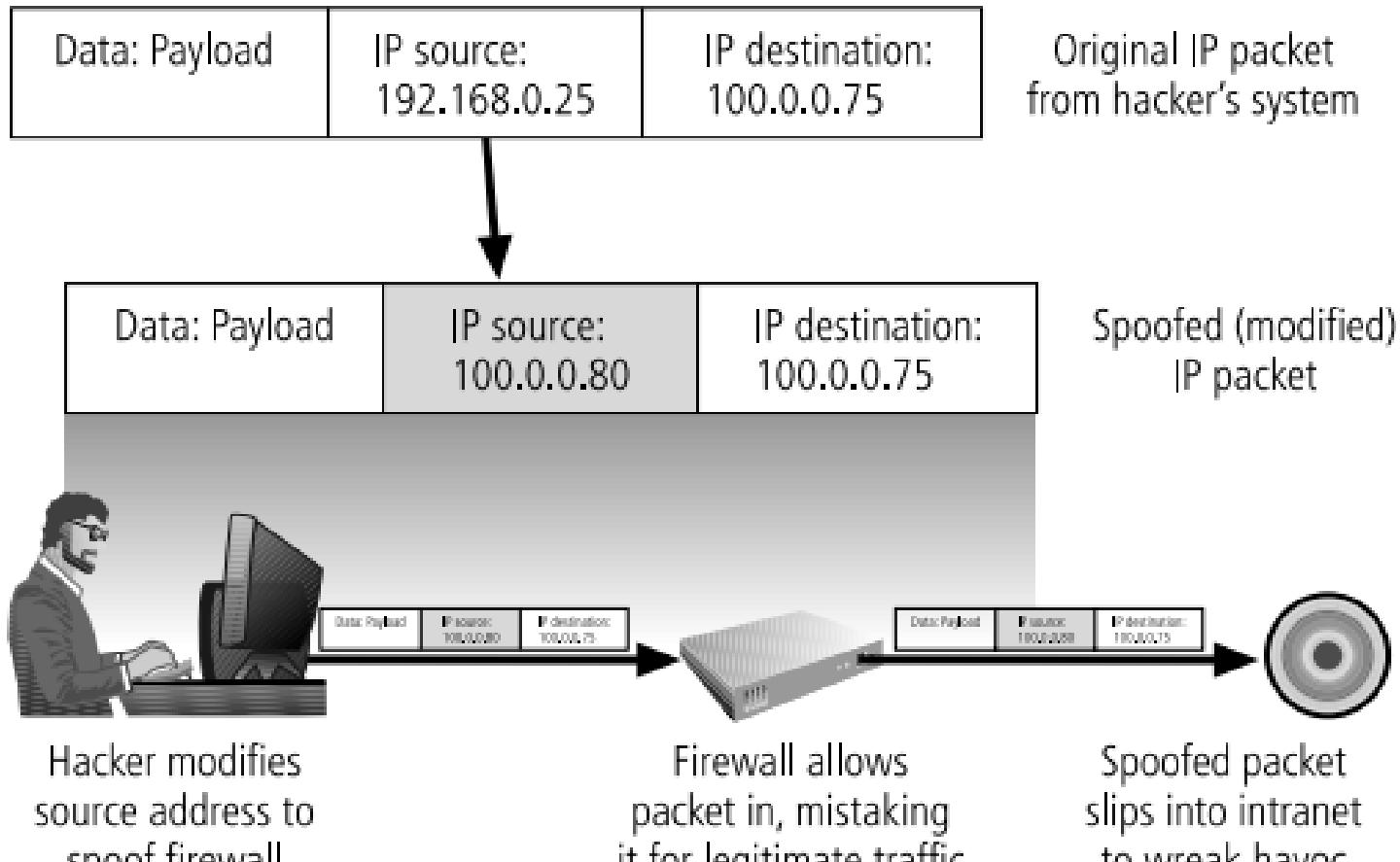
- Là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua các hàng rào kiểm soát an ninh;
- Nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội đột nhập vào các máy khác trong LAN do chính sách kiểm soát an ninh với các máy trong mạng LAN thường được giảm nhẹ.
- Nếu router hoặc firewall của mạng không được cấu hình để nhận ra IP giả mạo của mạng LAN nội bộ → kẻ tấn công có thể thực hiện.

3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ

0	4	8	15	16	31				
Version	IHL	Type of Service	Total Length						
Identification		Flags	Fragment Offset						
Time to Live	Protocol	Header Checksum							
Source IP Address									
Destination IP Address									
Options				Padding					

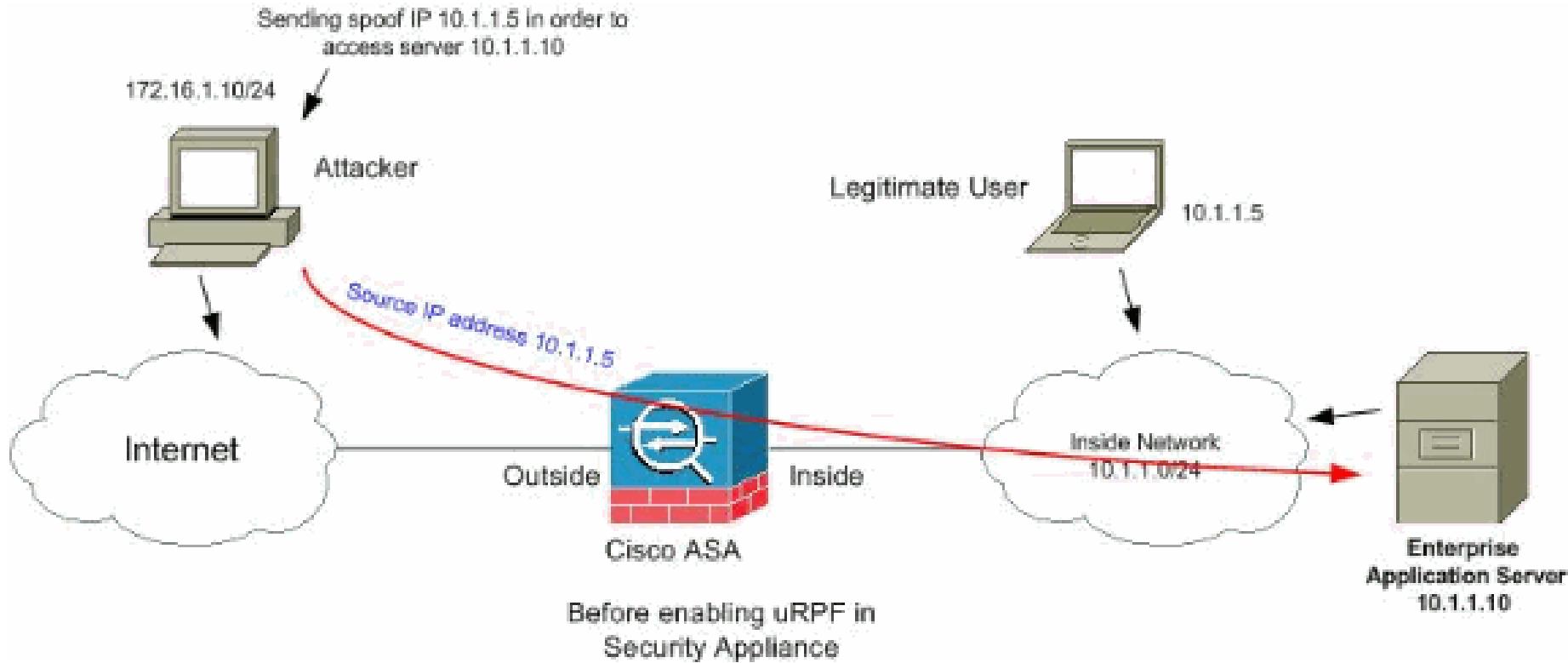
Định dạng gói tin IPv4

3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ



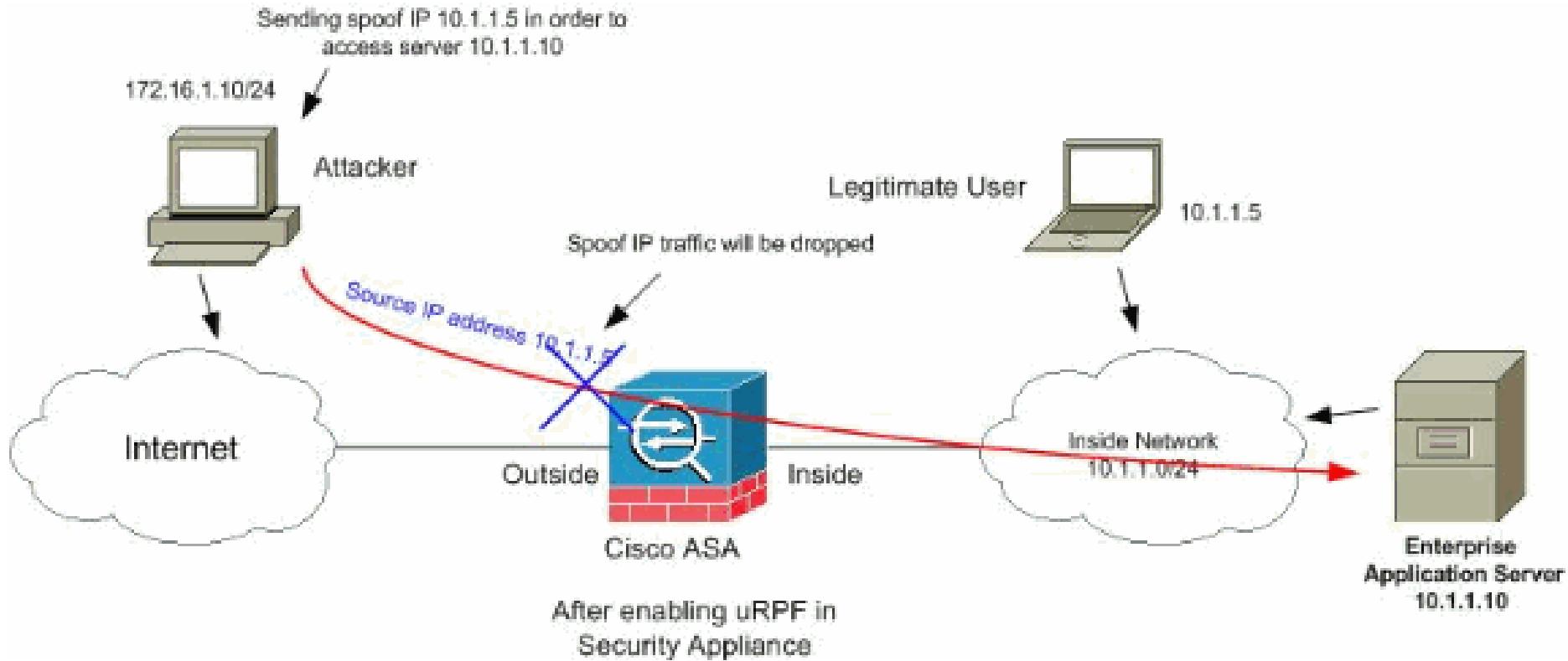
Tấn công giả mạo địa chỉ IP

3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ



Tấn công giả mạo địa chỉ thành công do router không nhận ra địa chỉ cục bộ bị giả mạo

3.3 Các dạng tấn công - Tấn công giả mạo địa chỉ

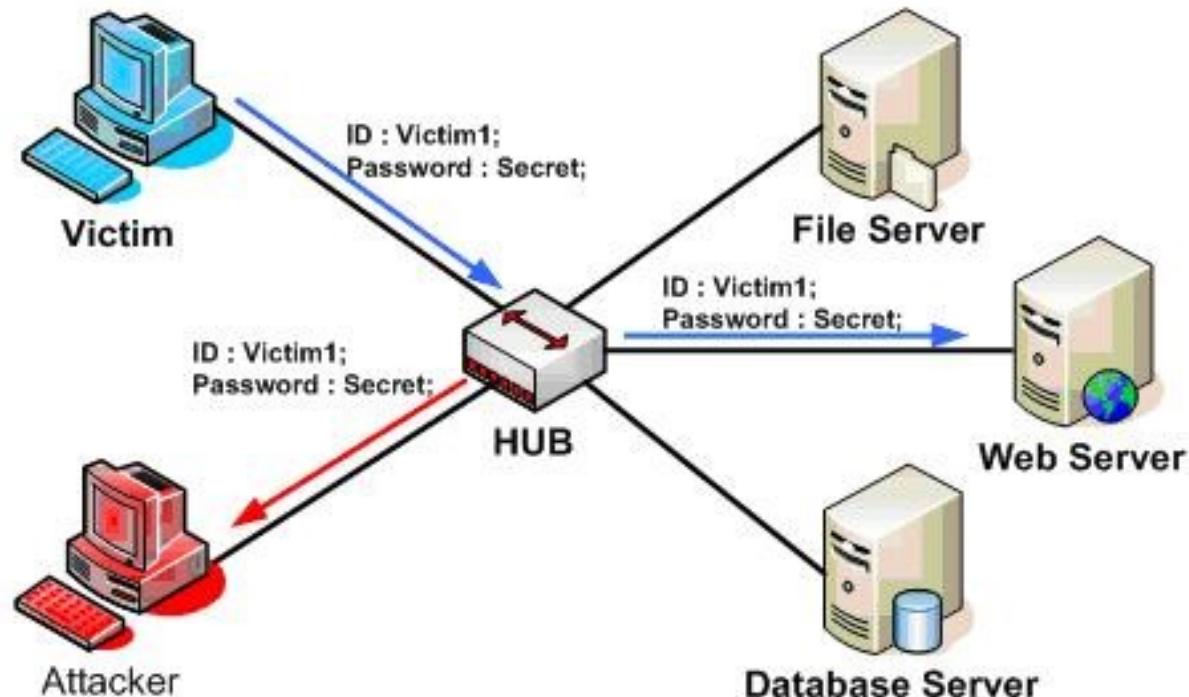


Tấn công giả mạo địa chỉ không thành công do router nhận ra địa chỉ cục bộ bị giả mạo

3.3 Các dạng tấn công - Tấn công nghe trộm

❖ Tấn công nghe trộm (Sniffing/Eavesdropping) :

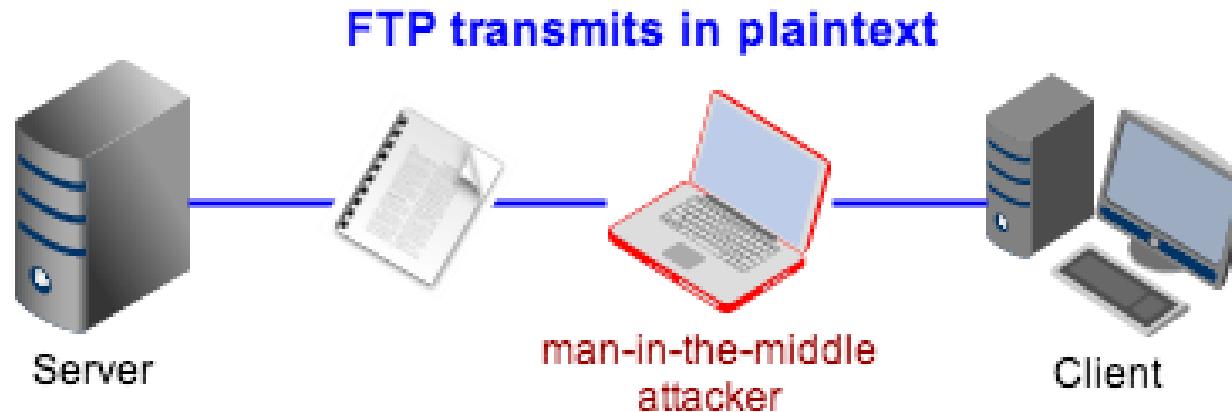
- Là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub, switch, hoặc router để bắt các gói tin dùng cho phân tích về sau.



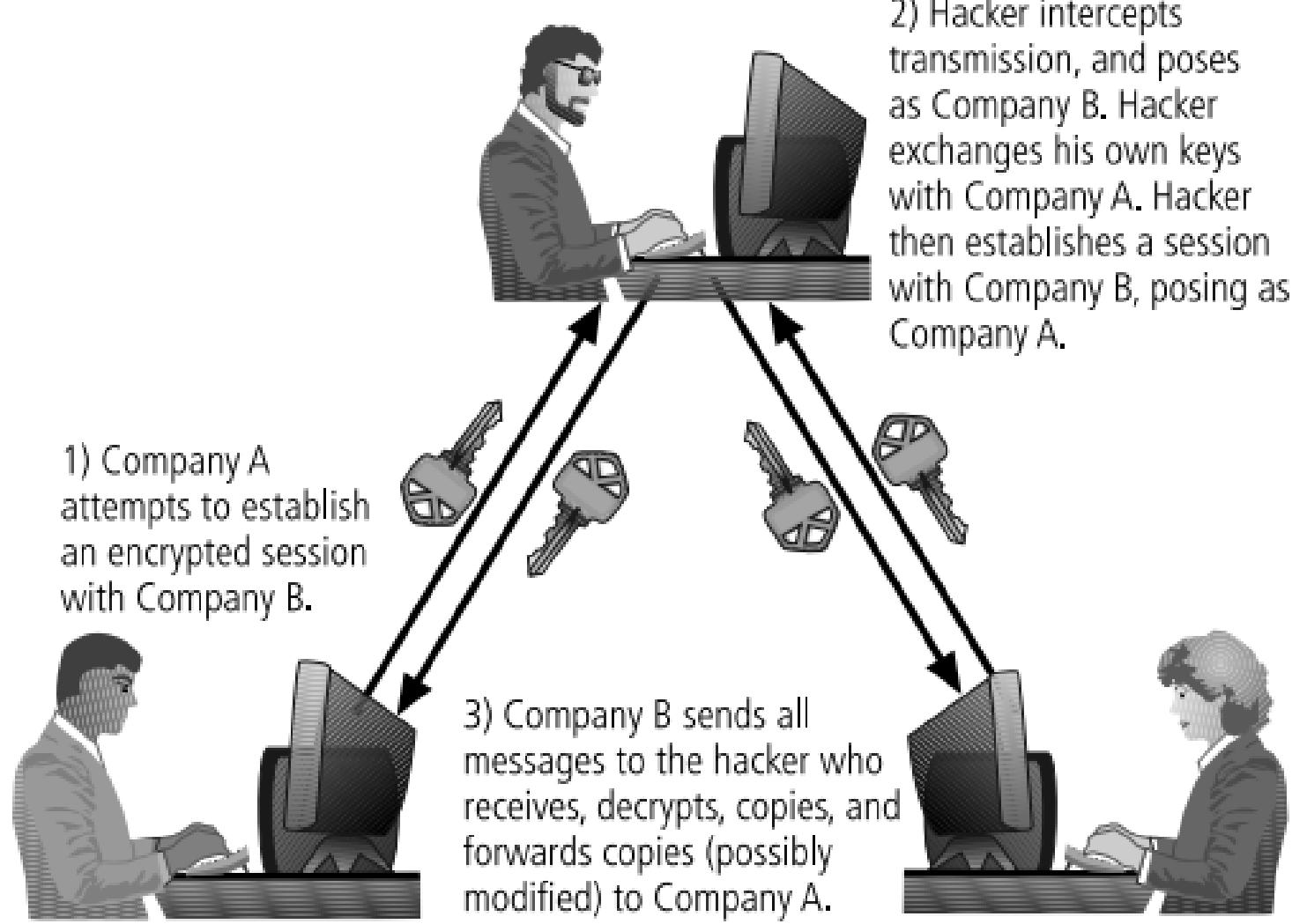
3.3 Các dạng tấn công - Tấn công kiểu người đứng giữa

❖ Tấn công người đứng giữa (Man in the middle)

- Lợi dụng quá trình chuyển gói tin đi qua nhiều trạm (hop) thuộc các mạng khác nhau;
- Kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông, có thể xem, sửa đổi và chuyển thông điệp lại cho bên kia.
- Thường được sử dụng để đánh cắp thông tin.



3.3 Các dạng tấn công - Tấn công kiểu người đứng giữa



3.3 Các dạng tấn công - Tấn công bằng bom thư và thư rác

❖ Tấn công bằng bom thư và thư rác

- Tấn công bằng bom thư (Mail bombing) là dạng tấn công DoS khi kẻ tấn công chuyển một lượng lớn email đến nạn nhân;
 - Có thể thực hiện được bằng kỹ thuật Social Engineering;
 - Hoặc khai thác lỗi trong hệ thống gửi nhận email SMTP.
 - Kẻ tấn công có thể lợi dụng các máy chủ email không được cấu hình tốt để gửi email cho chúng.
- Tấn công bằng thư rác (Spam emails)
 - Spams là những email không mong muốn, thường là các email quảng cáo;
 - Spams gây lãng phí tài nguyên tính toán và thời gian của người dùng (phải lọc, xóa);
 - Spams cũng có thể dùng để chuyển các phần mềm độc hại.

3.3 Các dạng tấn công - Tấn công sử dụng cửa hậu

❖ Tấn công sử dụng cửa hậu (Back doors)

- Cửa hậu thường được các lập trình viên tạo ra, dùng để gỡ rối và test chương trình.
- Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường.
- Khi cửa hậu được lập trình viên tạo ra để truy nhập hệ thống bất hợp pháp, nó trở thành một mối đe doạ đến an ninh hệ thống.
- Rất khó phát hiện ra cửa hậu vì nó thường được thiết kế và cài đặt khéo léo: cửa hậu chỉ được kích hoạt trong một ngữ cảnh nào đó.

3.3 Các dạng tấn công - Tấn công kiểu Social Engineering

- ❖ Tấn công kiểu Social Engineering là dạng tấn công sử dụng các kỹ thuật xã hội nhằm thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công.
 - Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng;
 - Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân/tổ chức.
 - Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân và thông tin tài khoản, thẻ tín dụng,...

3.3 Các dạng tấn công - Tấn công kiểu Social Engineering

- ❖ Trò lừa đảo Nigeria 4-1-9: lợi dụng sự ngây thơ và lòng tham của nhiều người.
 - Kẻ lừa đảo gửi thư tay hoặc email đến nhiều người nhận, mô tả về việc có 1 khoản tiền lớn (thừa kế, lợi tức,...) cần chuyển ra nước ngoài, nhờ người nhận giúp đỡ để hoàn thành giao dịch. Khoản tiền có thể lên đến hàng chục hoặc trăm triệu USD. Kẻ tấn công hứa sẽ trả cho người tham gia một phần số tiền (20-30%);
 - Nếu người nhận có phản hồi và đồng ý tham gia, kẻ tấn công sẽ gửi tiếp thư/email khác, yêu cầu chuyển cho hắn 1 khoản phí giao dịch (từ vài ngàn đến hàng chục ngàn USD);
 - Nếu người nhận gửi tiền cho kẻ tấn công → người đó mất tiền, do giao dịch mà kẻ tấn công hứa là giả mạo.

3.3 Các dạng tấn công - Tấn công kiểu phishing

- ❖ Phishing là một dạng của tấn công Social Engineering, lừa người dùng để lấy thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,...
 - Kẻ tấn công có thể giả mạo trang web của các tổ chức tài chính, ngân hàng;
 - Chúng gửi email cho người dùng (địa chỉ email thu thập trên mạng), yêu cầu xác thực thông tin;
 - Nếu người dùng làm theo hướng dẫn → cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng cho kẻ tấn công.

3.3 Các dạng tấn công - Tấn công kiểu phishing

Please Verify Your eBay Identity [Inbox](#)

★ eBay Billing Department to me

[More options](#) 5:36 pm (3 hours ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. [Learn more](#)



Dear valued eBay member

It has come to our attention that your eBay billing updates are out of order. If you could please take 5-10 minutes out of your online experience and update your billing records you will not run into any future problems with the online service.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of your account, Terms of Service (TOS) violations or future billing

3.3 Các dạng tấn công - Tấn công kiểu phishing

From: CustomerSecurity@royalbank.com¹
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder²

Royal Bank

Dear valued Royal Bank customer,³

It has come to our attention that you have not logged into your online banking account for some time⁴ now and, as a security measure, we must suspend your online account.⁵ If you would like to continue to use the online banking facility⁶ offered by Royal Bank, please click the link below and renew your security details⁷ immediately. Failure to do so will result in your online account being suspended.⁸

Renew your security details immediately and continue to use our online banking facility:
<https://customerbankingrenewal.royalbank.com/>⁹

We are sorry for any convenience¹⁰ caused and hope you continue to use our online banking facility.

The Royal Bank Online Security Team¹¹

Link: <http://customerbankingrenewal.royalbank.com/>

3.3 Các dạng tấn công - Tấn công kiểu pharming

❖ Pharming là kiểu tấn công vào trình duyệt người dùng:

- Người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu 1 website khác (độc hại);
- Kẻ tấn công thường sử dụng sâu, virus hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng;
- Kẻ tấn công cũng có thể tấn công vào hệ thống DNS để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.

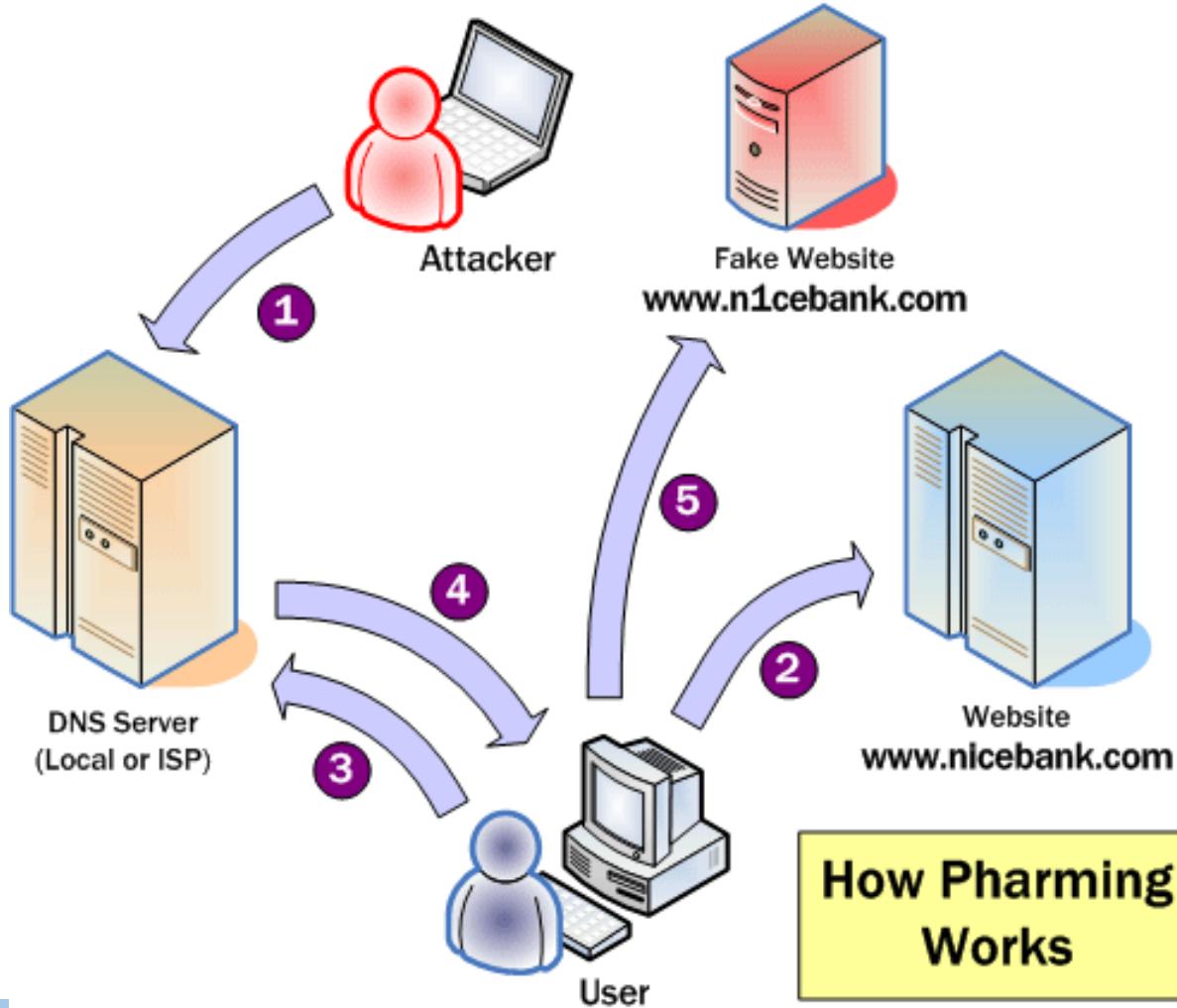
3.3 Các dạng tấn công - Tấn công kiểu pharming

Sửa đổi file hosts, hoặc điều khiển trình duyệt để chuyển hướng và giả mạo website



3.3 Các dạng tấn công - Tấn công kiểu pharming

Tấn
công vào
hệ thống
DNS để
chuyển
hướng
website



3.3 Các dạng tấn công - Tấn công APT

- ❖ Tấn công APT (Advanced Persistent Threat), hay còn được gọi là tấn công có chủ đích là hình thức tấn công tập trung, có chủ đích, được thiết kế riêng cho từng mục tiêu, từng đối tượng cụ thể nhằm mục đích tìm kiếm các thông tin giá trị và gửi ra bên ngoài;
- ❖ Hai thuộc tính quan trọng của tấn công APT là
 - Tiên tiến, hay cao cấp (Advanced) và
 - Kiên trì, dai dẳng (Persistent).

3.3 Các dạng tấn công - Tấn công APT

❖ Ví dụ:

- Để tấn công vào người dùng, chúng kiên trì tìm hiểu thông tin về người dùng đó như sở thích, tính cách hay cách đặt tên file, mối quan hệ của nạn nhân trên thế giới ảo;
- Khi chúng đã xâm nhập được vào hệ thống và đã đánh cắp được dữ liệu và gửi ra ngoài, chúng không bao giờ dừng việc đánh cắp dữ liệu mà mục đích của chúng là cài cắm mã độc vào hệ thống để lấy được càng nhiều dữ liệu càng tốt.

❖ Vụ tấn công vào hệ thống mạng của Vietnam Airlines vào tháng 7.2016 là 1 cuộc tấn công ATP điển hình.

- Tham khảo:

vi.wikipedia.org/wiki/Vụ_tin_tặc_tấn_công_các_sân_bay_tại_Việt_Nam_2016

3.3 Các dạng tấn công - Tấn công APT

- Thuộc tính “tiên tiến” có nghĩa là các kỹ thuật tiên tiến được sử dụng để tấn công vào hệ thống mục tiêu một cách bài bản, rất khó phát hiện;
- Thuộc tính “kiên trì” có nghĩa là mục tiêu được xác định rất cụ thể để thực hiện tấn công, ẩn mình và khai thác theo từng giai đoạn;
 - Nhiều kỹ thuật, phương pháp tấn công khác nhau vào mục tiêu được sử dụng cho đến khi thành công;
 - Có thể sử dụng hàng tháng, thậm chí hàng năm chỉ để thu thập thông tin của nạn nhân làm tiền đề cho cuộc tấn công.

3.3 Các dạng tấn công - Tấn công APT

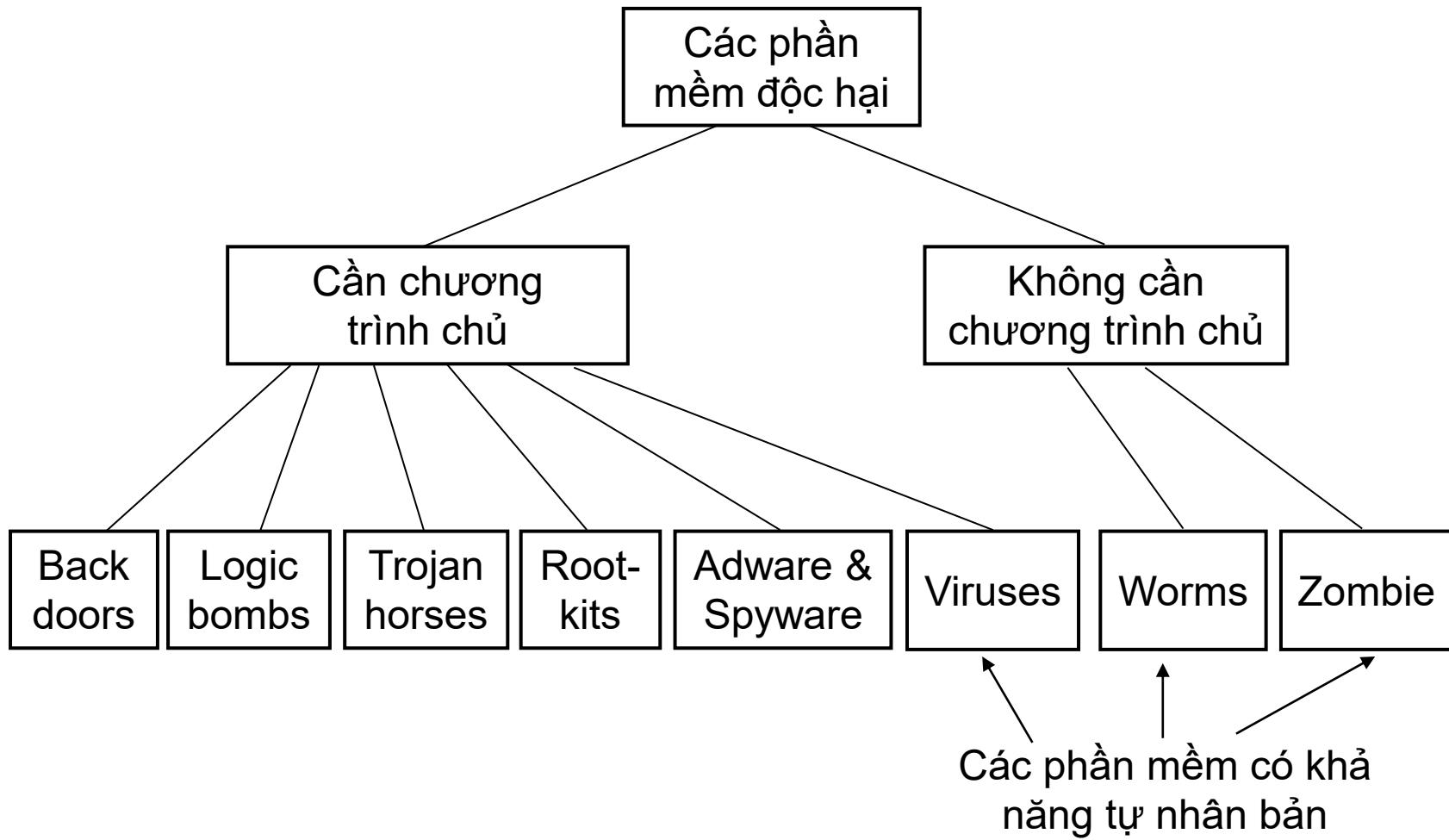
❖ Một cuộc tấn công APT điển hình thường được thực hiện theo các giai đoạn sau:

- Truy cập ban đầu
- Thâm nhập lần đầu và triển khai mã độc
- Mở rộng truy cập và di chuyển ngang
- Giai đoạn tấn công
- Gây thiệt hại
- Tấn công tiếp theo.

3.4 Các dạng phần mềm độc hại

- ❖ Các phần mềm độc hại, còn gọi là phần mềm mã độc (Malware hay Malicious software), hay ngắn gọn là mã độc, là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống.
- ❖ Khi mới được phát hiện vào những năm 1970-1980, các phần mềm độc hại còn tương đối ít chủng loại và được gọi chung là vi rút (virus) .
- ❖ Tuy nhiên, theo thời gian vi rút đã phát triển rất mạnh thành nhiều dạng khác nhau, và thuật ngữ “phần mềm độc hại” hay “mã độc” (malware) được sử dụng chỉ các dạng mã độc thay thế cho thuật ngữ “vi rút”.

3.4 Các dạng phần mềm độc hại - Phân loại



3.4 Các dạng phần mềm độc hại - Logic bombs

- ❖ Bom logic (Logic bombs) thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể.
- ❖ Điều kiện để bom “phát nổ” có thể là:
 - Sự xuất hiện hoặc biến mất của các files cụ thể;
 - Một ngày nào đó, hoặc một ngày trong tuần.
- ❖ Khi “phát nổ” bom logic có thể xoá dữ liệu, files, tắt cả hệ thống...
- ❖ Ví dụ: Quả bom logic do Tim Lloyd cài lại đã “phát nổ” tại công ty Omega Engineering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom logic này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD. Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.

3.4 Các dạng phần mềm độc hại - Trojan horses

- ❖ Trojan horses lấy tên theo tích "Con ngựa thành Troy"



3.4 Các dạng phần mềm độc hại - Trojan horses

- ❖ Trojan horses chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng.
- ❖ Trojan horses thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập.
- ❖ VD: trong một hệ thống nhiều users, một user có thể tạo ra một trojan đội lốt một chương trình hữu ích đặt ở thư mục chung. Khi trojan này được thực thi bởi một user khác, nó sẽ cho phép tất cả các users truy nhập vào các files của user đó.

3.4 Các dạng phần mềm độc hại - Zombie

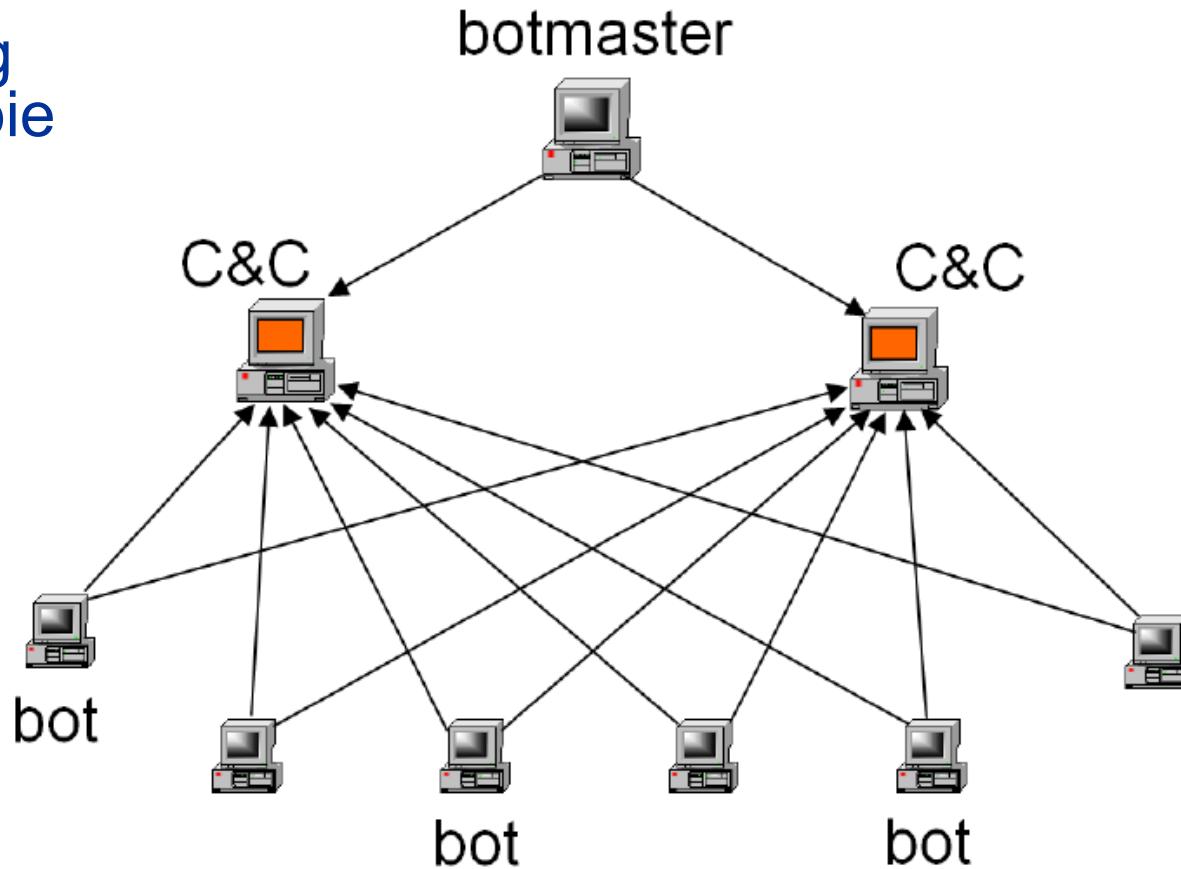


3.4 Các dạng phần mềm độc hại - Zombie

- ❖ Zombie (còn gọi là bot hoặc automated agent) là một chương trình được thiết kế để giành quyền kiểm soát một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác.
- ❖ Các zombies thường được dùng để gửi thư rác và tấn công DDoS các máy chủ, các website lớn.
- ❖ Rất khó để lẩn vết và phát hiện ra tác giả tạo ra và điều khiển các zombies.

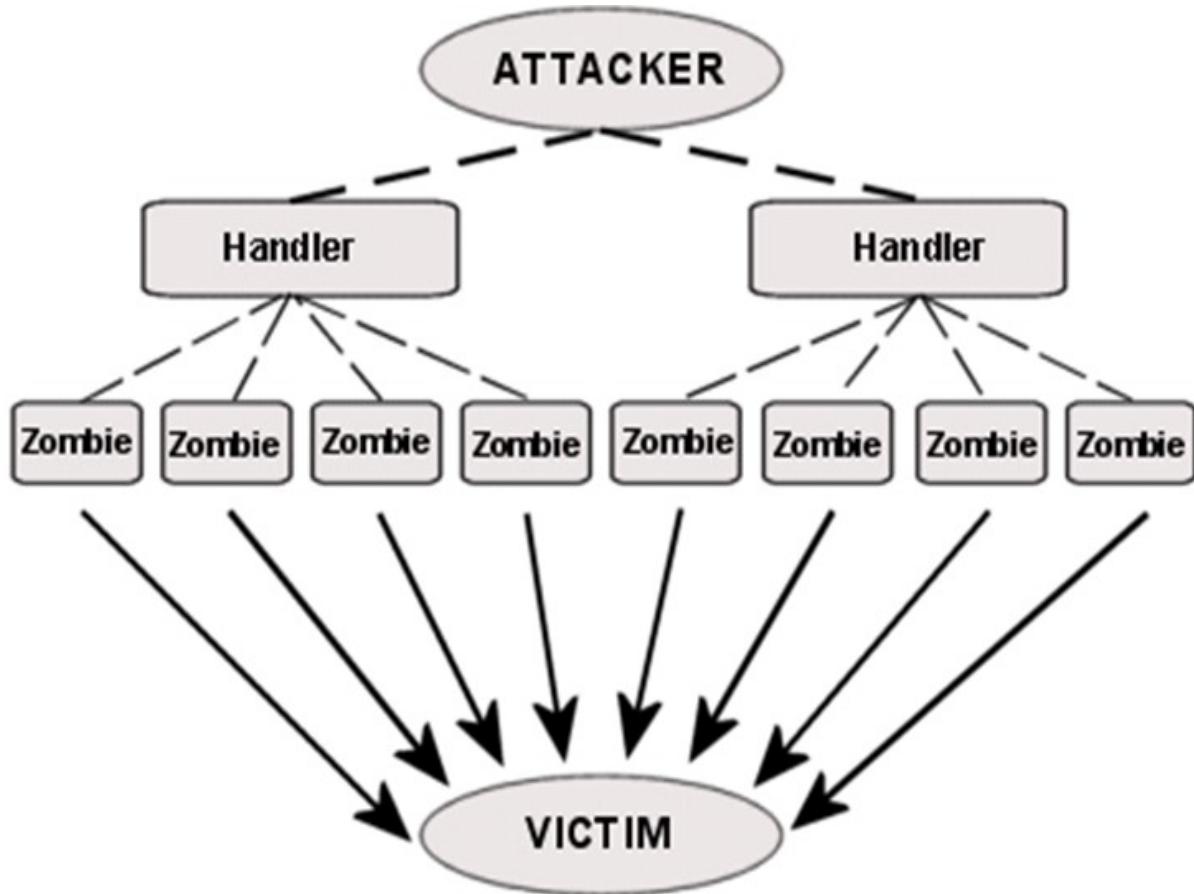
3.4 Các dạng phần mềm độc hại - Zombie

Mô hình hoạt động của zombie network / botnet



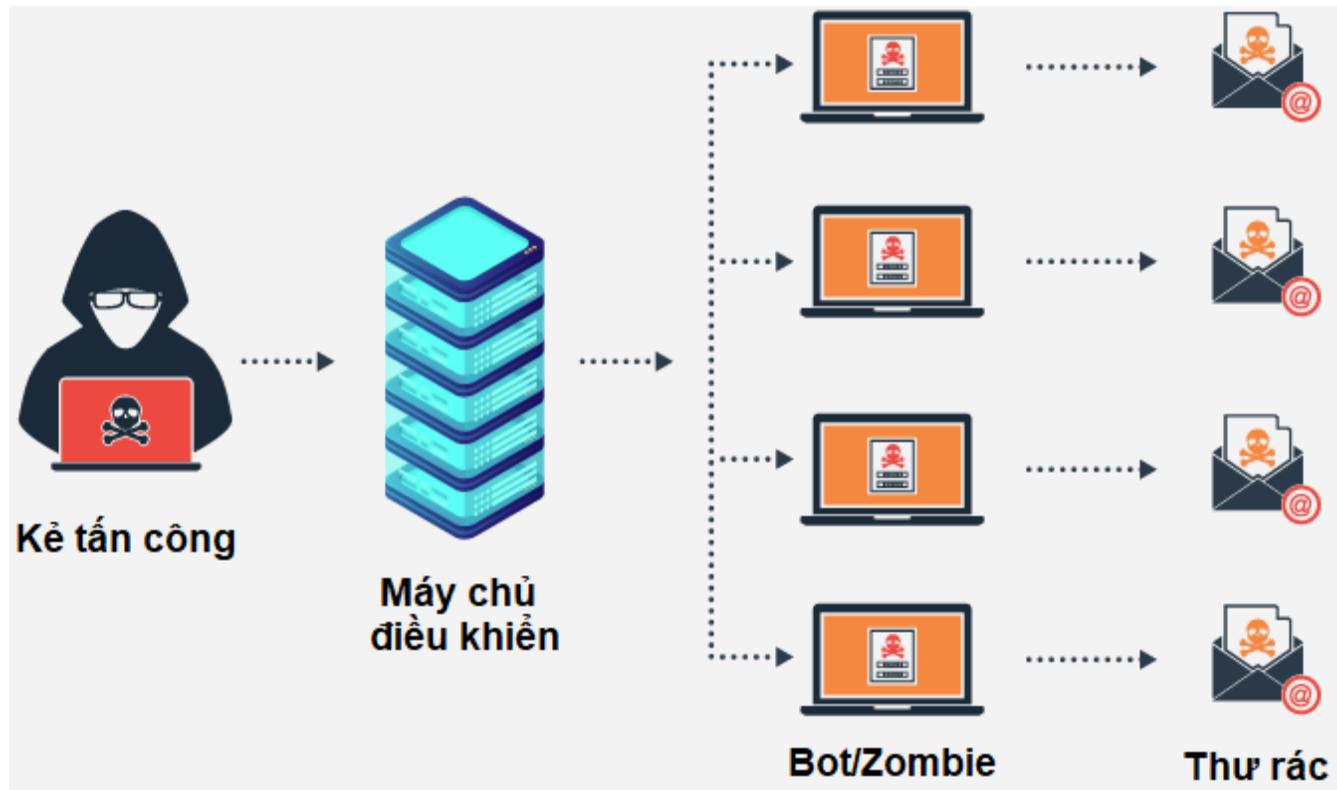
3.4 Các dạng phần mềm độc hại - Zombie

Sử dụng zombie network / botnet để tấn công DDoS



3.4 Các dạng phần mềm độc hại - Zombie

Sử dụng
zombie
network /
botnet để
gửi thư rác



3.4 Các dạng phần mềm độc hại - Viruses



3.4 Các dạng phần mềm độc hại - Viruses

- ❖ Virus là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này.
- ❖ Nếu các chương trình đã bị sửa đổi chứa virus được kích hoạt thì virus sẽ tiếp tục “lây nhiễm” sang các chương trình khác.
- ❖ Giống như virus sinh học, virus máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc.
- ❖ Có nhiều con đường lây nhiễm virus: sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...
- ❖ Virus có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, virus tự động được thực hiện khi chương trình này chạy.

3.4 Các dạng phần mềm độc hại - Viruses

❖ 4 giai đoạn của vòng đời virus:

- Giai đoạn “nằm im”: Virus trong giai đoạn không được kích hoạt. Trong giai đoạn này virus có thể được kích hoạt nhờ một sự kiện nào đó.
- Giai đoạn phát tán: Virus “cài” một bản sao của nó vào các chương trình khác.
- Giai đoạn kích hoạt: virus được kích hoạt để thực thi các tác vụ đã thiết kế được định sẵn. Virus cũng thường được kích hoạt dựa trên một sự kiện nào đó.
- Giai đoạn thực hiện: thực thi các tác vụ. Một số viruses có thể vô hại, nhưng một số khác có thể xoá dữ liệu, chương trình...

3.4 Các dạng phần mềm độc hại - Viruses

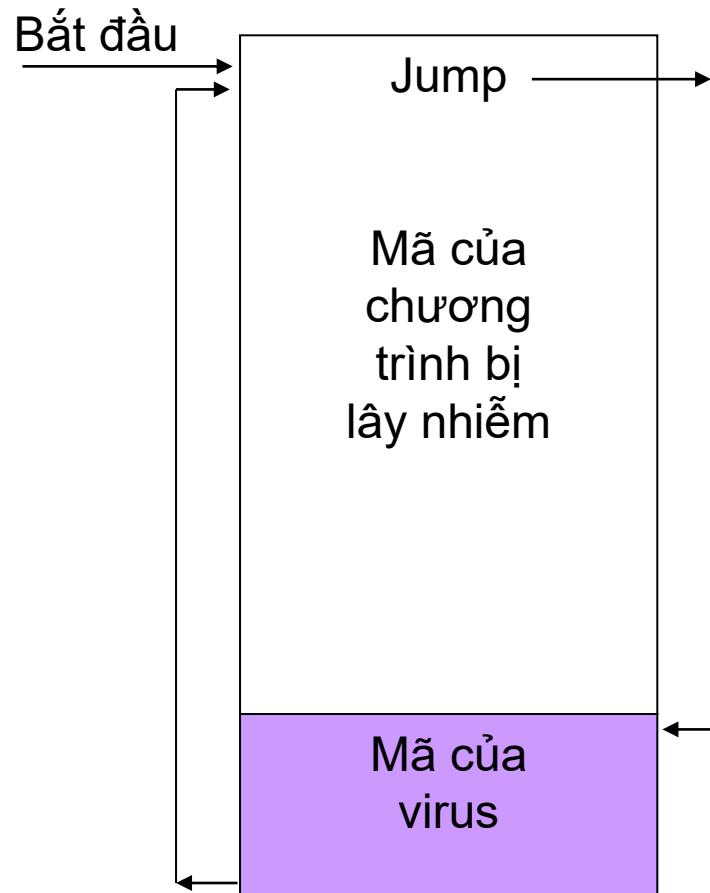
❖ Các loại viruses:

- Boot virus là virus lây nhiễm vào cung khởi động của đĩa.
- File virus là virus lây nhiễm vào các file chương trình, hoặc một số file tài liệu (pdf, ảnh, video,...)
- Macro virus là virus lây nhiễm vào các file tài liệu của bộ chương trình Microsoft Office
- Email virus là virus lây nhiễm thông qua việc gửi, nhận và xem email.

3.4 Các dạng phần mềm độc hại – File Viruses

❖ Cơ chế chèn mã virus vào chương trình chủ của file virus:

- Virus có thể chèn mã của nó vào đầu hoặc cuối của chương trình bị lây nhiễm.
- Khi chương trình nhiễm virus được thực hiện, mã virus được thực hiện trước, sau đó mã chương trình mới được thực hiện.



3.4 Các dạng phần mềm độc hại – Macro Viruses

- ❖ Macro viruses thường lây nhiễm vào các files tài liệu của MS-Word và ứng dụng office khác.
- ❖ Macro viruses hoạt động được nhờ:
 - Tính năng cho phép tạo và thực hiện các đoạn mã macro trong các tài liệu của bộ ứng dụng MS Office;
 - Các đoạn mã macro thường được dùng để tự động hóa 1 số việc và được viết bằng ngôn ngữ Visual Basic for Applications (VBA);
- ❖ Các ứng dụng văn phòng khác như Open Office không hỗ trợ VBA không bị ảnh hưởng bởi macro virus.

3.4 Các dạng phần mềm độc hại – Macro Viruses

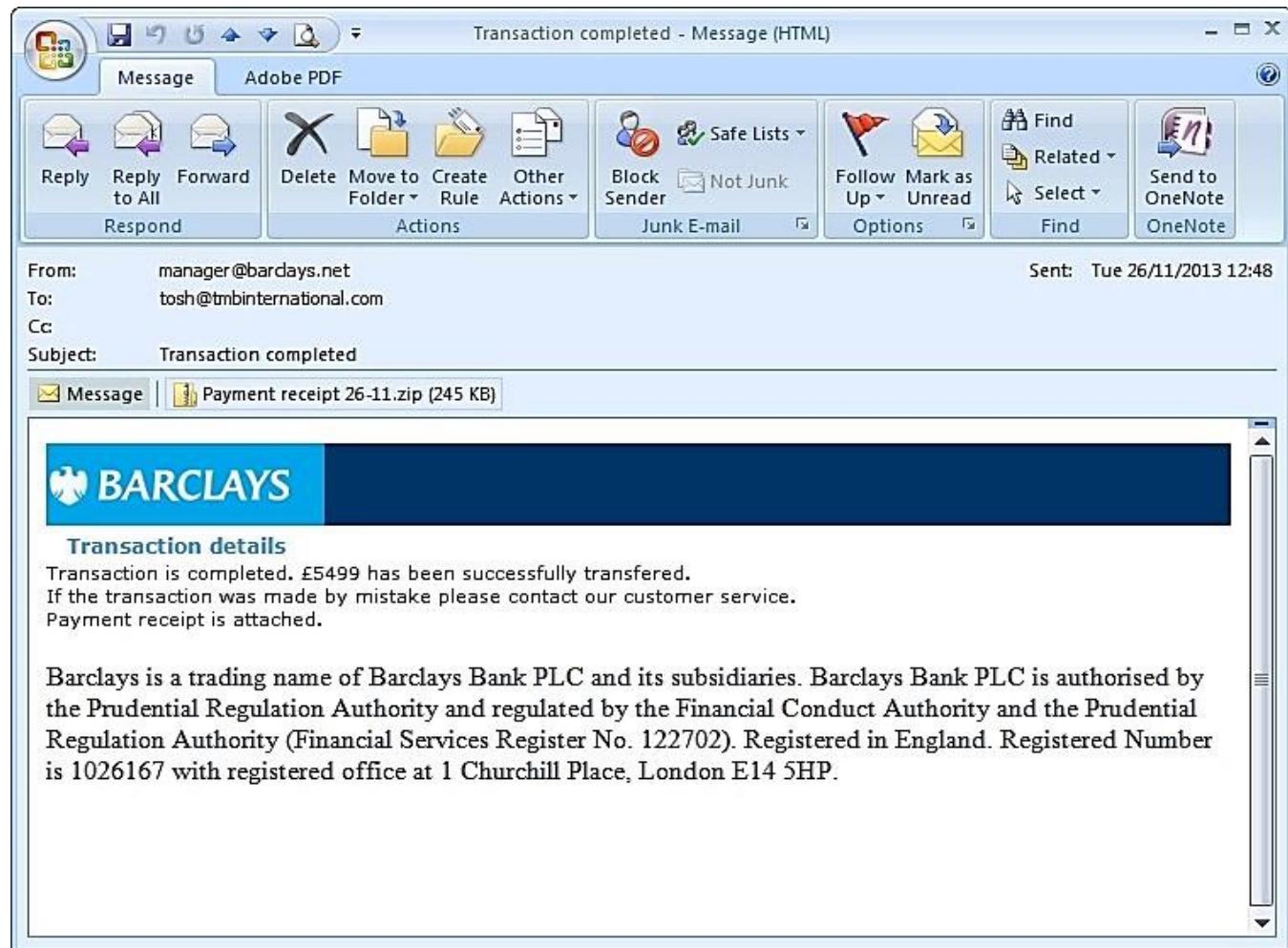
- ❖ Macro viruses thường lây nhiễm vào các files định dạng chuẩn và từ đó lây nhiễm vào tất cả các files tài liệu được mở.
- ❖ Macro viruses cũng có thể được tự động kích hoạt nhờ các auto-executed macros: AutoExecute, Automacro và Command macro.
- ❖ Theo thống kê, macro viruses chiếm khoảng 2/3 tổng lượng viruses đã được phát hiện;
 - Lượng tài liệu bị lây nhiễm macro virus đã giảm đáng kể từ khi Microsoft Office 2010 có thiết lập ngầm định – cấm chạy các macro.

3.4 Các dạng phần mềm độc hại – E-mail Viruses

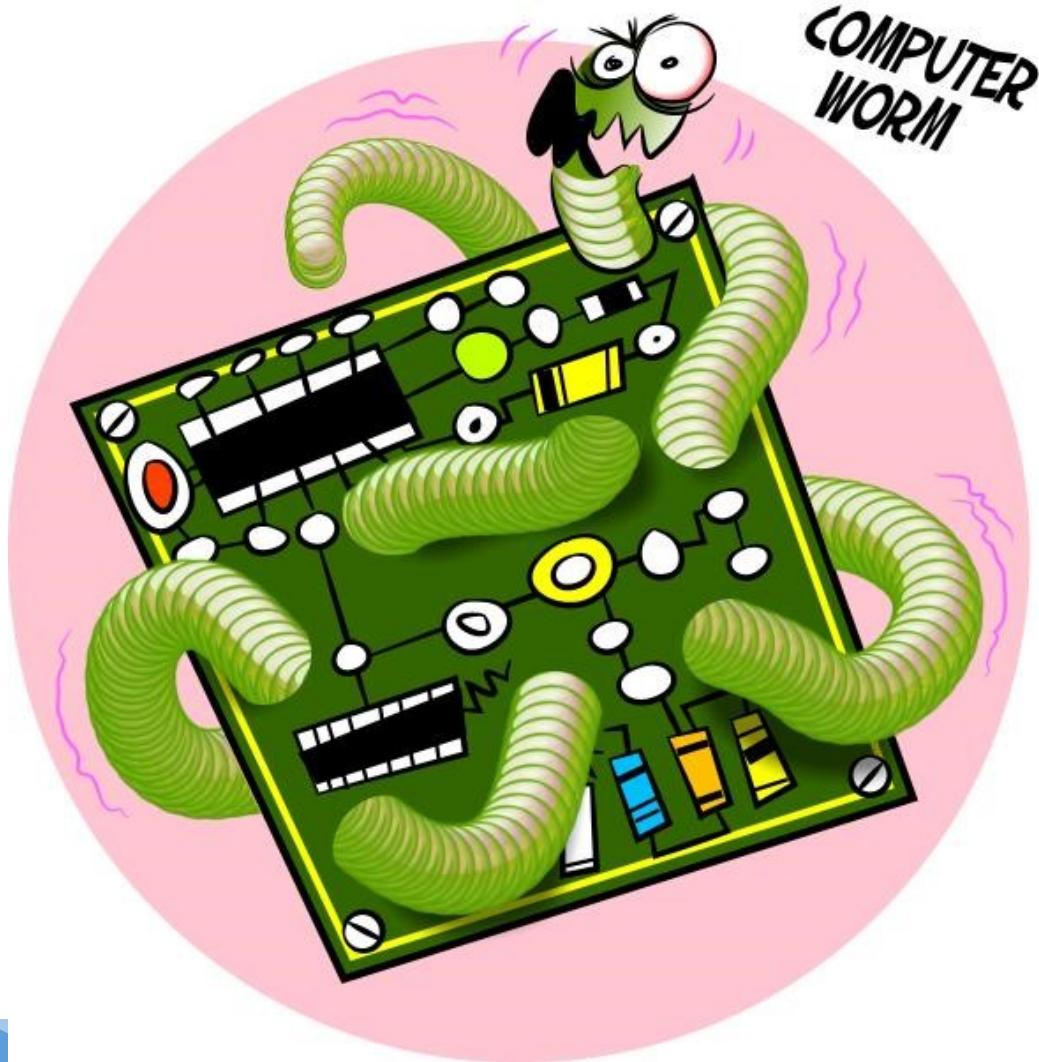
- ❖ E-mail viruses lây nhiễm bằng cách tự động gửi một bản copy của nó như 1 file đính kèm đến tất cả các địa chỉ email trong sổ địa chỉ của user trên máy bị lây nhiễm.
- ❖ Nếu user mở email hoặc file đính kèm, virus được kích hoạt.
- ❖ E-mail viruses có thể lây nhiễm rất nhanh chóng, lan tràn trên khắp thế giới trong một thời gian ngắn.

3.4 Các dạng phần mềm độc hại – E-mail Viruses

Một mẫu email do virus gửi đến người dùng



3.4 Các dạng phần mềm độc hại - Worms

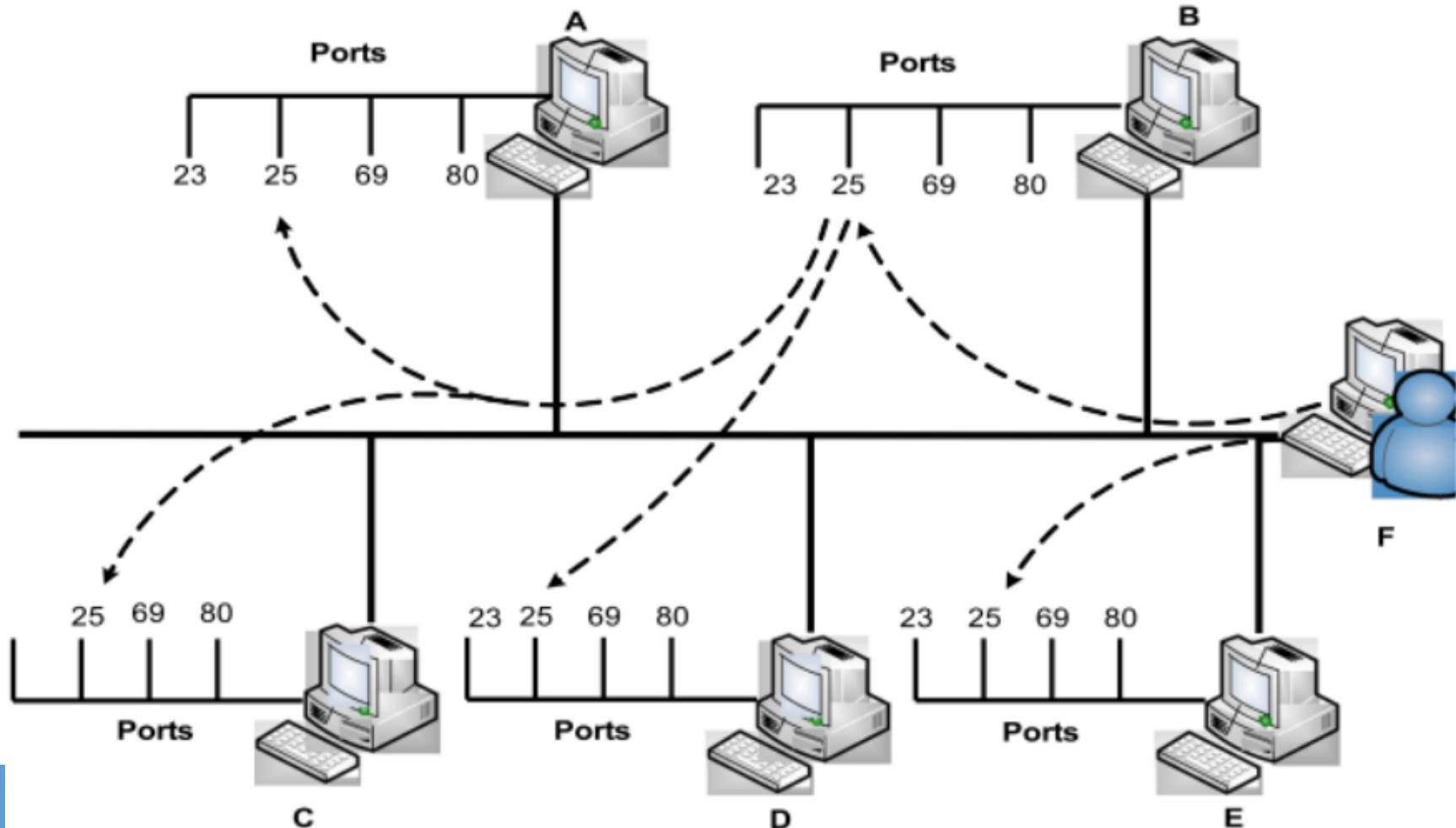


3.4 Các dạng phần mềm độc hại - Worms

- ❖ Sâu (Worms) có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần sự trợ giúp của người dùng (khác email viruses).
- ❖ Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm “bàn đạp” để tiếp tục tấn công các máy khác.
- ❖ Các sâu trên mạng sử dụng kết nối mạng để lây lan từ máy này sang máy khác.
- ❖ Khi sâu hoạt động, nó tương tự virus.

3.4 Các dạng phần mềm độc hại - Worms

- ❖ Một mô hình lây lan của sâu:



3.4 Các dạng phần mềm độc hại - Worms

❖ Các phương pháp lây lan của sâu:

- Lây lan qua thư điện tử: sử dụng email để gửi bản copy của sâu đến các máy khác.
- Lây lan thông qua khả năng thực thi từ xa: Sâu thực thi một bản copy của nó trên một máy khác nhờ lợi dụng các lỗ hổng an ninh của hệ điều hành, các dịch vụ hoặc phần mềm ứng dụng.
- Lây lan thông qua khả năng log-in (đăng nhập) từ xa: sâu đăng nhập vào hệ thống ở xa như một user và sử dụng lệnh để copy bản thân từ máy này sang máy khác.

3.4 Các dạng phần mềm độc hại – Worms – Ví dụ

❖ Code Red (7/2001):

- Lợi dụng một lỗi hỏng an ninh trong MS IIS để lây lan (lỗi tràn bộ đệm khi xử lý các file .ida của IIS).
- Quét các địa chỉ IP ngẫu nhiên để tìm các hệ thống có lỗi.
- Lây nhiễm vào 360.000 máy chủ trong vòng 14 giờ.

3.4 Các dạng phần mềm độc hại – Worms – Ví dụ

- ❖ Nimda (9/2001): có khả năng lây lan theo nhiều con đường:
 - Qua email từ máy client sang client
 - Qua các thư mục chia sẻ trên mạng
 - Từ máy chủ web sang trình duyệt
 - Từ máy khách đến máy chủ nhờ khai thác các lỗi máy chủ.
 - 22 phút sau khi ra đời Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet.

3.4 Các dạng phần mềm độc hại – Rootkits

- ❖ Rootkit là một dạng phần mềm độc hại gồm một tập các công cụ có mục đích giành quyền truy cập vào hệ thống máy tính mà người dùng không có thẩm quyền không thể truy cập;
- ❖ Rootkit thường che giấu mình bằng cách đội lốt một phần mềm khác;
- ❖ Rootkit có thể được cài đặt tự động, hoặc kẻ tấn công cài đặt rootkit khi chiếm được quyền quản trị hệ thống;
- ❖ Do rootkit có quyền truy cập hệ thống ở mức quản trị nên nó có toàn quyền truy cập vào các thành phần trong hệ thống và rất khó bị phát hiện.

3.4 Các dạng phần mềm độc hại – Adware và Spyware

❖ Adware:

- Adware (tên đầy đủ là advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm;
- Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm đó hoặc một dịch vụ miễn phí;
- Adware cũng có thể được cài đặt như một trình cắm chạy trong trình duyệt web của người dùng nhằm hiển thị các pop-up quảng cáo;
- Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được cài đặt và kích hoạt tự động mà không được sự đồng ý của người dùng.

3.4 Các dạng phần mềm độc hại – Adware và Spyware

❖ Spyware:

- Spyware (Spy software) là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân;
- Có 4 loại spyware thường gặp, gồm: system monitor (công cụ giám sát hệ thống), trojan, adware và tracking cookie (các cookie theo dõi người dùng).
- Spyware có thể được cài đặt vào hệ thống nạn nhân thông qua nhiều phương pháp, như tích hợp, đóng gói vào các phần mềm khác, bẫy nạn nhân tự tải và cài đặt, hoặc kẻ tấn công có thể sử dụng vi rút, sâu để tải và cài đặt.
- Spyware thường được trang bị khả năng ẩn mình nên rất khó có thể phát hiện bằng các phương pháp thông thường.

3.4 Các dạng phần mềm độc hại – Phòng chống

❖ Ngăn chặn viruses lây nhiễm vào hệ thống:

- Luôn cập nhật hệ thống để hạn chế các lỗi phần mềm
- Sử dụng các biện pháp kiểm soát truy nhập

❖ Khi hệ thống đã bị nhiễm virus:

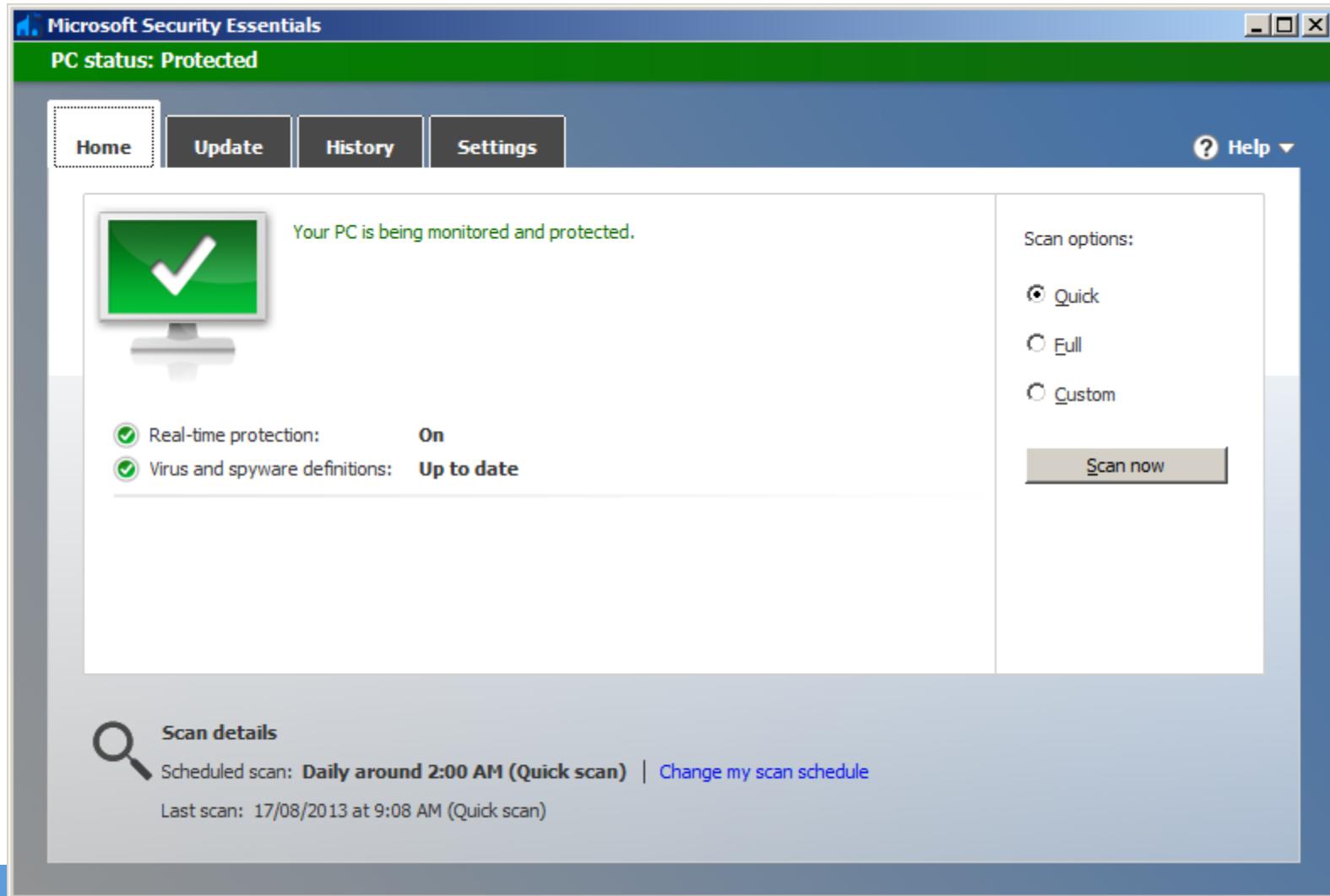
- Phát hiện virus
- Nhận dạng virus
- Loại bỏ virus

3.4 Các dạng phần mềm độc hại – Phòng chống

❖ Một số phần mềm diệt virus và phần mềm độc hại:

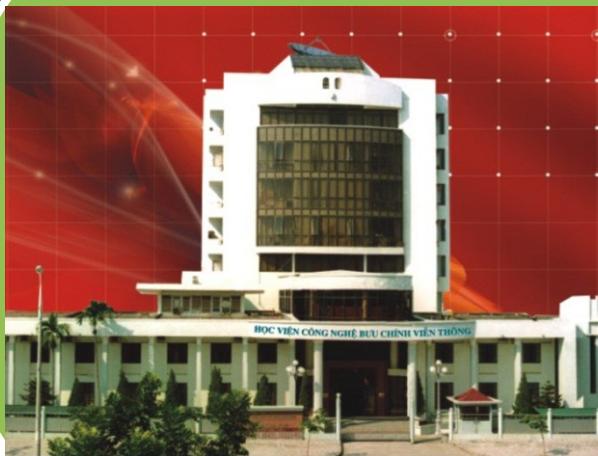
- Microsoft Security Essentials (Windows 7 trở lên)
- Microsoft Defenders (Windows 8 trở lên)
- Semantec Norton Antivirus
- Kaspersky Antivirus
- BitDefender Antivirus
- AVG Antivirus
- McAfee VirusScan
- Trend Micro Antivirus
- F-secure
- BKAV

3.4 Các dạng phần mềm độc hại – Phòng chống





HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN**

**CHƯƠNG 4 – ĐẢM BẢO ATTT
DỰA TRÊN MÃ HÓA**

Giảng viên:

PGS.TS. Hoàng Xuân Dậu

E-mail:

dauhx@ptit.edu.vn

Khoa:

An toàn thông tin

NỘI DUNG CHƯƠNG 4

1. Khái quát về mã hóa thông tin và ứng dụng
2. Các phương pháp mã hóa
3. Các giải thuật mã hóa
4. Chữ ký số, chứng chỉ số và PKI
5. Các giao thức đảm bảo an toàn thông tin dựa trên mã hóa.

4.1 Khái quát về mã hóa thông tin và ứng dụng

1. Mã hóa thông tin là gì?
2. Vai trò của mã hóa
3. Các thành phần của một hệ mã hóa
4. Lịch sử mã hóa
5. Mã hóa dòng và mã hóa khối
6. Các tiêu chuẩn đánh giá hệ mã hóa
7. Ứng dụng của mã hóa

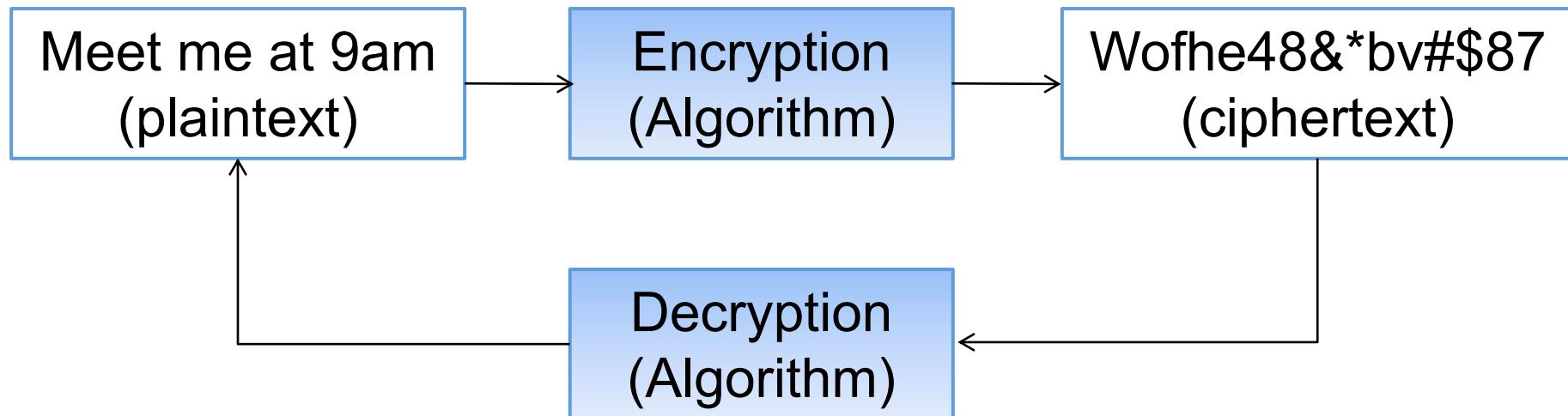
4.1.1 Mã hóa thông tin là gì?

- ❖ Định nghĩa theo Webster's Revised Unabridged Dictionary: cryptography is "the act or art of writing secret characters" – mật mã là một hành động hoặc nghệ thuật viết các ký tự bí mật.
- ❖ Định nghĩa theo Free Online Dictionary of Computing: cryptography is "encoding data so that it can only be decoded by specific individuals." – mật mã là việc mã hóa dữ liệu mà nó chỉ có thể được giải mã bởi một số người chỉ định.

4.1.1 Mã hóa thông tin là gì?

❖ Một hệ mã hóa gồm 2 khâu:

- Mã hóa (encryption)
- Giải mã (decryption)



4.1.1 Mã hóa thông tin – Các thuật ngữ

- ❖ Thông tin chưa được mã hóa (Unencrypted information) là thông tin ở dạng có thể hiểu được.
 - Cũng được gọi là bản rõ (plaintext hay cleartext)
- ❖ Thông tin đã được mã hóa (Encrypted information) là thông tin ở dạng đã bị xáo trộn.
 - Cũng được gọi là bản mã (ciphertext hay encrypted text)

4.1.1 Mã hóa thông tin – Các thuật ngữ

❖ Mã hóa (Encryption):

- Là hành động xáo trộn (scrambling) bản rõ để chuyển thành bản mã.

❖ Giải mã (Decryption):

- Là hành động giải xáo trộn (unscrambling) bản mã để chuyển thành bản rõ.

❖ Mã hóa/Giải mã sử dụng một thuật toán (Algorithm) để mã hóa/giải mã thông tin;

- Thuật toán mã hóa/giải mã có thể giống, hoặc khác nhau.

❖ Một bộ mã hóa (Cipher) là một giải thuật để mã hóa và giải mã thông tin.

4.1.1 Mã hóa thông tin – Các thuật ngữ

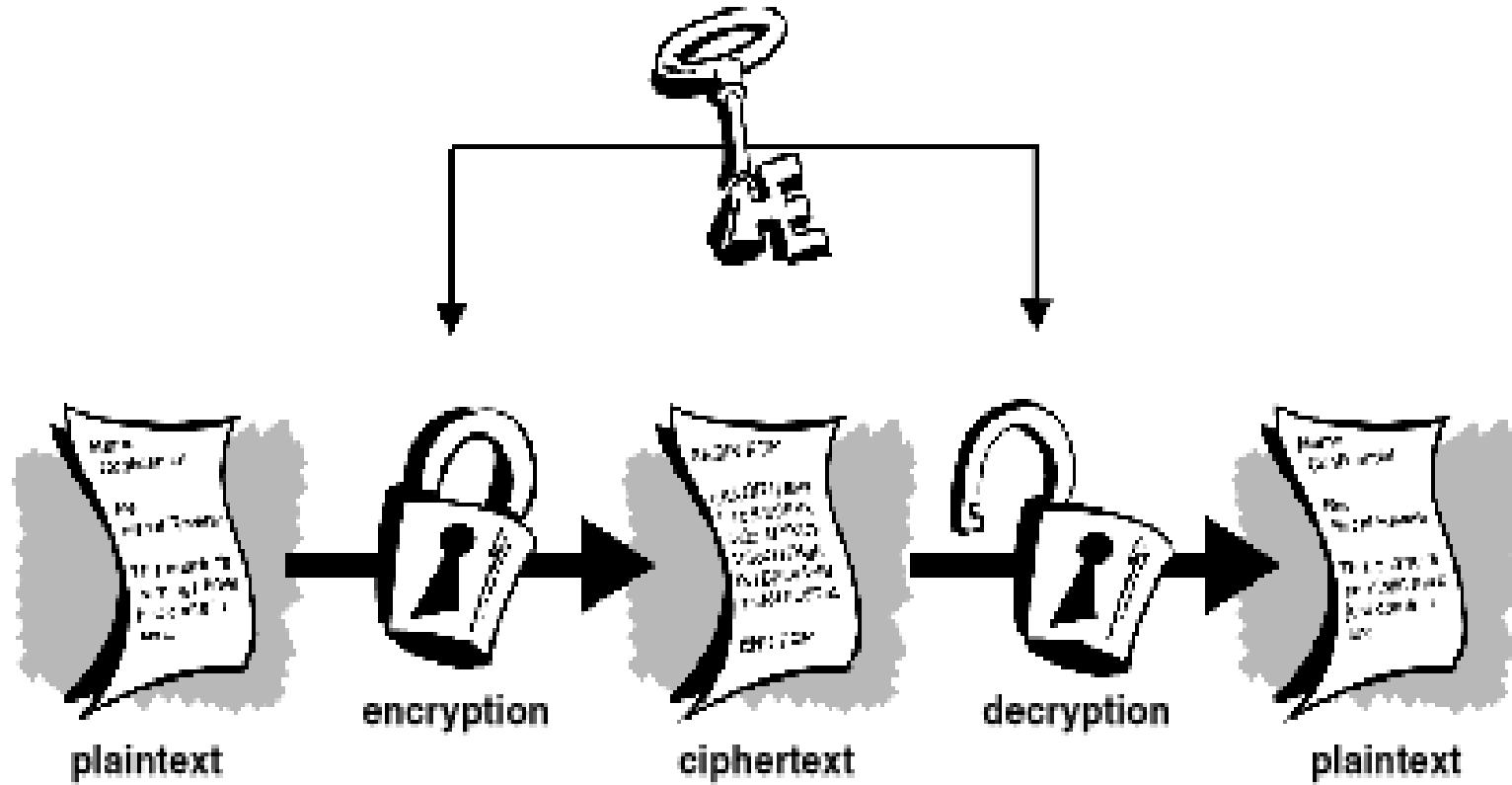
- ❖ Khóa/Chìa (Key) là một chuỗi được sử dụng trong giải thuật mã hóa và giải mã.
- ❖ Không gian khóa (Keyspace) là tổng số khóa có thể có của một hệ mã hóa.
 - Ví dụ nếu sử dụng khóa kích thước 64 bit → không gian khóa là 2^{64} .

4.1.1 Mã hóa thông tin – Các thuật ngữ

❖ Mã hóa khóa bí mật (Secret key cryptography):

- Một khóa được sử dụng cho cả giải thuật mã hóa và giải mã;
- Khóa này được gọi là khóa bí mật (secret key) hay khóa chia sẻ (shared key).

4.1.1 Mã hóa thông tin – Các thuật ngữ



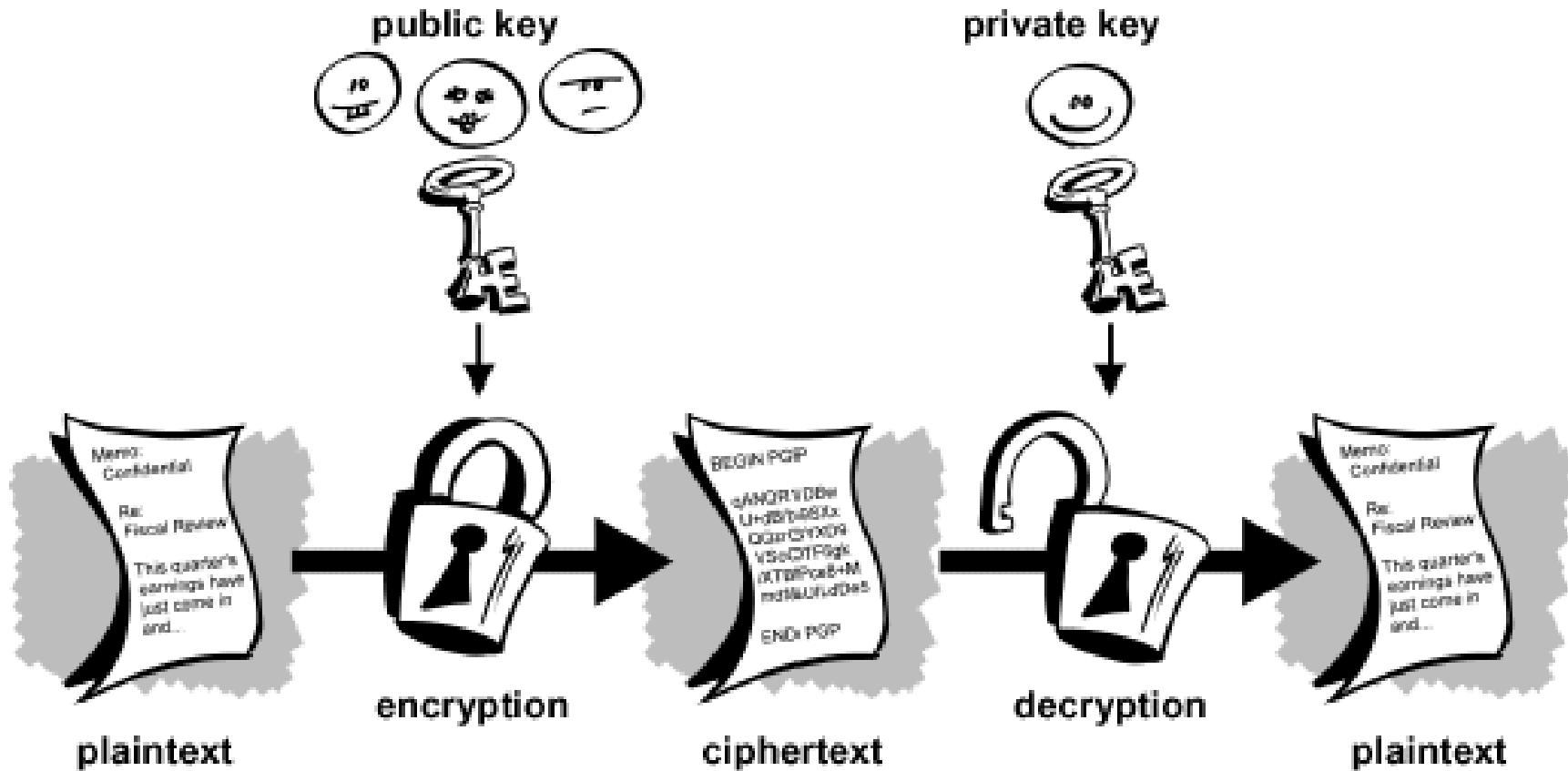
Mã hóa khóa bí mật

4.1.1 Mã hóa thông tin – Các thuật ngữ

❖ Mã hóa khóa công khai (Public key cryptography):

- Một cặp khóa được sử dụng, trong đó một khóa để mã hóa, một khóa để giải mã;
- Khóa để mã hóa được gọi là khóa công khai (public key);
- Khóa để giải mã được gọi là khóa riêng (private key).

4.1.1 Mã hóa thông tin – Các thuật ngữ



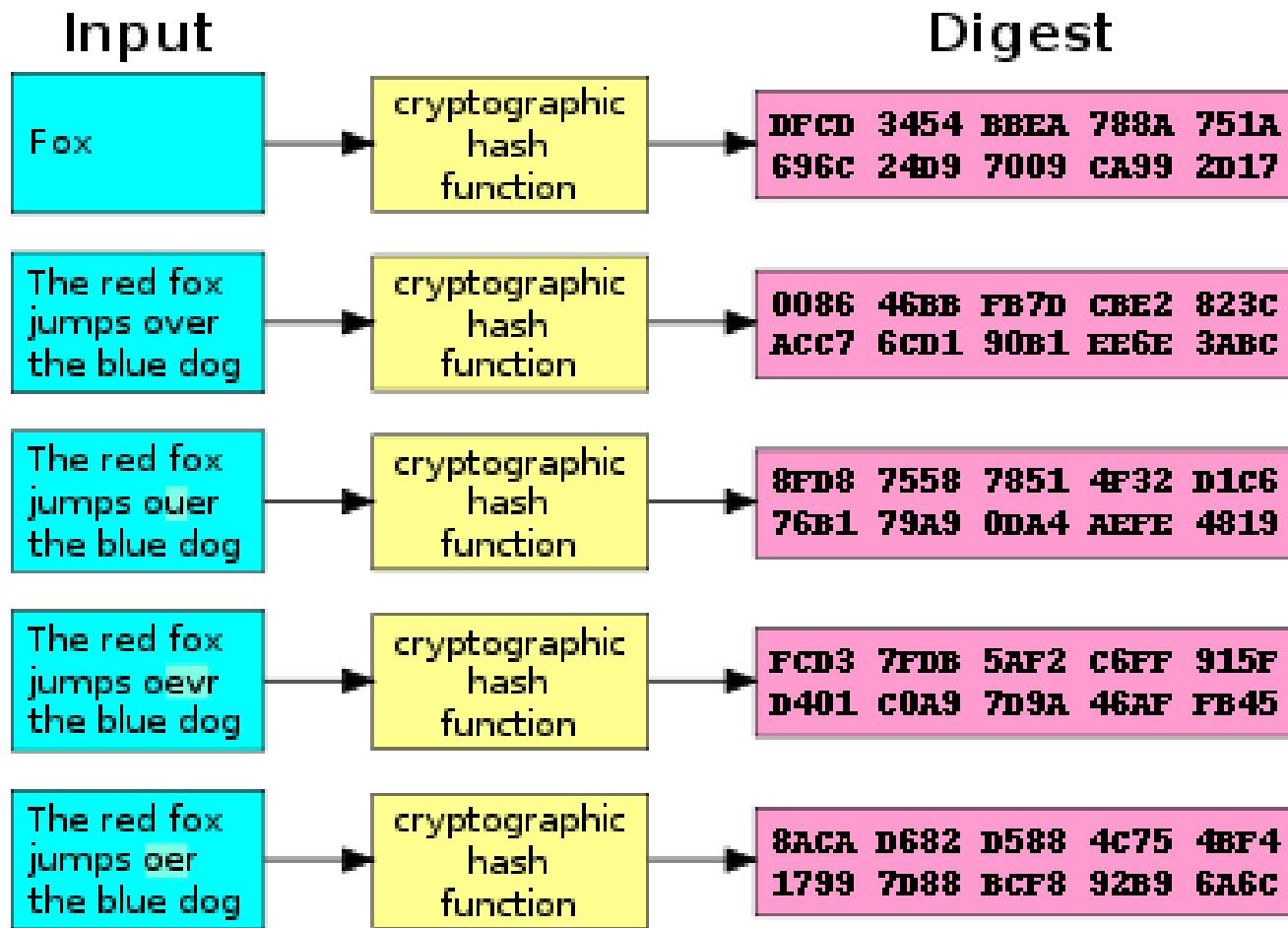
Mã hóa khóa công khai

4.1.1 Mã hóa thông tin – Các thuật ngữ

- ❖ **Hàm băm (Hash function)** là một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định.
 - Hàm băm 1 chiều (One-way hash function) là hàm băm trong đó việc thực hiện mã hóa tương đối đơn giản, còn việc giải mã thường có độ phức tạp rất lớn, hoặc không khả thi về mặt tính toán.

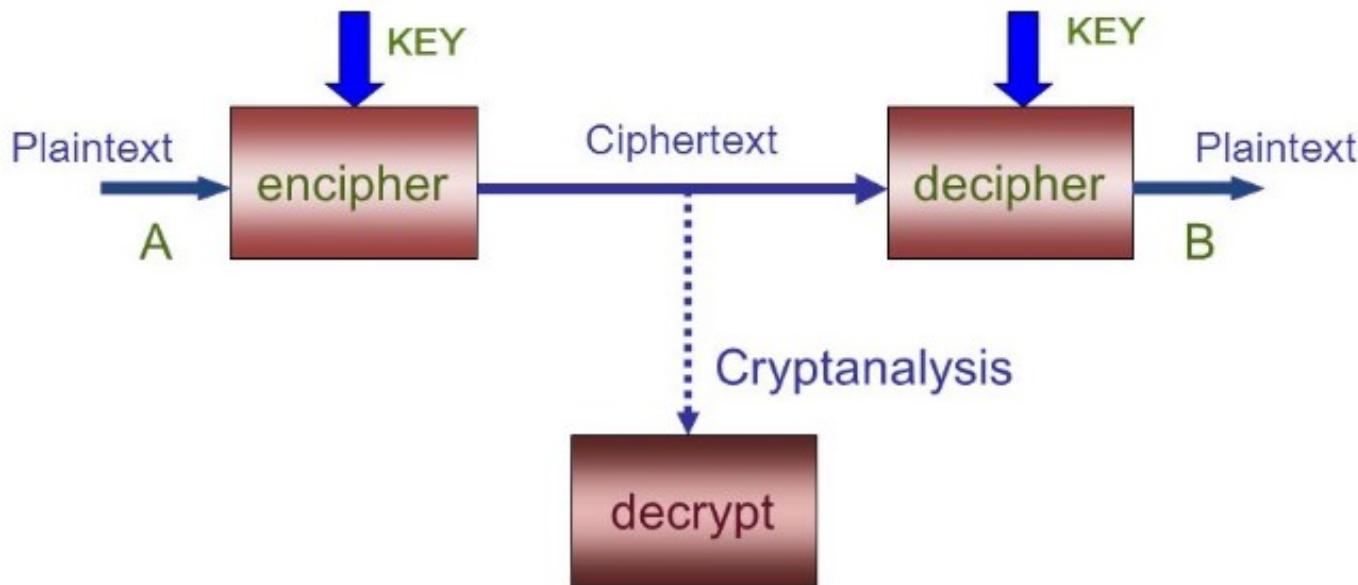
4.1.1 Mã hóa thông tin – Các thuật ngữ

Ví dụ
về
hàm
băm
(hash
function)



4.1.1 Mã hóa thông tin – Các thuật ngữ

- ❖ Phá mã/Thám mã (Cryptanalysis) là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước:
 - Thông tin về giải thuật mã hóa (Encryption algorithm) và
 - Thông tin về khóa mã (Key).



4.1.2 Vai trò của mã hóa trong ATTT

- ❖ Mã hóa thông tin có thể được sử dụng để đảm bảo an toàn thông tin trên đường truyền với các thuộc tính:
 - Bí mật (confidentiality): đảm bảo chỉ những người có thẩm quyền mới có khả năng truy nhập vào thông tin;
 - Toàn vẹn (integrity): đảm bảo dữ liệu không bị sửa đổi bởi các bên không có đủ thẩm quyền;
 - Xác thực (authentication): thông tin nhận dạng về các chủ thể tham gia phiên truyền thông có thể xác thực;
 - Không thể chối bỏ (non-repudiation): cho phép ngăn chặn một chủ thể chối bỏ hành vi hoặc phát ngôn đã thực hiện.

4.1.3 Các thành phần của một hệ mã hóa

- ❖ Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính:
 - Phương pháp mã hóa, còn gọi là “giải thuật” (Algorithm)
 - Một tập các khoá, còn gọi là không gian khoá (Keyspace)
- ❖ Nguyên lý Kerckhoff:
 - *“tính an toàn của một hệ mã hóa không nên thuộc vào việc giữ bí mật giải thuật mã hóa, mà chỉ nên thuộc vào việc giữ bí mật khoá mã”.*

4.1.4 Lịch sử mã hóa

- ❖ Các kỹ thuật mã hóa thô sơ đã được người cổ Ai cập sử dụng cách đây 4000 năm.
- ❖ Người cổ Hy lạp, Ấn độ cũng đã sử dụng mã hóa cách đây hàng ngàn năm.
- ❖ Các kỹ thuật mã hóa chỉ thực sự phát triển mạnh từ thế kỷ 1800 nhờ công cụ toán học, và phát triển vượt bậc trong thế kỷ 20 nhờ sự phát triển của máy tính và ngành CNTT.
- ❖ Trong chiến tranh thế giới thứ I và II, các kỹ thuật mã hóa được sử dụng rộng rãi trong liên lạc quân sự sử dụng sóng vô tuyến.
 - Sử dụng các công cụ phá mã/thám mã để giải mã các thông điệp của quân địch.

4.1.4 Lịch sử mã hóa

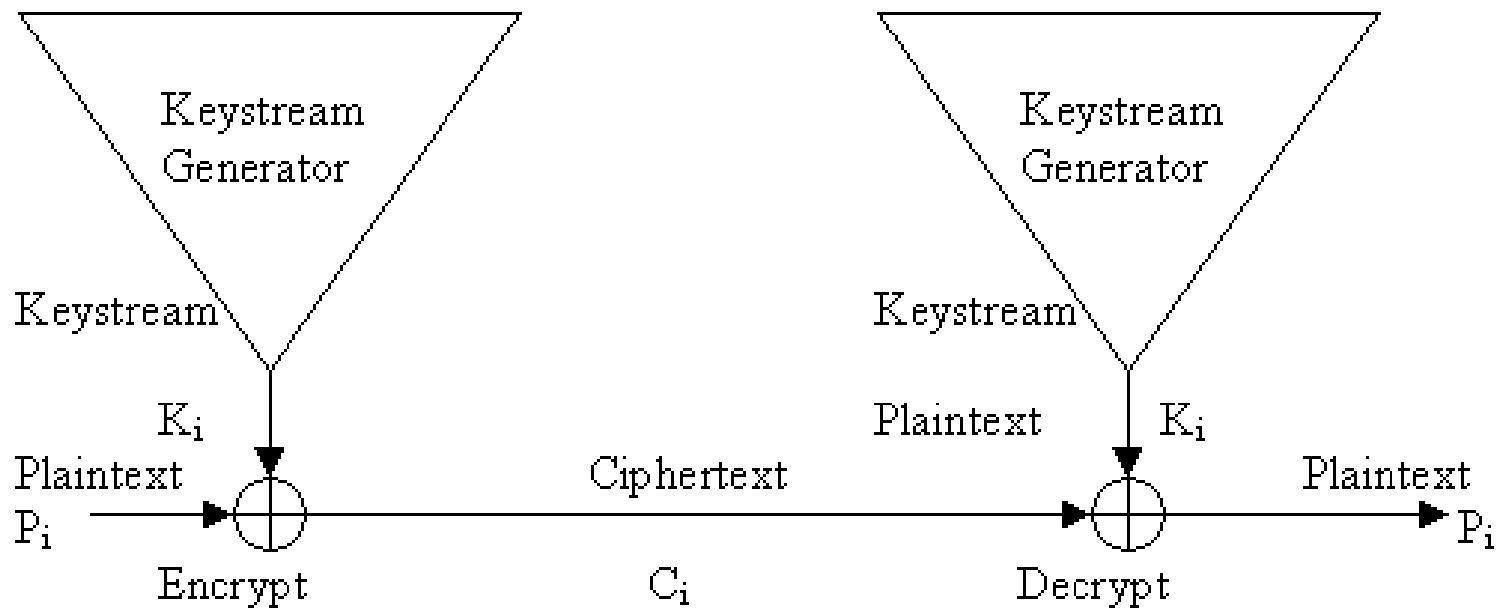
- ❖ Năm 1976 chuẩn mã hóa DES (Data Encryption Standard) được cơ quan an ninh quốc gia Mỹ (NSA – National Security Agency) thừa nhận và sử dụng rộng rãi.
- ❖ Năm 1976, hai nhà khoa học Whitman Diffie và Martin Hellman đã đưa ra khái niệm mã hóa bất đối xứng (Asymmetric key cryptography) hay mã hóa khóa công khai (Public key cryptography) đưa đến những thay đổi lớn trong kỹ thuật mật mã:
 - Các hệ mã hóa khóa công khai hỗ trợ trao đổi khóa dễ dàng hơn;
 - Các hệ mã hóa khóa bí mật gấp khó khăn trong quản lý và trao đổi khóa, đặc biệt khi số lượng người dùng lớn.

4.1.4 Lịch sử mã hóa

- ❖ Năm 1977, ba nhà khoa học Ronald Rivest, Adi Shamir, và Leonard Adleman giới thiệu giải thuật mã hóa khóa công khai RSA:
 - RSA trở thành giải thuật mã hóa khóa công khai được sử dụng rộng rãi nhất.
 - RSA có thể vừa được sử dụng để mã hóa thông tin và sử dụng trong chữ ký số.
- ❖ Năm 1991, phiên bản đầu tiên của chuẩn bảo mật PGP (Pretty Good Privacy) ra đời.
- ❖ Năm 2001, chuẩn mã hóa AES (Advanced Encryption Standard) được xây dựng và sử dụng rộng rãi.

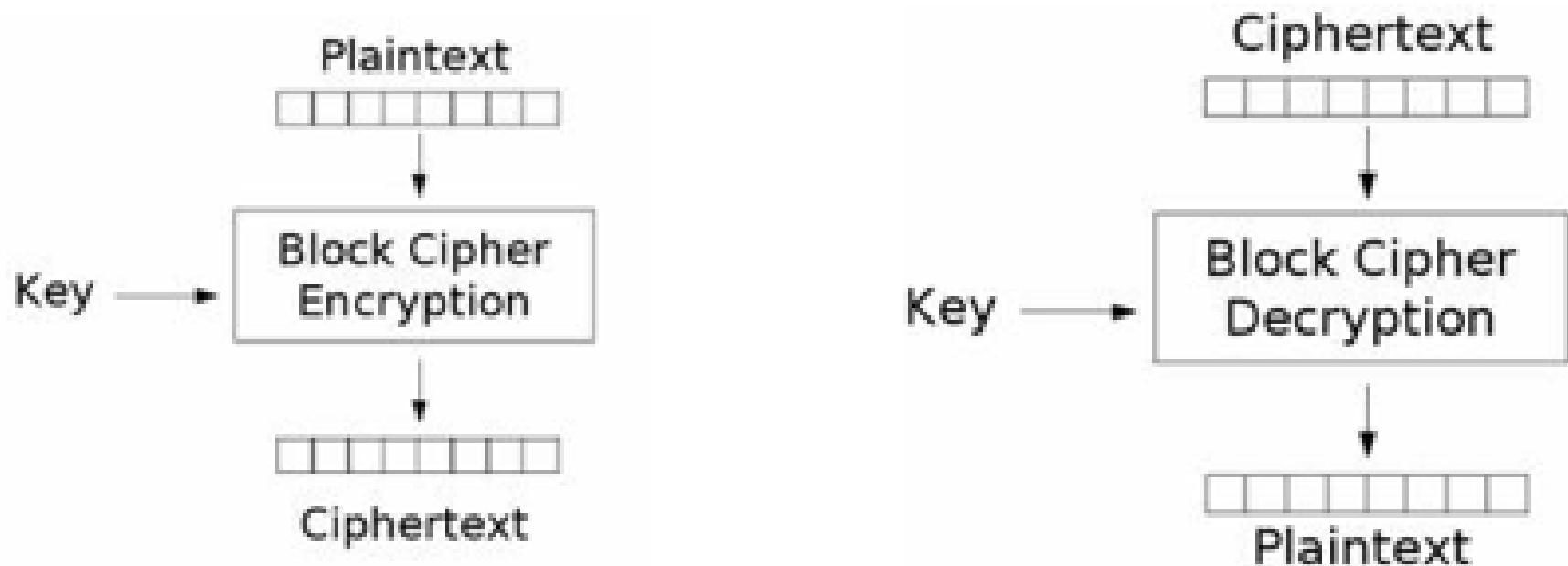
4.1.5 Mã hóa dòng và mã hóa khối

- ❖ Mã hóa dòng (Stream cipher) là kiểu mã hóa mà từng bít (hoặc ký tự) của dữ liệu được kết hợp với từng bít (hoặc ký tự) tương ứng của khóa để tạo thành bản mã.



4.1.5 Mã hóa dòng và mã hóa khối

- ❖ Mã hóa khối (Block cipher) là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa.



4.1.5 Mã hóa dòng và mã hóa khối

❖ Các chế độ hoạt động, hay cách chia khối (Modes of Operation) của mã hóa khối:

- Chế độ ECB (Electronic Codebook): cùng khối bản rõ đầu vào, khối bản mã giống nhau. Các khối mã hoàn toàn độc lập nhau ($c_j = E_k(x_j)$).
- Chế độ CBC (Cipher-Block Chaining): cùng khối bản rõ đầu vào, khối bản mã giống nhau với cùng khóa và véc tơ khởi tạo (IV). Khối mã c_j phụ thuộc vào khối rõ x_j và các khối rõ trước đó (x_1-x_{j-1}) thông qua khối mã c_{j-1} ($c_j = E_k(x_j \text{ XOR } c_{j-1})$, $c_0 = \text{IV}$).
- Chế độ CFB (Cipher Feedback): cùng khối bản rõ đầu vào, khối bản mã khác nhau. Khối mã c_j phụ thuộc vào khối rõ x_j và các khối rõ trước đó (x_1-x_{j-1}) thông qua khối mã c_{j-1} ($c_j = E_k(c_{j-1}) \text{ XOR } x_j$, $c_0 = \text{IV}$).
- Chế độ OFB (Output Feedback): cùng khối bản rõ đầu vào, khối bản mã khác nhau. Hệ thống sinh luồng khóa và XOR với các khối mã để tạo bản mã. Luồng khóa độc lập với bản rõ.

4.1.6 Các tiêu chuẩn đánh giá hệ mã hóa

- ❖ **Độ an toàn** (level of security): thường được đánh giá thông qua số lượng tính toán để có thể phá được hệ mã hóa.
- ❖ **Hiệu năng** (performance): có thể được đo bằng tốc độ mã hóa (bits/giây).
- ❖ **Tính năng** (functionality): hệ thống có thể được sử dụng cho nhiều mục đích bảo mật.
- ❖ **Chế độ hoạt động** (modes of operation): cung cấp các tính năng khác nhau theo chế độ hoạt động.
- ❖ **Độ dễ cài đặt** (ease of implementation): độ khó của việc cài đặt thuật toán trong thực tế trên phần cứng hoặc phần mềm.

4.1.7 Ứng dụng của mã hóa

❖ Các kỹ thuật mã hóa được ứng dụng rộng rãi trong các hệ thống/công cụ/dịch vụ bảo mật:

- Dịch vụ xác thực (Kerberos, RADIUS,...)
- Điều khiển truy nhập
- Các công cụ đánh giá và phân tích logs
- Các sản phẩm quản lý ATTT
- Các công cụ cho đảm bảo an toàn cho truyền thông không dây
- Các nền tảng bảo mật như PKI, PGP
- Các giao thức bảo mật như SSL/TLS, SSH, SET, IPSec
- Các hệ thống như VPN.

4.2 Các phương pháp mã hóa

1. Phương pháp thay thế
2. Phương pháp hoán vị
3. Phương pháp XOR
4. Phương pháp Vernam
5. Phương pháp sách hoặc khóa chạy
6. Phương pháp hàm băm

4.2.1 Phương pháp thay thế

❖ Là phương pháp thay thế một giá trị này bằng một giá trị khác:

- Thay một ký tự bằng một ký tự khác;
- Thay một bít bằng một bít khác.
- Caesar cipher: dịch 3 chữ sang bên phải (A→D, B→E,...)

Bộ chữ gốc

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Bộ chữ mã

DEFGHIJKLMNOPQRSTUVWXYZABC

LOVE → ORYH

4.2.1 Phương pháp thay thế

❖ Số bộ chữ mã có thể là 1 hoặc nhiều:

- Một 1 gốc → 1 chữ mã: dễ đoán theo sự lặp lại
- Một 1 gốc → 1 trong n chữ mã: khó đoán do phức tạp hơn

Plaintext =

ABCDEFGHIJKLMNPQRSTUVWXYZ

Substitution cipher 1 =

DEFGHIJKLMNOPQRSTUVWXYZABC

Substitution cipher 2 =

GHIJKLMNOPQRSTUVWXYZABCDE

Substitution cipher 3 =

JKLMNOPQRSTUVWXYZABCDEFGHI

Substitution cipher 4 =

MNOPQRSTUVWXYZABCDEFGHIJKL

Ký tự số 1 dùng bộ mã 1, ký tự 2 dùng bộ mã 2,...

TEXT → WKGF

4.2.2 Phương pháp đổi chỗ

- ❖ Phương pháp đổi chỗ hoặc hoán vị (permutation) thực hiện sắp xếp lại các giá trị trong một khối để tạo bản mã:
 - Có thể thực hiện với từng bit hoặc từng byte (ký tự).

Khóa đổi chỗ (khối 8 phần tử) tính từ bên phải

Key $1 \rightarrow 4, 2 \rightarrow 8, 3 \rightarrow 1, 4 \rightarrow 5, 5 \rightarrow 7, 6 \rightarrow 2, 7 \rightarrow 6, 8 \rightarrow 3$

Bit locations: 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1

Plaintext 8-bit blocks: 0 0 1 0 0 1 0 1 | 0 1 1 0 1 0 1 1 | 1 0 0 1 0 1 0 1 | 0 1 0 1 0 1 0 0

Ciphertext: 0 0 0 0 1 0 1 1 | 1 0 1 1 1 0 1 0 | 0 1 0 0 1 1 0 1 | 0 1 1 0 0 0 0 1

4.2.2 Phương pháp đổi chỗ

- Thực hiện đổi chỗ ký tự trong khối 8 ký tự, tính từ bên phải:

Letter locations: 8 7 6 5 4 3 2 1 | 8 7 6 5 4 3 2 1 | 8 7 6 5 4 3 2 1 | 8 7 6 5 4 3 2 1 |

Plaintext: SACKGAUL | SPARENNO | NE | |

Key: 1→4, 2→8, 3→1, 4→5, 5→7, 6→2, 7→6, 8→3

Ciphertext: UKAGLSCA | ORPEOSAN | E N |

4.2.2 Phương pháp XOR

- ❖ Phương pháp XOR sử dụng phép toán logic XOR để tạo bản mã:
 - Từng bít của bản rõ được XOR với bít tương ứng của khóa.

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Bảng giá trị chân thực của XOR

4.2.3 Phương pháp XOR

- Ví dụ: mã hóa từ CAT (biểu diễn theo mã ASCII là 01000011 01000001 01010100) sử dụng khóa là "V" (01010110)

Text Value	Binary Value
CAT as bits	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 0
VVV as key	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Cipher	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0

4.2.4 Phương pháp Vernam

- ❖ Phương pháp Vernam sử dụng một tập ký tự để nối vào các ký tự của bản rõ để tạo bản mã.
 - Mỗi ký tự trong tập chỉ dùng 1 lần trong một tiến trình mã hóa (được gọi là one-time pad).
- ❖ Ví dụ: với bộ chữ tiếng Anh có 26 chữ
 - Các ký tự của bản rõ được chuyển thành số trong khoảng 1-26;
 - Cộng giá trị của ký tự với giá trị tương ứng trong tập nối thêm;
 - Nếu giá trị cộng lớn hơn 26 → đem trừ cho 26.
 - Đây là phép lấy modulo (phần dư).

4.2.4 Phương pháp Vernam

Plaintext:

S A C K G A U L S P A R E N O O N E
19 01 03 11 07 01 21 12 19 16 01 18 05 14 15 15 14 05

Plaintext value:

One-time pad text:

F P Q R N S B I E H T Z L A C D G J

One time pad value:

06 16 17 18 14 19 02 09 05 08 20 26 12 01 03 04 07 10

Sum of plaintext and pad: 25 17 20 29 21 20 23 21 24 24 21 44 17 15 18 19 21 15

After modulo Subtraction:

03 18

Ciphertext:

Y Q T C U T W U X X U R Q O R S U O

Tiến trình mã hóa sử dụng phương pháp Vernam

4.2.5 Phương pháp sách hoặc khóa chạy

- ❖ Phương pháp sách hoặc khóa chạy thường được dùng trong các bộ phim trinh thám, trong đó việc mã hóa và giải mã sử dụng các khóa mã chứa trong các cuốn sách.
- ❖ Ví dụ: với bản mã là 259,19,8;22,3,8;375,7,4;394,17,2 và cuốn sách được dùng là "A Fire Up on the Deep":
 - Trang 259, dòng 19, từ thứ 8 → sack
 - Trang 22, dòng 3, từ thứ 8 → island
 - Trang 375, dòng 7, từ thứ 4 → sharp
 - Trang 394, dòng 17, từ thứ 2 → path
 - Bản rõ tương ứng của bản mã "259,19,8;22,3,8;375,7,4;394,17,2 " là "sack island sharp path".

4.2.6 Phương pháp hàm băm

- ❖ Các hàm băm (Hash functions) là các thuật toán để tạo các bản tóm tắt của thông điệp được sử dụng để nhận dạng và đảm bảo tính toàn vẹn của thông điệp.
 - Các hàm băm là các hàm công khai được dùng để tạo các giá trị băm hay thông điệp rút gọn (message digest);
 - Chiều dài của thông điệp là bất kỳ, nhưng đầu ra có chiều dài cố định.

4.2.6 Phương pháp hàm băm

❖ Một số hàm băm thông dụng:

- MD2, MD4, MD5 (128 bit)
- MD6 (0-512 bit)
- SHA0, SHA1 (160 bit)
- SHA2 (SHA256, SHA384, SHA512), SHA3
- CRC32 (32 bit)

4.3 Các giải thuật mã hóa

1. Các giải thuật mã hóa khóa đối xứng

- DES, Triple-DES
- AES, IDEA
- Blowfish, Twofish
- RC4, RC5

2. Các giải thuật mã hóa khóa bất đối xứng

- RSA
- Rabin
- ElGamal

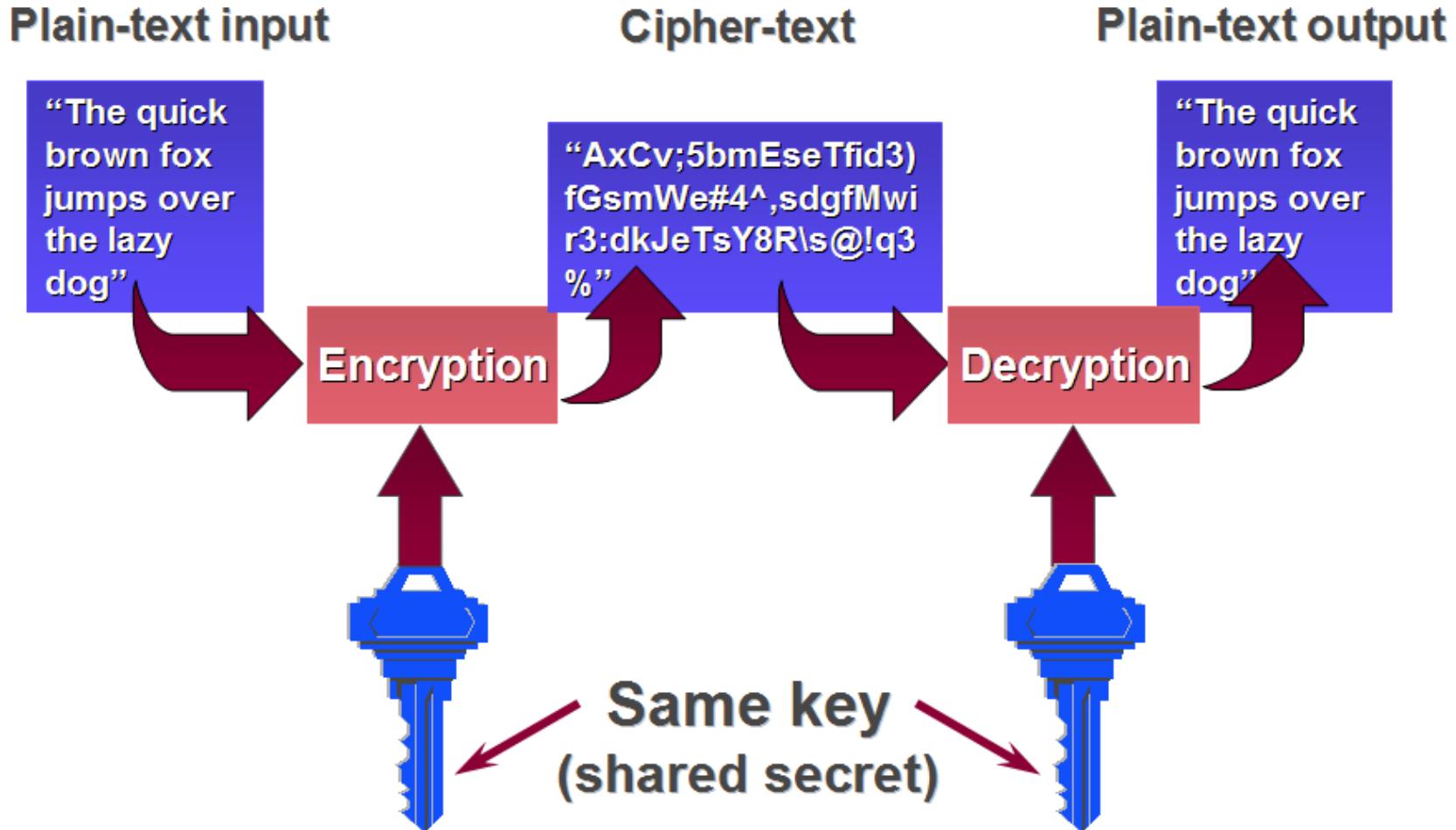
3. Các hàm băm

- MD2, MD4, MD5, MD6
- SHA0, SHA1, SHA2, SHA3

4.3.1 Các giải thuật mã hóa khóa đối xứng

- ❖ Các giải thuật mã hóa khóa đối xứng (symetric key encryption)
 - Còn gọi là mã hóa khóa riêng hay bí mật (secret/private key encryption):
 - Sử dụng một khóa (key) duy nhất cho cả quá trình mã hóa và giải mã.
- ❖ Đặc điểm:
 - Kích thước khóa tương đối ngắn (64, 128, 192, 256 bít)
 - Tốc độ nhanh
 - Độ an toàn cao
 - Khó khăn trong quản lý và phân phối khóa.

4.3.1 Các giải thuật mã hóa khóa đối xứng



4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

- ❖ DES (Data Encryption Standard) được sử dụng phổ biến:
 - DES được phát triển tại IBM vào đầu những năm 1970;
 - Được thừa nhận là chuẩn mã hóa tại Mỹ (NSA) vào năm 1976;
 - DES được sử dụng rộng rãi trong những năm 70 và 80.
- ❖ Hiện nay DES không được coi là an toàn do:
 - Không gian khóa nhỏ (khóa 64 bit, trong đó thực sự sử dụng 56 bit)
 - Tốc độ tính toán của các hệ thống máy tính ngày càng nhanh.

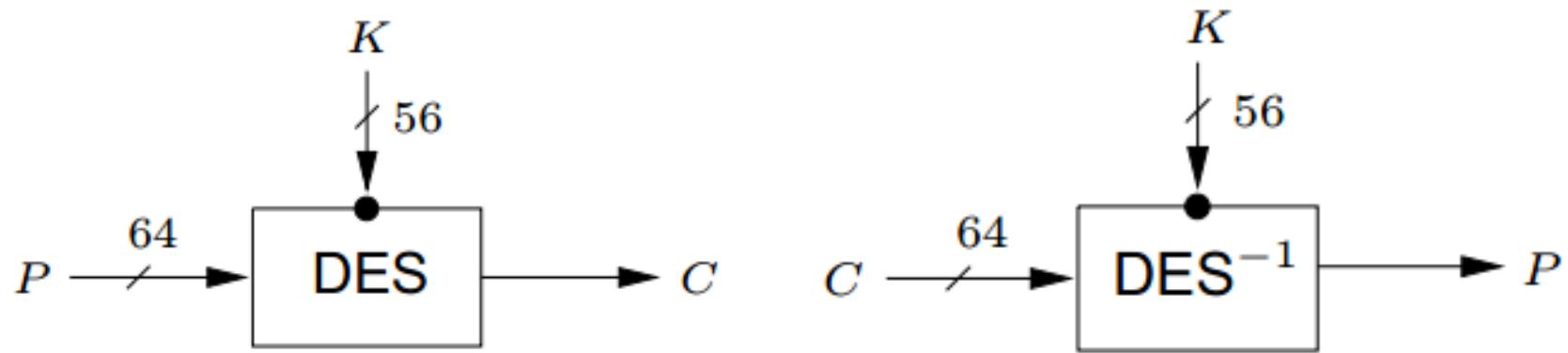
4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

❖ Đặc điểm của DES:

- Là dạng mã hóa khối, kích thước khối vào 64 bit
- Khóa 64 bit, trong đó thực sử dụng 56 bit, 8 bit dùng cho kiểm tra chẵn lẻ
- DES sử dụng chung một giải thuật cho cả hai khâu mã hóa và giải mã.

4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

- ❖ Mã hóa và giải mã một khối dữ liệu với DES



plaintext P

ciphertext C

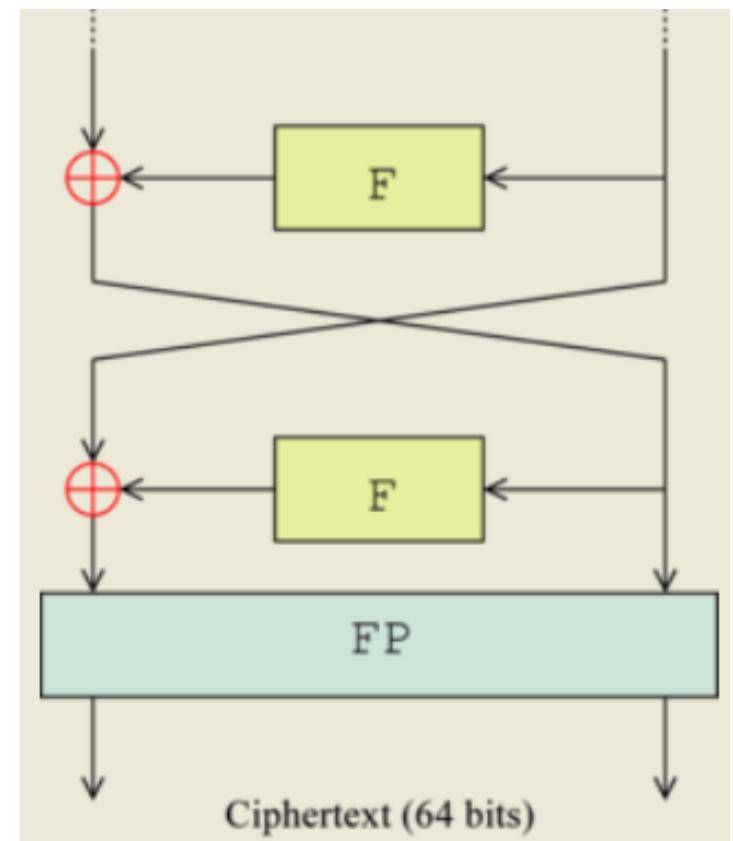
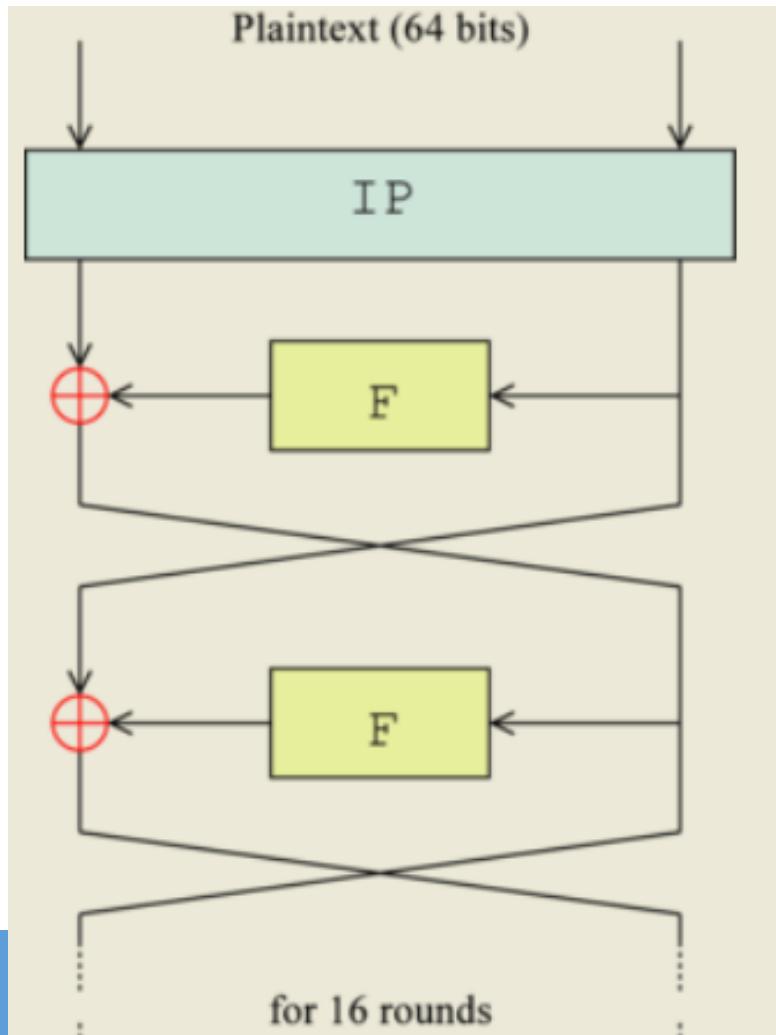
key K

4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

- ❖ Các bước thực hiện mã hóa của DES với mỗi khối dữ liệu 64 bit:
 - Bước hoán vị khởi tạo (IP – Initial Permutation);
 - 16 vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F);
 - Bước hoán vị kết thúc (FP – Final Permutation).
- ❖ Sử dụng phép \oplus (XOR) để kết hợp trong quá trình lặp.

4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

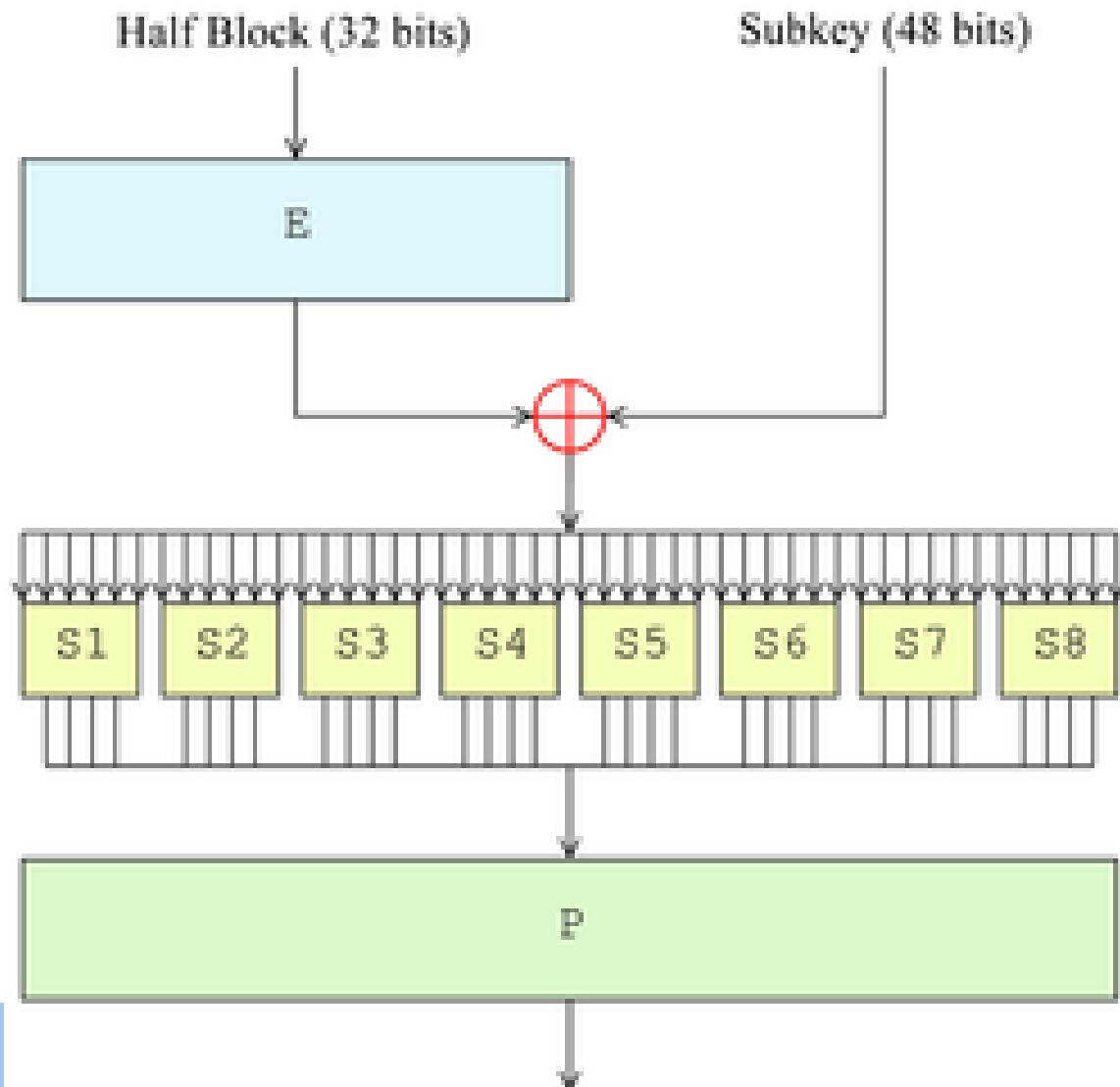
- ❖ Tiến trình mã hóa một khối dữ liệu với DES



4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

Các bước thực hiện hàm F (Fiestel) của DES:

- E (Expansion) – mở rộng
- \oplus : trộn với một phần khóa
- S_i (Substitution) - thay thế
- P – Hoán vị.



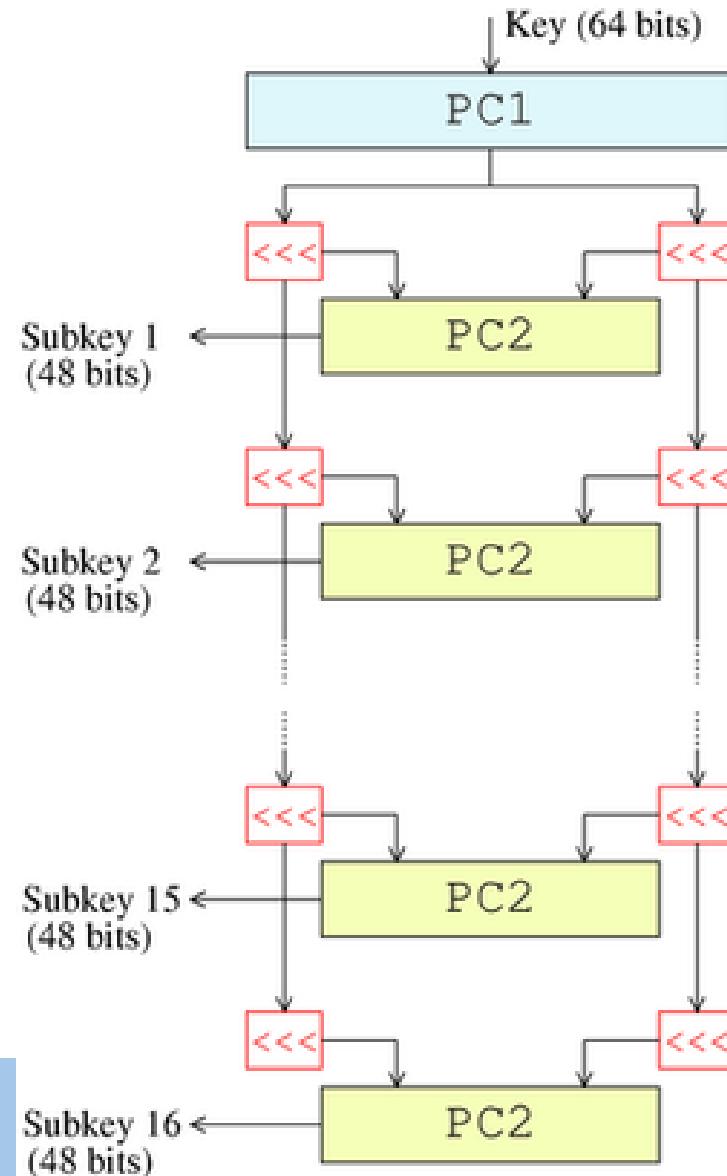
4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

- ❖ Chia khối 64 bit thành 2 khối 32 bit và xử lý lần lượt.
- ❖ Các bước thực hiện hàm F (Fiestel) với khối dữ liệu 32 bit của DES:
 - E (Expansion): thực hiện mở rộng 32 bit đầu vào thành 48 bit bằng cách nhân đôi một nửa số bit.
 - \oplus : Trộn 48 bit ở bước E với khóa phụ 48 bit. Có 16 khóa phụ được tạo từ khóa chính để sử dụng cho 16 vòng lặp.
 - S_i (Substitution): Khối dữ liệu 48 bit được chia thành 8 khối 6 bit và được chuyển cho các bộ thay thế (S_1-S_8).
 - Mỗi bộ thay thế sử dụng phép chuyển đổi phi tuyến tính để chuyển 6 bit đầu vào thành 4 bit đầu ra theo bảng tham chiếu. Các bộ thay thế là thành phần nhân an ninh (security core) của DES.
 - P: 32 bit đầu ra từ các bộ thay thế được sắp xếp bằng phép hoán vị cố định (fixed permutation) cho ra đầu ra 32 bit.

4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

❖ Tạo bộ khóa phụ cho 16 vòng lặp:

- 56 bít khóa được chọn từ khóa 64 bit ban đầu bởi PC1 (Permuted Choice 1). 8 bit còn lại được hủy hoặc dùng để kiểm tra chẵn lẻ;
- 56 bít được chia thành 2 phần 28 bit, mỗi phần được xử lý riêng;
- Mỗi phần được quay trái 1 hoặc 2 bit.
- Hai phần được ghép lại và 48 bit được chọn làm khóa phụ 1 bởi PC2;
- Lặp lại bước trên để tạo 15 khóa phụ còn lại.



4.3.1 Các giải thuật mã hóa khóa đối xứng - DES

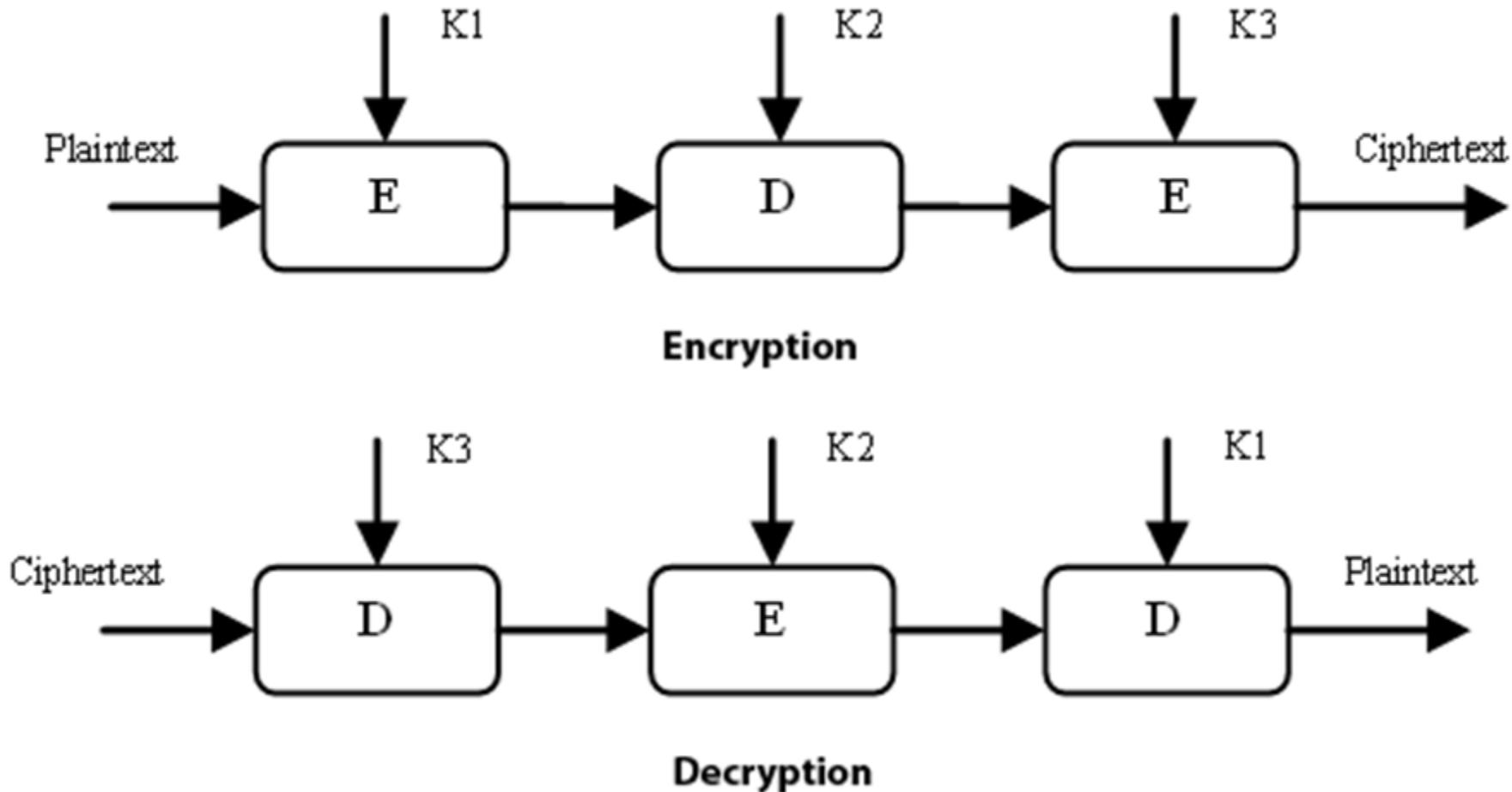
❖ Giải mã trong DES:

- Có thể sử dụng giải thuật mã hóa DES để giải mã;
- Các bước thực hiện giống quá trình mã hóa;
- Các khóa phụ sử dụng cho các vòng lặp được sử dụng theo trật tự ngược lại: Khóa phụ 16, 15,..., 2, 1 cho các vòng 1, 2,..., 15, 16 tương ứng.

4.3.1 Các giải thuật mã hóa khóa đối xứng – Triple DES

- ❖ Triple DES (3-DES) còn được gọi là Triple Data Encryption Algorithm (TDEA hoặc Triple DEA) được phát triển từ DES bằng cách áp dụng DES 3 lần cho mỗi khối dữ liệu;
- ❖ Triple DES sử dụng bộ 3 khóa DES: K1, K2, K3, mỗi khóa kích thước hiệu dụng 56 bit;
- ❖ Các lựa chọn bộ khóa:
 - Lựa chọn 1: cả 3 khóa độc lập (168 bit)
 - Lựa chọn 2: K1 và K2 độc lập, K3 = K1 (112 bit)
 - Lựa chọn 3: 3 khóa giống nhau, K1 = K2 = K3 (56 bit).
- ❖ Kích thước khối dữ liệu vào: 64 bit.

4.3.1 Các giải thuật mã hóa khóa đối xứng – Triple DES



4.3.1 Các giải thuật mã hóa khóa đối xứng – Triple DES

❖ Giải thuật mã hóa:

- ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$
→ Mã hóa bằng khóa K1, giải mã bằng K2 và mã hóa bằng K3.

❖ Giải thuật giải mã:

- plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$
→ Giải mã bằng K3, mã hóa bằng K2 và giải mã bằng K1.

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

- ❖ AES (Advanced Encryption Standard) là một chuẩn mã hóa dữ liệu được NIST công nhận năm 2001;
- ❖ AES được xây dựng dựa trên Rijndael cipher phát triển bởi 2 nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen;
 - Rijndael cipher là bộ mã hóa được lựa chọn để xây dựng AES sau khi giành chiến thắng trong cuộc thi tuyển chọn bộ mã hóa làm chuẩn mã hóa mới thay cho DES.
 - AES về cơ bản giống Rijndael cipher.

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Đặc điểm của AES:

- Kích thước khối dữ liệu của AES là 128 bít;
- Kích thước khóa có thể là 128, 192, hoặc 256 bit;
- AES được thiết kế dựa trên mạng hoán vị-thay thế (substitution-permutation network);
 - Có thể đạt tốc độ cao trên cả cài đặt phần mềm và phần cứng.

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

- ❖ AES vận hành dựa trên một ma trận 4×4 , được gọi là *state* (trạng thái);
- ❖ Kích thước của khóa quyết định số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã:
 - 10 vòng lặp với khóa 128 bit;
 - 12 vòng lặp với khóa 192 bit;
 - 14 vòng lặp với khóa 256 bit.

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Mô tả khái quát giải thuật AES:

1. Mở rộng khóa (KeyExpansion): các khóa phụ dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.
2. Vòng khởi tạo (InitialRound)
 - a) AddRoundKey: Mỗi byte trong state được kết hợp với khóa phụ sử dụng XOR.

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Mô tả khái quát giải thuật AES:

3. Các vòng lặp chính (Rounds)

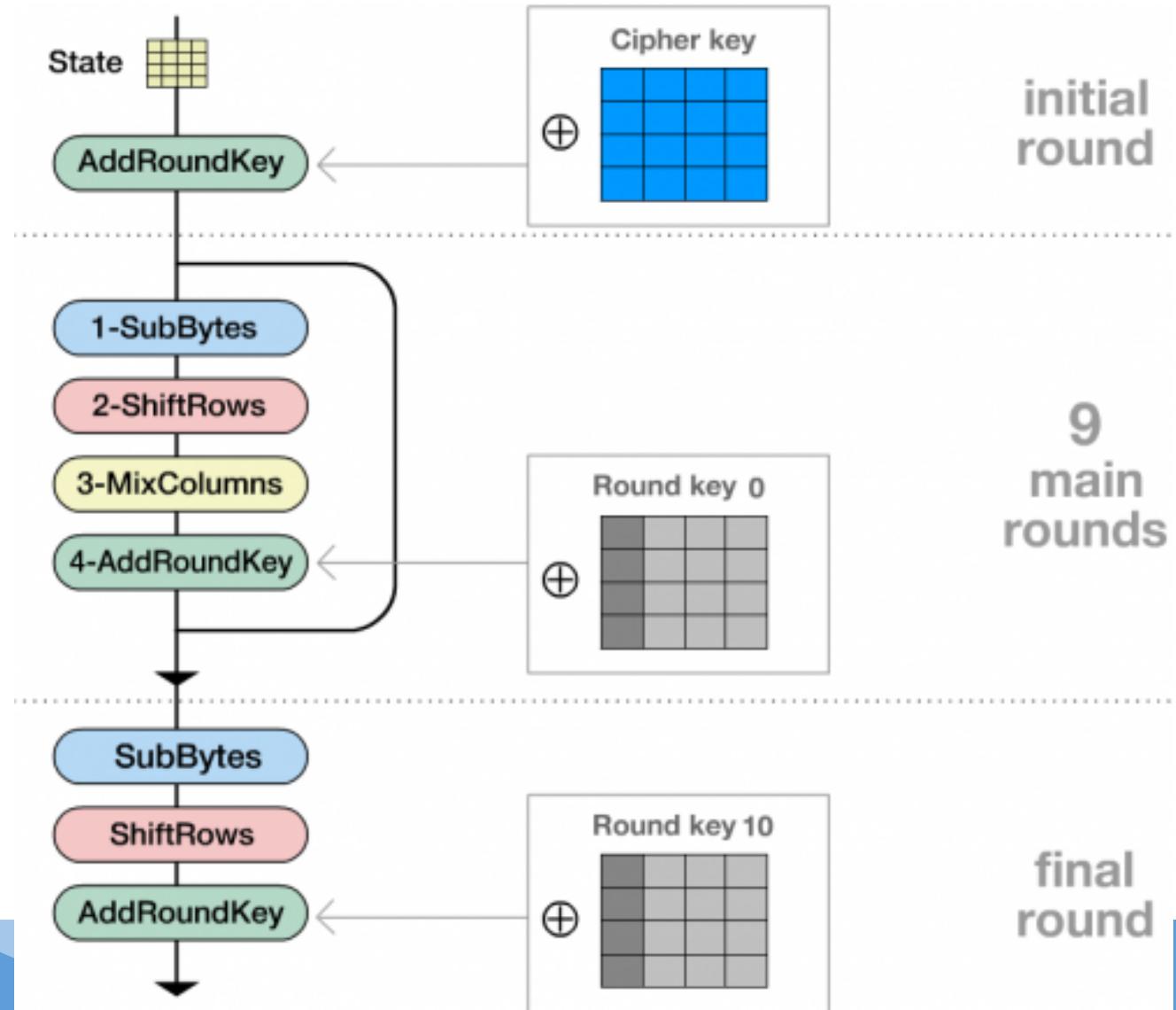
- a) SubBytes: bước thay thế phi tuyến tính, trong đó mỗi byte trong *state* được thay thế bằng một byte khác sử dụng bảng tham chiếu;
- b) ShiftRows: bước đổi chỗ, trong đó mỗi dòng trong *state* được dịch một số bước theo chu kỳ;
- c) MixColumns: trộn các cột trong *state*, kết hợp 4 bytes trong mỗi cột.
- d) AddRoundKey.

4. Vòng cuối (Final Round - không MixColumns)

- a) SubBytes;
- b) ShiftRows;
- c) AddRoundKey.

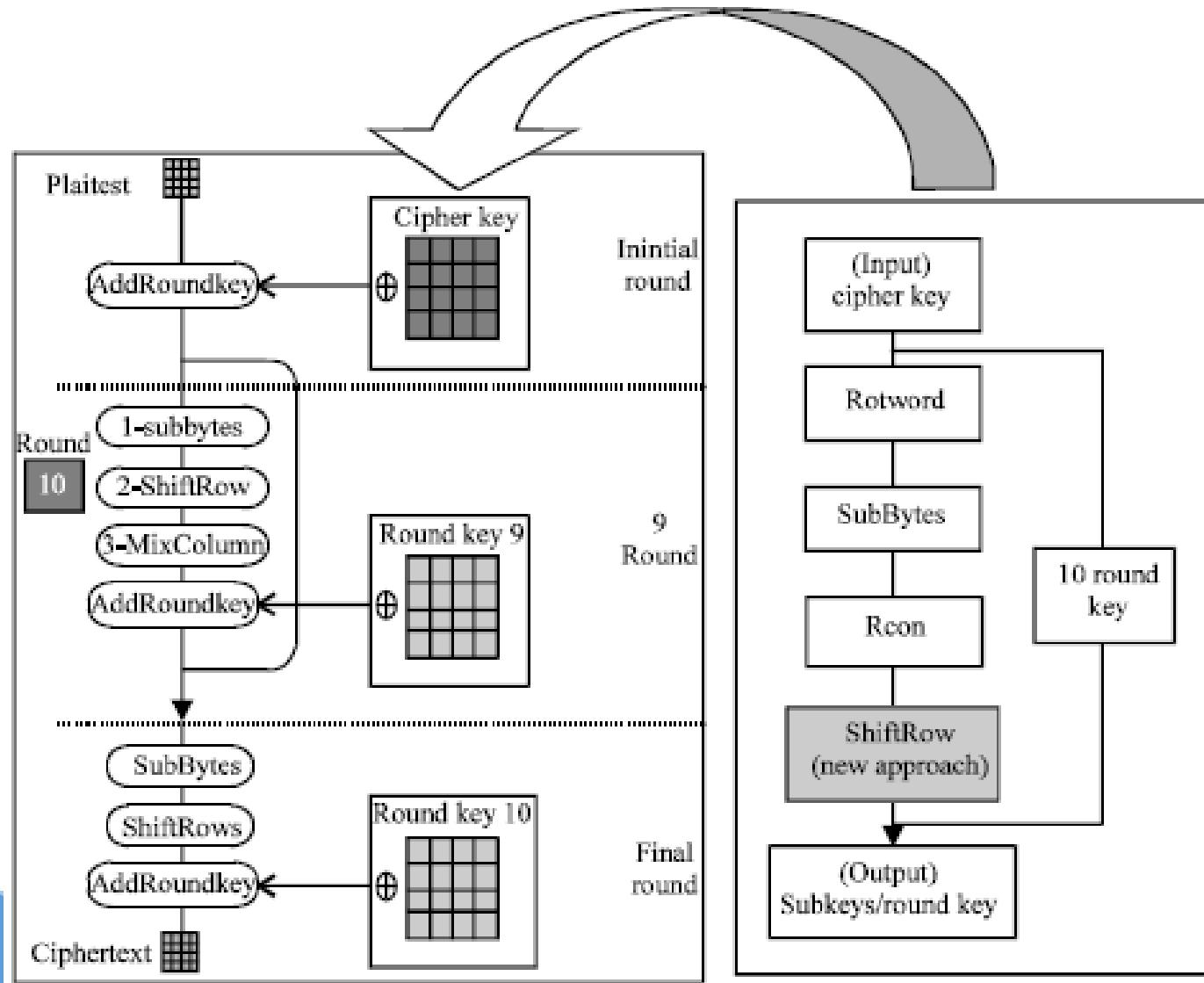
4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

Các bước xử lý chính của AES



4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

Các bước xử lý chính của AES



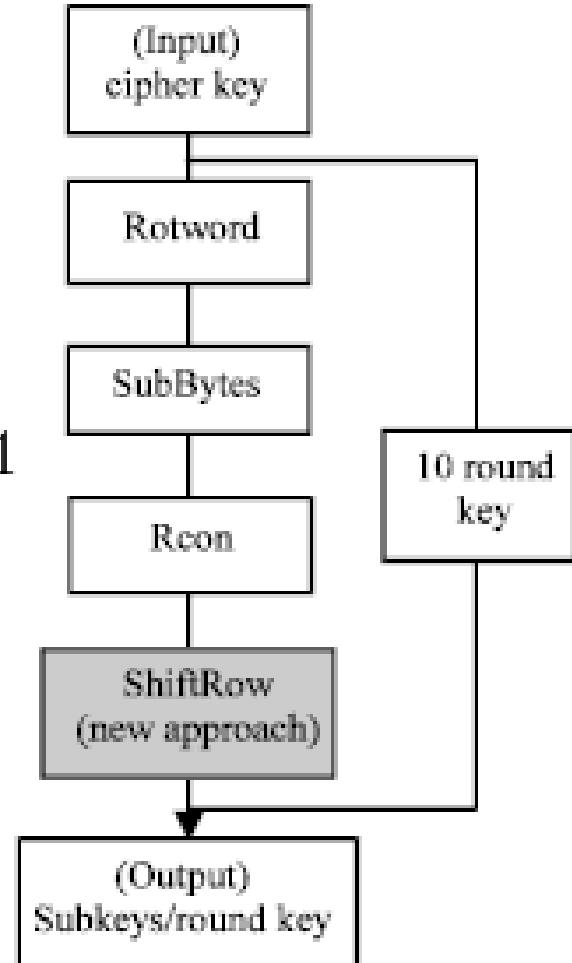
4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Mở rộng khóa sử dụng thủ tục sinh khóa Rijndael:

- Rotword: quay trái 8 bit;
- SubBytes
- Rcon: tính toán giá trị Rcon(i)

$$\text{rcon}(i) = x^{(i-1)} \mod x^8 + x^4 + x^3 + x + 1$$

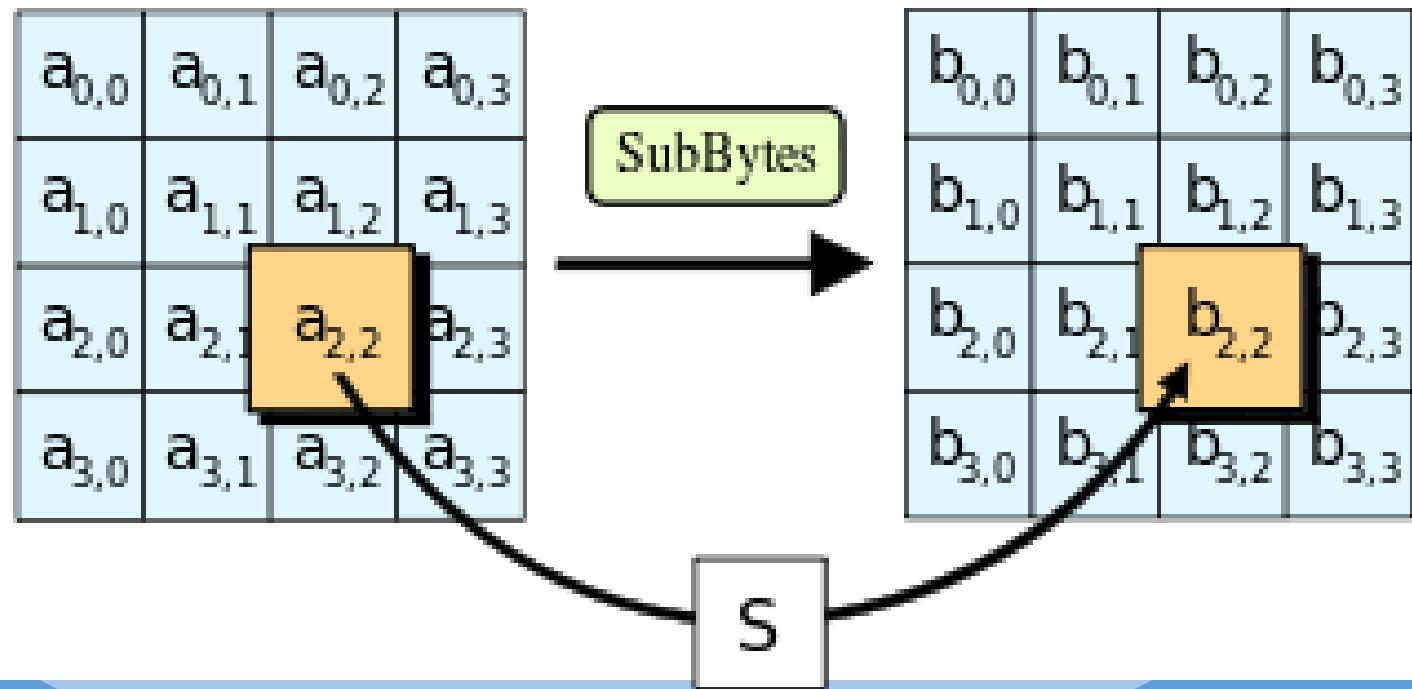
- ShiftRow



4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Bước SubBytes:

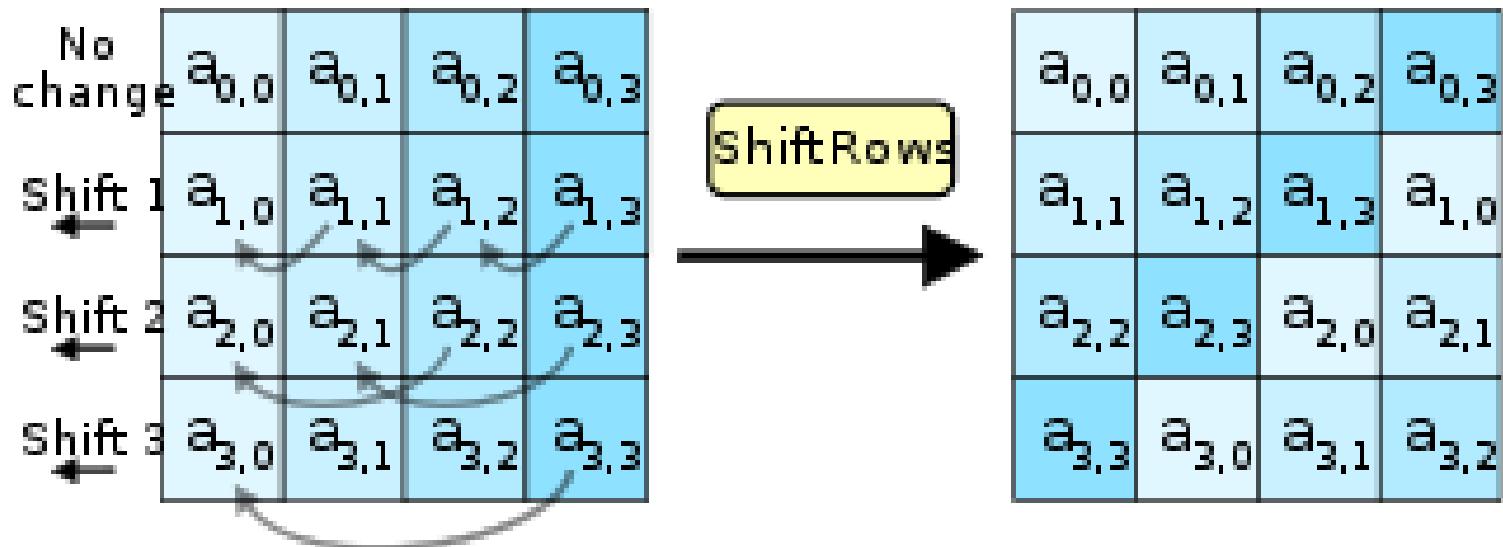
- Mỗi byte trong ma trận state được thay thế bởi 1 byte trong Rijndael S-box, hay $b_{ij} = S(a_{ij})$



4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Bước ShiftRows:

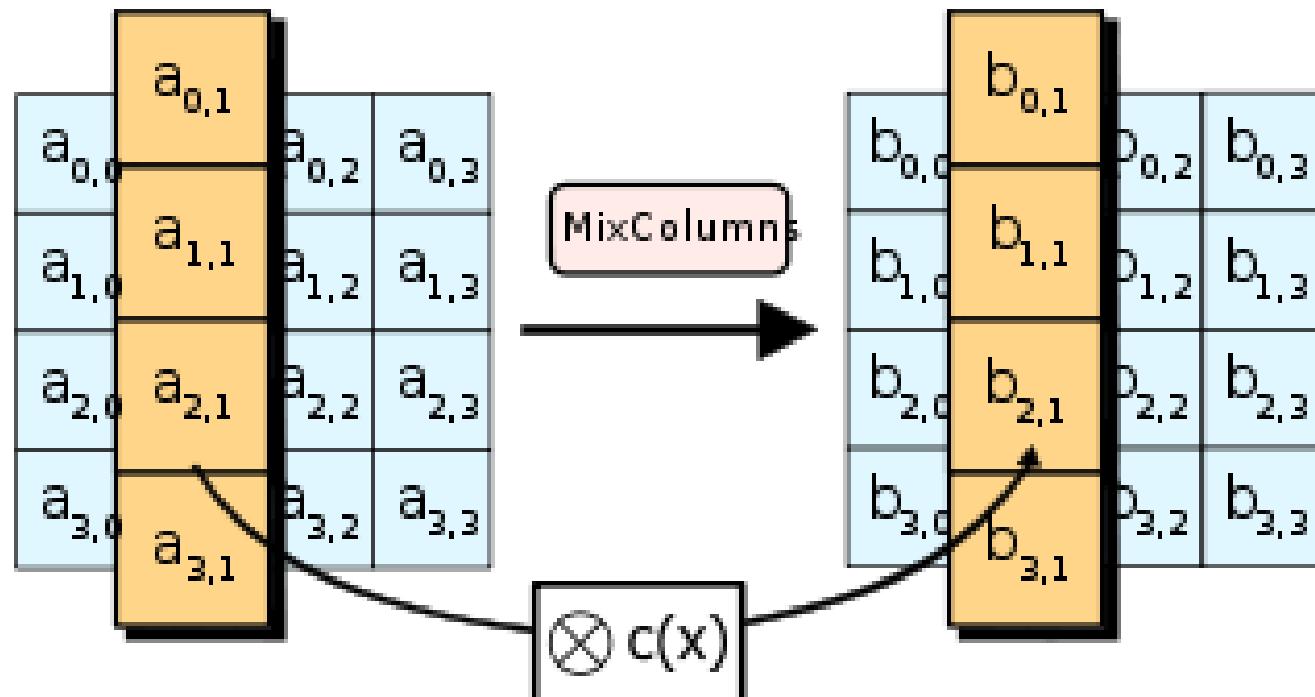
- Các dòng của ma trận state được dịch theo chu kỳ sang trái;
- Dòng thứ nhất giữ nguyên.



4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

❖ Bước MixColumns:

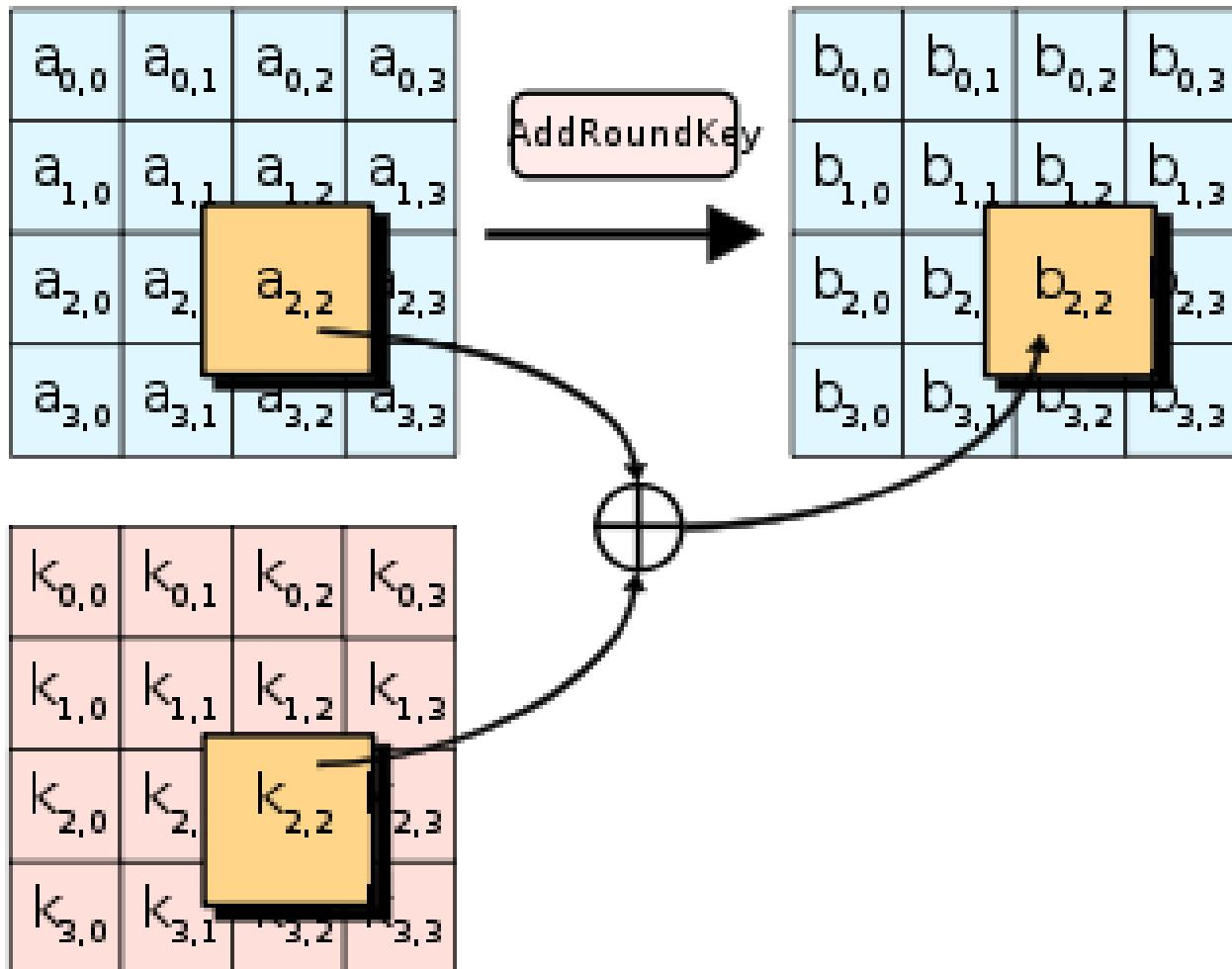
- Mỗi cột của ma trận state được nhân với một đa thức $c(x)$



4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

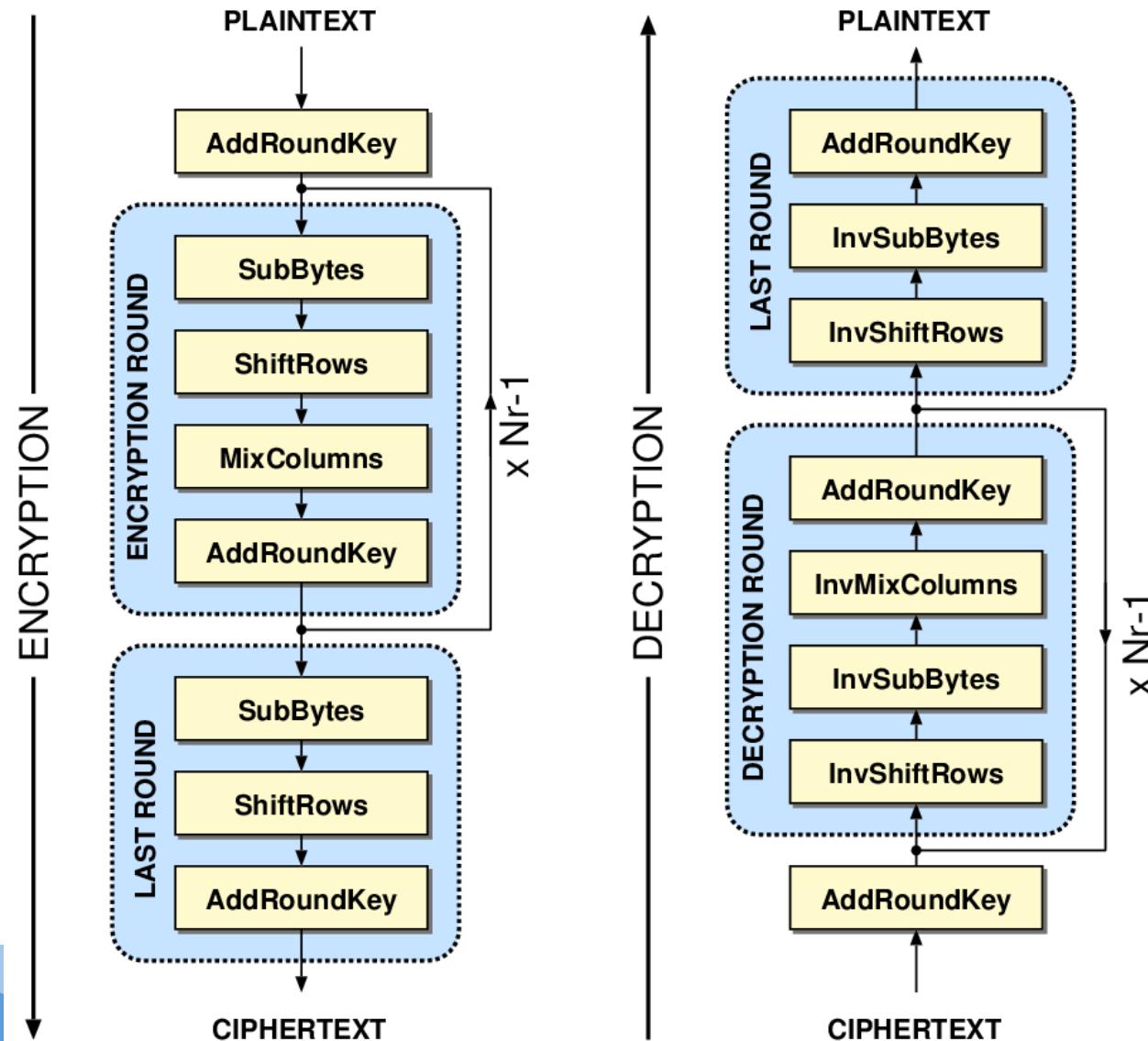
❖ Bước AddRoundKey:

- Mỗi byte của ma trận state được kết hợp với một byte của khóa phụ sử dụng phép \oplus (XOR).



Quá
trình
mã
hóa
và
giải
mã
của
AES

4.3.1 Các giải thuật mã hóa khóa đối xứng – AES

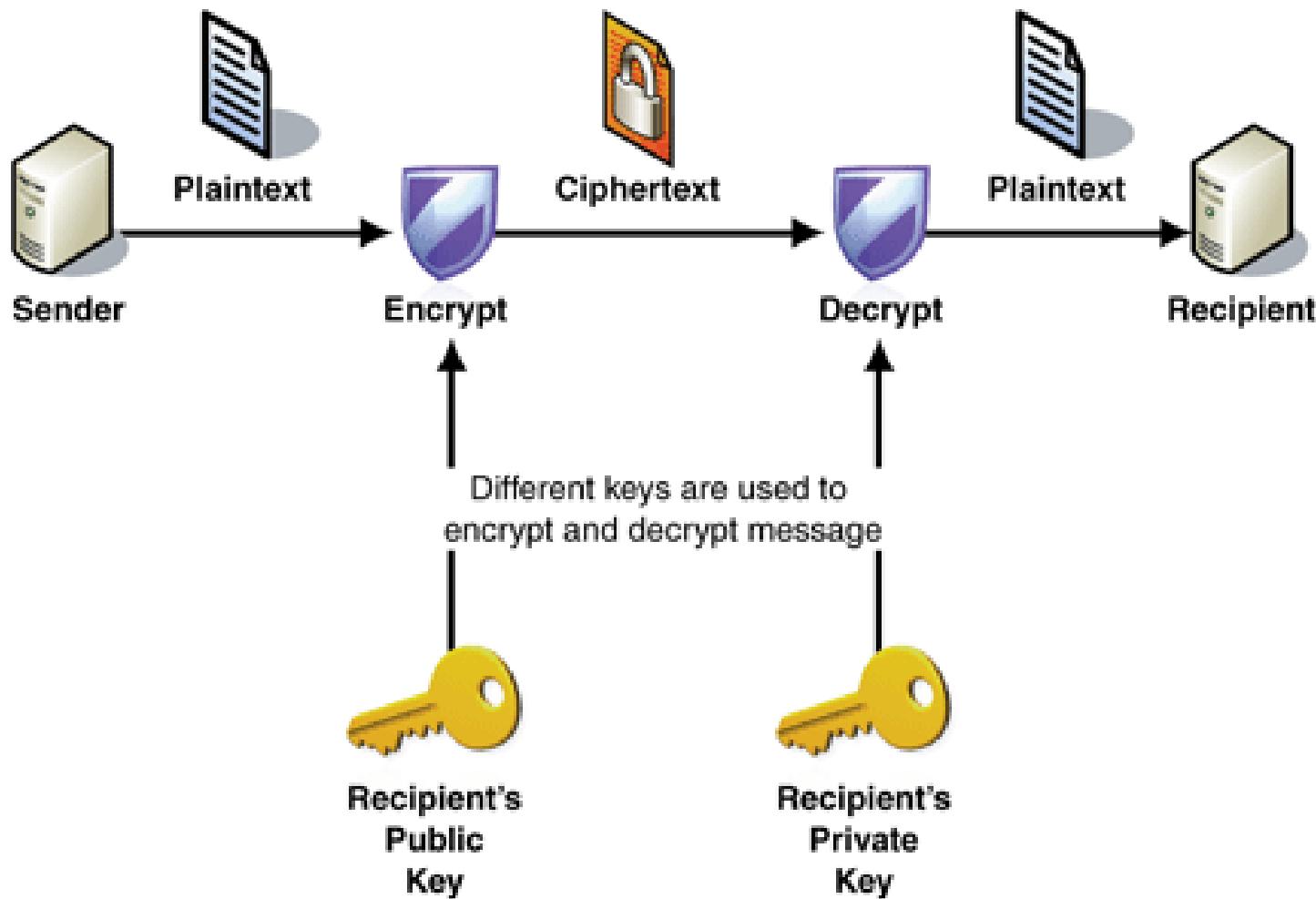


4.3.1 Các giải thuật mã hóa khóa bất đối xứng

❖ Các giải thuật mã hóa khóa bất đối xứng (asymmetric key encryption)

- Còn gọi là mã hóa khóa công khai (public key encryption):
- Sử dụng một cặp khóa (key pair):
 - một khóa (public key) cho mã hóa và
 - một khóa (private key) cho giải mã.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng



4.3.1 Các giải thuật mã hóa khóa bất đối xứng

❖ Đặc điểm:

- Kích thước khóa lớn (1024 – 3072 bít)
- Tốc độ chậm
 - Phần lớn do khóa có kích thước lớn.
- Độ an toàn cao
- Thuận lợi trong quản lý và phân phối khóa:
 - Do khóa mã hóa là công khai và có thể trao đổi dễ dàng.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng

- Các giải thuật mã hóa khóa bất đối xứng điển hình:
 - RSA
 - Rabin
 - ElGamal
 - McEliece
 - Knapsack

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

- ❖ Giải thuật mã hóa RSA được 3 nhà khoa học Ronald Rivest, Adi Shamir và Leonard Adleman phát minh năm 1977;
 - Tên giải thuật RSA lấy theo chữ cái đầu của tên 3 ông.
- ❖ Độ an toàn của RSA dựa trên tính khó của việc phân tích số nguyên rất lớn:
 - Khóa RSA là số nguyên rất lớn có hàng trăm chữ số thập phân.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ RSA sử dụng một cặp khóa:

- Khóa công khai (Public key) dùng để mã hóa;
- Khóa riêng (Private key) dùng để giải mã.
- Chỉ khóa riêng cần giữ bí mật. Khóa công khai có thể công bố rộng rãi.

❖ Kích thước khóa của RSA:

- Khóa < 1024 bít không an toàn hiện nay.
- Khuyến nghị dùng khóa ≥ 2048 bít với các ứng dụng mật mã dân sự hiện nay.
- Tương lai nên dùng khóa ≥ 3072 bít.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Thủ tục sinh khóa RSA:

- Tạo 2 số nguyên tố p và q;
- Tính $n = p \times q$
- Tính $\Phi(n) = (p-1) \times (q-1)$
- Chọn số nguyên tố e sao cho $1 < e < \Phi(n)$ và $\text{gcd}(e, \Phi(n)) = 1$, hay e, $\Phi(n)$ là 2 số nguyên tố cùng nhau
- Chọn số d sao cho $d \equiv e^{-1} \pmod{\Phi(n)}$,
hoặc $(d \times e) \pmod{\Phi(n)} = 1$
(d là molulo nghịch đảo của e)

❖ Ta có (n, e) là khóa công khai, (n, d) là khóa riêng.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Thủ tục mã hóa RSA:

- Thông điệp m đã được chuyển thành số, $m < n$
- Bản mã $c = m^e \text{ mod } n$

❖ Thủ tục giải mã RSA:

- Bản mã c , $c < n$
- Bản rõ $m = c^d \text{ mod } n$

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Ví dụ 1:

- Chọn 2 số nguyên tố $p=3$ và $q=11$
- Tính $n = p \times q = 3 \times 11 = 33$
- Tính $\Phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$
- Chọn số e sao cho $1 < e < 20$, và e và $\Phi(n)$ là số nguyên tố cùng nhau ($\Phi(n)$ không chia hết cho e). Chọn $e = 7$
- Tính $(d \times e) \bmod \Phi(n) \rightarrow (d \times 7) \bmod 20 = 1$
 $d = (20*k + 1)/7 \rightarrow d = 3 \text{ (k=1)}$
- Khóa công khai $(33, 7)$
- Khóa bí mật $(33, 3)$

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Ví dụ 1:

■ Mã hóa:

- Với $m = 6$,
- $c = m^e \text{ mod } n = 6^7 \text{ mod } 33 = 279936 \text{ mod } 33 = 30$
- $\rightarrow c = 30$

■ Giải mã:

- $m = c^d \text{ mod } n = 30^3 \text{ mod } 33 = 27000 \text{ mod } 33 = 6$
- $\rightarrow m = 6$

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Ví dụ 2:

- Chọn 2 số nguyên tố $p=61$ và $q=53$
- Tính $n = p \times q = 61 \times 53 = 3233$
- Tính $\Phi(n) = (p-1) \times (q-1) = 60 \times 52 = 3120$
- Chọn số e sao cho $1 < e < 3120$ và e và $\Phi(n)$ là số nguyên tố cùng nhau ($\Phi(n)$ không chia hết cho e). Chọn $e = 17$
- Tính $(d \times e) \bmod \Phi(n) \rightarrow (d \times 17) \bmod 3120 = 1$
 $d = (3120*k + 1)/17 \rightarrow d = 2753 \quad (k=15)$
- Khóa công khai $(3233, 17)$
- Khóa bí mật $(3233, 2753)$

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Ví dụ 2:

■ Mã hóa:

- Với $m = 65$,
- $c = m^e \text{ mod } n = 65^{17} \text{ mod } 3233 = 2790$
- $\rightarrow c = 2790$

■ Giải mã:

- $m = c^d \text{ mod } n = 2790^{2753} \text{ mod } 3233$
- $\rightarrow m = 65$

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

- ❖ Một số yêu cầu với quá trình sinh khóa RSA:
 - Các số nguyên tố p và q phải được chọn sao cho việc phân tích n ($n = pq$) là không khả thi về mặt tính toán;
 - p và q nên có cùng độ lớn (tính bằng bit) và phải là các số đủ lớn;
 - Nếu n có kích thước 1024 bít thì p và q nên có kích thước khoảng 512 bít.
 - Nếu n có kích thước 2048 bít thì p và q nên có kích thước khoảng 1024 bít.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

- ❖ Một số yêu cầu với quá trình sinh khóa RSA:
 - Hiệu số $p - q$ không nên quá nhỏ, do nếu $p - q$ quá nhỏ, tức $p \approx q$ và $p \approx \sqrt{n}$ \rightarrow chọn các số nguyên tố ở gần \sqrt{n} và thử nhiều lần.
 - Khi có được $p \rightarrow$ tính q , và tìm ra d là khóa bí mật từ khóa công khai e và $\Phi(n)$.
 - Nếu p và q được chọn ngẫu nhiên và $p - q$ đủ lớn, khả năng hai số này bị phân tích từ n giảm đi.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Sử dụng số mũ mã hóa (e) nhỏ:

- Khi sử dụng số mũ mã hóa (e) nhỏ, chẳng hạn $e=3$ có thể tăng tốc độ mã hóa;
- Kẻ tấn công có thể nghe trộm và lấy được bản mã, từ đó phân tích bản mã để khôi phục bản rõ. Do số mũ nhỏ nên chi phí cho phân tích/vết cạn không quá lớn;
- Phòng chống:
 - Sử dụng số mũ e lớn;
 - Thêm chuỗi ngẫu nhiên vào khối rõ trước khi mã hóa.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Sử dụng số mũ giải mã (d) nhỏ:

- Khi sử dụng số mũ giải mã (d) nhỏ, có thể tăng tốc độ giải mã;
- Nếu d nhỏ và $\text{gcd}(p-1, q-1)$ (gcd : ước số chung lớn nhất) cũng nhỏ thì d có thể tính được tương đối dễ dàng từ khóa công khai (n, e);
- Phòng chống:
 - Sử dụng số mũ d đủ lớn.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Cài đặt RSA trên thực tế:

- Do kích thước cặp khóa của RSA rất lớn (n cỡ 2048 bít – khoảng hơn 600 chữ số thập phân), việc thực hiện RSA trực tiếp có chi phí tính toán và lưu trữ rất lớn:
 - Mã hóa $c = m^e \text{ mod } n$
 - Giải mã $m = c^d \text{ mod } n$
 - Do m , e và d thường rất lớn nên giá trị mũ m^e hoặc c^d thường rất rất lớn.
- → cần có giải thuật hiệu quả để giảm chi phí tính toán → cài đặt trên máy tính.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Cài đặt trong java:

- Ngôn ngữ lập trình java định nghĩa lớp BigInteger cung cấp hầu hết các hàm dựng và các hàm số học cho phép thao tác thuận lợi với số nguyên lớn.
- Một số hàm có thể dùng để cài đặt RSA:
 - Hàm dựng BigInteger(int bitLength, int certainty, Random rnd): sinh số nguyên tố ngẫu nhiên với số bit cho trước;
 - Hàm BigInteger add(BigInteger val): cộng hai số nguyên lớn;
 - Hàm BigInteger gcd(BigInteger val): tìm ƯSC lớn nhất của 2 số nguyên lớn;
 - Hàm BigInteger mod(BigInteger m): tính modulo (phần dư) của phép chia nguyên;
 - Hàm BigInteger modInverse(BigInteger m): tính modulo nghịch đảo ($this^{-1} \bmod m$);
 - BigInteger modPow(BigInteger exponent, BigInteger m): tính $(this^{exponent} \bmod m)$.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Cài đặt trên ngôn ngữ C:

- Do thư viện ngôn ngữ C không hỗ trợ số lớn nên việc cài đặt RSA trong C phải thực hiện từ các thao tác số học cơ sở;
- Có thể sử dụng 1 mảng để lưu các chữ số của số nguyên lớn và xây dựng các hàm thực hiện các phép toán số học và modulo cho số nguyên lớn;

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

❖ Cài đặt trên ngôn ngữ C:

- Lựa chọn cơ số:
 - Cơ số 10: đơn giản, dễ hiểu. Tuy nhiên, tốn không gian lưu trữ và chậm do không tận dụng được khả năng thực hiện các phép toán nhân/chia với số 2 thông qua phép dịch. → Cơ số nên là số mũ của 2 và cần đủ lớn;
 - Cơ số 256: một số được lưu trong 1 phần tử mảng là 1 byte → tiết kiệm không gian lưu trữ. Tuy nhiên, số phần tử mảng vẫn có thể khá lớn → chậm trong thao tác;
 - Cơ số 2^{16} (65536): khá phù hợp do một số được lưu trong 1 phần tử mảng là 2 byte và số phần tử mảng sẽ giảm → nhanh hơn trong thao tác.

4.3.2 Các giải thuật mã hóa khóa bất đối xứng - RSA

- ❖ Cài đặt trên ngôn ngữ C: định nghĩa cấu trúc BigInt

```
typedef struct {  
    unsigned short *digits; // pointer to array of digits  
                           // the least significant digit at index 0  
    unsigned int size;     // number of digits of the big integer  
    short sign;           // sign of the big integer,  
                           // sign = -1 for negative number, and 1 otherwise  
} BigInt ;
```

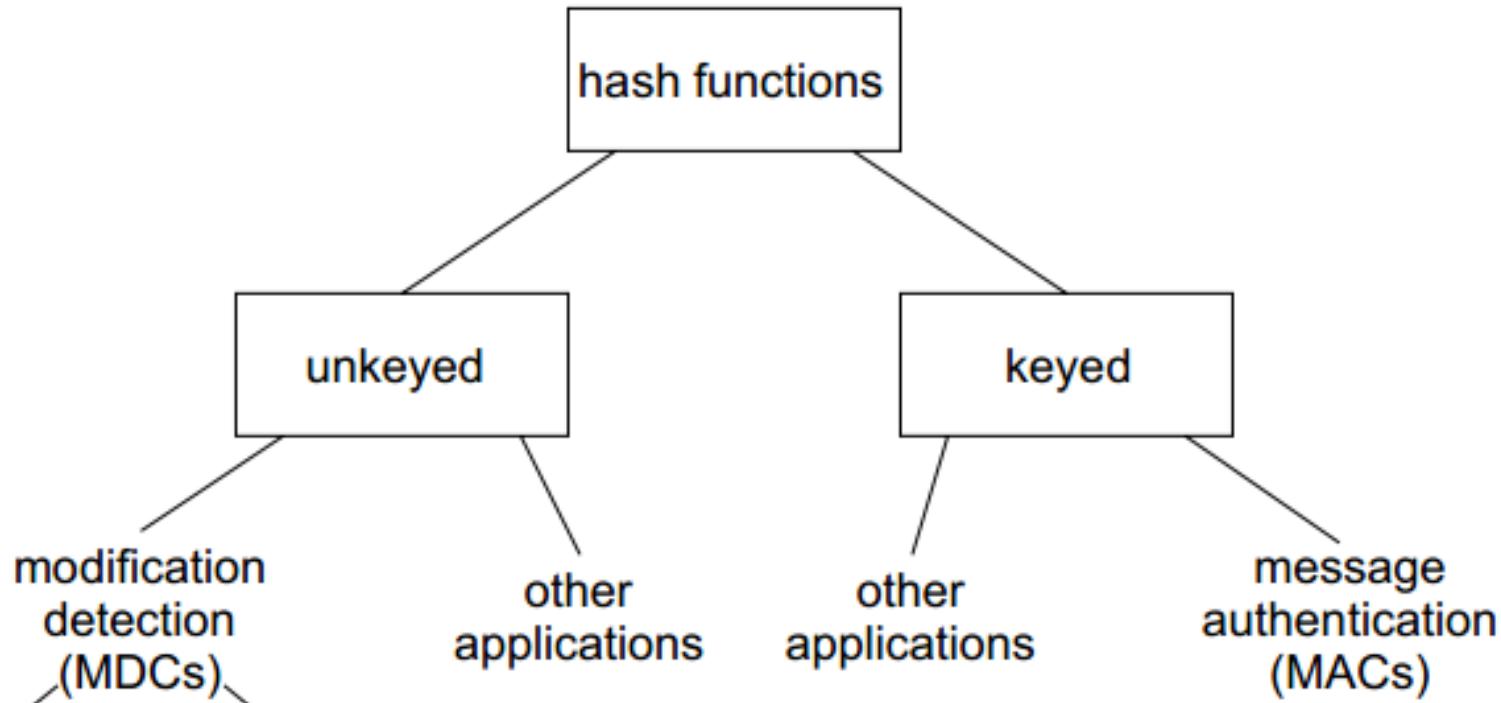
4.3.3 Các hàm băm

- ❖ **Hàm băm (hash function)** là một hàm toán học h có tối thiểu 2 thuộc tính cơ bản:
 - Nén (compression): h là một ánh xạ từ chuỗi đầu vào x có chiều dài bất kỳ sang một chuỗi đầu ra $h(x)$ có chiều dài cố định n bit;
 - Dễ tính toán (ease of computation): cho trước hàm h và đầu vào x , việc tính toán $h(x)$ là dễ dàng.

4.3.3 Các hàm băm

❖ Phân loại hàm băm theo khóa sử dụng:

- Hàm băm không khóa (unkeyed): đầu vào chỉ là thông điệp;
- Hàm băm có khóa (keyed): đầu vào gồm thông điệp và khóa.



4.3.3 Các hàm băm

❖ Phân loại hàm băm theo tính năng:

- Mã phát hiện sửa đổi (MDC - Modification detection codes)
- Mã xác thực thông điệp (MAC - Message authentication codes).

4.3.3 Các hàm băm

❖ Phân loại hàm băm theo tính năng:

- Mã phát hiện sửa đổi (MDC - Modification detection codes)
 - MDC thường được sử dụng để tạo chuỗi đại diện cho thông điệp và dùng kết hợp với các biện pháp khác để đảm bảo tính toàn vẹn của thông điệp;
 - MDC thuộc loại hàm băm không khóa;
 - MDC thường được sử dụng trong các quá trình tạo và kiểm tra chữ ký số để đảm bảo tính toàn vẹn thông điệp.

4.3.3 Các hàm băm

❖ Phân loại hàm băm theo tính năng:

- Mã phát hiện sửa đổi (MDC - Modification detection codes)
 - Hai loại MDC:
 - Hàm băm một chiều (OWHF - One-way hash functions): dễ dàng tính giá trị băm, nhưng khôi phục thông điệp từ giá trị băm rất khó khăn;
 - Hàm băm chống đụng độ (CRHF - Collision resistant hash functions): Rất khó tìm được 2 thông điệp trùng giá trị băm.

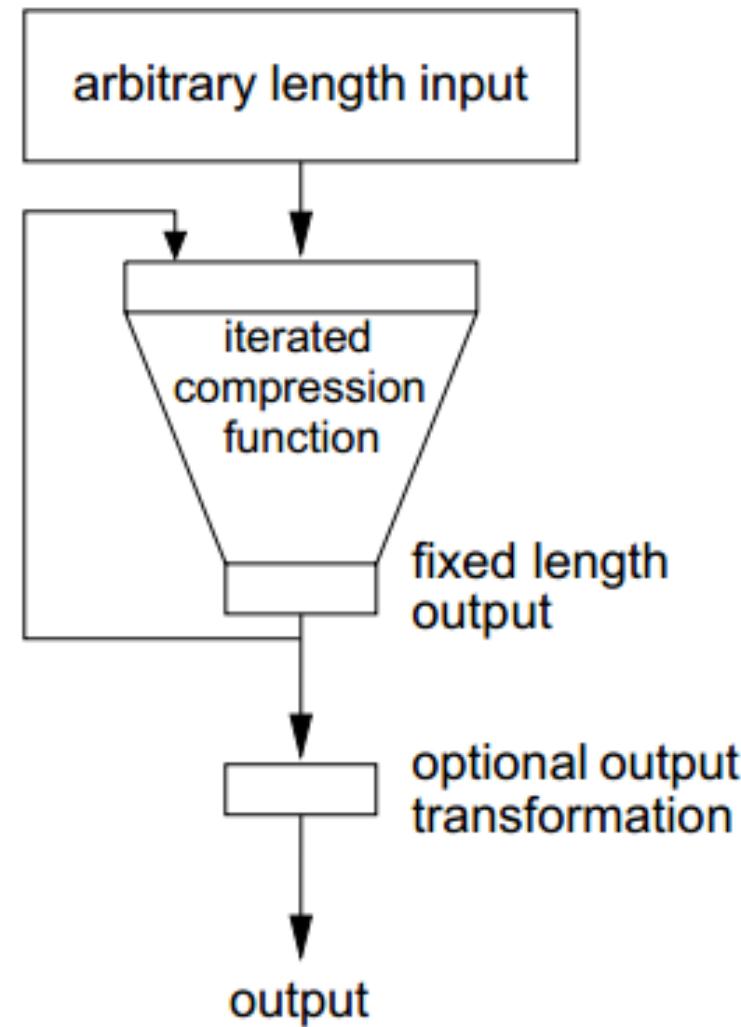
4.3.3 Các hàm băm

❖ Phân loại hàm băm theo tính năng:

- Mã xác thực thông điệp (MAC - Message authentication codes)
 - MAC cũng được dùng để đảm bảo tính toàn vẹn của thông điệp mà không cần một biện pháp bổ sung khác;
 - MAC là loại hàm băm có khóa: đầu vào là thông điệp và một khóa;
 - MAC được sử dụng trong các giao thức bảo mật SSL/TLS, IPSec,... để đảm bảo tính toàn vẹn thông điệp.

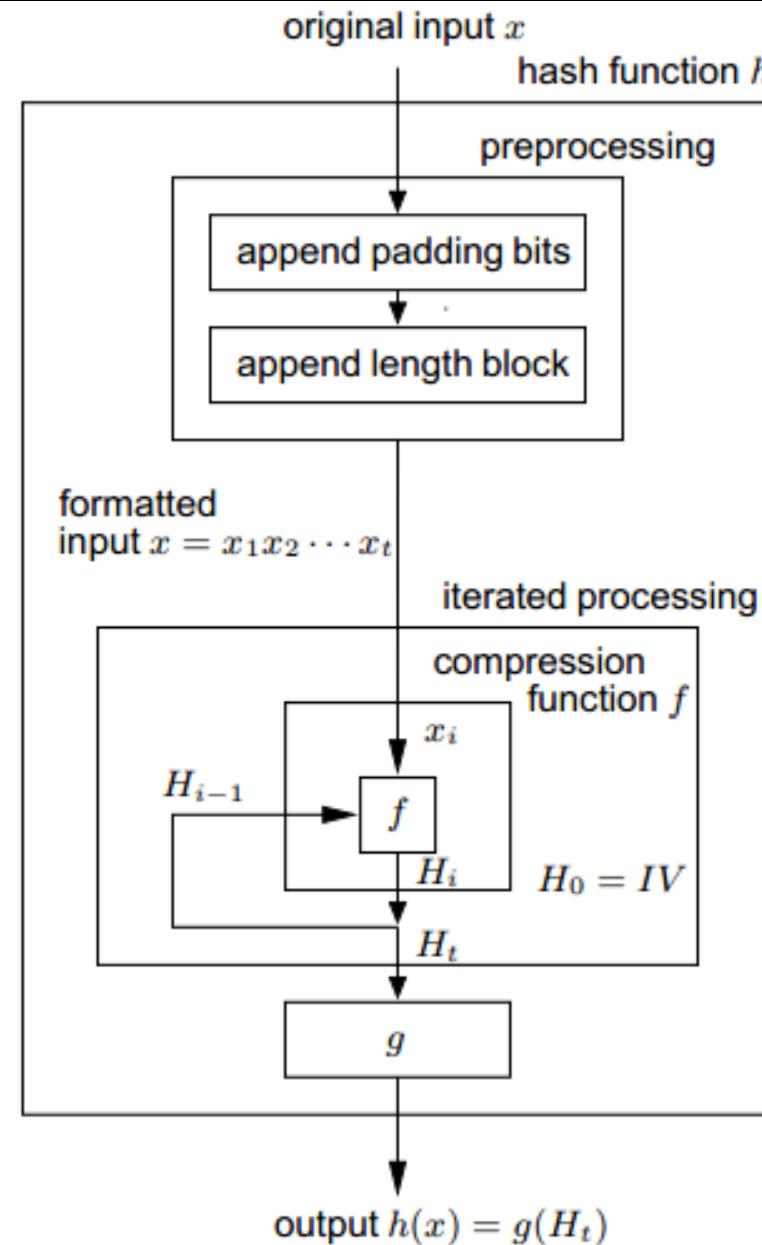
4.3.3 Các hàm băm

Mô hình
lắp tổng
quát tạo
giá trị
băm



4.3.3 Các hàm băm

Mô hình
lắp chi
tiết tạo
giá trị
băm



4.3.3 Các hàm băm

- ❖ Một số giải thuật hàm băm điển hình:
 - CRC (Cyclic redundancy checks)
 - Checksums
 - MD2, MD4, MD5
 - MD6
 - SHA0, SHA1
 - SHA2, SHA3

4.3.3 Các hàm băm – MD5

- ❖ MD5 (Message Digest) là hàm băm không khóa được Ronald Rivest thiết kế năm 1991 để thay thế MD4;
- ❖ Chuỗi đầu ra (giá trị băm) của MD5 là 128 bit (16 bytes) và thường được biểu diễn thành 32 số hexa;
- ❖ MD5 được sử dụng khá rộng rãi trong nhiều ứng dụng:
 - Chuỗi đảm bảo tính toàn vẹn thông điệp;
 - Tạo chuỗi kiểm tra lỗi – Checksum;
 - Mã hóa mật khẩu.

4.3.3 Các hàm băm – MD5

❖ Quá trình xử lý thông điệp của MD5:

- Thông điệp được chia thành các khối 512 bít. Nếu kích thước thông điệp không là bội số của 512 → nối thêm số bít thiếu;
- Phần xử lý chính của MD5 làm việc trên state 128 bít, chia thành 4 từ 32 bít (A, B, C, D);
 - Các từ A, B, C, D được khởi trị bằng một hằng cố định;
 - Từng phần 32 bít của khối đầu vào 512 bít được đưa dần vào để thay đổi state;
- Quá trình xử lý gồm 4 vòng, mỗi vòng gồm 16 thao tác tương tự nhau;
- Mỗi thao tác gồm:
 - Hàm F (4 hàm khác nhau cho mỗi vòng);
 - Cộng modulo;
 - Quay trái.

4.3.3 Các hàm băm – MD5

❖ Lưu đồ xử lý một thao tác của MD5:

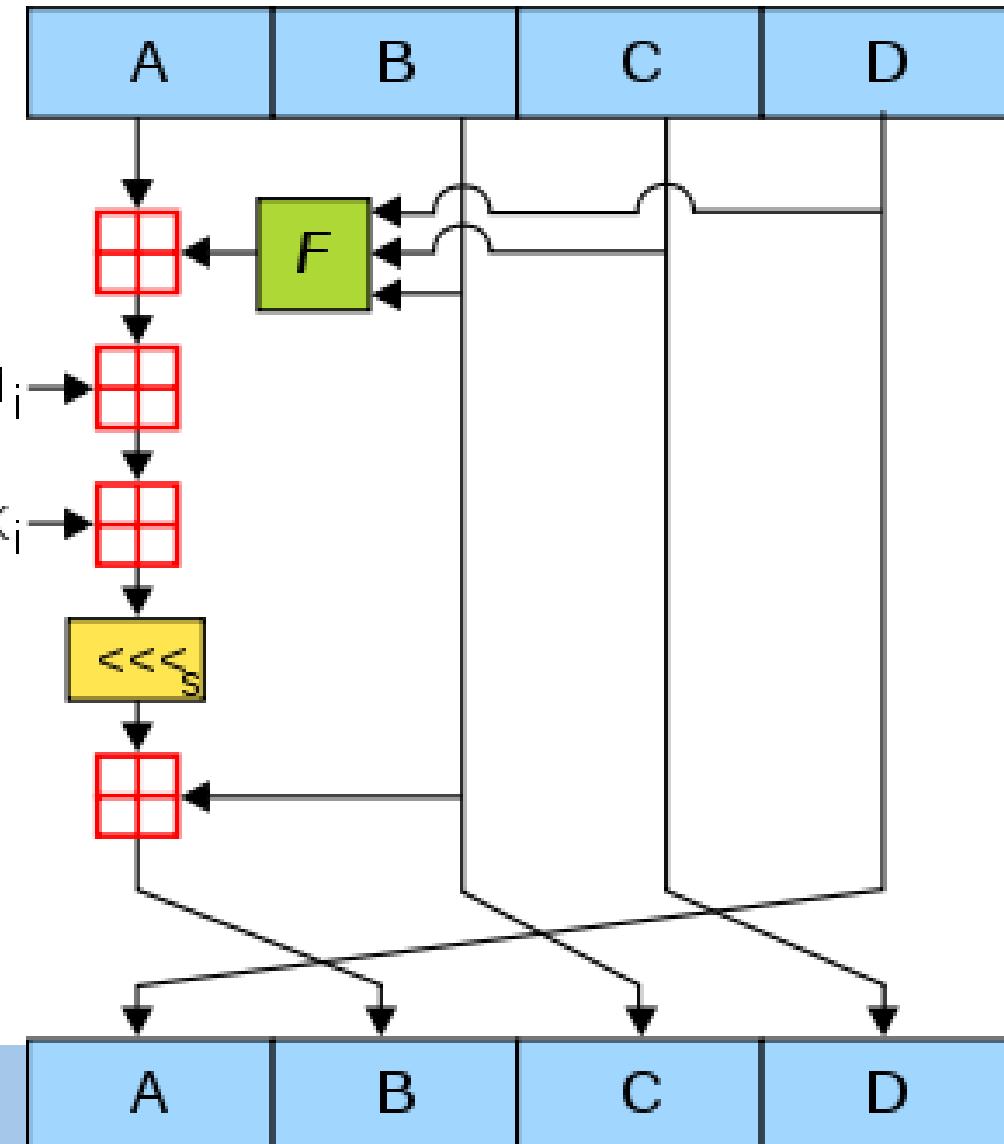
- A, B, C, D: các từ 32 bit
- M_i : khối 32 bit thông điệp đầu vào;
- K_i : 32 bit hằng. Mỗi thao tác sử dụng một hằng khác nhau;
- $<<<s$: thao tác dịch trái s bit
- \oplus biểu diễn cộng modulo 32 bit;
- F: hàm phi tuyến tính, gồm 4 loại:

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$

$$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$$

$$H(B, C, D) = B \oplus C \oplus D$$

$$I(B, C, D) = C \oplus (B \vee \neg D)$$



4.3.3 Các hàm băm – SHA1

- ❖ SHA1 (Secure Hash Function) được NSA (Mỹ) thiết kế năm 1995 để thay thế cho SHA0;
- ❖ Chuỗi đầu ra của SHA1 có kích thước 160 bit và thường được biểu diễn thành 40 số hexa;
- ❖ SHA1 được sử dụng rộng rãi để:
 - Đảm bảo tính xác thực và toàn vẹn thông điệp;
 - Mã hóa mật khẩu.

4.3.3 Các hàm băm – SHA1

❖ Họ hàm băm SHA: SHA-0, SHA-1, SHA-2, SHA-3:

- SHA0 ít được sử dụng trên thực tế;
- SHA1 tương tự SHA0, nhưng đã khắc phục một số lỗi;
- SHA2 ra đời năm 2001 khắc phục lỗi của SHA1 và có nhiều thay đổi. Kích thước chuỗi đầu ra có thể là 224, 256, 384 và 512 bit;
- SHA3 ra đời năm 2012, cho phép chuỗi đầu ra có kích thước không cố định.

4.3.3 Các hàm băm – SHA1

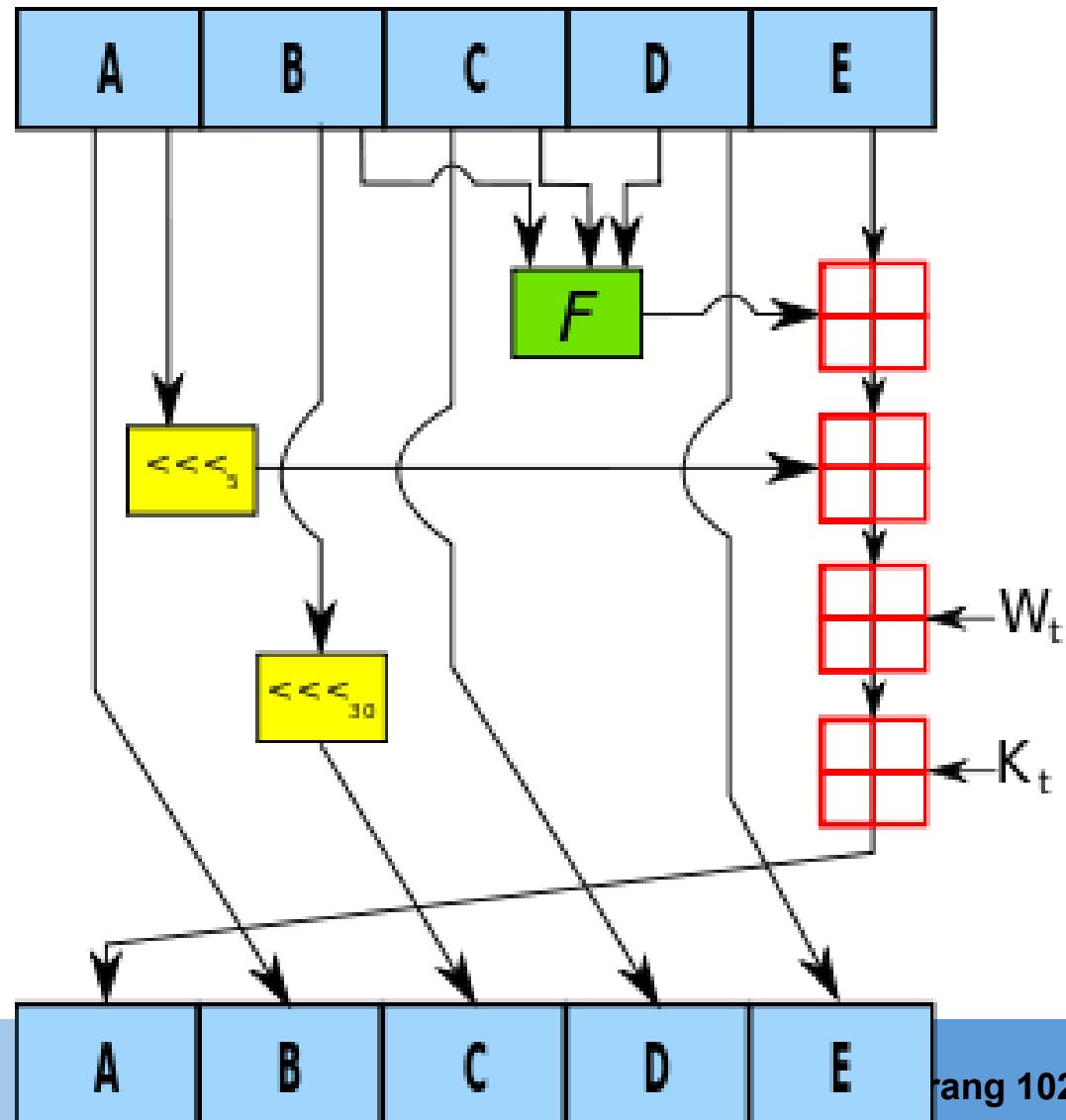
❖ Quá trình xử lý thông điệp của SHA1:

- SHA1 sử dụng thủ tục xử lý thông điệp tương tự MD5;
- Thông điệp được chia thành các khối 512 bít. Nếu kích thước thông điệp không là bội số của 512 → nối thêm số bít thiếu;
- Phần xử lý chính của SHA1 làm việc trên state 160 bít, chia thành 5 từ 32 bít (A, B, C, D, E);
 - Các từ A, B, C, D, E được khởi trị bằng một hằng cố định;
 - Từng phần 32 bít của khối đầu vào 512 bít được đưa dần vào để thay đổi state;
- Quá trình xử lý gồm 80 vòng, mỗi vòng gồm các thao tác: add, and, or, xor, rotate, mod.

4.3.3 Các hàm băm – SHA1

❖ Lưu đồ xử lý một vòng của SHA1:

- A, B, C, D, E: các từ 32 bit
- W_t: khối 32 bit thông điệp đầu vào;
- K_t: 32 bit hằng. Mỗi sử dụng một hằng khác nhau;
- <<<_n: thao tác dịch trái n bit
- \oplus biểu diễn cộng modulo 32 bit;
- F: hàm phi tuyến tính.



4.4 Chữ ký số, chứng chỉ số và PKI

1. Chữ ký số

- Khái niệm
- Quá trình ký và kiểm tra chữ ký số
- Thuật toán chữ ký số RSA
- Thuật toán chữ ký số DSA

2. Chứng chỉ số

3. Hạ tầng khóa công khai - PKI – Public Key Infrastructure

4.4.1 Chữ ký số

❖ Một số khái niệm:

- Chữ ký số (Digital Signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp;
- Giải thuật tạo chữ ký số (Digital Signature generation algorithm) là một phương pháp sinh chữ ký số;
- Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định;

4.4.1 Chữ ký số

❖ Một số khái niệm:

- Một hệ chữ ký số (Digital Signature Scheme) bao gồm giải thuật tạo chữ ký số và giải thuật kiểm tra chữ ký số.
- Quá trình tạo chữ ký số (Digital signature signing process) bao gồm:
 - Giải thuật tạo chữ ký số, và
 - Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.
- Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm:
 - Giải thuật kiểm tra chữ ký số, và
 - Phương pháp khôi phục dữ liệu từ thông điệp.

4.4.1 Chữ ký số

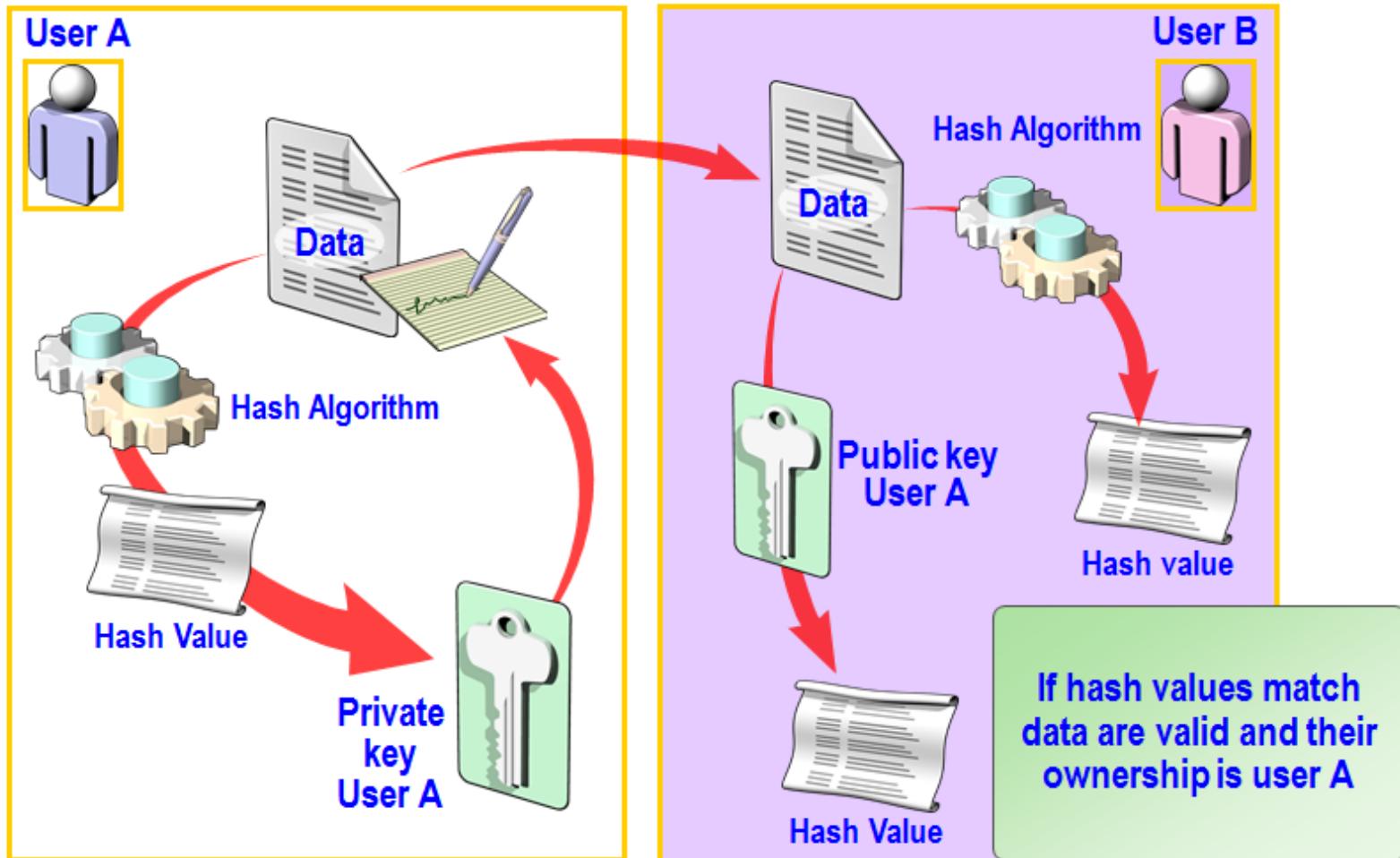
NGÂN HÀNG TMCP KỸ THƯƠNG VIỆT NAM
TECHCOMBANK TÂN BÌNH



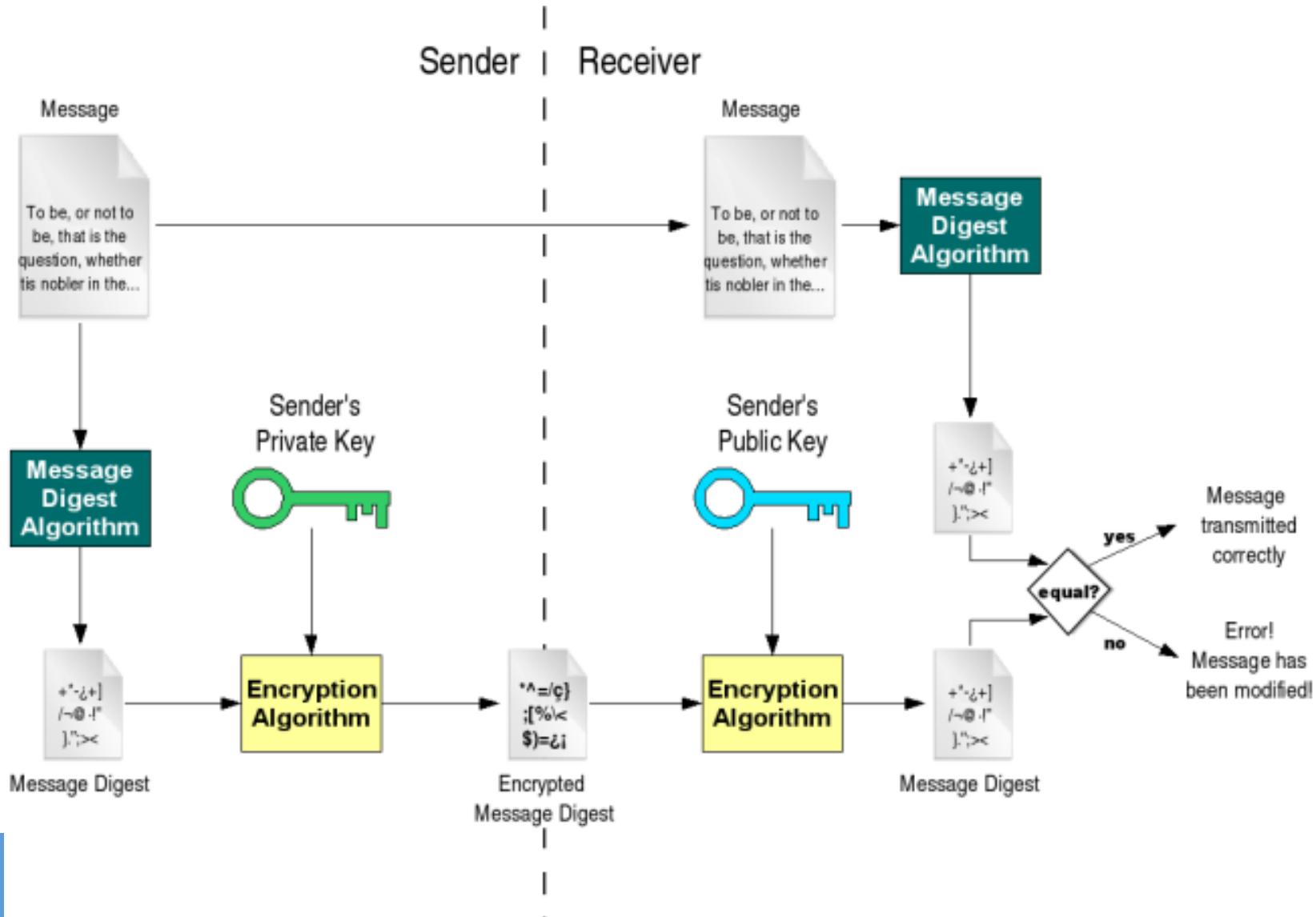
Ngõ Quang Trưởng

4.4.1 Chữ ký số

Digital signature



4.4.1 Chữ ký số - Quá trình ký và kiểm tra



4.4.1 Chữ ký số - Quá trình ký

❖ Các bước của quá trình ký một thông điệp (bên người gửi):

- Tính toán chuỗi đại diện (message digest/hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm);
- Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và một giải thuật tạo chữ ký (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted message digest);
- Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message);
- Thông điệp đã được ký (Signed message) được gửi cho người nhận.

4.4.1 Chữ ký số - Quá trình kiểm tra

❖ Các bước của quá trình kiểm tra chữ ký (bên người nhận):

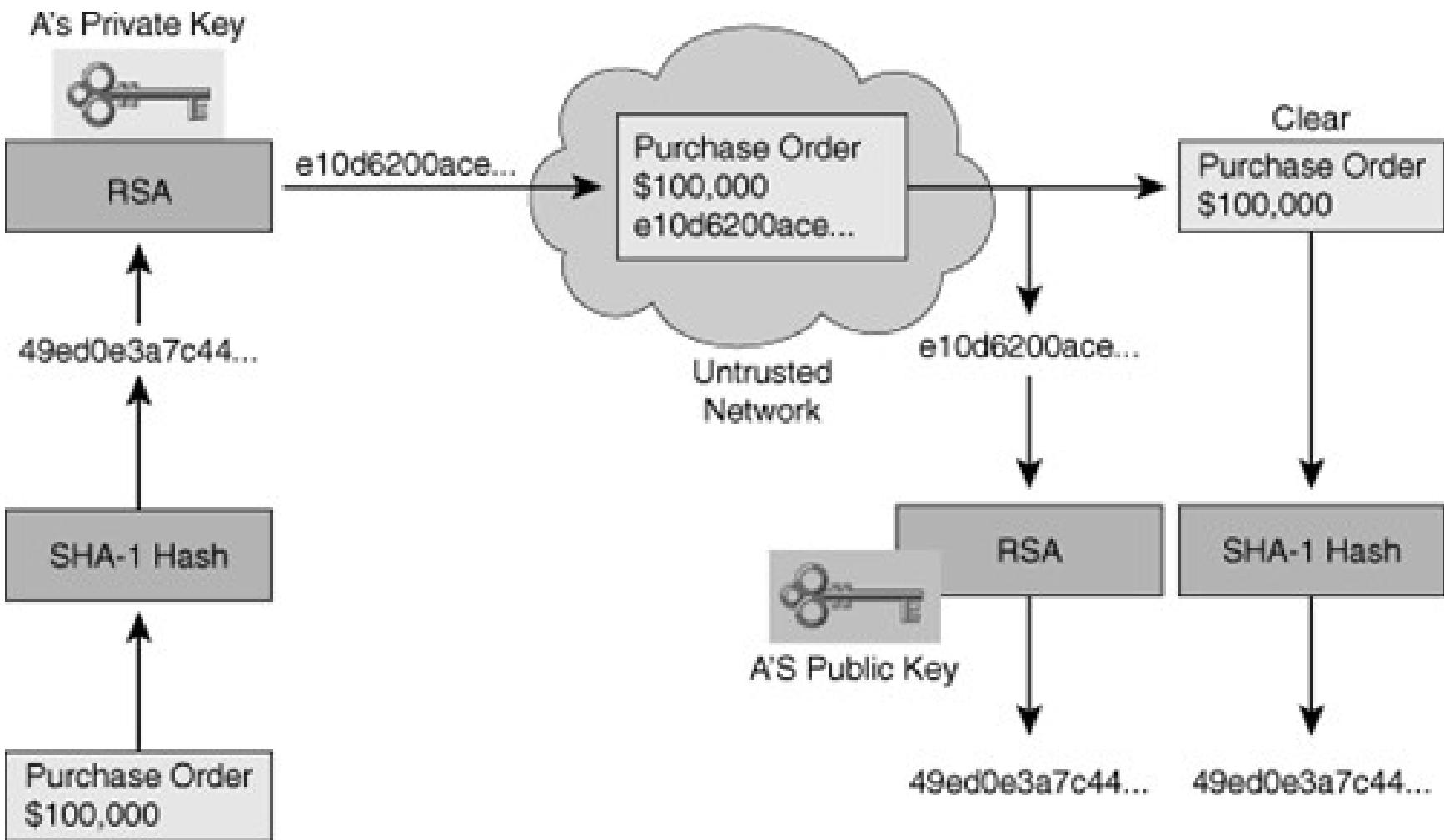
- Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký);
- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số → chuỗi đại diện thông điệp MD2;
- So sánh MD1 và MD2:
 - Nếu $MD1 = MD2 \rightarrow$ chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
 - Nếu $MD1 <> MD2 \rightarrow$ chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

4.4.1 Chữ ký số - Giải thuật chữ ký số RSA

❖ RSA là giải thuật cho phép thực hiện 2 tính năng:

- Mã hóa thông điệp:
 - Người gửi mã hóa thông điệp sử dụng khóa công khai của người nhận;
 - Người nhận giải mã thông điệp sử dụng khóa riêng của mình.
- Tạo chữ ký số:
 - Người gửi tạo chữ ký số sử dụng khóa bí mật của mình;
 - Người nhận kiểm tra chữ ký sử dụng khóa công khai của người gửi.

4.4.1 Chữ ký số - Giải thuật chữ ký số RSA



4.4.1 Chữ ký số - Giải thuật chữ ký số DSA

- ❖ DSA (Digital Signature Algorithm) là chuẩn chữ ký số được phát triển bởi NIST (Mỹ) năm 1991;
- ❖ DSA được phát triển từ giải thuật Digital Signature Standard (DSS);
- ❖ Các thành phần của DSA:
 - Sinh khóa: sinh cặp khóa. Gồm 2 giai đoạn:
 - Lựa chọn tham số của giải thuật;
 - Sinh cặp khóa cho người dùng.
 - Quá trình ký: ký thông điệp
 - Quá trình kiểm tra chữ ký: kiểm tra chữ ký.

4.4.1 Chữ ký số - Giải thuật chữ ký số DSA

❖ Sinh khóa:

- Lựa chọn tham số:
 - Lựa chọn giải thuật băm chuẩn H. Giải thuật băm có thể được lựa chọn là SHA-1 hoặc SHA-2;
 - Chọn kích thước cho các khóa L và N.
 - L có thể là 1024, 2048, 3072;
 - N có thể là 160, 224, 256. N phải nhỏ hơn hoặc bằng kích thước chuỗi băm đầu ra của hàm H đã chọn;
 - Chọn số nguyên tố q N bít;
 - Chọn modulo p L bít sao cho $p-1$ là bội số của q;
 - Chọn g là hệ số nhân sao cho $(g^q) \bmod p = 1$;
 - Các tham số (q, p và g) được chia sẻ giữa các người dùng.

4.4.1 Chữ ký số - Giải thuật chữ ký số DSA

❖ Sinh khóa:

- Sinh khóa cho một người dùng:
 - Chọn số ngẫu nhiên x sao cho $0 < x < q$;
 - Tính $y = g^x \text{ mod } p$;
 - Khóa công khai là (q, p, g, y) ;
 - Khóa riêng là x .

4.4.1 Chữ ký số - Giải thuật chữ ký số DSA

❖ Ký thông điệp:

- H là hàm băm sử dụng và m là thông điệp gốc;
- Tính $H(m)$ từ thông điệp gốc;
- Tạo số ngẫu nhiên k cho mỗi thông điệp, $0 < k < q$;
- Tính $r = (g^k \text{ mod } p) \text{ mod } q$;
- Nếu $r = 0$, chọn một k mới và tính lại r ;
- Tính $s = k^{-1}(H(m) + xr) \text{ mod } q$;
- Nếu $s = 0$, chọn một k mới và tính lại r và s ;
- Chữ ký là cặp (r, s) .

4.4.1 Chữ ký số - Giải thuật chữ ký số DSA

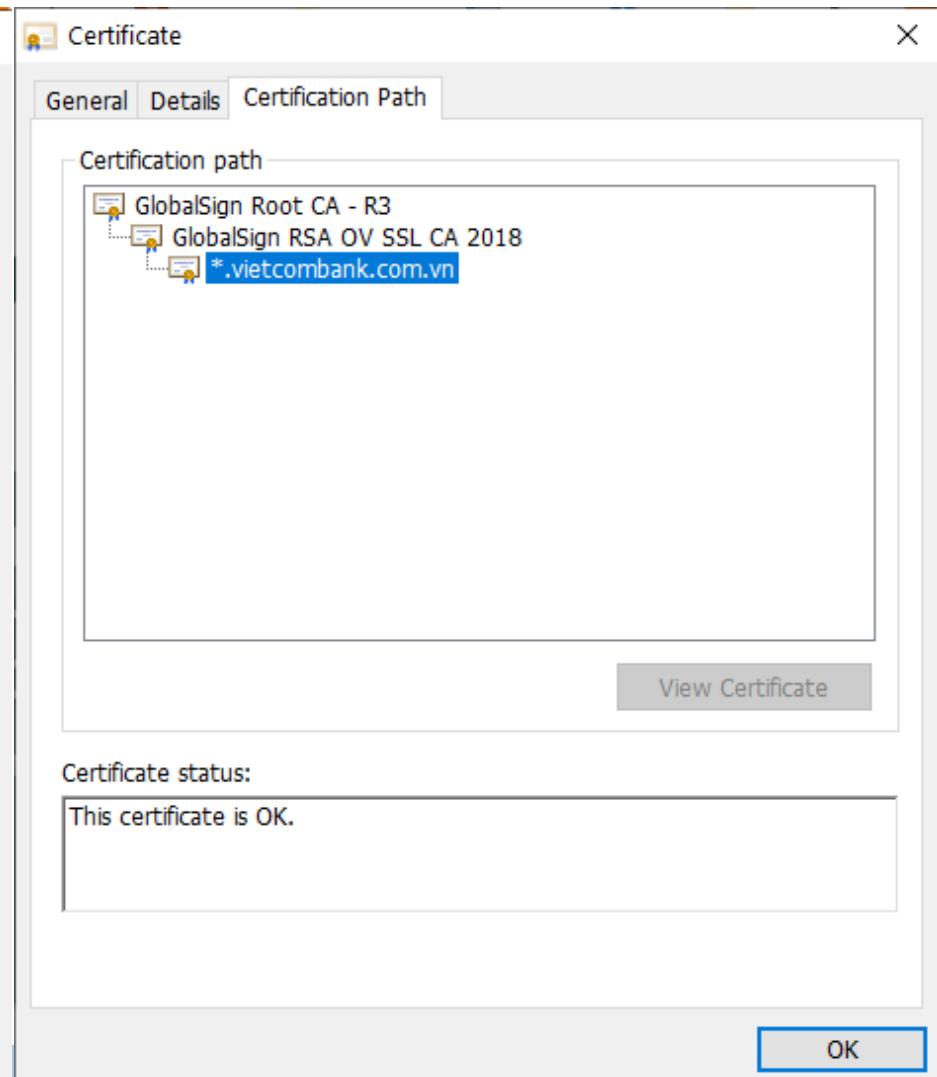
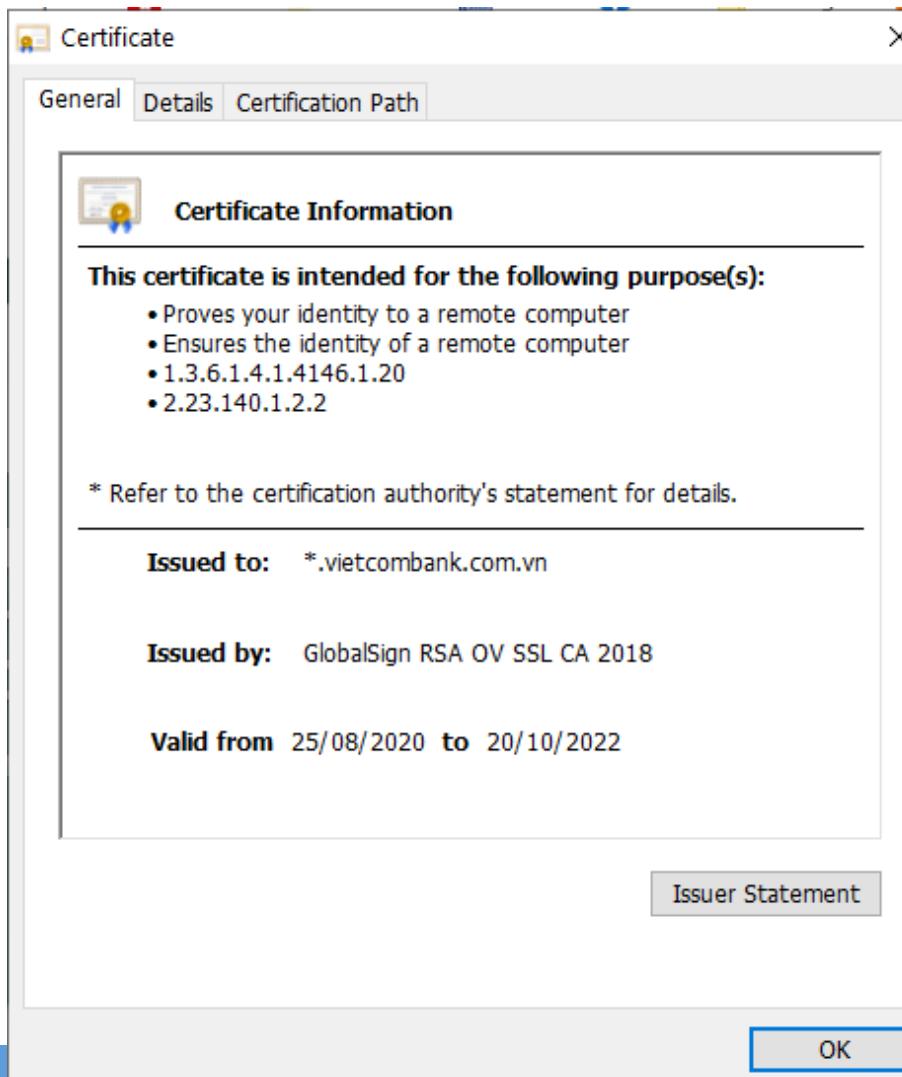
❖ Kiểm tra chữ ký của thông điệp:

- Loại bỏ chữ ký nếu r và s không thỏa mãn $0 < r, s < q$;
- Tính $H(m)$ từ thông điệp nhận được;
- Tính $w = s^{-1} \text{ mod } q$;
- Tính $u_1 = H(m) * w \text{ mod } q$;
- Tính $u_2 = r * w \text{ mod } q$;
- Tính $v = ((g^{u_1} * y^{u_2}) \text{ mod } p) \text{ mod } q$;
- Chữ ký là xác thực nếu $v = r$.

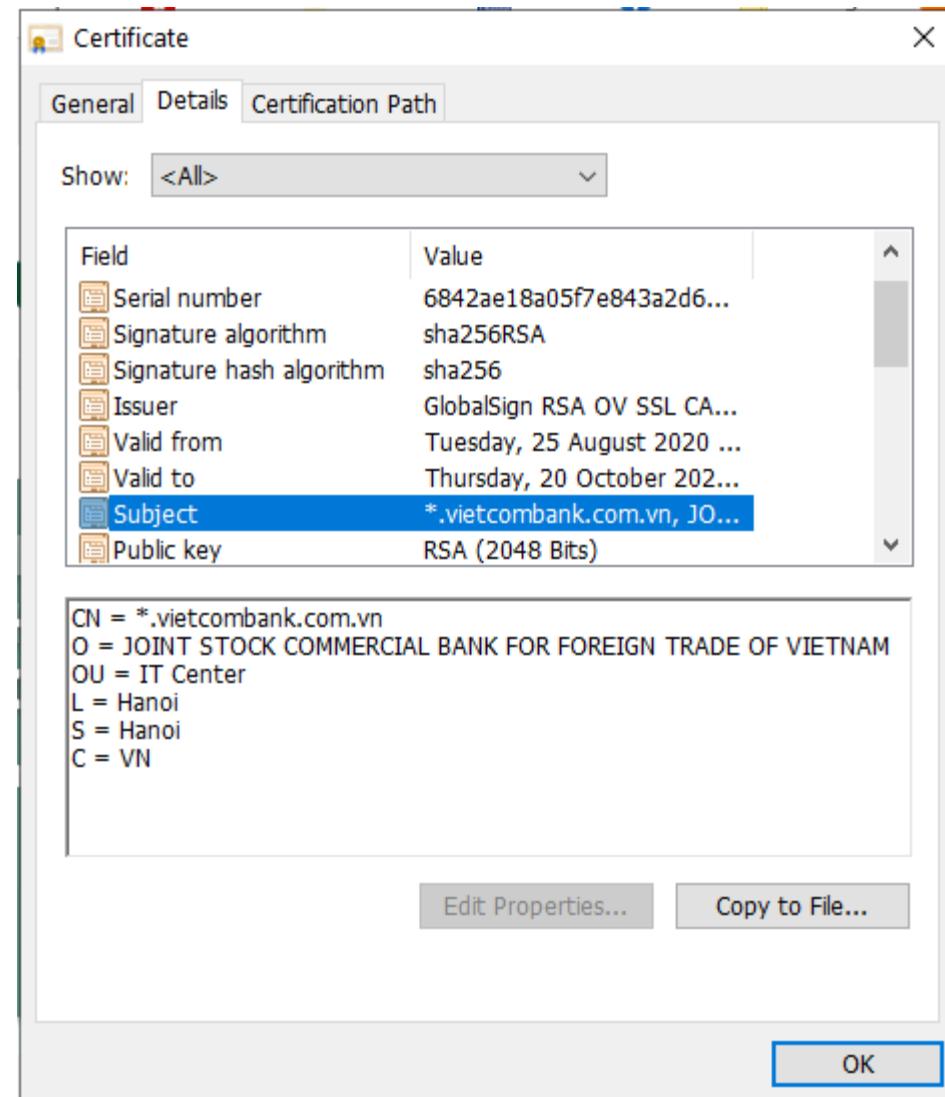
4.4.2 Chứng chỉ số - Giới thiệu

- ❖ Chứng chỉ số (Digital certificate), còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một **chữ ký số** để liên kết một **khóa công khai** và **thông tin nhận dạng** của một thực thể:
 - Chữ ký số: là chữ ký của một bên thứ 3 tin cậy, thường gọi là CA – Certificate Authority;
 - Khóa công khai: là khóa công khai trong cặp khóa công khai của thực thể;
 - Thông tin nhận dạng: là tên, địa chỉ, tên miền hoặc các thông tin định danh của thực thể.
- ❖ Chứng chỉ số có thể được sử dụng để xác minh chủ thể thực sự của một khóa công khai.

4.4.2 Chứng chỉ số - Nội dung



4.4.2 Chứng chỉ số - Nội dung



4.4.2 Chứng chỉ số - Nội dung

❖ Chứng chỉ số gồm các trường chính sau:

- Serial Number: Số nhận dạng của chứng chỉ số;
- Subject: Thông tin nhận dạng một cá nhân hoặc một tổ chức;
- Signature Algorithm: Giải thuật tạo chữ ký;
- Signature Hash Algorithm: Giải thuật tạo chuỗi băm cho tạo chữ ký;
- Signature: Chữ ký của người/tổ chức cấp chứng chỉ;
- Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;

4.4.2 Chứng chỉ số - Nội dung

❖ Chứng chỉ số gồm các trường chính sau:

- Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;
- Valid-From: Ngày bắt đầu có hiệu lực của chứng chỉ;
- Valid-To: Ngày hết hạn sử dụng chứng chỉ;
- Key-Usage: Mục đích sử dụng khóa (chữ ký số, mã hóa,...);
- Public Key: Khóa công khai của chủ thẻ;
- Thumbprint Algorithm: Giải thuật hash sử dụng để tạo chuỗi băm cho khóa công khai;
- Thumbprint: Chuỗi băm tạo từ khóa công khai;

4.4.2 Chứng chỉ số - Nội dung

❖ Nội dung của trường Subject:

- CN (Common Name): Tên chung, nhưng một tên miền được gán chứng chỉ;
- OU (Organisation Unit): Tên bộ phận/phòng ban;
- O (Organisation): Tổ chức/Cơ quan/công ty;
- L (Location): Địa điểm/Quận huyện;
- S (State/Province): Bang/Tỉnh/Thành phố;
- C (Country): Đất nước.

4.4.2 Chứng chỉ số - Sử dụng

❖ Đảm bảo an toàn cho giao dịch trên nền web:

- Dùng chứng chỉ số cho phép website chạy trên SSL (tối thiểu máy chủ phải có chứng chỉ số): HTTP → HTTPS: toàn bộ thông tin chuyển giữa server và client được đảm bảo tính bí mật (sử dụng mã hóa khóa đối xứng), toàn vẹn và xác thực (sử dụng hàm băm có khóa MAC/HMAC);
- Chứng chỉ số để các bên xác thực thông tin nhận dạng của nhau.

❖ Chứng chỉ số có thể được sử dụng cho nhiều ứng dụng:

- Email;
- FTP;
- Các ứng dụng khác.

4.4.3 Hạ tầng khóa công khai - PKI

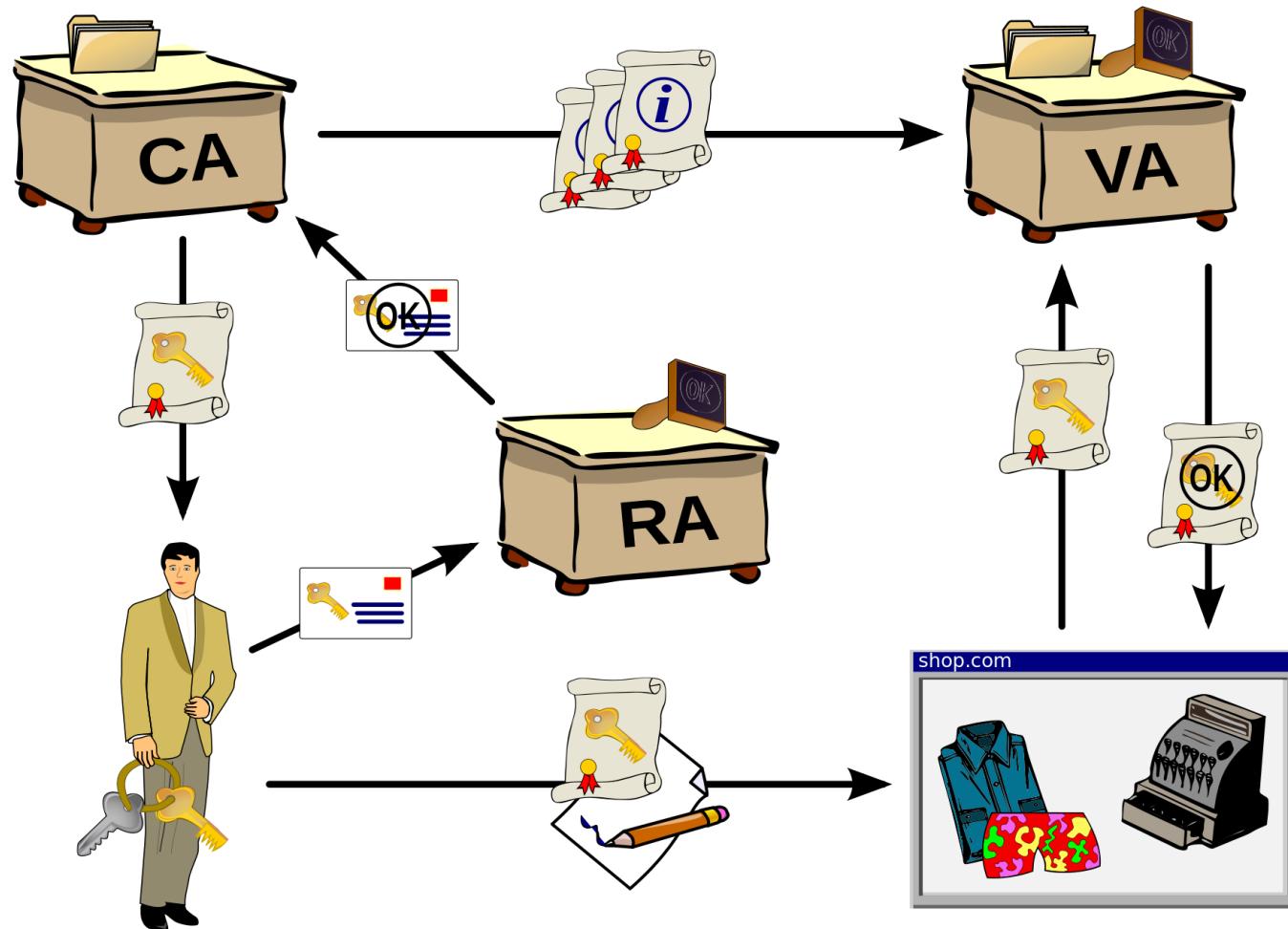
- ❖ Hạ tầng khóa công khai (Public-key infrastructure - PKI) là một tập các phần cứng, phần mềm, nhân lực, chính sách và các thủ tục để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số;

4.4.3 Hạ tầng khóa công khai - PKI

❖ Một PKI gồm:

- Certificate Authority (CA): Cơ quan cấp và kiểm tra chứng chỉ số;
- Registration Authority (RA): Bộ phận kiểm tra thông tin nhận dạng của người dùng theo yêu cầu của CA;
- Validation Authority (VA): Cơ quan xác nhận thông tin nhận dạng của người dùng thay mặt CA;
- Central Directory (CD): Là nơi lưu danh mục và lập chỉ số các khóa;
- Certificate Management System: Hệ thống quản lý chứng chỉ;
- Certificate Policy: Chính sách về chứng chỉ;

4.4.3 Hạ tầng khóa công khai – Lưu đồ cấp và sử dụng



4.5 Các giao thức đảm bảo ATTT dựa trên mã hóa

❖ Các giao thức phổ biến đảm bảo an toàn thông tin dựa trên mã hóa gồm:

- SSL/TLS (Secure Socket Layer/Transport Layer Security)
- SET (Secure Electronic Transactions)
- PGP (Pretty Good Privacy)
- IPSec (IP Security)
- SSH (Secure Shell)

4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

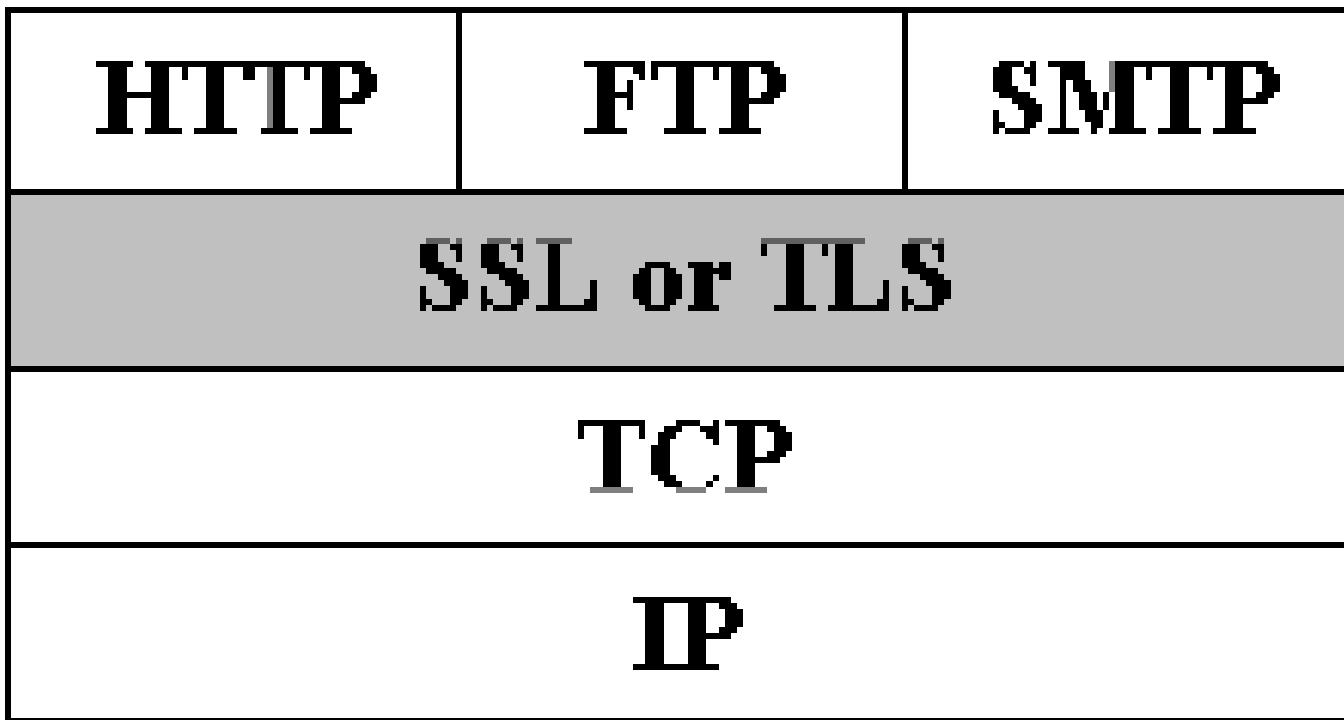
- ❖ SSL do công ty Netscape phát minh năm 1993;
 - Các phiên bản 1.0 (1993), 2.0 (1995) và 3.0 (1996);
 - SSL hiện ít được sử dụng do có nhiều lỗi và không được cập nhật.
- ❖ TLS được xây dựng vào năm 1999 dựa trên SSL 3.0 và do IETF phê chuẩn.
 - Các phiên bản của TLS: 1.0 (1999), 1.1 (2005), 1.2 (2008), 1.3 (2015 –draft).

4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

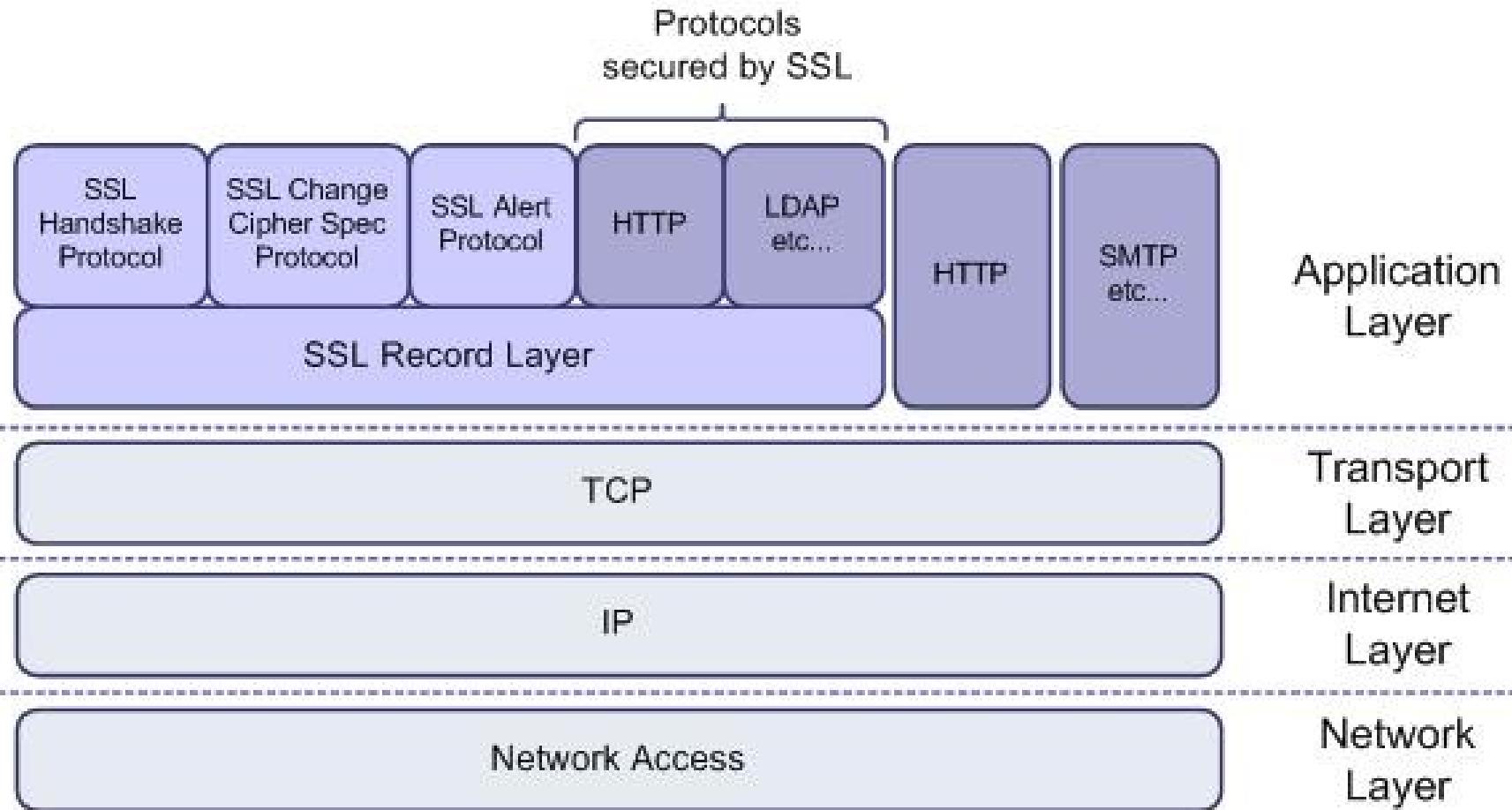
❖ Đặc điểm của SSL/TLS:

- Sử dụng mã hoá khoá công khai để trao đổi khoá phiên. Mỗi khoá phiên chỉ được sử dụng trong 1 phiên làm việc.
- Sử dụng khoá phiên và mã hoá khoá bí mật để mã hoá toàn bộ dữ liệu trao đổi.
- Sử dụng hàm băm có khóa (MAC) để đảm bảo tính toàn vẹn và xác thực thông điệp.
- Ít nhất một thực thể (thường là server) phải có chứng chỉ số cho khoá công khai (Public key certificate).

4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS



4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS



4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

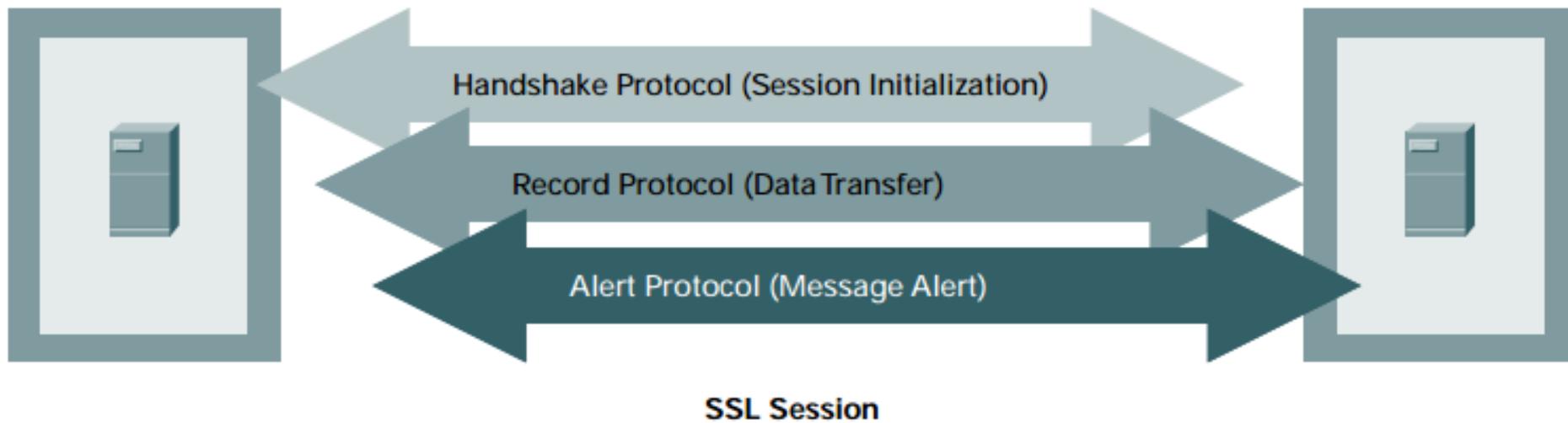
❖ Các giao thức con của SSL:

- SSL Handshake Protocol: Giao thức bắt tay của SSL. Có nhiệm vụ trao đổi các thông điệp xác thực thực thể và thiết lập các thông số cho phiên làm việc;
- SSL Change Cipher Spec Protocol: Giao thức thiết lập việc sử dụng các bộ mã hóa được hỗ trợ bởi cả 2 bên truyền thông;
- SSL Alert Protocol: Giao thức cảnh báo của SSL
- SSL Record Protocol: Giao thức truyền các bản ghi của SSL có nhiệm vụ tạo đường hầm an toàn để chuyển thông tin đảm bảo tín bí mật, toàn vẹn và xác thực.

4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

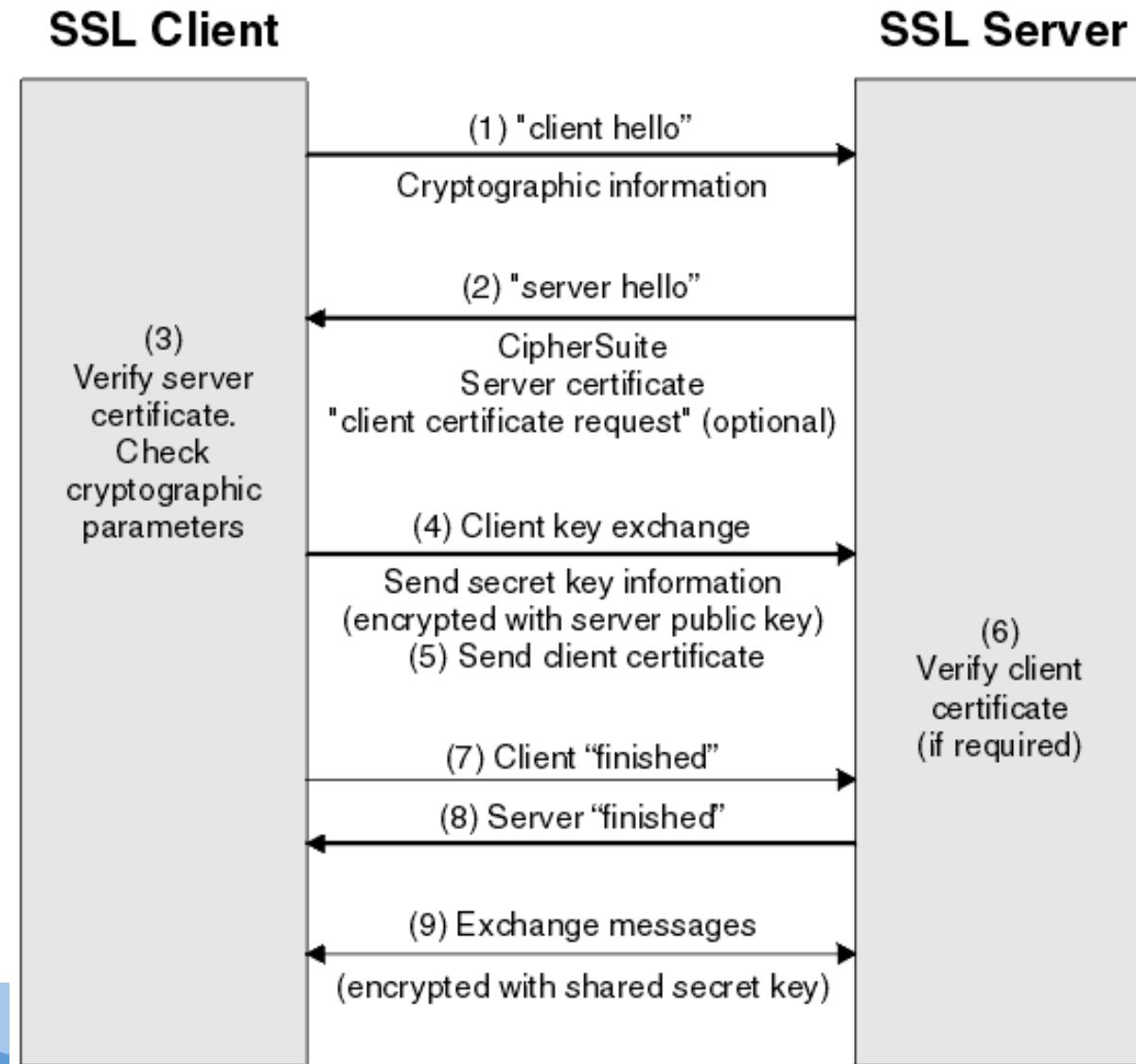
Browser

Web Server



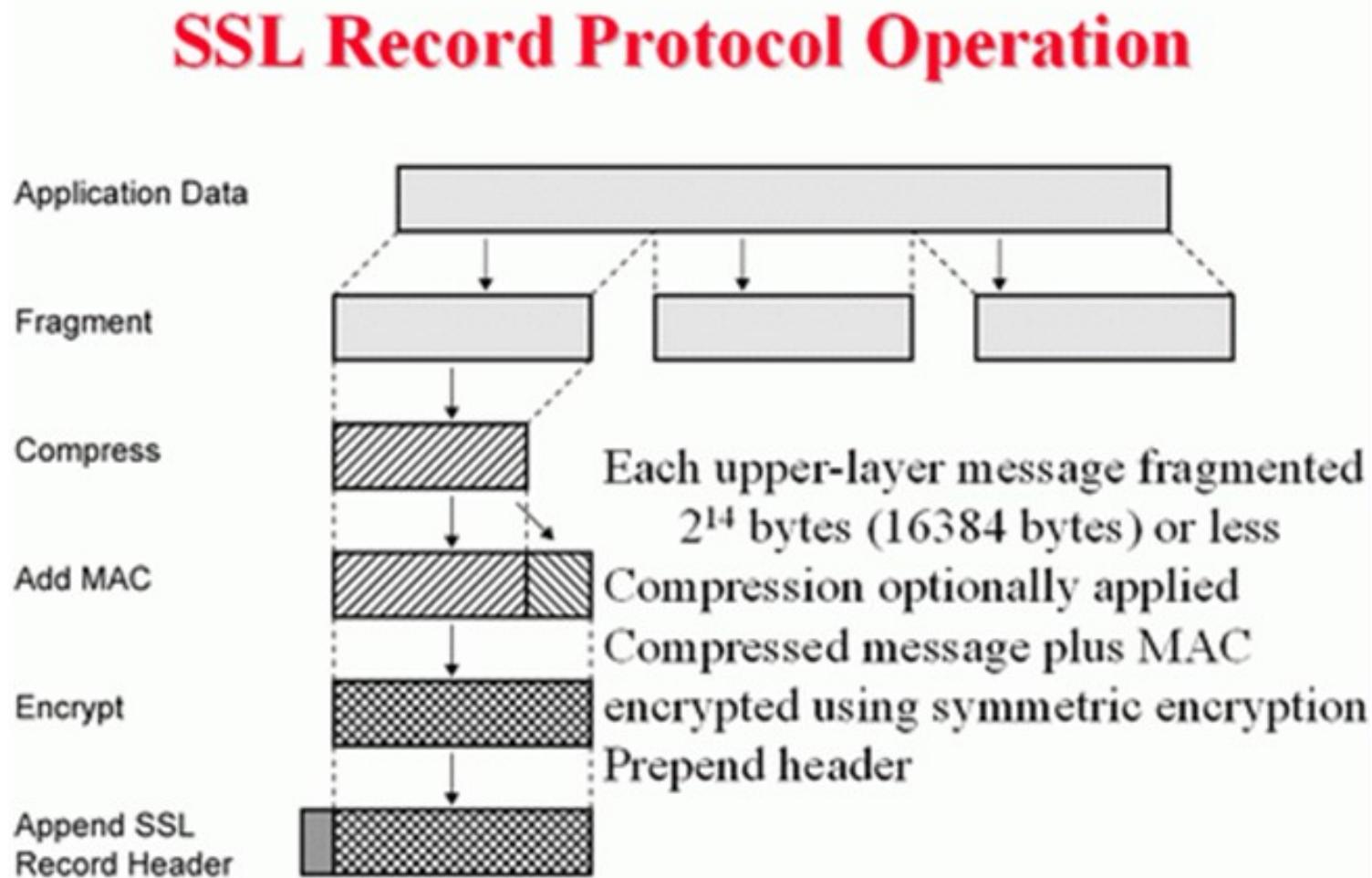
4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

❖ SSL
Handshake
Protocol:



4.5.1 Các giao thức đảm bảo ATTT – SSL/TLS

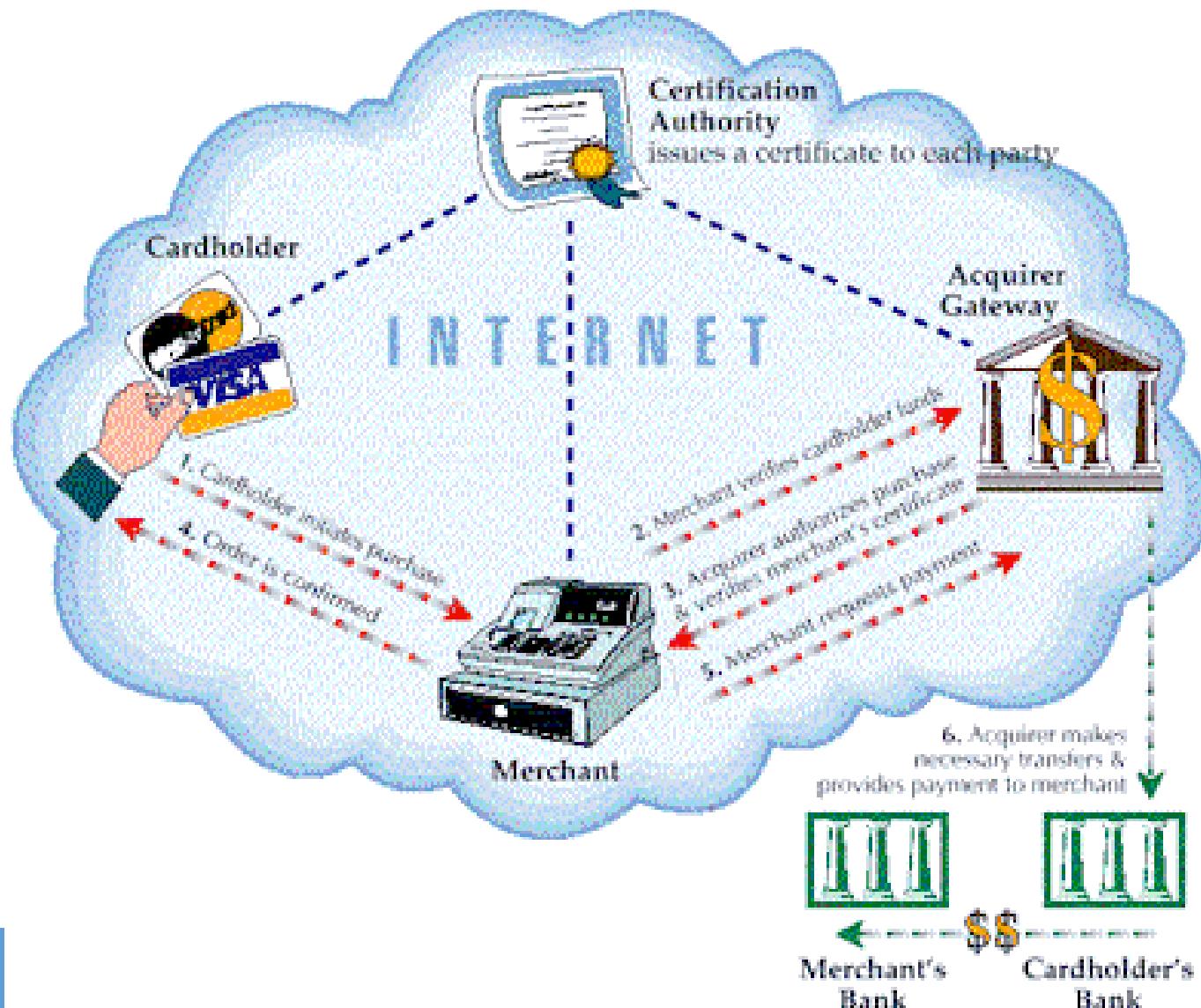
- ❖ Hoạt động của SSL:



4.5.2 Các giao thức đảm bảo ATTT – SET

- ❖ SET là giao thức cho phép thanh toán điện tử an toàn sử dụng thẻ tín dụng do 2 công ty Visa International và MasterCard phát triển;
- ❖ SET có khả năng đảm bảo các thuộc tính sau của thông tin truyền:
 - Bí mật thông tin
 - Toàn vẹn thông tin
 - Xác thực tài khoản chủ thẻ
 - Xác thực nhà cung cấp

4.5.2 Các giao thức đảm bảo ATTT – SET



4.5.3 Các giao thức đảm bảo ATTT – PGP

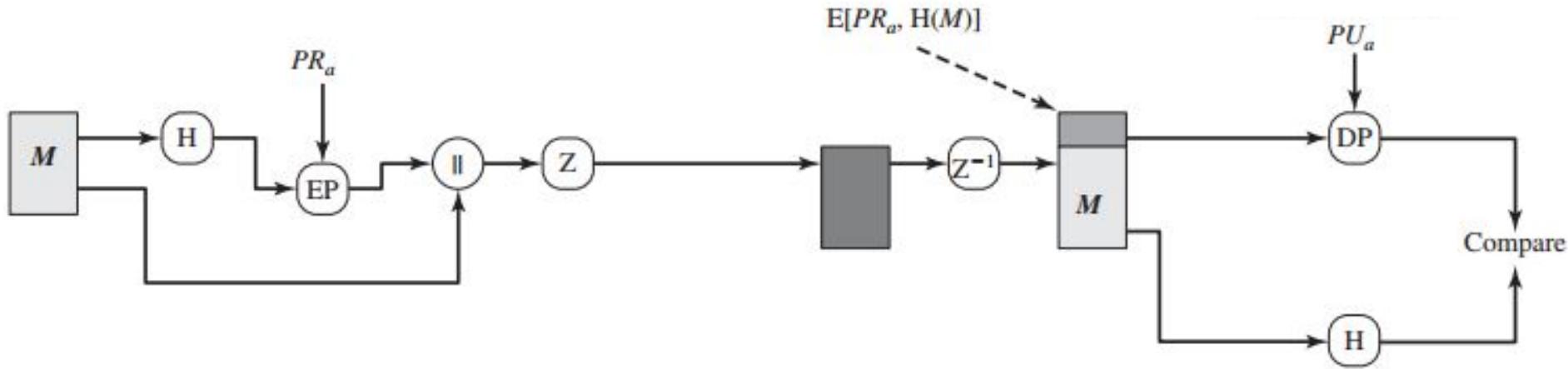
- ❖ PGP do Philip Zimmermann phát triển năm 1991:
 - Cung cấp tính riêng tư
 - Cung cấp tính xác thực
- ❖ PGP được sử dụng rộng rãi và đã được thừa nhận thành chuẩn (RFC 3156).
- ❖ PGP cho phép:
 - Mã hoá dữ liệu sử dụng mã hoá khoá bí mật và khoá công khai
 - Tạo và kiểm tra chữ ký điện tử.

4.5.3 Các giao thức đảm bảo ATTT – PGP

Bên gửi

=====>

Bên nhận



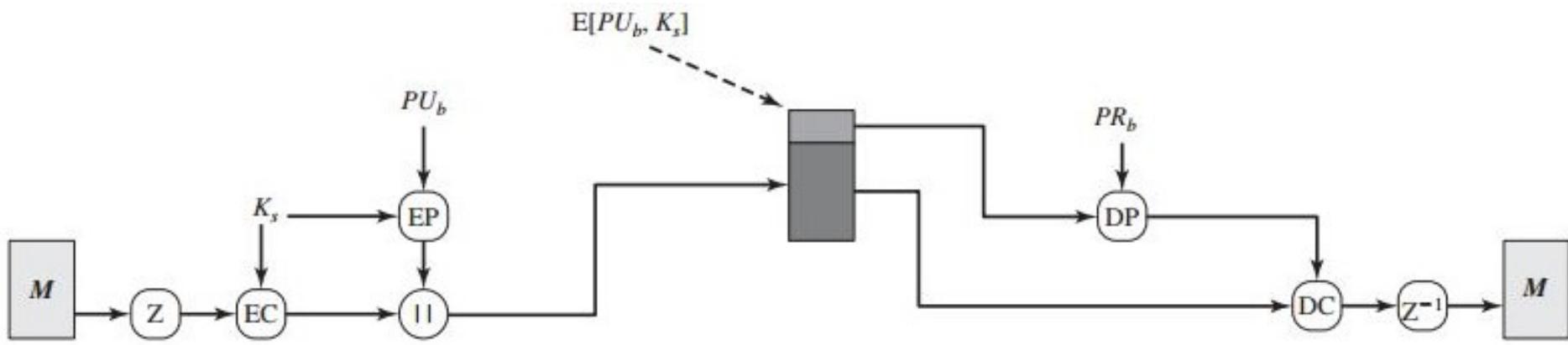
Mô hình PGP chỉ đảm bảo tính xác thực thông điệp

4.5.3 Các giao thức đảm bảo ATTT – PGP

Bên gửi

=====>

Bên nhận



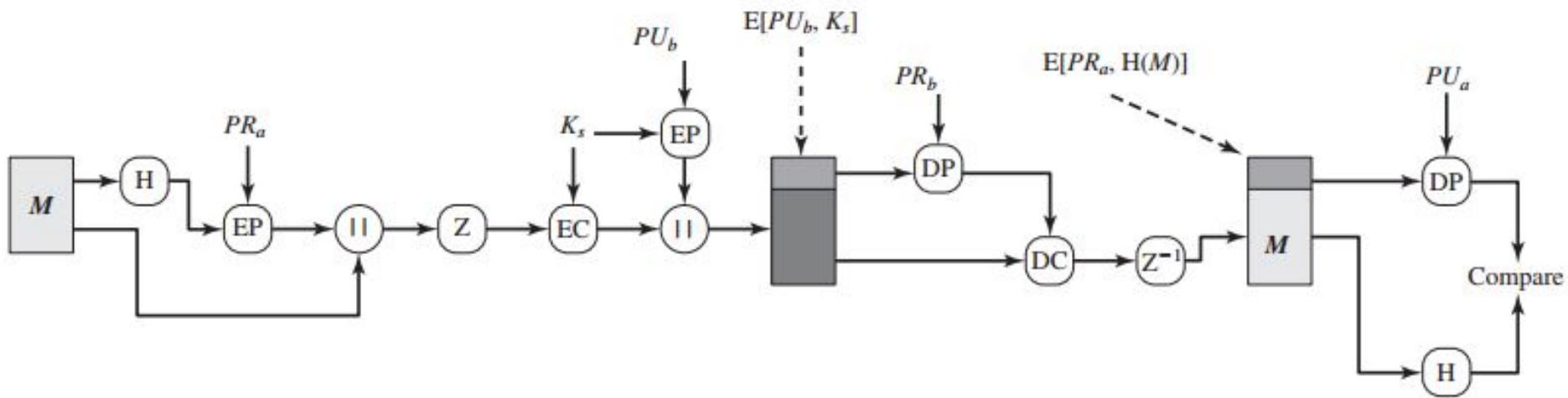
Mô hình PGP chỉ đảm bảo tính bí mật thông điệp

4.5.3 Các giao thức đảm bảo ATTT – PGP

Bên gửi

=====>

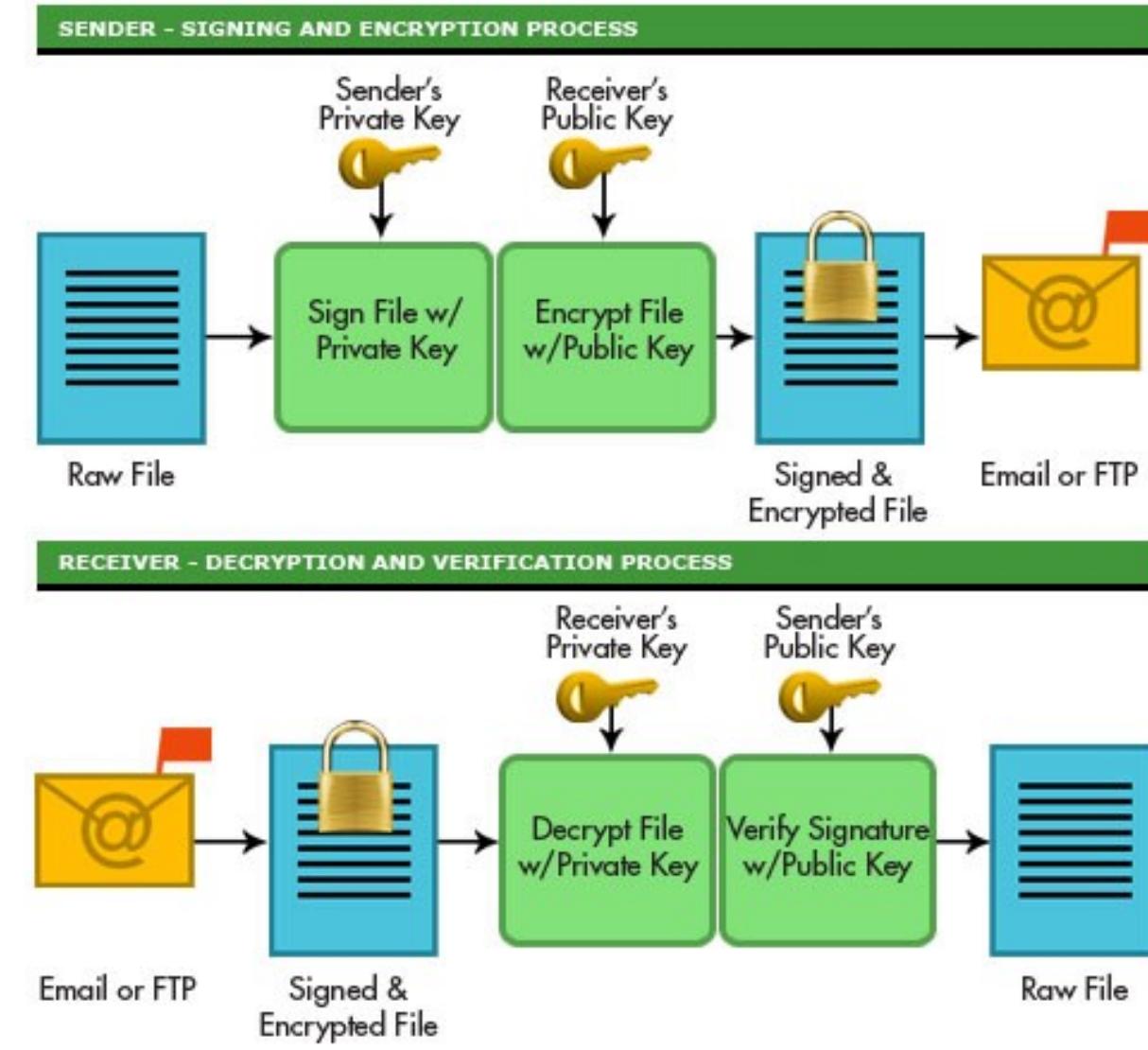
Bên nhận



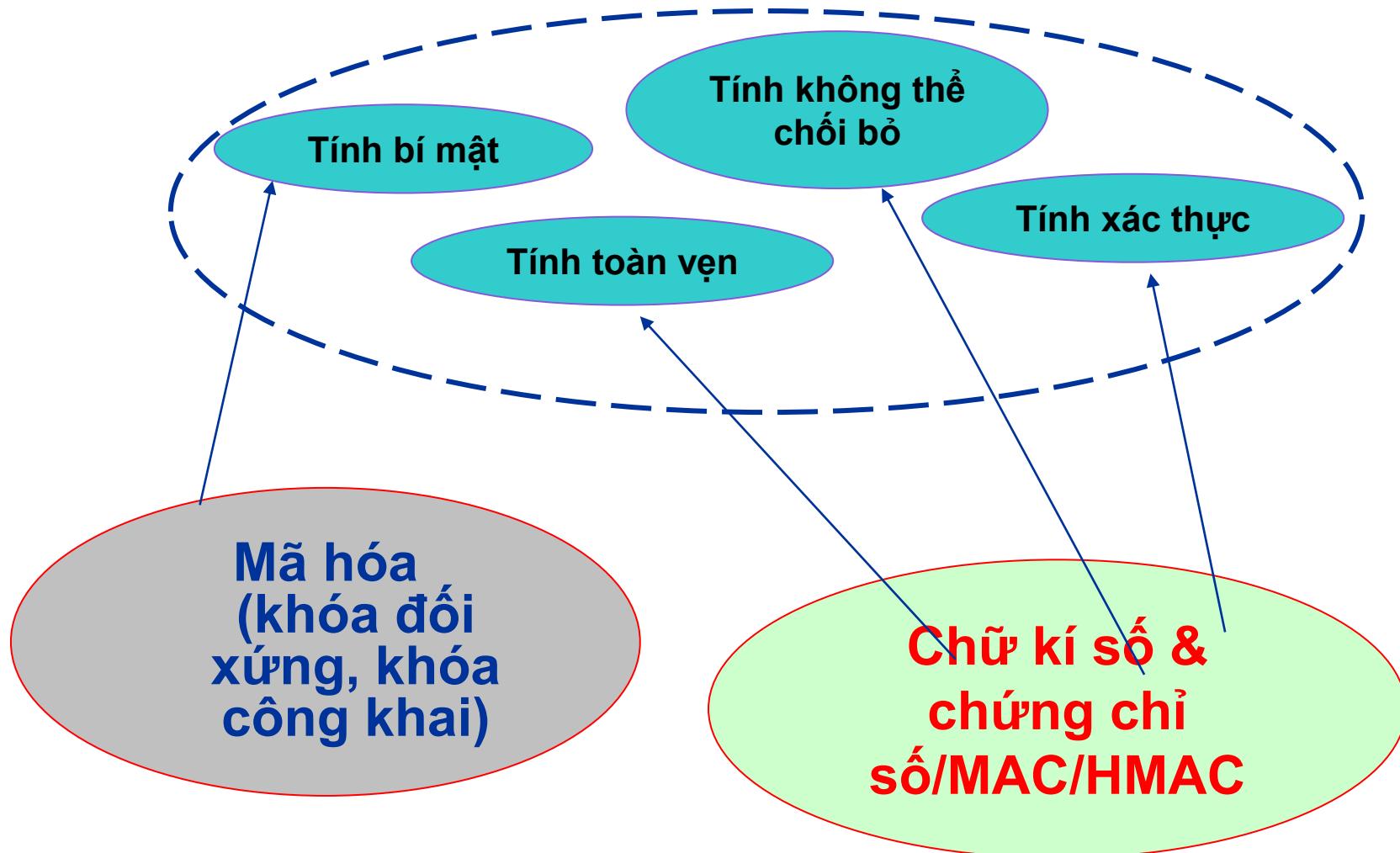
Mô hình PGP đảm bảo tính bí mật và xác thực thông điệp

4.5.3 Các giao thức đảm bảo ATTT – PGP

Mô hình trao đổi file đảm bảo tính bí mật và toàn vẹn sử dụng mã hóa khóa công khai và chữ ký số



Tổng kết các PP đảm bảo ATTT dựa trên mã hóa





HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN**

**CHƯƠNG 5 – CÁC KỸ THUẬT &
CÔNG NGHỆ ĐẢM BẢO ATTT**

Giảng viên:

PGS.TS. Hoàng Xuân Dậu

E-mail:

dauhx@ptit.edu.vn

Khoa:

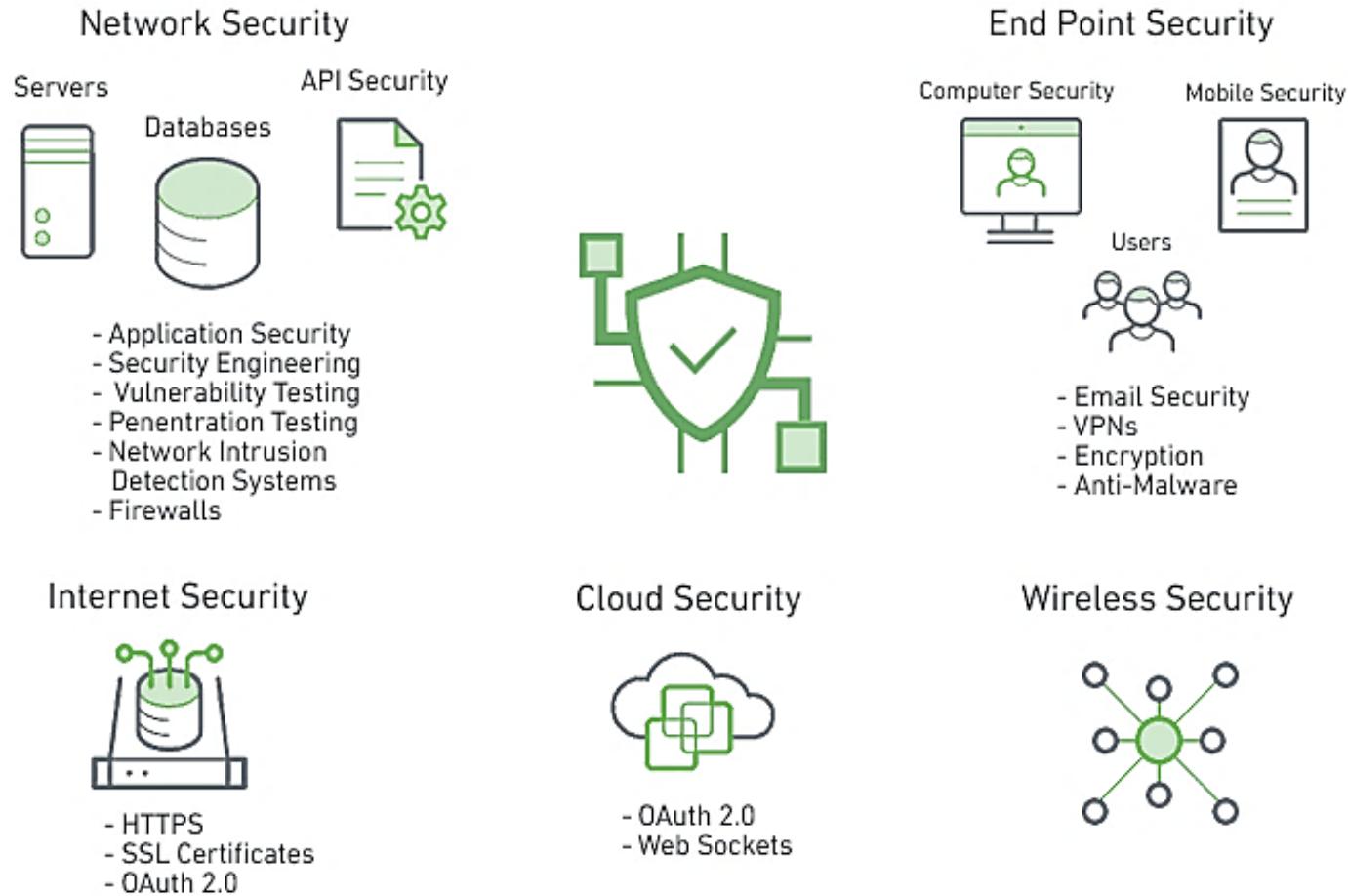
An toàn thông tin

NỘI DUNG CHƯƠNG 5

1. Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT
2. Kiểm soát truy cập
3. Tường lửa
4. IDS và IPS

5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

Các kỹ thuật và công nghệ đảm bảo an toàn cho thông tin, hệ thống và mạng trong các lĩnh vực khác nhau của ATTT



5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

❖ Các miền/lĩnh vực khác nhau của ATTT:

- An ninh mạng (Network Security)
- An ninh thiết bị đầu cuối (End Point Security)
- An ninh Internet (Internet Security)
- An ninh đám mây (Cloud Security)
- An ninh mạng không dây (Wireless Security)

5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

❖ Lĩnh vực an ninh mạng (Network Security) gồm:

- An toàn ứng dụng (Application Security)
- Kỹ nghệ an toàn (Security Engineering)
- Kiểm thử lỗ hổng (Vulnerability Testing)
- Kiểm thử xâm nhập (Penetration Testing)
- Các hệ thống phát hiện xâm nhập mạng (Network Intrusion Detection Systems)
- Tường lửa (Firewalls).

5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

- ❖ Lĩnh vực an ninh thiết bị đầu cuối (End Point Security) gồm:
 - Kiểm soát truy cập
 - Bảo mật email (Email Security)
 - Mạng VPNs
 - Mã hóa (Encryption)
 - Quét và ngăn chặn phần mềm độc hại (Anti-Malware).

5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

❖ Lĩnh vực an ninh Internet (Internet Security) gồm:

- Secure HTTP (HTTPS)
- Chứng chỉ SSL (SSL Certificate)
- Chuẩn xác thực mở (OAuth 2.0).

5.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT

- ❖ Lĩnh vực an ninh đám mây (Cloud Security) gồm:
 - Chuẩn xác thực mở (OAuth 2.0)
 - Web Sockets.
- ❖ Lĩnh vực an ninh mạng không dây (Wireless Security) gồm:
 - Mã hóa (Encryption)
 - Kiểm soát truy cập.

5.2 Kiểm soát truy cập

1. Khái niệm kiểm soát truy cập
2. Các biện pháp kiểm soát truy cập
3. Một số công nghệ kiểm soát truy cập

5.2.1 Khái niệm kiểm soát truy cập

- ❖ Kiểm soát truy cập là quá trình mà trong đó người dùng được *nhận dạng* và *trao quyền* truy cập đến các thông tin, các hệ thống và tài nguyên.



ACCESS CONTROL

5.2.1 Khái niệm kiểm soát truy cập

- ❖ Một hệ thống kiểm soát truy cập có thể được cấu thành từ 3 dịch vụ:
 - Xác thực (Authentication):
 - Là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp.
 - Trao quyền (Authorization):
 - Trao quyền xác định các tài nguyên mà người dùng được phép truy cập sau khi người dùng đã được xác thực.
 - Quản trị (Administration):
 - Cung cấp khả năng thêm, bớt và sửa đổi các thông tin tài khoản người dùng, cũng như quyền truy cập của người dùng.
- ❖ Trong 3 dịch vụ trên, 2 dịch vụ thiết yếu của một hệ thống kiểm soát truy cập là xác thực và trao quyền.

5.2.1 Khái niệm kiểm soát truy cập

- ❖ Mục đích chính của kiểm soát truy cập là để đảm bảo tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và các tài nguyên:
 - Tính bí mật (Confidentiality): đảm bảo chỉ những người có thẩm quyền mới có khả năng truy cập vào dữ liệu và hệ thống.
 - Tính toàn vẹn (Integrity): đảm bảo dữ liệu không bị sửa đổi bởi các bên không có đủ thẩm quyền.
 - Tính sẵn dùng: đảm bảo tính sẵn sàng (đáp ứng nhanh/kịp thời) của dịch vụ cung cấp cho người dùng thực sự.

5.2.2 Các biện pháp kiểm soát truy cập

- ❖ Kiểm soát truy cập tuỳ chọn –
Discretionary Access Control (DAC)
- ❖ Kiểm soát truy cập bắt buộc –
Mandatory Access Control (MAC)
- ❖ Kiểm soát truy cập dựa trên vai trò –
Role-Based Access Control (RBAC)
- ❖ Kiểm soát truy cập dựa trên luật –
Rule-Based Access Control.

5.2.2 Các biện pháp kiểm soát truy cập - DAC

- ❖ Kiểm soát truy cập tuỳ chọn được định nghĩa là các cơ chế hạn chế truy cập đến các đối tượng dựa trên thông tin nhận dạng của các chủ thẻ và/hoặc nhóm của các chủ thẻ.
- ❖ Thông tin nhận dạng có thể gồm:
 - Bạn là ai? (CMND, bằng lái xe, vân tay,...)
 - Những cái bạn biết (tên truy cập, mật khẩu, số PIN...)
 - Bạn có gì? (Thẻ ATM, thẻ tín dụng, ...)

5.2.2 Các biện pháp kiểm soát truy cập - DAC

- ❖ DAC cho phép người dùng có thể cấp hoặc huỷ quyền truy cập cho các người dùng khác đến các đối tượng thuộc quyền điều khiển của họ.
- ❖ Chủ sở hữu của các đối tượng (owner of objects) là người dùng có toàn quyền điều khiển các đối tượng này.

5.2.2 Các biện pháp kiểm soát truy cập - DAC

❖ Ví dụ: Với DAC:

- Người dùng được cấp 1 thư mục riêng và là chủ sở hữu của thư mục này;
- Người dùng có quyền tạo, sửa đổi và xoá các files trong thư mục của riêng mình (home directory);
- Họ cũng có khả năng trao hoặc huỷ quyền truy cập vào các files của mình cho các người dùng khác.

5.2.2 Các biện pháp kiểm soát truy cập - DAC

❖ Hai kỹ thuật được sử dụng phổ biến để cài đặt DAC:

- Ma trận kiểm soát truy cập (Access Control Matrix - ACM);
- Danh sách kiểm soát truy cập (Access Control List - ACL).

5.2.2 Các biện pháp kiểm soát truy cập – DAC - ACM

- ❖ Ma trận kiểm soát truy cập (Access Control Matrix - ACM) là một phương pháp mô tả kiểm soát truy cập thông qua 1 ma trận 2 chiều gồm chủ thể (subject), đối tượng (object) và các quyền truy cập.
 - Đối tượng/Khách thě (Objects) là các thực thě cần bảo vệ. Objects có thể là các files, các tiến trình (processes).
 - Chủ thě (Subjects) là người dùng (users), tiến trình tác động lên objects.
 - Quyền truy cập là hành động mà Subject thực hiện trên Object.

5.2.2 Các biện pháp kiểm soát truy cập – DAC - ACM

Objects \ Subjects	O1	O2	O3	O4
S1	rw	rwxo	r	rwxo
S2	rw	rx	rw	rwx
S3	r	rw	rwo	rw

Các chủ thể: S1, S2, S3

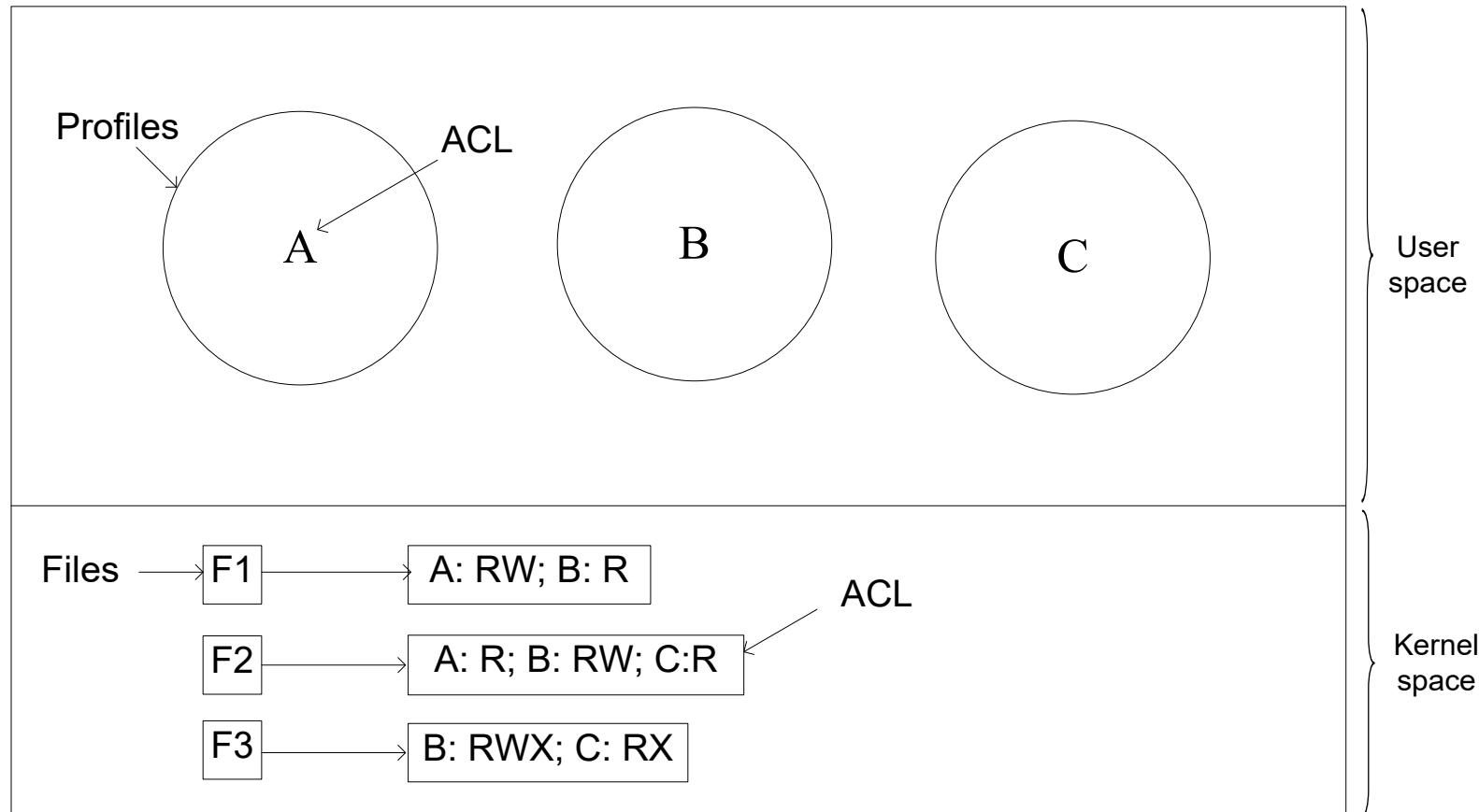
Các đối tượng: O1, O2, O3

Các quyền: r(read), w(write), x(execute) và o(own)

5.2.2 Các biện pháp kiểm soát truy cập – DAC - ACL

- ❖ Danh sách kiểm soát truy cập (Access Control List - ACL) là một danh sách các quyền truy cập của một chủ thể đối với một đối tượng.
 - Một ACL chỉ ra các người dùng hoặc tiến trình được truy cập vào đối tượng nào và các thao tác cụ thể (quyền) được thực hiện trên đối tượng đó.
 - Một bản ghi điển hình của ACL có dạng (subject, operation). Ví dụ bản ghi (Alice, write) của 1 file có nghĩa là Alice có quyền ghi vào file đó.
 - Khi chủ thể yêu cầu truy cập, hệ điều hành sẽ kiểm tra ACL xem yêu cầu đó có được phép hay không.
 - ACL có thể được áp dụng cho một hoặc 1 nhóm đối tượng.

5.2.2 Các biện pháp kiểm soát truy cập – DAC - ACL



Sử dụng ACL để quản lý việc truy cập file

5.2.2 Các biện pháp kiểm soát truy cập - MAC

- ❖ Điều khiển truy bắt buộc được định nghĩa là các cơ chế hạn chế truy cập đến các đối tượng dựa trên
 - Tính nhạy cảm (sensitivity) của thông tin (thường được gán nhãn) chứa trong các đối tượng, và
 - Sự trao quyền chính thức (formal authorization) cho các chủ thể truy cập các thông tin nhạy cảm này.

5.2.2 Các biện pháp kiểm soát truy cập - MAC

❖ Các mức nhạy cảm của thông tin:

- Tối mật (Top Secret - T): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến những thiệt hại trầm trọng đối với an ninh quốc gia.
- Tuyệt mật (Secret - S): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến một loạt thiệt hại đối với an ninh quốc gia.
- Mật (Confidential - C): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến thiệt hại đối với an ninh quốc gia.
- Không phân loại (Unclassified - U): Những thông tin không gây thiệt hại đối với an ninh quốc gia nếu bị tiết lộ.

5.2.2 Các biện pháp kiểm soát truy cập - MAC

- ❖ MAC không cho phép người tạo ra các đối tượng (thông tin/tài nguyên) có toàn quyền truy cập các đối tượng này.
- ❖ Quyền truy cập đến các đối tượng (thông tin/tài nguyên) do người quản trị hệ thống định ra trước trên cơ sở chính sách an toàn thông tin của tổ chức đó.
- ❖ MAC thường được sử dụng phổ biến trong các cơ quan an ninh, quân đội và ngân hàng.

5.2.2 Các biện pháp kiểm soát truy cập - MAC

- ❖ Ví dụ: một tài liệu được tạo ra và được đóng dấu “Mật”:
 - Chỉ những người có trách nhiệm trong tổ chức mới được quyền xem và phổ biến cho người khác;
 - Tác giả của tài liệu không được quyền phổ biến đến người khác.

5.2.2 Các biện pháp kiểm soát truy cập - MAC

❖ Mô hình kiểm soát truy cập Bell-LaPadula:

- Mô hình Bell-LaPadula là mô hình bảo mật đa cấp thường được sử dụng trong quân sự, nhưng nó cũng có thể áp dụng cho các lĩnh vực khác.
- Trong quân sự, các tài liệu được gán một mức độ bảo mật, chẳng hạn như không phân loại, mật, bí mật và tối mật. Người dùng cũng được ấn định các cấp độ bảo mật tương ứng, tùy thuộc vào những tài liệu mà họ được phép xem.
 - Một vị tướng quân đội có thể được phép xem tất cả các tài liệu, trong khi một trung úy có thể bị hạn chế chỉ được xem các tài liệu mật và thấp hơn.
 - Một tiến trình chạy nhân danh một người sử dụng có được mức độ bảo mật của người dùng đó.

5.2.2 Các biện pháp kiểm soát truy cập - MAC

❖ Nguyên tắc bảo mật tài nguyên của mô hình Bell-LaPadula:

▪ Nguyên tắc đọc xuống:

- Một người dùng ở mức độ bảo mật k chỉ có thể đọc các đối tượng ở cùng mức bảo mật hoặc thấp hơn.
- Ví dụ:
 - Một vị tướng có thể đọc các tài liệu của một trung úy;
 - Nhưng một trung úy không thể đọc các tài liệu của vị tướng đó.

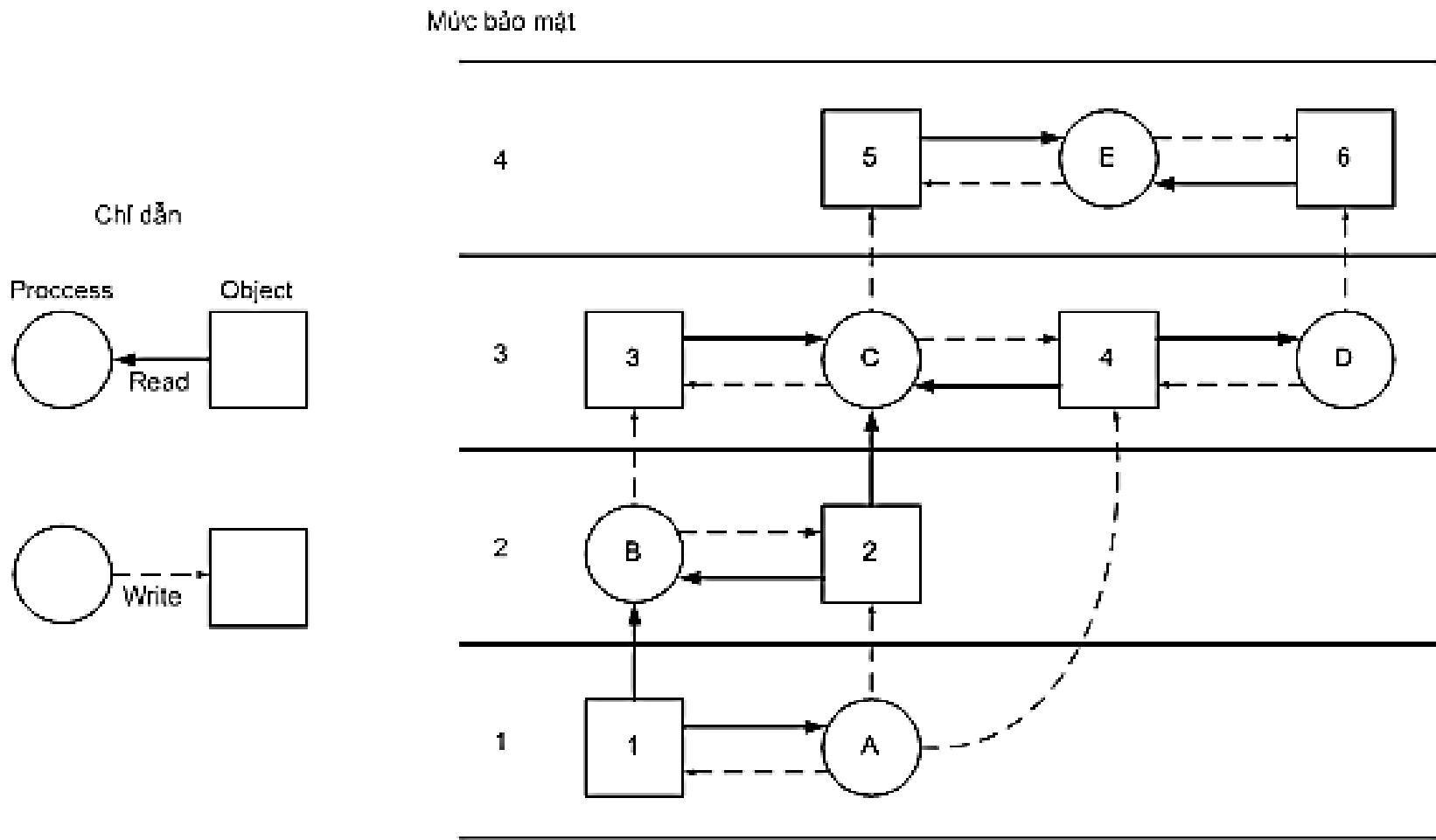
5.2.2 Các biện pháp kiểm soát truy cập - MAC

❖ Nguyên tắc bảo mật tài nguyên của mô hình Bell-LaPadula:

- Nguyên tắc ghi lê:

- Một người dùng ở mức độ bảo mật k chỉ có thể ghi các đối tượng ở cùng mức bảo mật hoặc cao hơn.
- Ví dụ:
 - Một trung úy có thể nối thêm một tin nhắn vào hộp thư của chung về tất cả mọi thứ ông biết;
 - Nhưng một vị tướng không thể ghi thêm một tin nhắn vào hộp thư của trung úy với tất cả mọi thứ ông ấy biết vì vị tướng có thể đã nhìn thấy tài liệu có mức độ bảo mật cao mà không thể được tiết lộ cho một trung úy.

5.2.2 Các biện pháp kiểm soát truy cập - MAC



Mô hình bảo mật đa cấp Bell-LaPadula

5.2.2 Các biện pháp kiểm soát truy cập - RBAC

- ❖ Kiểm soát truy cập dựa trên vai trò cho phép người dùng truy cập vào thông tin và hệ thống dựa trên vai trò (role) của họ trong công ty/tổ chức đó.
- ❖ Kiểm soát truy cập dựa trên vai trò có thể được áp dụng cho một nhóm người dùng hoặc từng người dùng riêng lẻ.
- ❖ Quyền truy cập được tập hợp thành các nhóm “vai trò” với các mức quyền truy cập khác nhau.

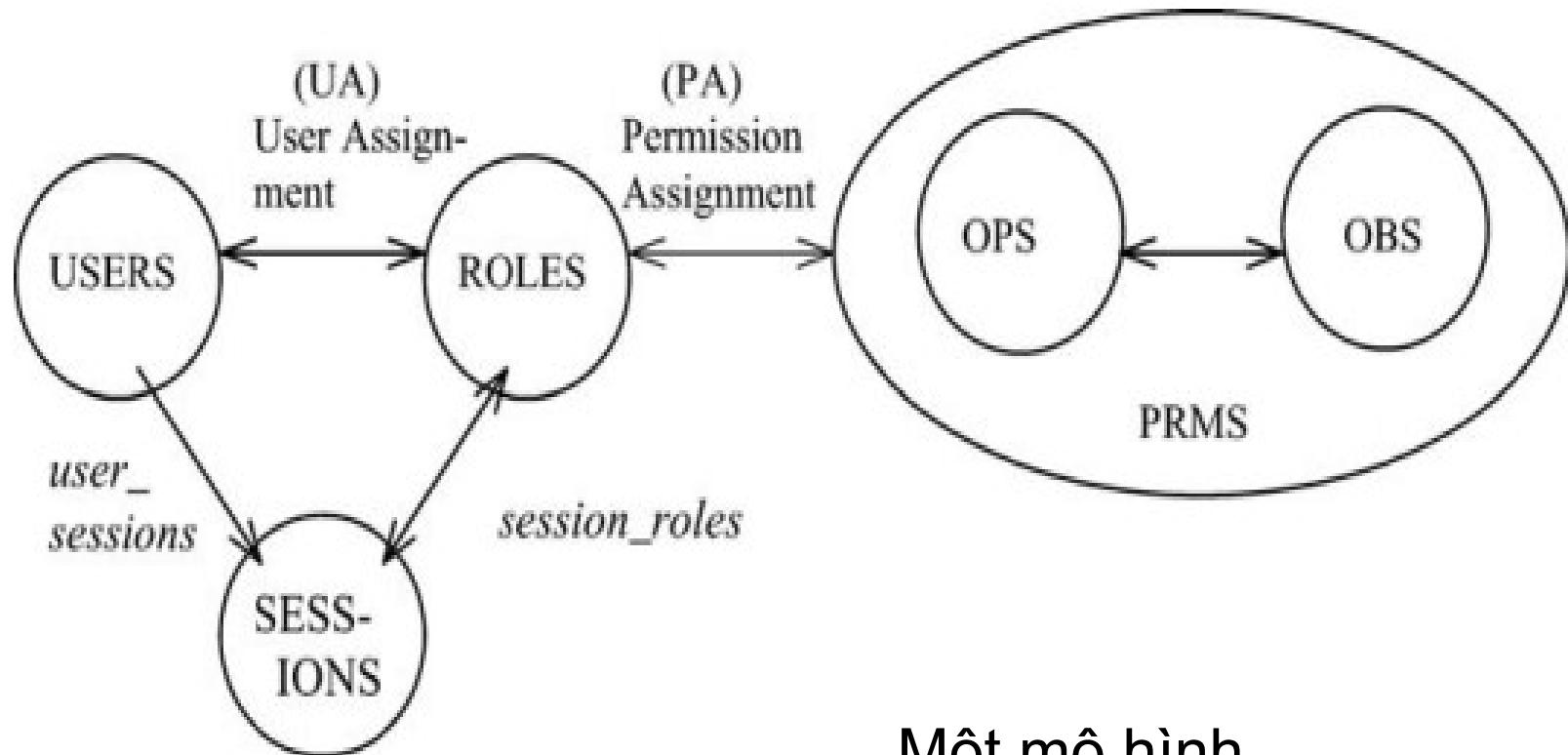
5.2.2 Các biện pháp kiểm soát truy cập - RBAC

- ❖ Ví dụ: một trường học chia người dùng thành các nhóm gán sẵn quyền truy cập vào các phần trong hệ thống:
 - Nhóm Quản lý được quyền truy cập vào tất cả các thông tin trong hệ thống;
 - Nhóm Giáo viên được truy cập vào CSDL các môn học, bài báo khoa học, cập nhật điểm các lớp phụ trách;
 - Nhóm Sinh viên chỉ được quyền xem nội dung các môn học, tải tài liệu học tập và xem điểm của mình.

5.2.2 Các biện pháp kiểm soát truy cập - RBAC

- ❖ Liên kết giữa người dùng và vai trò:
 - Người dùng được cấp “thẻ thành viên” của các nhóm “vai trò” trên cơ sở năng lực và vai trò, cũng như trách nhiệm của họ trong một tổ chức.
- ❖ Trong nhóm “vai trò”, người dùng được cấp vừa đủ quyền để thực hiện các thao tác cần thiết cho công việc được giao.
- ❖ Liên kết giữa người dùng và vai trò có thể được tạo lập và huỷ bỏ dễ dàng.
- ❖ Quản lý phân cấp vai trò: các vai trò được tổ chức thành một cây theo mô hình phân cấp tự nhiên của các công ty/tổ chức.

5.2.2 Các biện pháp kiểm soát truy cập - RBAC



5.2.2 Các biện pháp kiểm soát truy cập – Rule-Based AC

- ❖ Kiểm soát truy cập dựa trên luật cho phép người dùng truy cập vào hệ thống và thông tin dựa trên các luật (rules) đã được định nghĩa trước.
- ❖ Các luật có thể được thiết lập để hệ thống cho phép truy cập đến các tài nguyên của mình cho người dùng thuộc một tên miền, một mạng hay một dải địa chỉ IP.

5.2.2 Các biện pháp kiểm soát truy cập – Rule-Based AC

- ❖ Firewalls/Proxies là ví dụ điển hình về kiểm soát truy cập dựa trên luật;
- ❖ Các hệ thống này sử dụng một tập các luật (rules) để kiểm soát truy cập. Các thông tin sử dụng trong các luật có thể gồm:
 - Địa chỉ IP nguồn và đích của các gói tin;
 - Phần mở rộng các files để lọc các mã độc hại;
 - Địa chỉ IP hoặc các tên miền để lọc/chặn các website bị cấm;
 - Tập các từ khoá để lọc các nội dung bị cấm.

5.2.3 Một số công nghệ kiểm soát truy cập

- ❖ Kiểm soát truy cập dựa trên mật khẩu (password)
- ❖ Kiểm soát truy cập dựa trên các khoá mã (encrypted keys)
- ❖ Kiểm soát truy cập dựa trên thẻ thông minh (smart card)
- ❖ Kiểm soát truy cập dựa trên thẻ bài (token)
- ❖ Kiểm soát truy cập dựa trên các đặc điểm sinh trắc học (biometric).

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên mật khẩu

- ❖ Thông thường mỗi người dùng được cấp 1 tài khoản (account) để truy cập vào hệ thống. Để truy cập tài khoản, thường cần có:
 - Tên người dùng (username), email, số điện thoại,...
 - Mật khẩu (password)
 - Mật khẩu có thể ở dạng nguyên bản (plain text)
 - Mật khẩu có thể ở dạng mã hoá (encrypted text)
 - Các thuật toán thường dùng để mã hoá mật khẩu: MD4, MD5, SHA-1, SHA256,...
 - Mật khẩu có thể được dùng nhiều lần hoặc 1 lần (one time password).

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên mật khẩu

❖ Tính bảo mật của kỹ thuật kiểm soát truy cập sử dụng mật khẩu dựa trên:

- Độ khó đoán của mật khẩu
 - Dùng nhiều loại ký tự
 - Chữ thường, hoa, chữ số, ký tự đặc biệt:
 - » abc1234: mật khẩu tồi
 - » aBc*1#24: mật khẩu tốt (về mặt tính toán)
 - Độ dài của mật khẩu
 - Mật khẩu tốt có chiều dài ≥ 8 ký tự
 - Tuổi thọ của mật khẩu
 - Mật khẩu không hết hạn
 - Mật khẩu có thời hạn sống
 - Mật khẩu dùng 1 lần

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên mật khẩu

❖ Mật khẩu một lần (OTP-One Time Password):

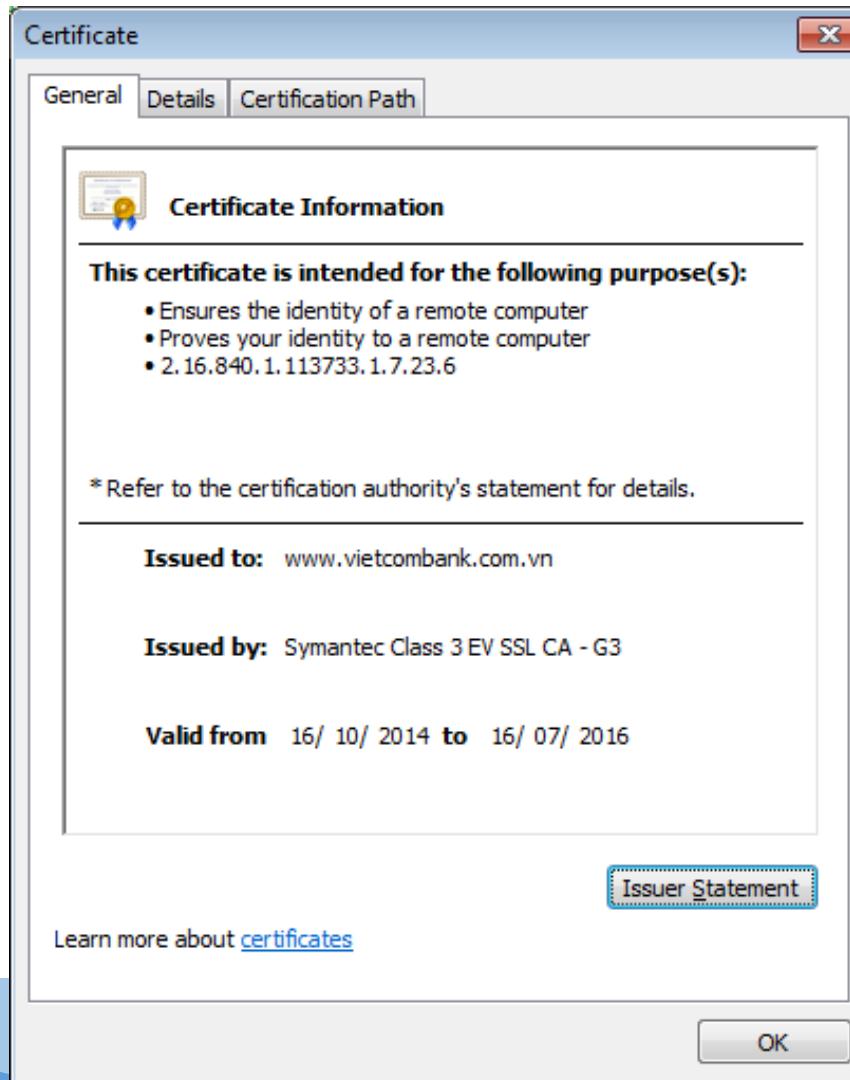
- Mật khẩu được sinh ra và chỉ được dùng 1 lần cho 1 phiên làm việc hoặc 1 giao dịch;
- Mật khẩu thường được sinh ngẫu nhiên
- Chuyển giao OTP:
 - In ra giấy một danh sách mật khẩu để dùng dần
 - Gửi qua các phương tiện khác như SMS
 - Sử dụng các thiết bị chuyên dụng, như các token,...
- Ưu điểm: an toàn hơn, tránh được tấn công kiểu replay (lấy được mật khẩu dùng lại).
- Nhược điểm: người sử dụng khó nhớ mật khẩu.

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các khóa mã

- ❖ Khoá mã là các giải thuật cho phép:
 - Đảm bảo an toàn thông tin bí mật
 - Cho phép kiểm tra thông tin nhận dạng của các bên tham gia giao dịch.
- ❖ Ứng dụng rộng rãi nhất là chứng chỉ số (Digital Certificate). Một chứng chỉ số thường gồm các thuộc tính:
 - Thông tin nhận dạng của chủ thẻ
 - Khoá công khai của chủ thẻ
 - Các thông tin nhận dạng và khoá công khai của chủ thẻ được mã hoá (ký) bởi một tổ chức có thẩm quyền (Certificate Authority – CA).

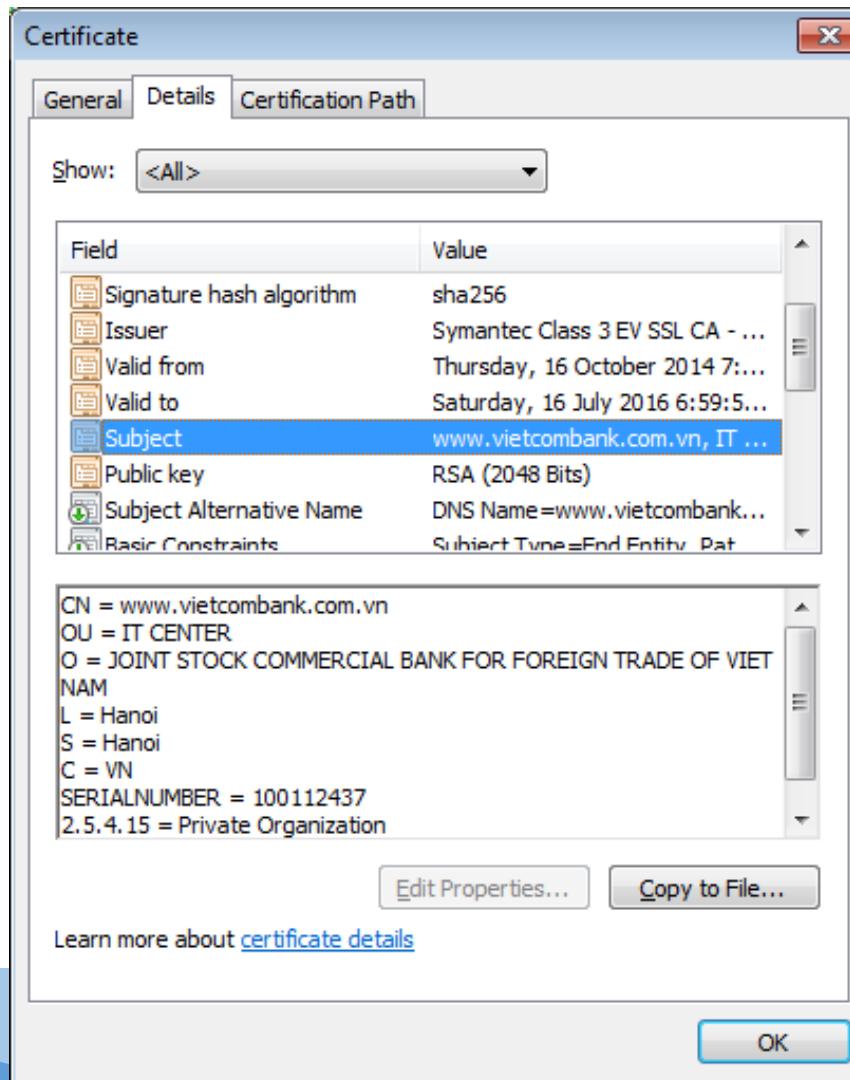
5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các khóa mã

Biểu
diễn
chứng
chỉ số
của
ngân
hàng
VCB



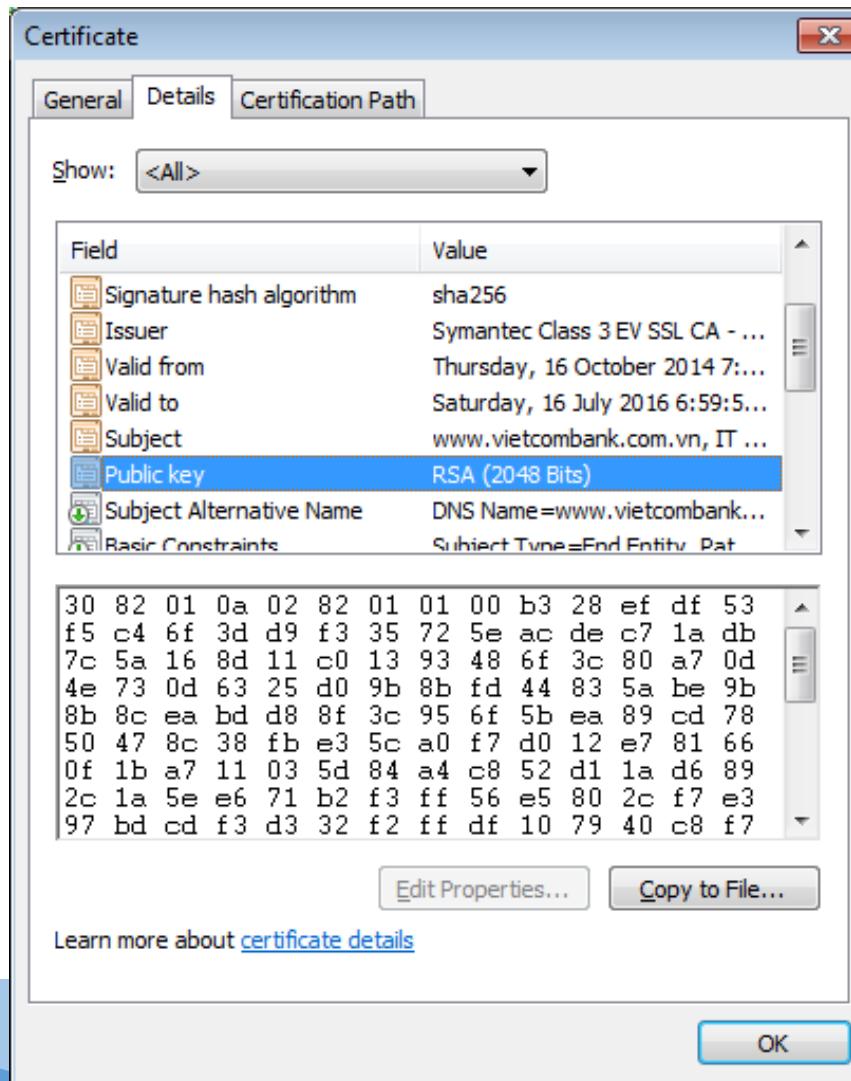
5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các khóa mã

Biểu
diễn
chứng
chỉ số
của
ngân
hàng
VCB



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các khóa mã

Biểu
diễn
chứng
chỉ số
của
ngân
hàng
VCB



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ thông minh

- ❖ Thẻ thông minh (Smartcard) là các thẻ nhựa có gắn các chip điện tử
- ❖ Có khả năng tính toán và các thông tin lưu trong thẻ được mã hoá
- ❖ Smartcard sử dụng hai yếu tố (two-factors) để xác thực và nhận dạng chủ thẻ:
 - Cái bạn có (what you have): thẻ
 - Cái bạn biết (what you know): số PIN

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ thông minh



Một loại thẻ thông minh (thẻ tiếp xúc)

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ thông minh



Một loại thẻ thông minh (thẻ không tiếp xúc)

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ bài (token)

- ❖ Các thẻ bài thường là các thiết bị cầm tay được thiết kế nhỏ gọn để có thể dễ dàng mang theo:
 - Được tích hợp pin cung cấp nguồn nuôi.
- ❖ Thẻ bài có thể được sử dụng để lưu:
 - Mật khẩu
 - Thông tin cá nhân
 - Các thông tin khác

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ bài (token)

- ❖ Thẻ bài thường được trang bị cơ chế xác thực 2 yếu tố tương tự smartcards:
 - Thẻ bài
 - Mật khẩu (thường dùng 1 lần)
- ❖ Thẻ bài thường có cơ chế xác thực mạnh hơn smartcards do năng lực tính toán cao hơn:
 - CPU có năng lực xử lý cao hơn smartcard;
 - Bộ nhớ lưu trữ lớn hơn.

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ bài (token)

Thẻ
bài
(token)
của
hãng
RSA
Security



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



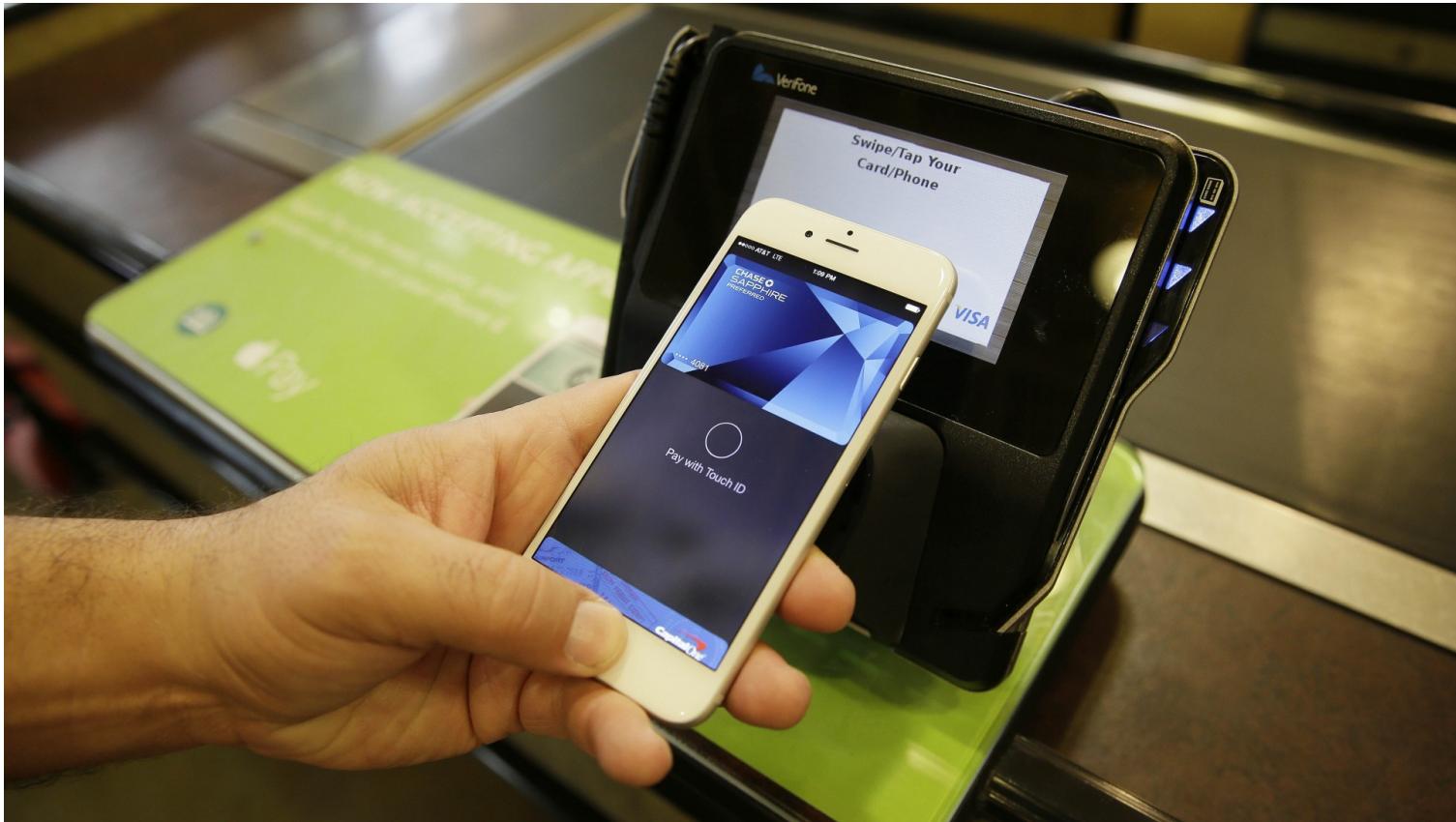
BlackBerry with
RSA SecurID software token

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ bài (token)

Thẻ bài (ví
điện tử)
của PayPal
dùng trong
thanh toán
trực tuyến



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên thẻ bài (token)



Hệ thống ApplePay tích hợp vào điện thoại di động

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh trắc

- ❖ Kiểm soát truy cập có thể sử dụng các đặc điểm sinh trắc học để nhận dạng chủ thẻ:
 - Dấu vân tay
 - Tròng mắt
 - Khuôn mặt
 - Tiếng nói
 - Chữ ký tay

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

❖ Ưu điểm:

- Có khả năng bảo mật cao
- Luôn đi cùng chủ thẻ

❖ Nhược điểm:

- Chi phí đắt
- Chậm do đòi hỏi khôi lượng tính toán lớn
- Tỷ lệ nhận dạng sai tương đối lớn do có nhiều yếu tố nhiễu ảnh hưởng.

5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Khoa
sử
dụng
vân
tay



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Khoá
sử
dụng
vân
tay



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Bộ
phận
đọc
vân tay
trên
laptop



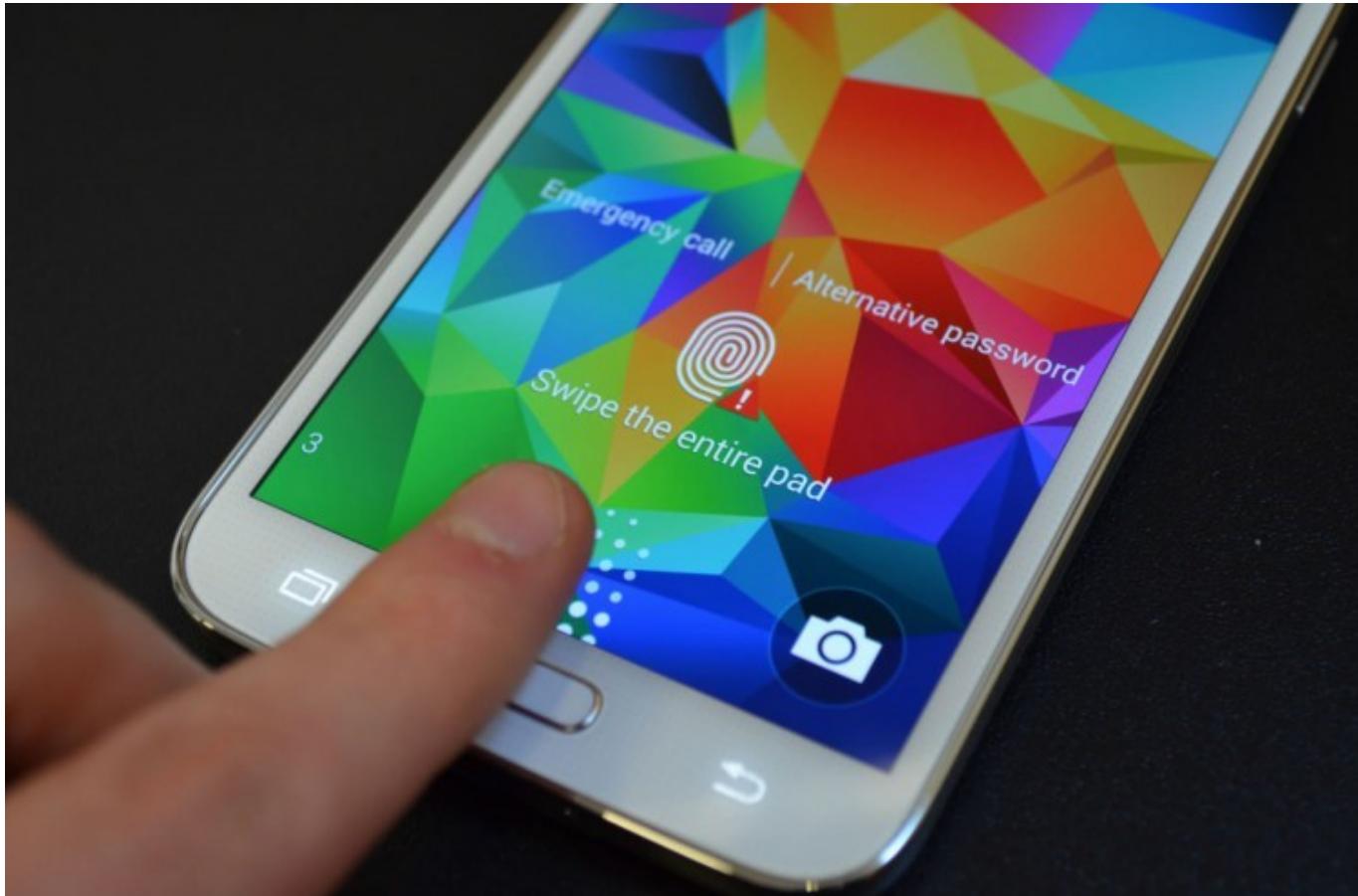
5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Bộ phận
đọc
vân tay
trên
điện thoại
iPhone



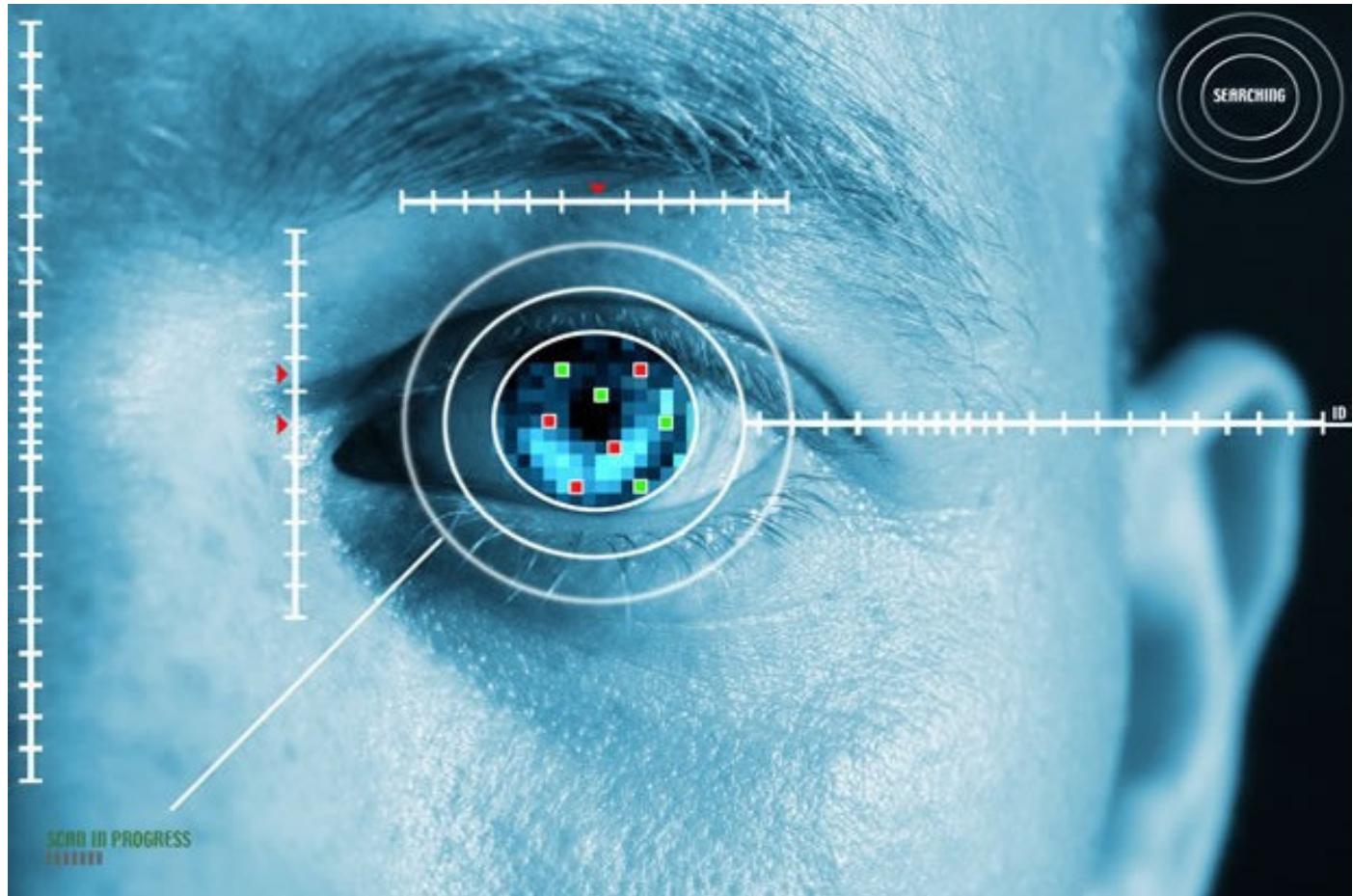
5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Bộ phận
đọc
vân tay
trên
điện thoại
Samsung



5.2.3 Một số công nghệ kiểm soát truy cập – Kiểm soát truy cập dựa trên các đặc điểm sinh học

Quét nhận
dạng tròng
mắt/ con
ngươi của
người dùng



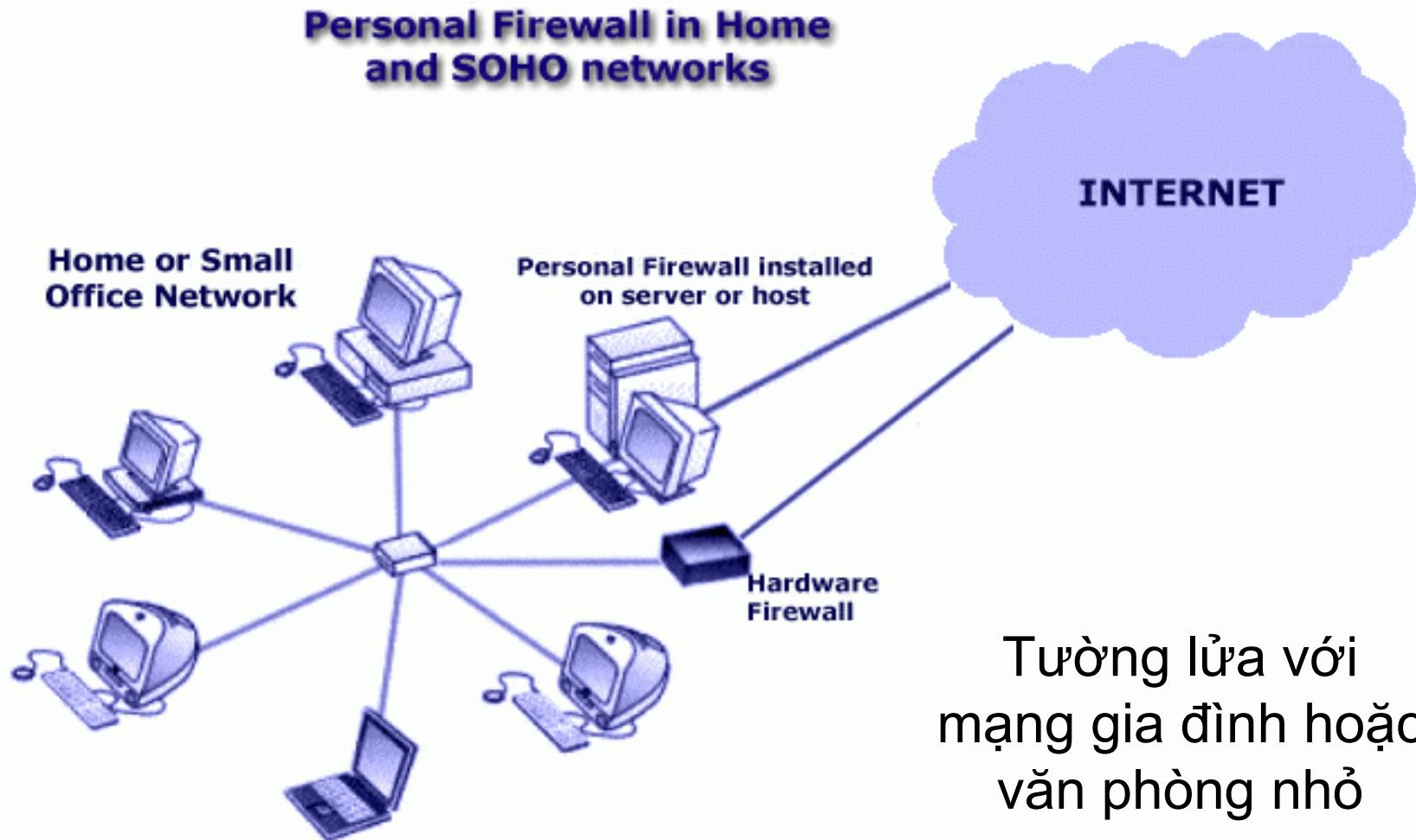
5.3 Tường lửa – Giới thiệu

- ❖ Tường lửa (firewall) có thể là thiết bị phần cứng hoặc công cụ phần mềm được dùng để bảo vệ hệ thống và mạng cục bộ tránh các đe doạ từ bên ngoài.
- ❖ Tường lửa thường được đặt ở vị trí cổng vào của mạng nội bộ của công ty hoặc tổ chức.

5.3 Tường lửa – Giới thiệu

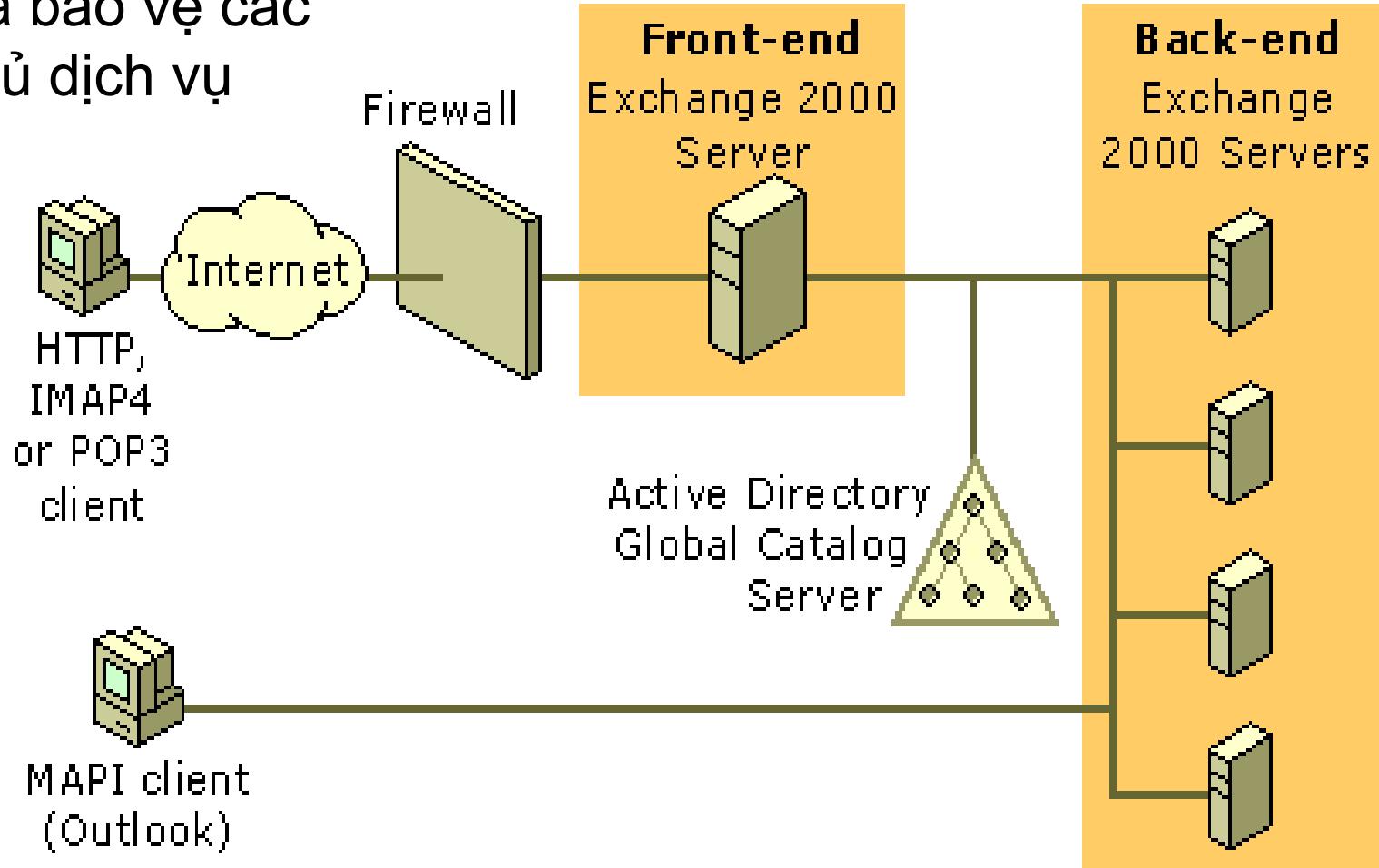
- ❖ Tất cả các gói tin từ trong ra và từ ngoài vào đều phải đi qua tường lửa.
- ❖ Chỉ các gói tin hợp lệ được phép đi qua tường lửa (xác định bởi chính sách an ninh – cụ thể hóa bằng các luật).
- ❖ Bản thân tường lửa phải miễn dịch với các loại tấn công.
- ❖ Tường lửa có thể ngăn chặn nhiều hình thức tấn công mạng, như IP spoofing.

5.3 Tường lửa – Tôpô mạng với tường lửa

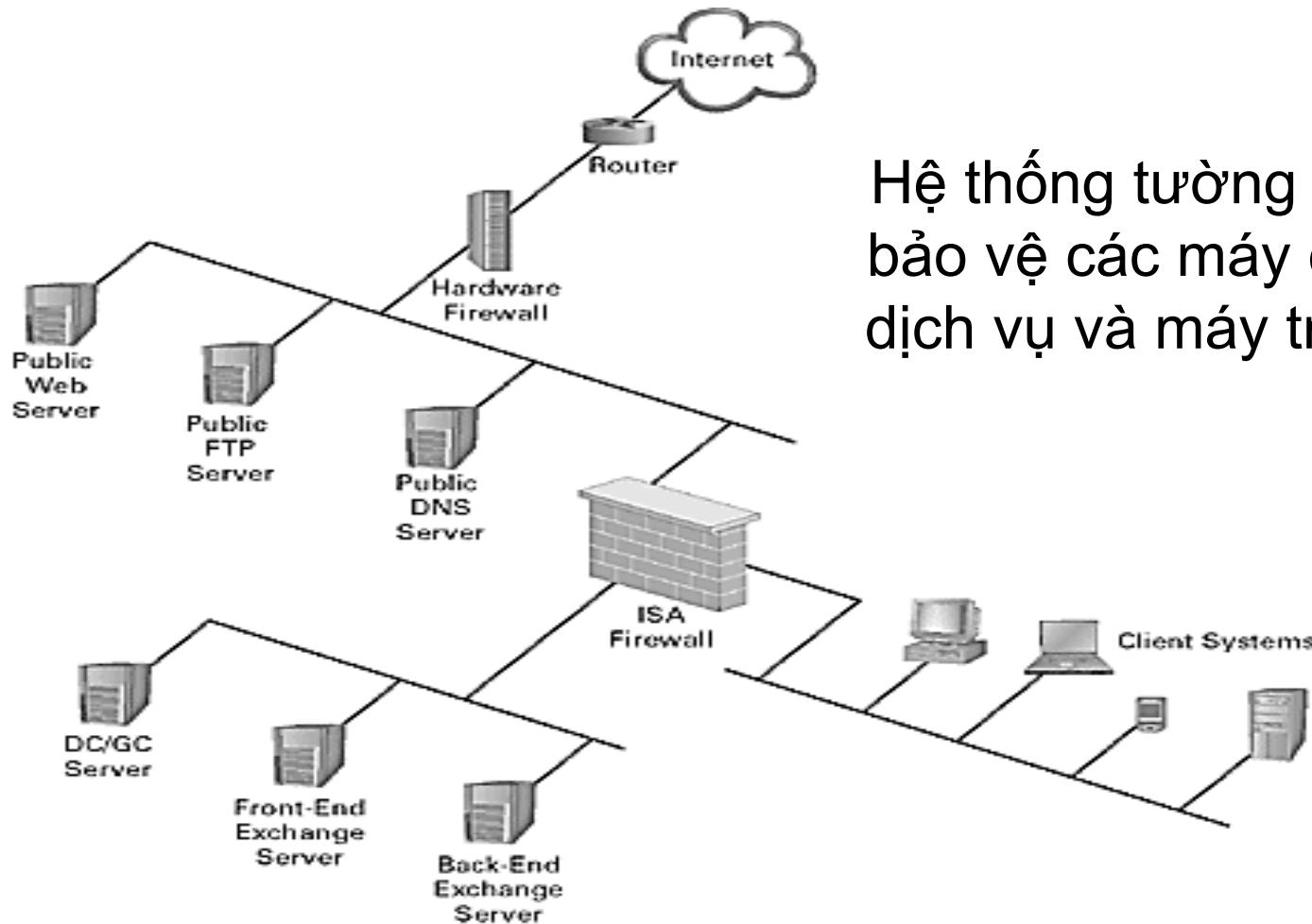


5.3 Tường lửa – Tôpô mạng với tường lửa

Tường lửa bảo vệ các máy chủ dịch vụ



5.3 Tường lửa – Tôpô mạng với tường lửa



5.3 Tường lửa – Các loại tường lửa

❖ Lọc gói tin (Packet-Filtering):

- Áp dụng một tập các luật cho mỗi gói tin đi/đến để quyết định chuyển tiếp hay loại bỏ gói tin.
- Các tường lửa dạng này thường lọc gói tin lớp IP.

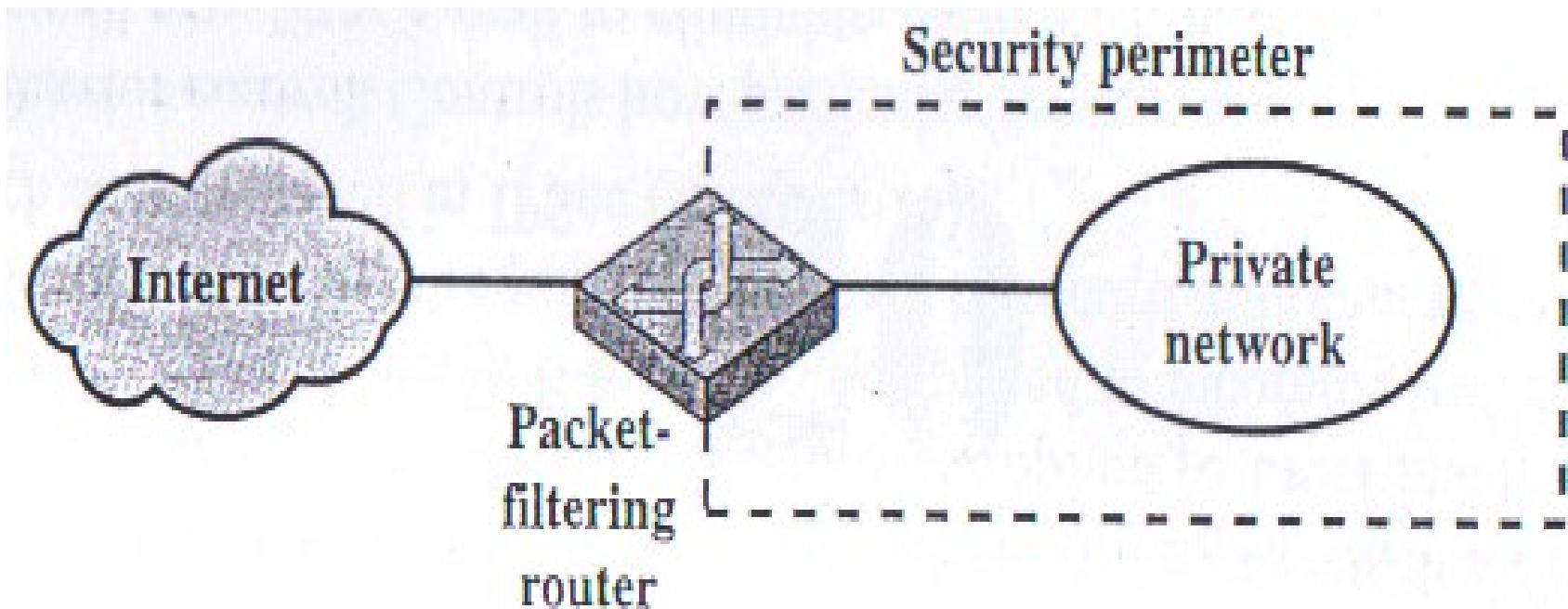
❖ Các cổng ứng dụng (Application-level gateway):

- Còn gọi là proxy server, thường dùng để phát lại (relay) traffic của mức ứng dụng.
- Tường lửa ứng dụng web (WAF – Web Application Firewall) là dạng cổng ứng dụng được sử dụng rộng rãi.

❖ Cổng chuyển mạch (Circuit-level gateway):

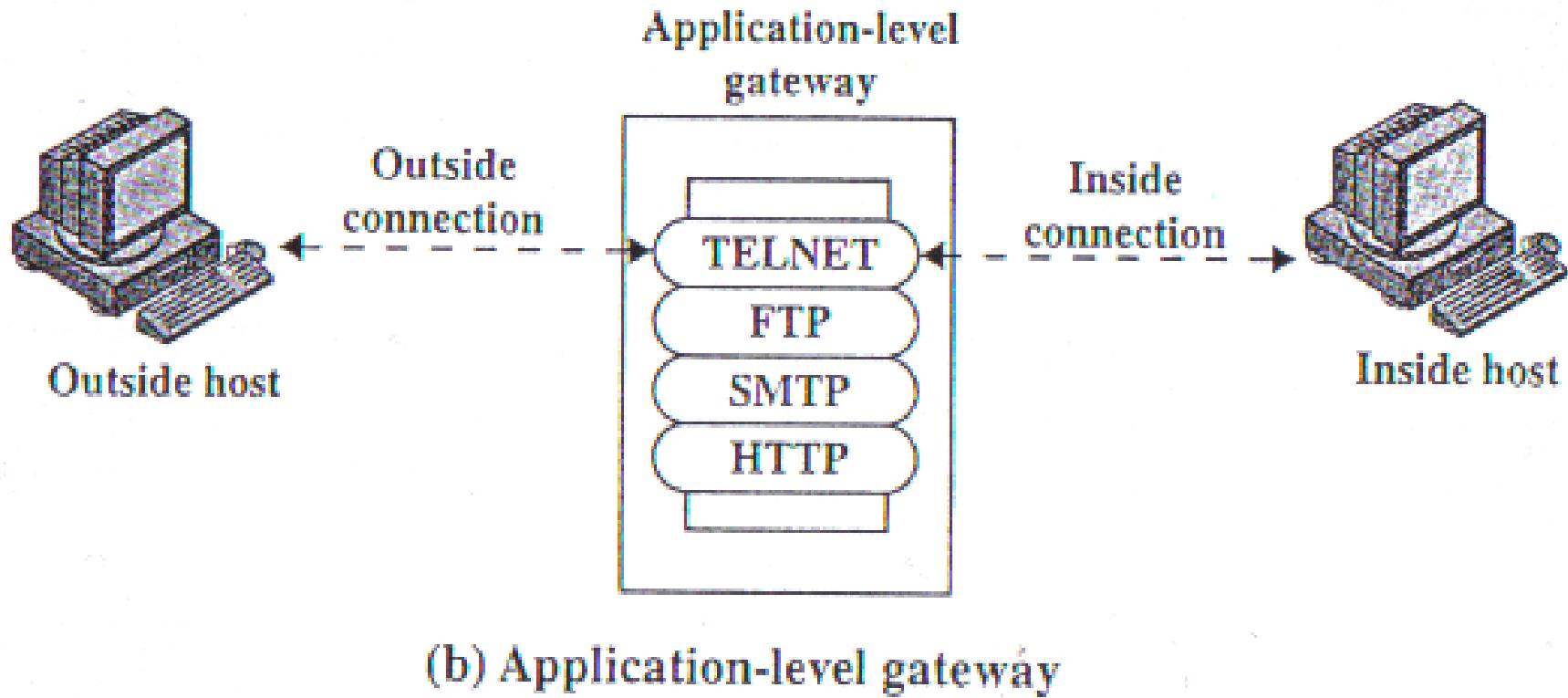
- Hoạt động tương tự các bộ chuyển mạch.

5.3 Tường lửa – Các loại tường lửa – Lọc gói tin

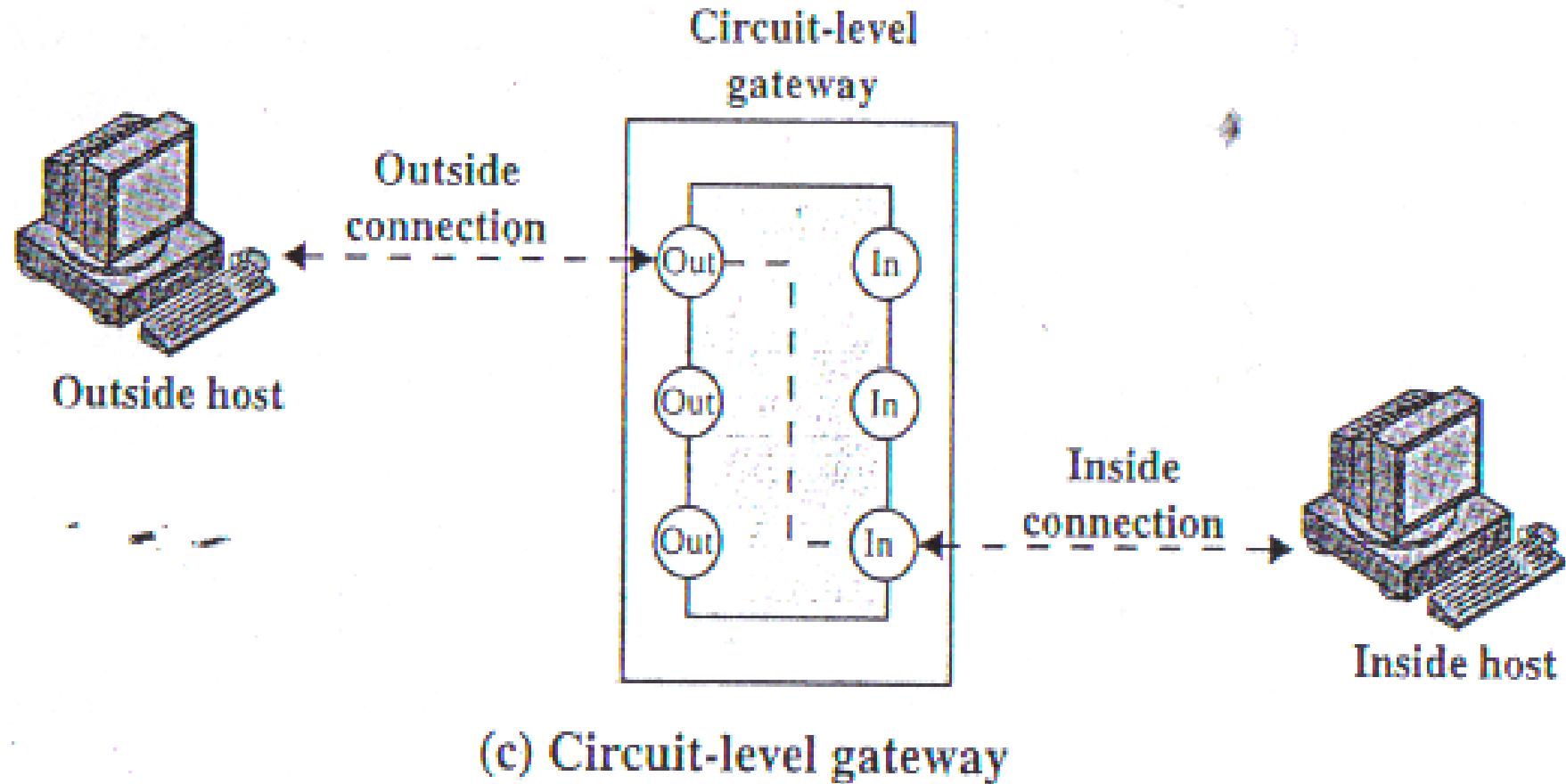


(a) Packet-filtering router

5.3 Tường lửa – Các loại tường lửa – Cổng ứng dụng



5.3 Tường lửa – Các loại tường lửa – Cổng chuyển mạch

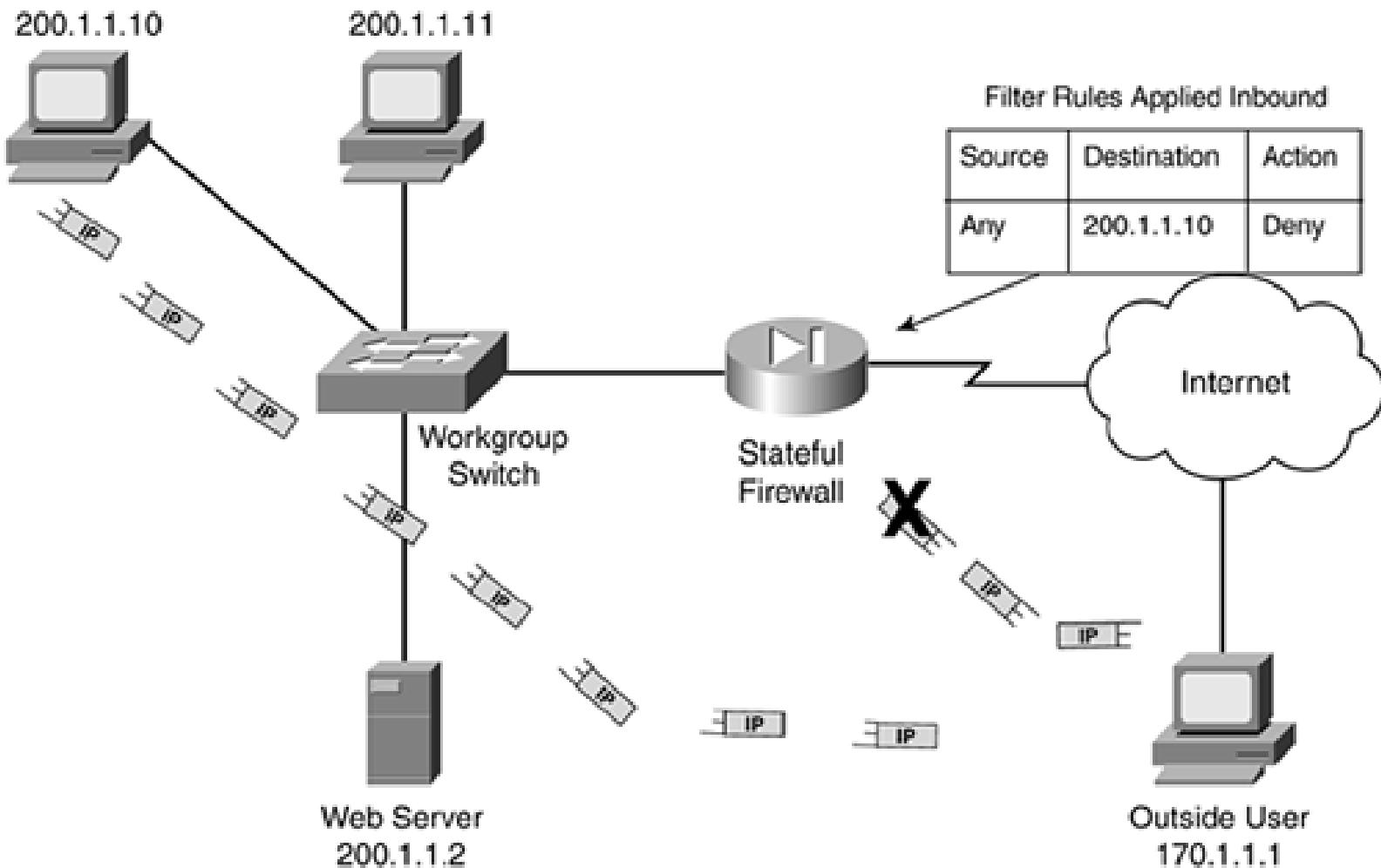


5.3 Tường lửa – Lọc có trạng thái

❖ Tường lửa có trạng thái (Stateful firewall):

- Có khả năng lưu trạng thái của các kết nối mạng đi qua nó;
- Nó được lập trình để phân biệt các gói tin thuộc về các kết nối mạng khác nhau;
- Chỉ những gói tin thuộc các kết nối mạng đang hoạt động mới được đi qua tường lửa, còn các gói tin khác (không thuộc kết nối đang hoạt động) sẽ bị chặn lại.

5.3 Tường lửa – Lọc có trạng thái



5.3 Tường lửa – Lọc không trạng thái

❖ Tường lửa không trạng thái (Stateless firewall):

- Lọc các gói tin riêng rẽ mà không quan tâm đến mỗi gói tin thuộc về kết nối mạng nào;
- Dễ bị tấn công bởi kỹ thuật giả mạo địa chỉ, giả mạo nội dung gói tin do tường lửa không có khả năng nhớ các gói tin đi trước thuộc cùng một kết nối mạng.

5.3 Tường lửa – Kỹ thuật kiểm soát truy cập

❖ Kiểm soát dịch vụ:

- Xác định dịch vụ nào có thể được truy cập, hướng đi ra hay đi vào.

❖ Kiểm soát hướng:

- Điều khiển hướng được phép đi của các gói tin của mỗi dịch vụ

❖ Kiểm soát người dùng:

- Xác định người dùng nào được quyền truy cập;
- Thường áp dụng cho người dùng mạng nội bộ.

❖ Kiểm soát hành vi:

- Kiểm soát việc sử dụng các dịch vụ cụ thể. Ví dụ: tường lửa có thể lọc để loại bỏ các thư rác, hoặc hạn chế truy cập đến một bộ phận thông tin của máy chủ web.

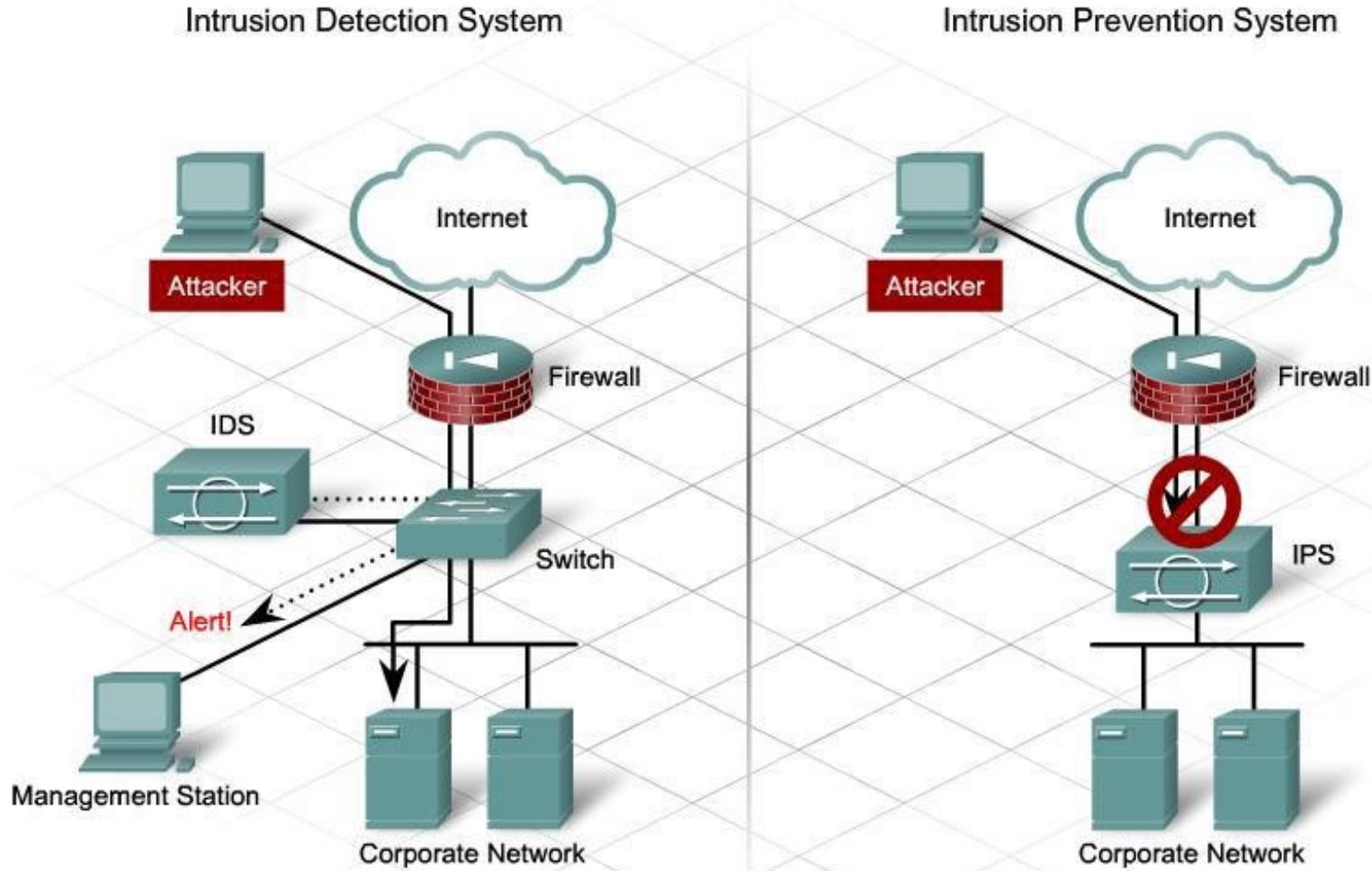
5.3 Tường lửa – Các hạn chế

- ❖ Không thể chống lại các tấn công không đi qua nó.
- ❖ Không thể chống lại các tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng an ninh của các phần mềm.
- ❖ Không thể chống lại các hiểm họa từ bên trong (mạng nội bộ).
- ❖ Không thể ngăn chặn việc vận chuyển các chương trình hoặc các file bị nhiễm virus hoặc các phần mềm độc hại.

5.3 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập

- ❖ Các hệ thống phát hiện/ngăn chặn tấn công, xâm nhập (IDS/IPS) thường được sử dụng như một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng;
 - IDS – Intrusion Detection System: hệ thống phát hiện tấn công, xâm nhập;
 - IPS - Intrusion Prevention System: hệ thống ngăn chặn tấn công, xâm nhập.
- ❖ Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa, tùy theo mục đích sử dụng.

5.4 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập



5.4 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập

❖ Nhiệm vụ chính của các hệ thống IDS/IPS:

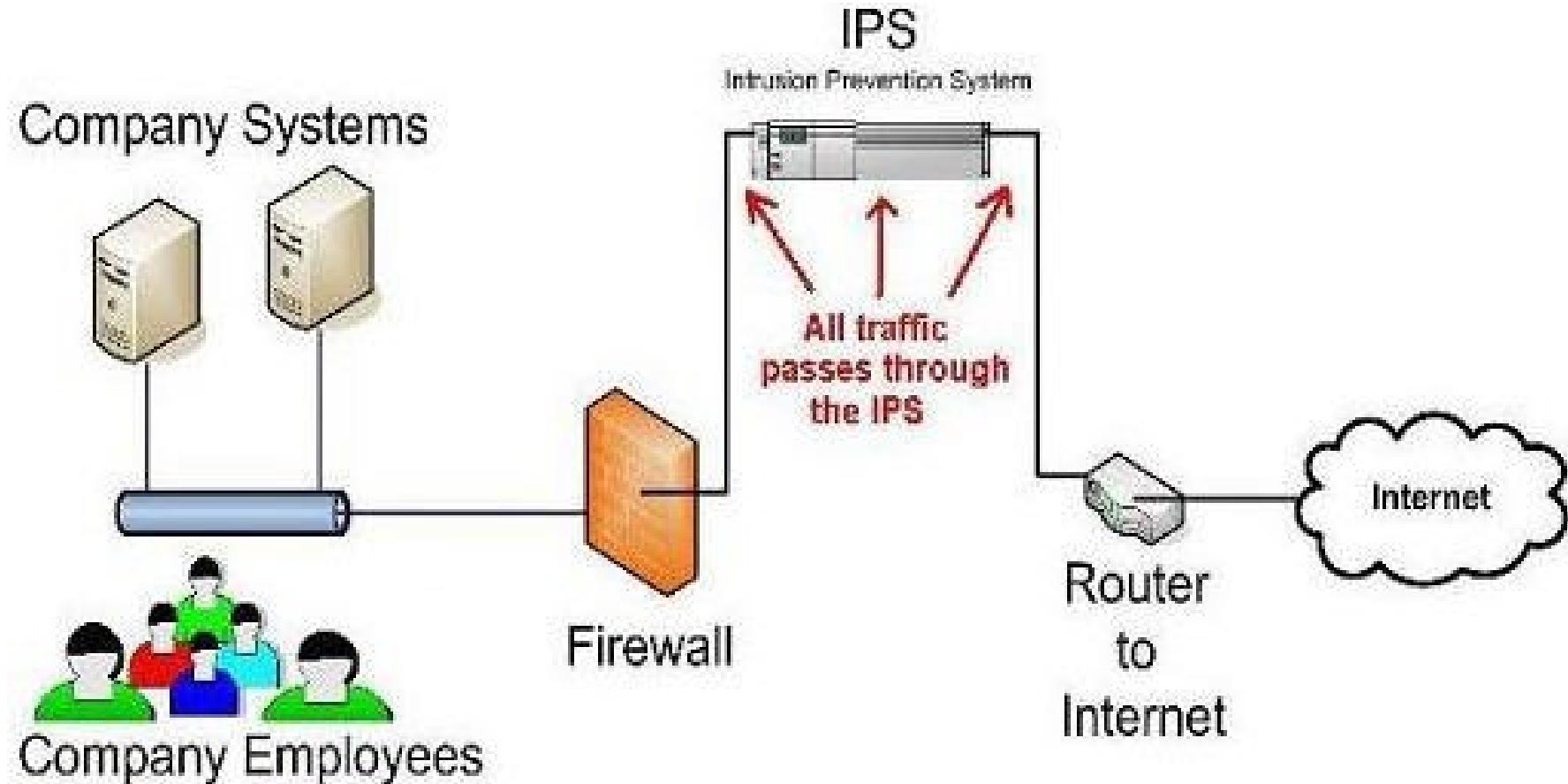
- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập;
- Khi phát hiện các hành vi tấn công, xâm nhập → ghi logs các hành vi này cho phân tích bổ sung sau này;
- Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập;
- Gửi thông báo cho người quản trị về các hành vi tấn công, xâm nhập đã phát hiện được.

5.4 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập

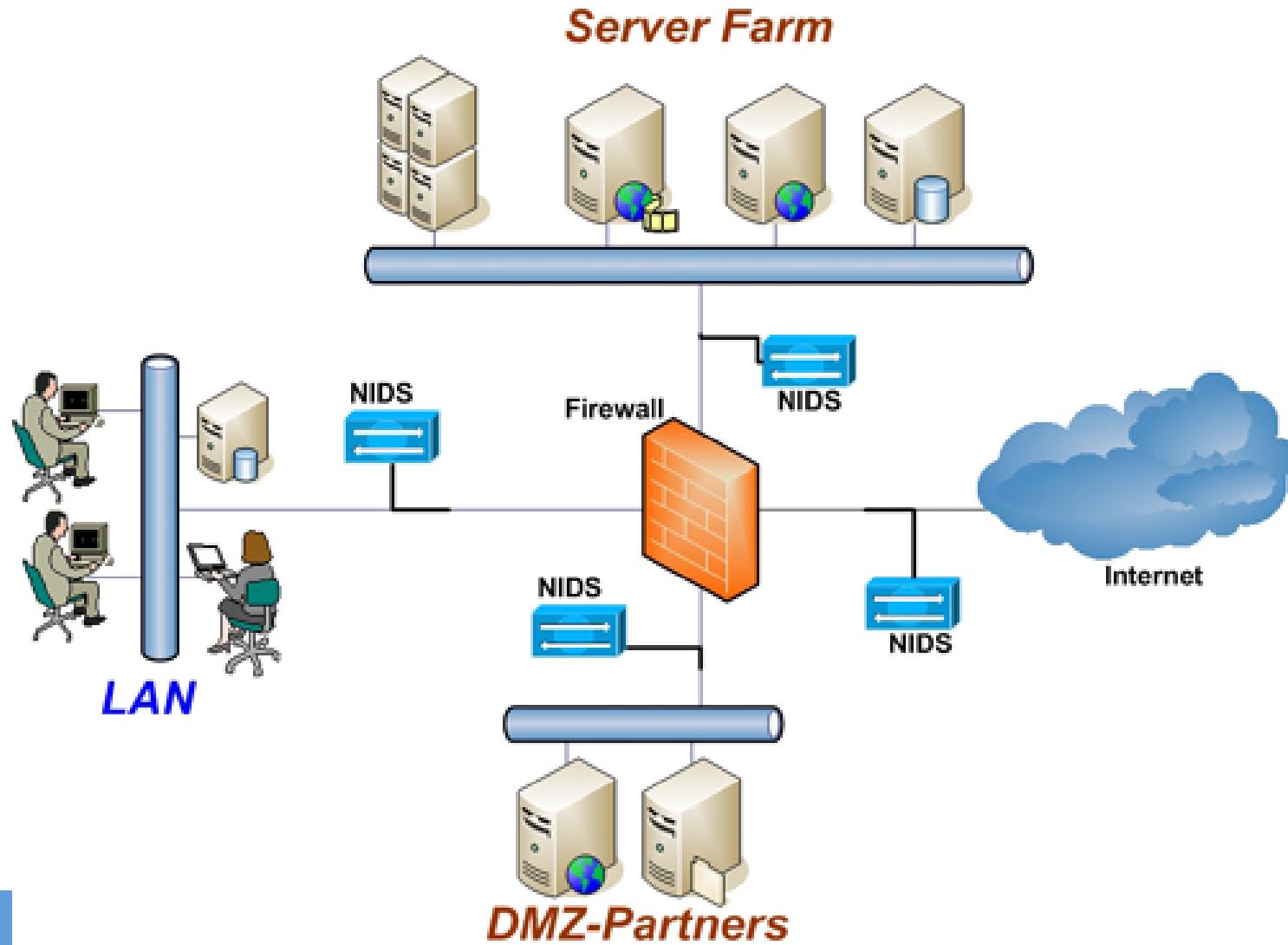
❖ So sánh IDS/IPS:

- Giống: Về cơ bản IPS và IDS giống nhau về chức năng giám sát.
- Khác:
 - IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công/xâm nhập bị phát hiện;
 - IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát/cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

5.4 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập



5.4 Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập



5.4 IDS/IPS – Phân loại

❖ Phân loại theo nguồn dữ liệu:

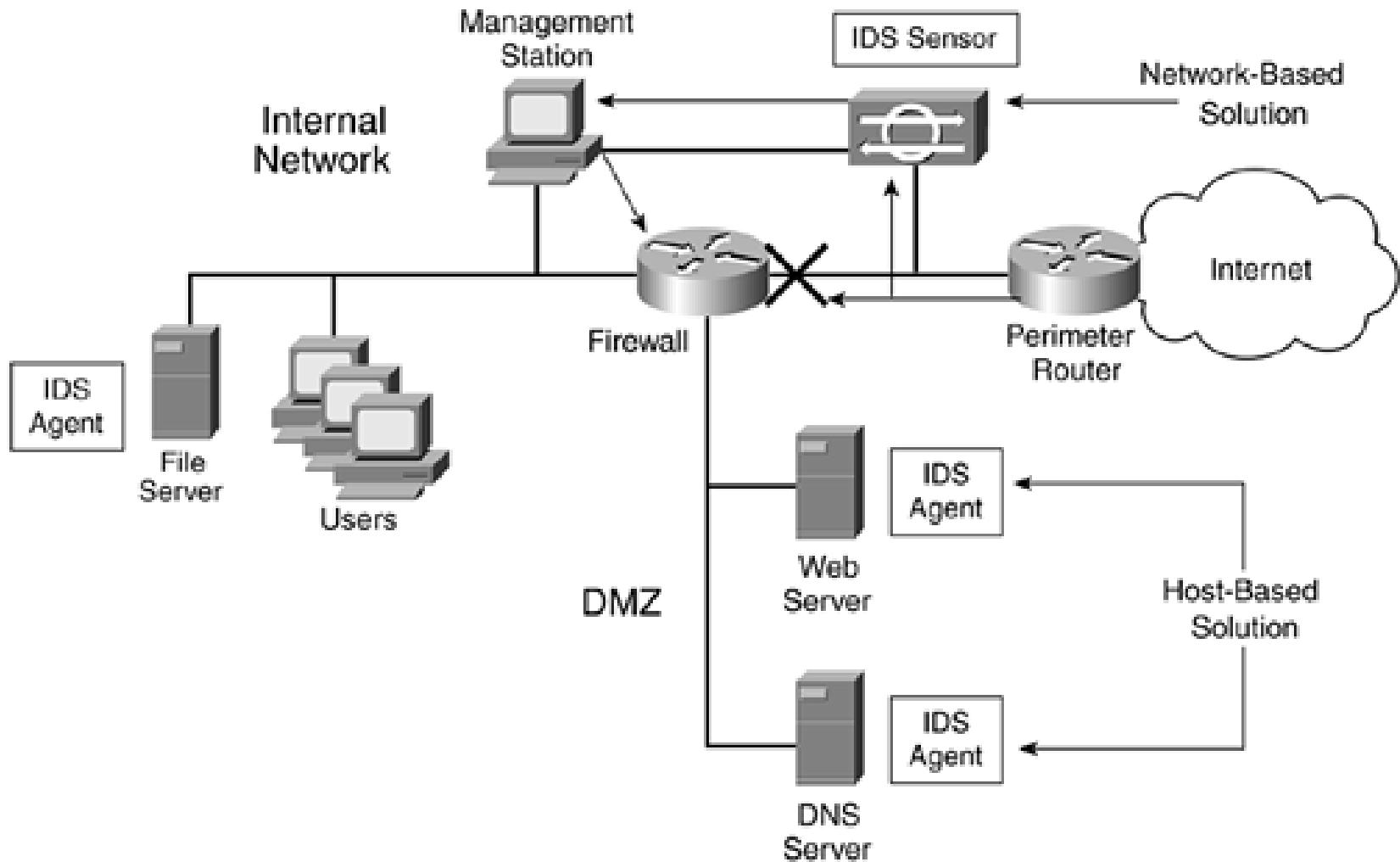
- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng.
- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó.

5.4 IDS/IPS – Phân loại

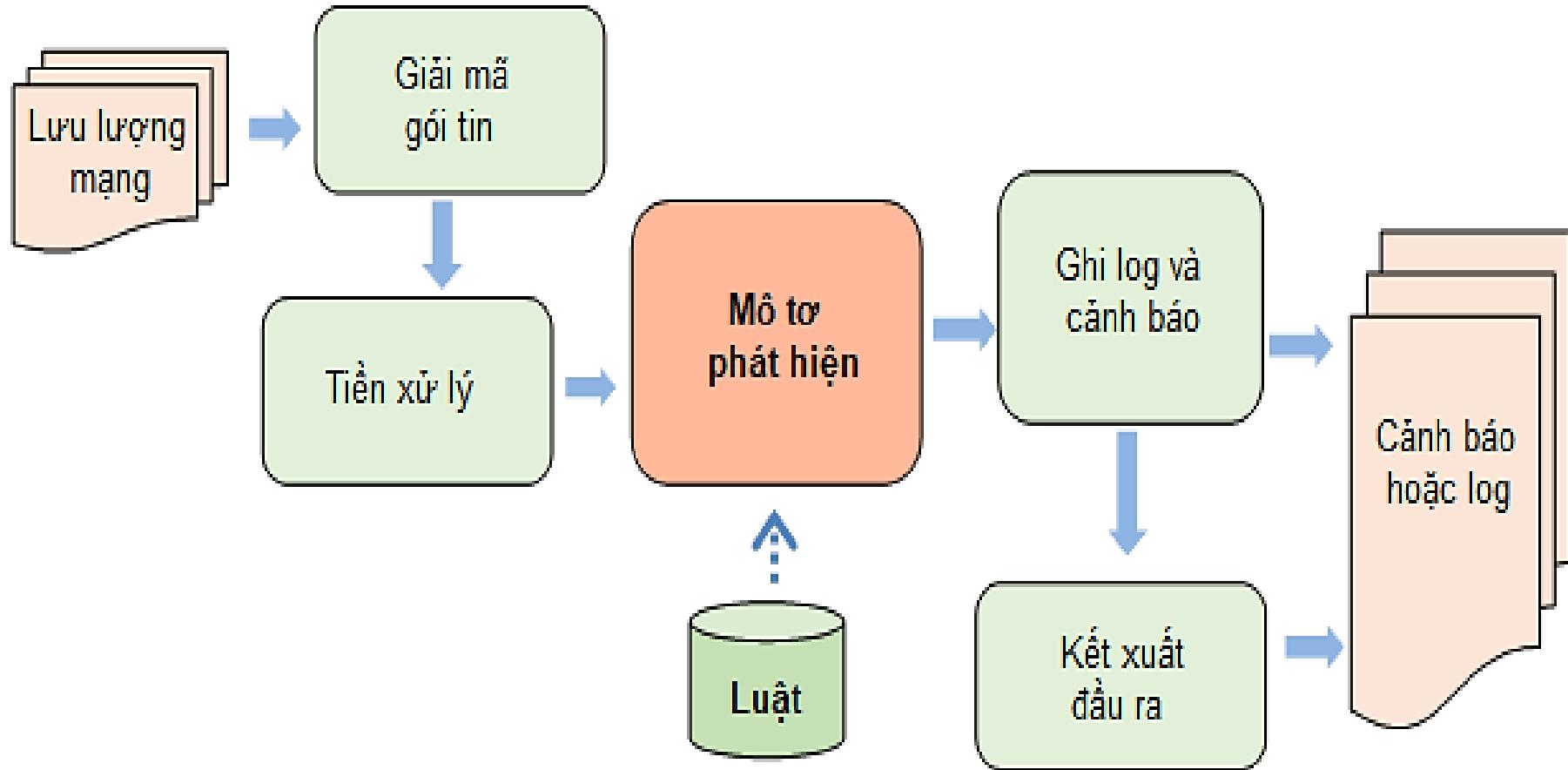
❖ Phân loại theo kỹ thuật phân tích:

- Phát hiện xâm nhập dựa trên chữ ký hoặc phát hiện sự lạm dụng (Signature-based / misuse instrusion detection);
- Phát hiện xâm nhập dựa trên các bất thường (Anomaly instrusion detection).

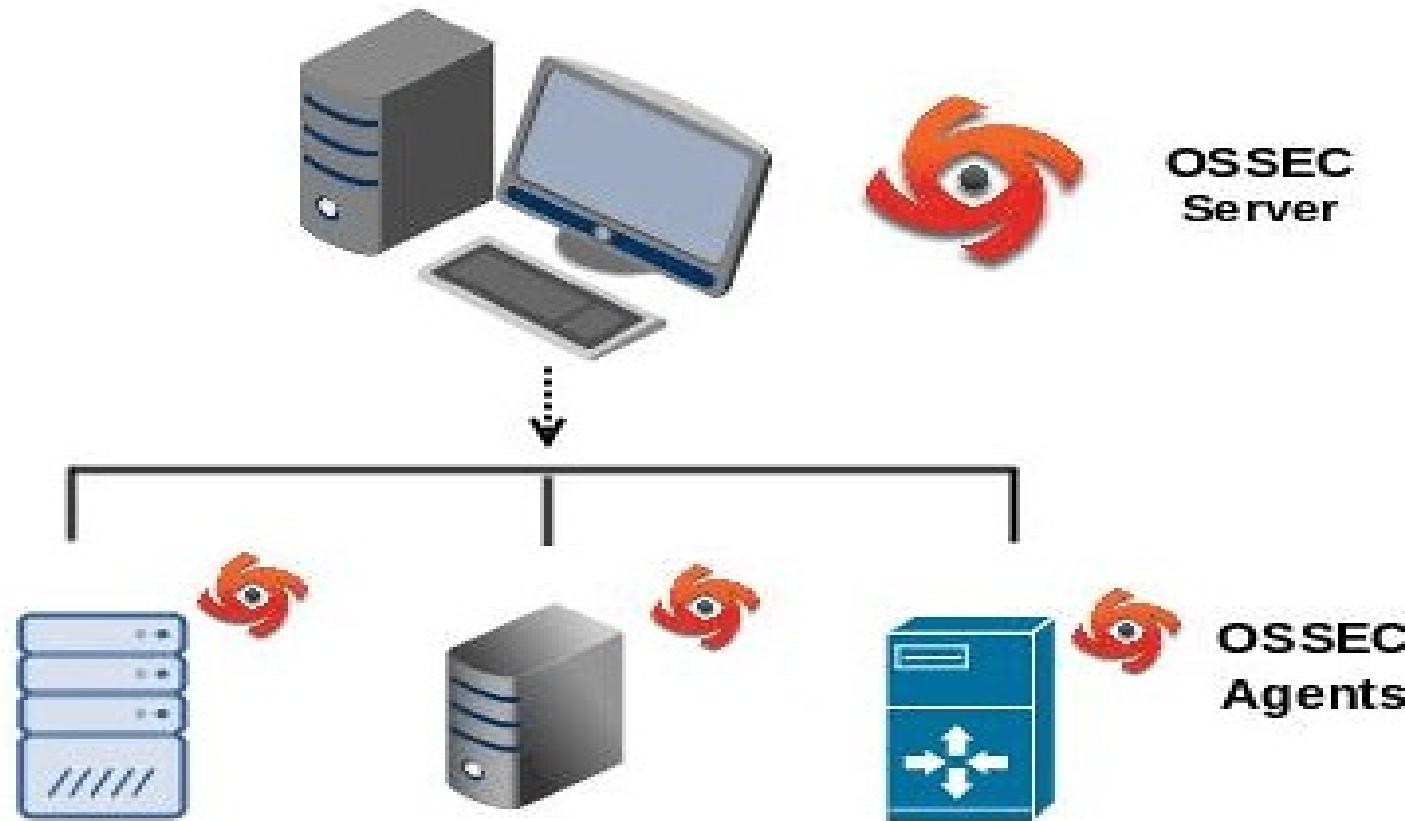
5.4 IDS/IPS – NIDS và HIDS



NIDS - Snort



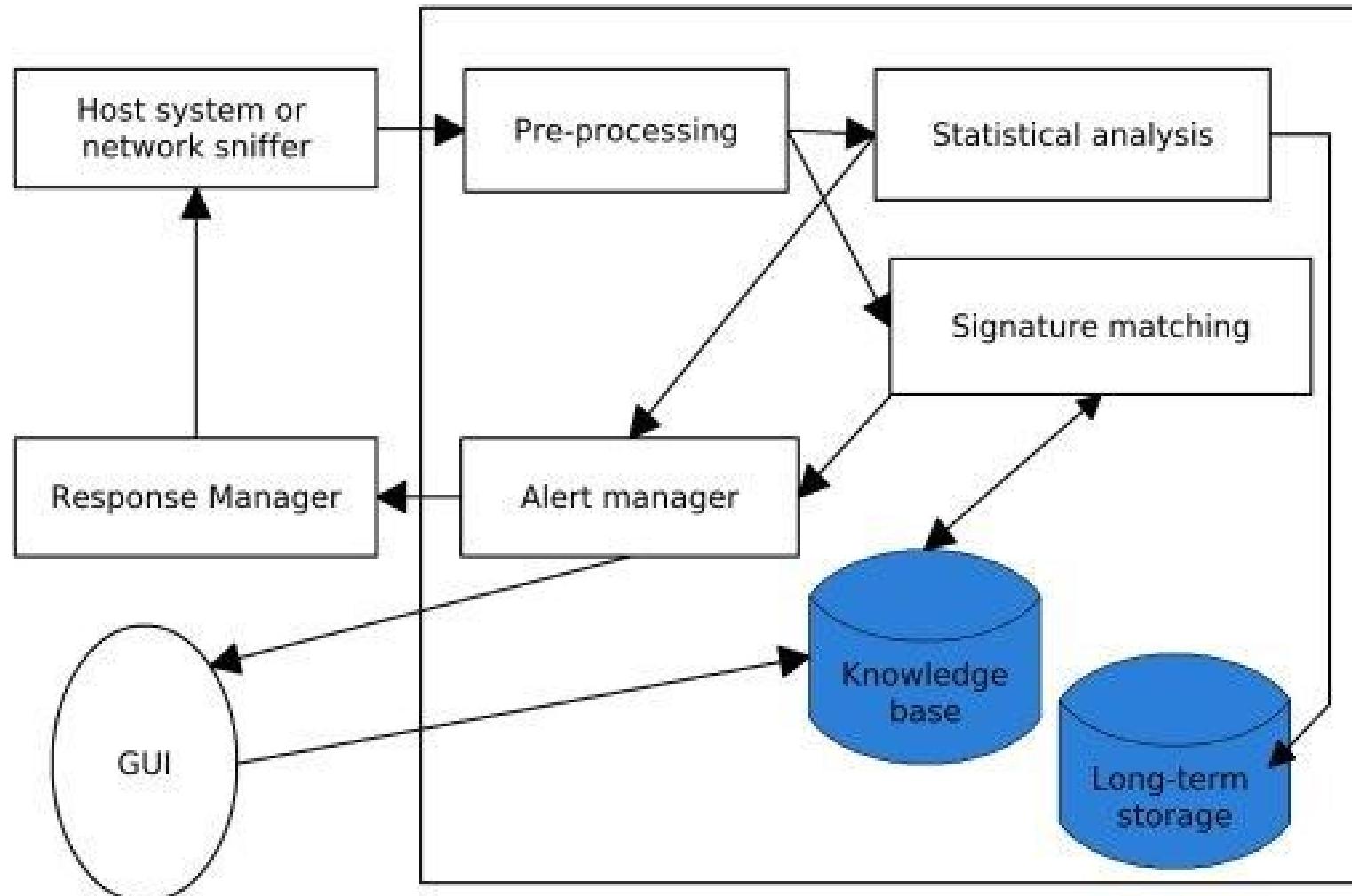
HIDS - OSSEC



5.4 IDS/IPS – Phát hiện xâm nhập dựa trên chữ ký

- ❖ Xây dựng cơ sở dữ liệu các chữ ký/dấu hiệu của các loại tấn công, xâm nhập đã biết;
 - Hầu hết các chữ ký/dấu hiệu được nhận dạng và mã hóa thủ công;
 - Dạng biểu diễn thường gặp là các luật (rule) phát hiện.
- ❖ Giám sát sát các hành vi của hệ thống, và cảnh báo nếu phát hiện chữ ký của tấn công, xâm nhập;

5.4 IDS/IPS – Phát hiện xâm nhập dựa trên chữ ký



5.4 IDS/IPS – Phát hiện xâm nhập dựa trên chữ ký

❖ Ưu điểm:

- Có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả;
- Tốc độ cao, yêu cầu tài nguyên tính toán tương đối thấp.

❖ Nhược điểm:

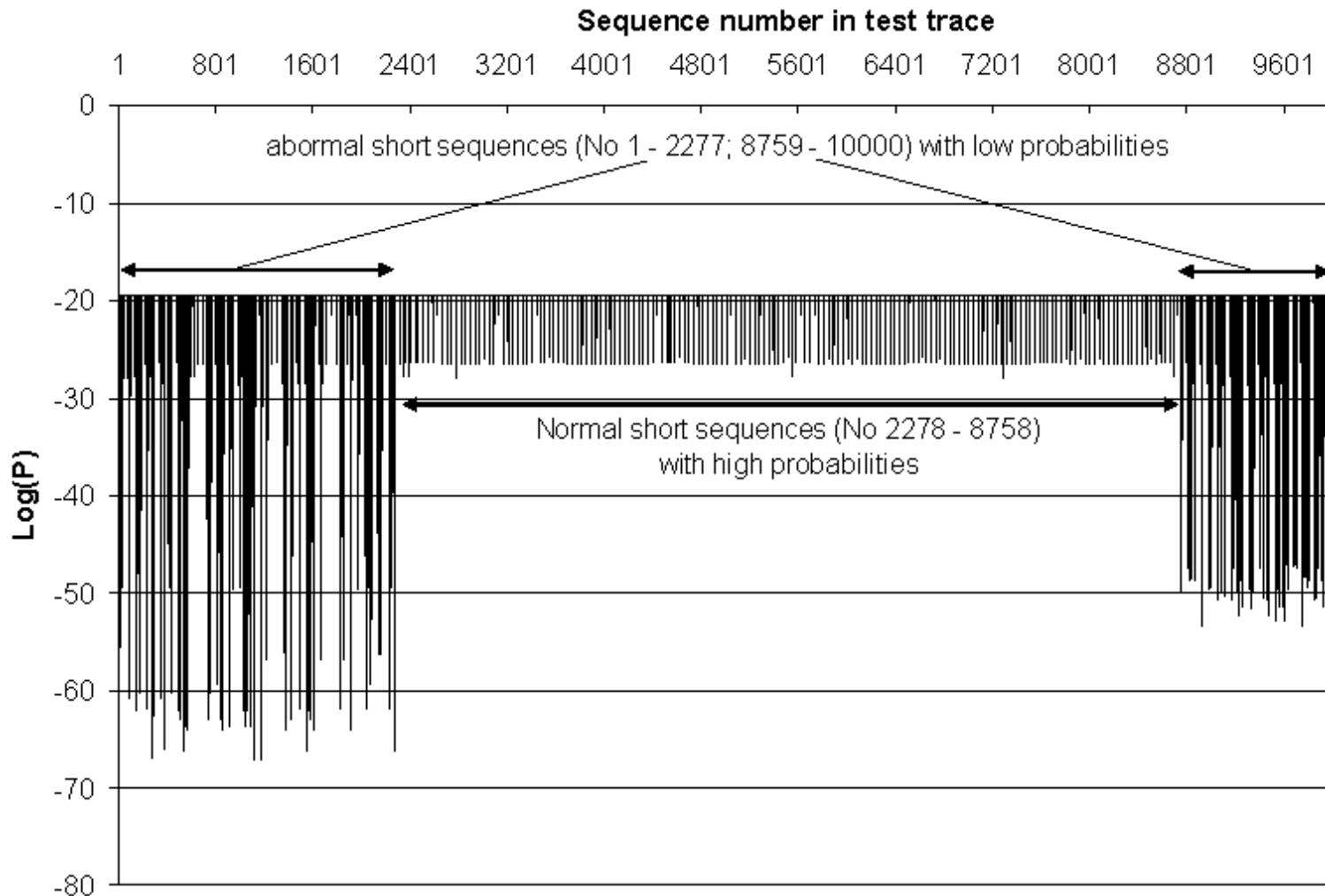
- Không có khả năng phát hiện các tấn công, xâm nhập mới, do chữ ký của chúng chưa có trong cơ sở dữ liệu các chữ ký;
- Đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký/dấu hiệu tấn công, xâm nhập.

5.4 IDS/IPS – Phát hiện xâm nhập dựa trên bất thường

- ❖ Phương pháp này dựa trên giả thiết: *các hành vi xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường.*
- ❖ Quá trình xây dựng và triển khai gồm 2 giai đoạn:
 - Xây dựng hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường.
 - Cần giám sát đối tượng trong điều kiện bình thường trong một khoảng thời gian đủ dài để thu thập dữ liệu huấn luyện.
 - Giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và hồ sơ của đối tượng.

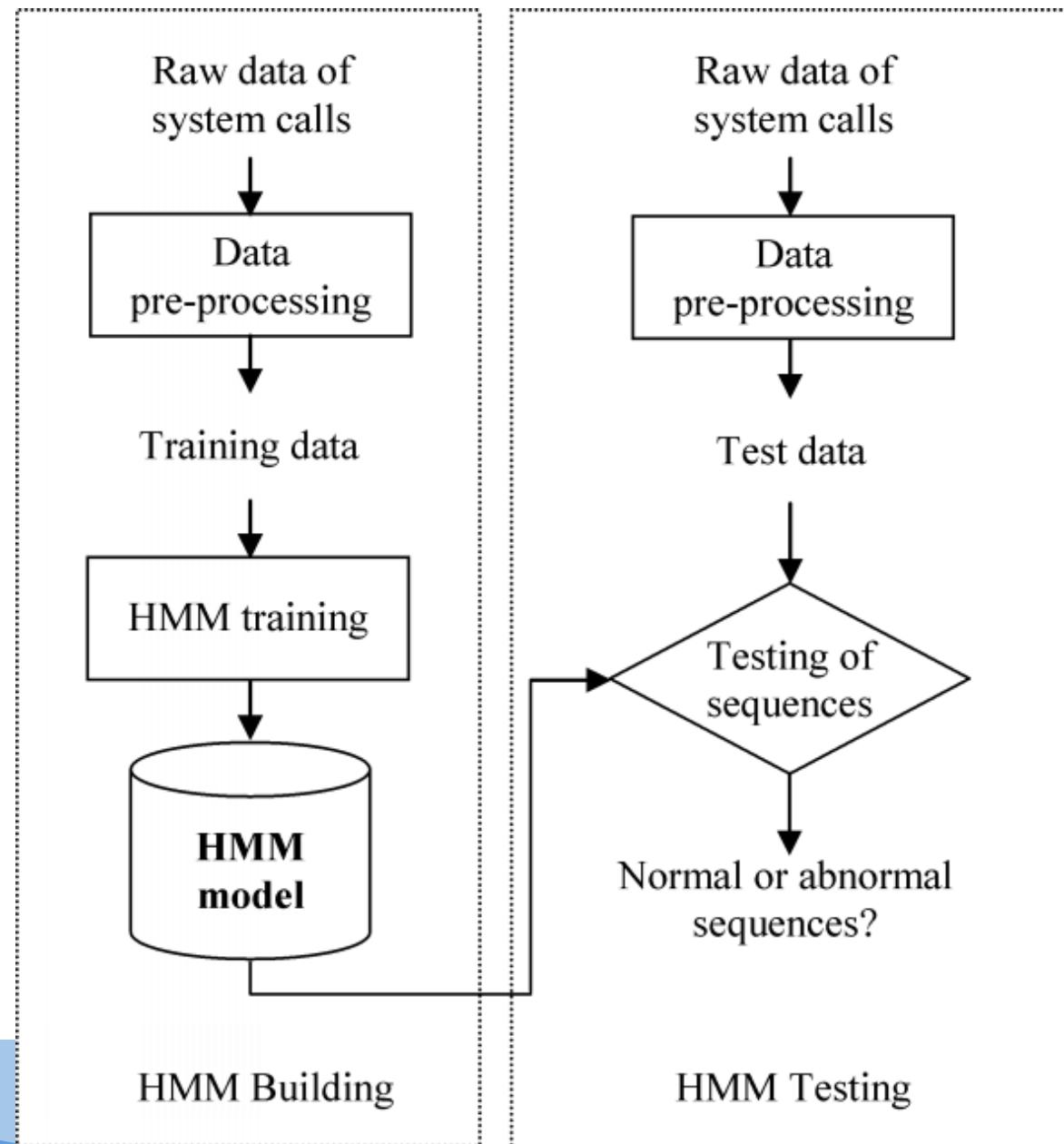
5.4 IDS/IPS – Phát hiện xâm nhập dựa trên bất thường

Một ví dụ về tình trạng bình thường ($\text{Log}(P)$ lớn) và bất thường ($\text{Log}(P)$ rất nhỏ)



5.4 IDS/IPS – Phát hiện xâm nhập dựa trên bất thường

HMM-Based Anomaly Detection



5.4 IDS/IPS – Phát hiện xâm nhập dựa trên bất thường

❖ Ưu điểm:

- Có tiềm năng phát hiện các loại xâm nhập mới mà không yêu cầu biết trước thông tin về chúng.

❖ Nhược điểm:

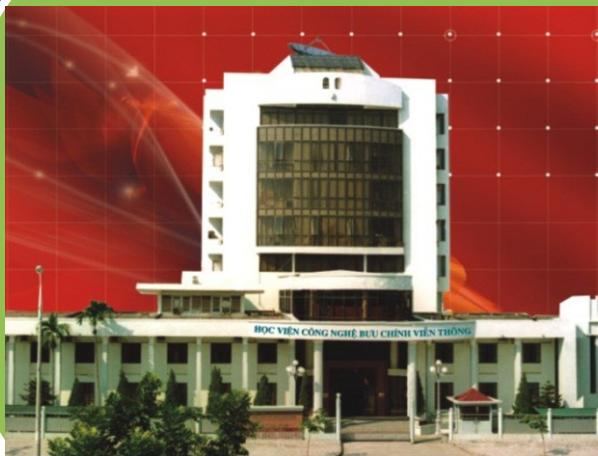
- Tỷ lệ cảnh báo sai tương đối cao so với phương pháp dựa trên chữ ký;
- Tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

5.4 IDS/IPS – Phát hiện xâm nhập dựa trên bất thường

- ❖ Các phương pháp xử lý, phân tích dữ liệu và mô hình hoá trong phát hiện xâm nhập dựa trên bất thường:
 - Thống kê (statistics).
 - Học máy (machine learning): HMM, máy trạng thái (state-based).
 - Khai phá dữ liệu (data mining).
 - Mạng nơ ron (neural networks).



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN HỌC
CƠ SỞ AN TOÀN THÔNG TIN**

**CHƯƠNG 6 – QUẢN LÝ, CHÍNH
SÁCH & PHÁP LUẬT ATTT**

Giảng viên:

PGS.TS. Hoàng Xuân Dậu

E-mail:

dauhx@ptit.edu.vn

Khoa:

An toàn thông tin

NỘI DUNG CHƯƠNG 6

1. Quản lý an toàn thông tin
2. Giới thiệu bộ chuẩn quản lý
ATTT ISO/IEC 27000
3. Pháp luật và chính sách ATTT
4. Vấn đề đạo đức ATTT

6.1 Quản lý an toàn thông tin

1. Khái quát về quản lý ATTT
2. Đánh giá rủi ro ATTT

Khái quát về quản lý ATTT

- ❖ Tài sản (Asset) trong lĩnh vực ATTT là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin.
- ❖ Tài sản ATTT có thể gồm:
 - Phần cứng (máy chủ, các thiết bị mạng,...)
 - Phần mềm (hệ điều hành, các phần mềm máy chủ dịch vụ,...)
 - Thông tin (thông tin khách hàng, nhà cung cấp, hoạt động kinh doanh,...)

Khái quát về quản lý ATTT

- ❖ Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm đảm bảo các tài sản quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ đầy đủ với chi phí phù hợp;
- ❖ Quản lý ATTT phải trả lời được 3 câu hỏi:
 - Những tài sản nào cần được bảo vệ?
 - Những đe dọa nào có thể có đối với các tài sản này?
 - Những biện pháp có thể thực hiện để ứng phó với các đe dọa đó?

Khái quát về quản lý ATTT

❖ Quản lý ATTT có thể gồm các khâu:

- Xác định rõ mục đích đảm bảo ATTT;
- Xây dựng hồ sơ tổng hợp về các rủi ro;
- Đánh giá rủi ro với từng tài sản ATTT cần bảo vệ;
- Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được.

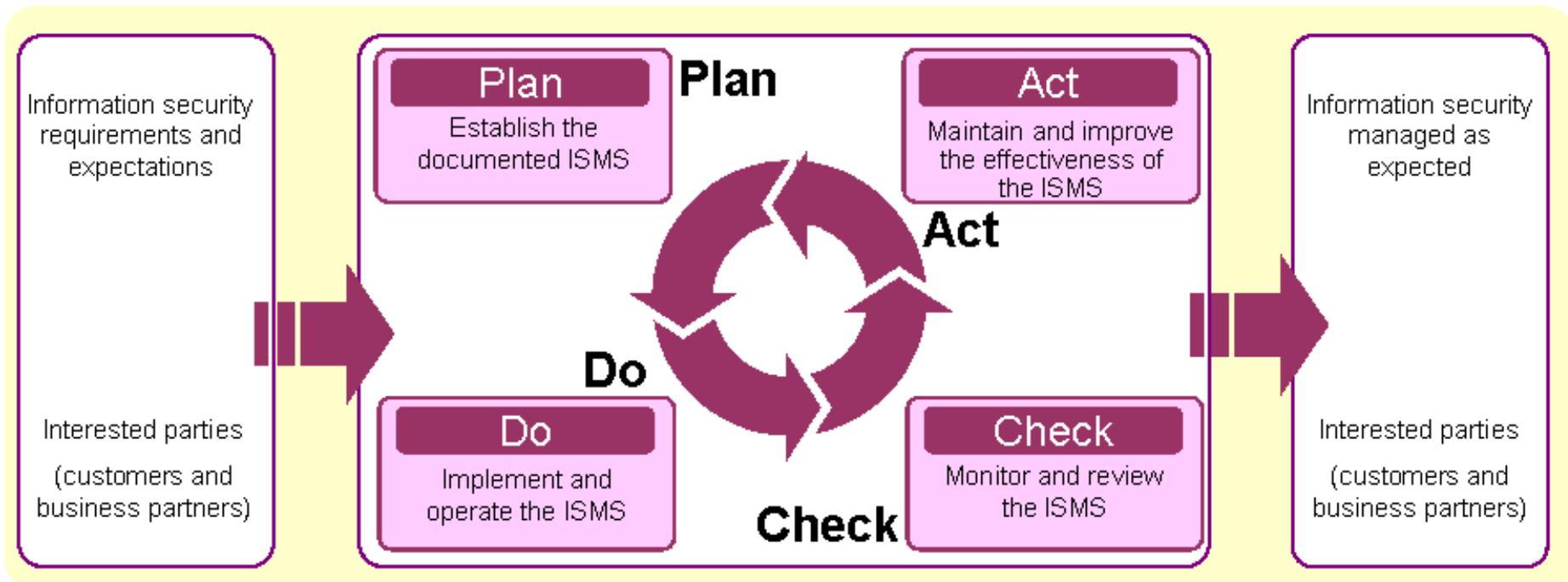
Khái quát về quản lý ATTT

❖ **Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình** do:

- Sự thay đổi nhanh chóng của công nghệ:
 - Nhiều công nghệ, kỹ thuật và công cụ mới xuất hiện
 - Độ phức tạp của hệ thống tăng nhanh.
- Môi trường xuất hiện rủi ro liên tục thay đổi:
 - Xuất hiện nhiều công cụ cho tấn công, phá hoại
 - Xuất hiện nhiều mối đe dọa mới
 - Trình độ của tin tặc được nâng lên nhanh chóng.

Khái quát về quản lý ATTT

- ❖ Chu trình Plan-Do-Check-Act (PDCA) thực hiện quản lý ATTT liên tục:



Đánh giá rủi ro ATTT

❖ Đánh giá rủi ro ATTT (Security risk assessment)

- Là một bộ phận quan trọng của vấn đề quản lý rủi ro;
- Mỗi tài sản của tổ chức cần được xem xét, nhận dạng các rủi ro có thể có và đánh giá mức rủi ro;
- Là một trong các cơ sở để xác định mức rủi ro chấp nhận được với từng loại tài sản;
- Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức chấp nhận được, với mức chi phí phù hợp.

Đánh giá rủi ro ATTT

- ❖ Các phương pháp tiếp cận đánh giá rủi ro:
 - Phương pháp đường cơ sở (Baseline approach)
 - Phương pháp không chính thức (Informal approach)
 - Phương pháp phân tích chi tiết rủi ro (Detailed risk analysis)
 - Phương pháp kết hợp (Combined approach)

Đánh giá rủi ro ATTT - Phương pháp đường cơ sở

- ❖ Mục đích của *Phương pháp đường cơ sở* là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên:
 - Các tài liệu cơ bản;
 - Các quy tắc thực hành;
 - Các thực tế tốt nhất của ngành đã được áp dụng.

Đánh giá rủi ro ATTT - Phương pháp đường cơ sở

❖ Ưu điểm:

- Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức;
- Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống.

❖ Nhược điểm:

- Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau;
- Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể. Mức quá cao: gây tốn kém, quá thấp: có thể gây mất an toàn.

❖ Phù hợp với các tổ chức với hệ thống CNTT có quy mô nhỏ, nguồn lực hạn chế.

Đánh giá rủi ro ATTT – Ph. pháp không chính thức

❖ Phương pháp không chính thức liên quan đến việc:

- Thực hiện một số dạng phân tích rủi ro hệ thống CNTT của tổ chức một cách không chính thức;
- Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài;
- Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức.

Đánh giá rủi ro ATTT – Ph.pháp không chính thức

❖ Ưu điểm:

- Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp;
- Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở.

❖ Nhược điểm:

- Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức;
- Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân.

❖ Phù hợp với các tổ chức với hệ thống CNTT có quy mô nhỏ và vừa, nguồn lực tương đối hạn chế.

Đánh giá rủi ro ATTT – P.P. phân tích chi tiết rủi ro

- ❖ *Phương pháp phân tích chi tiết rủi ro* là phương pháp đánh giá toàn diện, được thực hiện một cách chính thức và được chia thành nhiều giai đoạn:
 - Nhận dạng các tài sản;
 - Nhận dạng các mối đe dọa và lỗ hổng đối với các tài sản này;
 - Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với tổ chức;
 - Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn trên.

Đánh giá rủi ro ATTT – P.P. phân tích chi tiết rủi ro

❖ Ưu điểm:

- Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất;
- Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi.

❖ Nhược điểm:

- Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao;
- Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp.

Đánh giá rủi ro ATTT – P.P. phân tích chi tiết rủi ro

❖ Phù hợp với:

- Các tổ chức chính phủ cung cấp các dịch vụ thiết yếu cho người dân và doanh nghiệp;
- Các tổ chức có hệ thống CNTT quy mô lớn, hoặc các tổ chức cung cấp nền tảng hạ tầng truyền thông cho quốc gia;
 - Các tổ chức tài chính, ngân hàng;
 - Các doanh nghiệp viễn thông, nhà mạng;
 - Các công ty, tập đoàn có hệ thống CNTT đủ lớn.

Đánh giá rủi ro ATTT - Phương pháp kết hợp

- ❖ Phương pháp này kết hợp các thành phần của 3 phương pháp đường cơ sở, không chính thức và phân tích chi tiết;
- ❖ Mục tiêu:
 - Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt;
 - Sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian.

Đánh giá rủi ro ATTT - Phương pháp kết hợp

❖ Các bước thực hiện:

- Thực hiện phương pháp đường cơ sở với tất cả các thành phần của hệ thống CNTT của tổ chức;
- Tiếp theo, các thành phần có mức rủi ro cao, hoặc trọng yếu được xem xét đánh giá theo phương pháp không chính thức;
- Cuối cùng hệ thống được xem xét đánh giá toàn diện rủi ro ở mức chi tiết.

Đánh giá rủi ro ATTT - Phương pháp kết hợp

❖ Ưu điểm:

- Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT;
- Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu;
- Có thể giúp giảm chi phí với đa số các tổ chức.

❖ Nhược điểm:

- Nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết.

❖ Phù hợp các tổ chức với hệ thống CNTT quy mô vừa và lớn.

6.2 Giới thiệu bộ chuẩn quản lý ATTT ISO/IEC 27000

- ❖ Bộ chuẩn ISO 27000 là bộ chuẩn về quản lý ATTT (Information Technology - Code of Practice for Information Security Management) được tham chiếu rộng rãi nhất;
- ❖ Bộ chuẩn ISO/IEC 17799 (được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC)) là tiền thân của ISO 27000;
- ❖ Năm 2005, ISO 17799 được chỉnh sửa và trở thành ISO 17799:2005;
- ❖ Năm 2007, ISO 17799:2005 được đổi tên thành ISO 27002 song hành với ISO 27001.

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27002

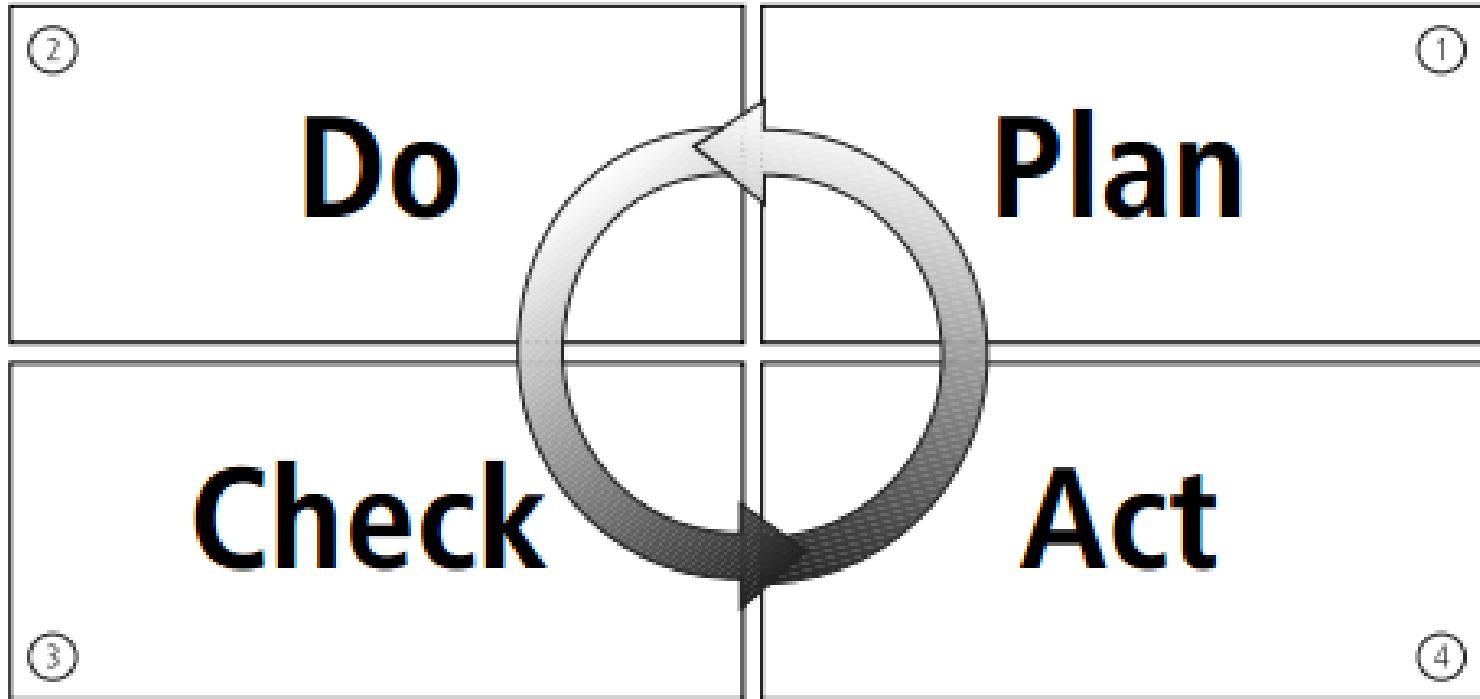
- ❖ ISO/IEC 27002 gồm 127 điều, cung cấp cái nhìn tổng quan về nhiều lĩnh vực trong ATTT;
- ❖ ISO/IEC 27002 đề ra các khuyến nghị về quản lý ATTT cho những người thực hiện việc khởi tạo, thực hiện và duy trì an ninh an toàn trong tổ chức của họ;
- ❖ ISO/IEC 27002 được thiết kế cung cấp nền tảng cơ sở giúp đề ra các chuẩn ATTT cho tổ chức và các thực tế quản lý ATTT một cách hiệu quả.

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

- ❖ ISO 27001 cung cấp các thông tin để:
 - Thực thi các yêu cầu của ISO/IEC 27002, và
 - Cài đặt một hệ thống quản lý an toàn thông tin (information security management system - ISMS).
- ❖ ISO/IEC 27001:2005: chuyên về hệ thống quản lý an toàn thông tin (Information Security Management System):
 - Cung cấp các chi tiết cho thực hiện chu kỳ Lập kế hoạch – Thực hiện – Kiểm tra – Hành động (Plan-Do-Check-Act)
- ❖ ISO 27001 cung cấp các thông tin để thực hiện việc quản lý ATTT, nhưng:
 - Nó chỉ tập trung vào các phần việc phải thực hiện;
 - Không chỉ rõ cách thức thực hiện.

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

- ❖ ISO/IEC 27001:2005: Plan-Do-Check-Act



Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

❖ ISO/IEC 27001:2005: Plan-Do-Check-Act → Plan:

- Đề ra phạm vi của ISMS;
- Đề ra chính sách của ISMS;
- Đề ra hướng tiếp cận đánh giá rủi ro;
- Nhận dạng các rủi ro;
- Đánh giá rủi ro;
- Nhận dạng và đánh giá các lựa chọn phương pháp xử lý rủi ro;
- Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát;
- Chuẩn bị tuyển bố/báo cáo áp dụng.

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

❖ ISO/IEC 27001:2005: Plan-Do-Check-Act → Do:

- Xây dựng kế hoạch xử lý rủi ro;
- Thực thi kế hoạch xử lý rủi ro;
- Thực thi các kiểm soát;
- Thực thi các chương trình đào tạo chuyên môn và giáo dục ý thức;
- Quản lý các hoạt động;
- Quản lý các tài nguyên;
- Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh.

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

❖ ISO/IEC 27001:2005: Plan-Do-Check-Act → Check:

- Thực thi các thủ tục giám sát;
- Thực thi việc đánh giá thường xuyên tính hiệu quả của ISMS;
- Thực hiện việc kiểm toán (audit) nội bộ với ISMS;
- Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý;
- Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS;

Bộ chuẩn ISO/IEC 27000 - ISO/IEC 27001

❖ ISO/IEC 27001:2005: Plan-Do-Check-Act → Act:

- Thực hiện các cải tiến đã được nhận dạng;
- Thực hiện các hành động sửa chữa và ngăn chặn;
- Áp dụng các bài đã được học;
- Thảo luận kết quả với các bên quan tâm;
- Đảm bảo các cải tiến đạt được các mục tiêu.

Bộ chuẩn ISO/IEC 27000 – Danh sách các chuẩn con

ISO 27000 Series Standard	Pub Date	Title or Topic	Comment
27000	2009	Series Overview and Terminology	Defines terminology and vocabulary for the standard series
27001	2005	Information Security Management System Specification	Drawn from BS 7799:2
27002	2007	Code of Practice for Information Security Management	Renamed from ISO/IEC 17799; drawn from BS 7799:1
27004	2009	Information Security Measurements and Metrics	
27005	2008	ISMS Risk Management	Supports 27001, but doesn't recommend any specific risk method
27006	2007	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification

Bộ chuẩn ISO/IEC 27000 – Danh sách các chuẩn con

Planned 27000 Series Standards			
27003	Planned	Information Security Management Systems Implementation Guidelines	Expected in 2010
27007	Planned	Guideline for ISMS Auditing	Focuses on management systems
27008	Planned	Guideline for Information Security Auditing	Focuses on security controls
27013	Planned	Guideline on the Integrated Implementation of ISO/IEC 20000-1 and ISO/IEC 27001	
27014	Planned	Information Security Governance Framework	
27015	Planned	Information Security Management Guidelines for Finance and Insurance Sectors	

6.3 Pháp luật và chính sách ATTT

1. Giới thiệu về pháp luật và chính sách an toàn thông tin
2. Luật quốc tế về an toàn thông tin
3. Luật Việt Nam về an toàn thông tin

Giới thiệu về pháp luật và chính sách ATTT

- ❖ Các chính sách và pháp luật có vai trò rất quan trọng trong việc đảm bảo an toàn cho thông tin, hệ thống và mạng:
 - Trong đó vai trò của nhân viên đảm bảo an toàn cho thông tin là rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho thông tin, hệ thống và mạng và giảm thiệt hại nếu xảy ra sự cố;
 - Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức ATTT:
 - Luôn nắm vững môi trường pháp lý hiện tại và các luật và các quy định luật pháp;
 - Luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp.
 - Thực hiện việc giáo dục ý thức về luật pháp và đạo đức ATTT cho cán bộ quản lý và nhân viên trong tổ chức, đảm bảo sử dụng đúng mục đích các công nghệ đảm bảo ATTT.

Giới thiệu về pháp luật và chính sách ATTT

❖ Phân biệt Luật (Law) và Đạo đức (Ethics):

- **Luật:** Gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể;
 - Các điều luật thường được xây dựng từ các vấn đề đạo đức.
- **Đạo đức:** Định nghĩa những hành vi xã hội chấp nhận được;
 - Đạo đức thường dựa trên các đặc điểm văn hóa. Do đó hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau là khác nhau;
 - Một số hành vi vi phạm đạo được được luật hóa trên toàn thế giới: trộm, cướp, cưỡng dâm, bạo hành trẻ em,...
- **Khác biệt giữa luật và đạo đức:**
 - Luật được thực thi bởi các cơ quan chính quyền;
 - Đạo đức không được thực thi bởi các cơ quan chính quyền.

Giới thiệu về pháp luật và chính sách ATTT

❖ Trách nhiệm của tổ chức (Organization Liability):

- Trách nhiệm của một tổ chức là trách nhiệm trước luật pháp của tổ chức đó được mở rộng ngoài phạm vi luật hình sự và luật hợp đồng;
- Gồm cả trách nhiệm pháp lý phải hoàn trả và đền bù cho những hành vi sai trái;
- Nếu một nhân viên của 1 công ty/tổ chức thực hiện hành vi phạm pháp hoặc phi đạo đức, gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm về pháp lý, tài chính;
- Ví dụ: Bảo vệ của 1 siêu thị giam giữ hoặc hành hung khách hàng gây thương tích:
 - NV bảo vệ có thể bị bắt tạm giam để điều tra;
 - Siêu thị phải có trách nhiệm đền bù cho khách hàng.

Giới thiệu về pháp luật và chính sách ATTT

❖ Chính sách (Policy) và Luật (Law):

- Trong một tổ chức, nhân viên ATTT có trách nhiệm duy trì an toàn thông qua việc thiết lập và các chính sách ATTT;
- Chính sách (còn gọi là quy định, nội quy) là các quy định về các hành vi chấp nhận được của các nhân viên trong tổ chức tại nơi làm việc;
- Chính sách là các "luật" của tổ chức có giá trị thực thi trong nội bộ, gồm một tập các quy định và các chế tài xử phạt bắt buộc phải thực hiện;
- Các chính sách/nội quy cần được nghiên cứu, soạn thảo kỹ lưỡng;
- Chính sách cần đầy đủ, đúng đắn và áp dụng công bằng với mọi nhân viên;
- Khác biệt giữa chính sách và luật:
 - Luật luôn bắt buộc;
 - Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được.

Giới thiệu về pháp luật và chính sách ATTT

❖ Các yêu cầu của chính sách:

- Phổ biến (Dissemination): có khả năng phổ biến rộng rãi, bằng tài liệu giấy hoặc điện tử;
- Xem xét (Review): Nhân viên có thể xem, hiểu được – cần thực hiện trên nhiều ngôn ngữ, ví dụ bằng tiếng Anh và tiếng địa phương;
- Có thể hiểu (Comprehension): Chính sách cần rõ ràng dễ hiểu – tổ chức cần có các điều tra/khảo sát về mức độ hiểu biết/nắm bắt các chính sách của nhân viên;
- Tuân thủ (Obligation): Cần có biện pháp để nhân viên cam kết thực hiện – thông qua ký văn bản cam kết hoặc tick vào ô xác nhận tuân thủ;
- Áp dụng đồng đều, bình đẳng (Uniform enforcement): Chính sách cần được thực hiện đồng đều, bình đẳng, nhất quán, không có ưu tiên với bất kỳ nhân viên nào, kể cả người quản lý.

Giới thiệu về pháp luật và chính sách ATTT

❖ Các kiểu luật:

- Luật dân sự (Civil Law): là luật điều chỉnh các quan hệ dân sự giữa các tổ chức và cá nhân trong một quốc gia;
- Luật hình sự (Criminal Law): là luật điều chỉnh các hành vi gây hại cho xã hội và nhà nước chủ động thực thi;
- Luật công cộng (Public Law): quy định cấu trúc của các đơn vị hành chính (quốc hội, chính phủ và các đơn vị trực thuộc), các quan hệ giữa công dân với công dân, giữa các tổ chức và quan hệ với các chính phủ các nước khác;
 - VD: Hiến pháp, luật hành chính.
- Luật riêng (Private Law): điều chỉnh các quan hệ trong phạm vi hẹp, như quan hệ gia đình, thương mại, lao động và quan hệ giữa các cá nhân với các tổ chức.

Luật quốc tế về ATTT

❖ Các luật ATTT của Mỹ:

- Các luật tội phạm máy tính
- Các luật về sự riêng tư
- Luật xuất khẩu và chống gián điệp
- Luật bản quyền
- Luật tự do thông tin

❖ Các luật ATTT và tổ chức luật quốc tế:

- Hội đồng châu Âu về chống tội phạm mạng
- Hiệp ước bảo vệ quyền sở hữu trí tuệ.

Luật quốc tế về ATTT – Luật Mỹ

❖ Các luật về tội phạm máy tính:

- Computer Fraud and Abuse Act of 1986 (CFA Act) – quy định về các tội phạm lừa đảo và lạm dụng máy tính;
- Computer Security Act, 1987: đề ra các nguyên tắc đảm bảo an toàn cho hệ thống máy tính;s
- National Information Infrastructure Protection Act of 1996 là bản sửa đổi của CFA Act, tăng khung hình phạt một số tội phạm máy tính đến 20 năm tù;
- USA PATRIOT Act, 2001: cho phép các cơ quan chính quyền một số quyền nhằm phòng chống khủng bố hiệu quả hơn;
- USA PATRIOT Improve-ment and Reauthorization Act: Mở rộng của USA PATRIOT Act, 2001, cấp cho các cơ quan chính quyền nhiều quyền hạn hơn cho nhiệm vụ phòng chống khủng bố.

Luật quốc tế về ATTT – Luật Mỹ

- ❖ Các luật về sự riêng tư: bảo vệ quyền riêng tư của người dùng, bảo vệ các thông tin cá nhân của người dùng:
 - Federal Privacy Act, 1974: luật Liên bang Mỹ bảo vệ quyền riêng tư của người dùng;
 - Electronic Communications Privacy Act , 1986: luật bảo vệ quyền riêng tư trong các giao tiếp điện tử;
 - Health Insurance Portability and Accountability Act, 1996 (HIPAA): bảo vệ tính bí mật và an toàn của các dữ liệu y tế của người bệnh;
 - Tổ chức/cá nhân vi phạm có thể bị phạt đến 250.000 USD hoặc 10 năm tù;
 - Financial Services Modernization Act or Gramm-Leach-Bliley Act, 1999: điều chỉnh các hoạt động liên quan đến ATTT của các ngân hàng, bảo hiểm và các hãng an ninh.

Luật quốc tế về ATTT – Luật Mỹ

- ❖ Luật xuất khẩu và chống gián điệp: hạn chế việc xuất khẩu các công nghệ và hệ thống xử lý thông tin và phòng chống gián điệp kinh tế;
 - Economic Espionage Act, 1996: phòng chống việc thực hiện giao dịch có liên quan đến bí mật kinh tế và công nghệ;
 - Security and Freedom through Encryption Act, 1999: quy định về các vấn đề có liên quan đến sử dụng mã hóa trong đảm bảo an toàn và tự do thông tin.

Luật quốc tế về ATTT – Luật Mỹ

- ❖ U.S. Copyright Law: Luật bản quyền của Mỹ.
 - Điều chỉnh các vấn đề có liên quan đến xuất bản, quyền tác giả của các tài liệu, phần mềm, bao gồm cả các tài liệu số.
- ❖ Luật tự do thông tin (Freedom of Information Act, 1966 (FOIA)):
 - Các cá nhân được truy nhập các thông tin không gây tổn hại đến an ninh quốc gia.

Luật quốc tế về ATTT – Luật Quốc tế

❖ Các luật ATTT và tổ chức luật quốc tế:

- Hội đồng châu Âu về chống tội phạm mạng (Council of Europe Convention on Cybercrime): Hiệp ước về chống tội phạm mạng được Hội đồng châu Âu phê chuẩn vào năm 2001;
- Hiệp ước bảo vệ quyền sở hữu trí tuệ (Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)): do Tổ chức Thương mại thế giới WTO chủ trì đàm phán trong giai đoạn 1986–1994;
- Digital Millennium Copyright Act (DMCA): luật bản quyền số Thiên niên kỷ.

Luật Việt Nam về ATTT

- ❖ Luật ATTT mạng của Việt Nam được Quốc hội thông qua vào tháng 11.2015 (86/2015/QH13) và có hiệu lực từ 1/7/2016: Đây là cơ sở pháp lý quan trọng nhất cho các hoạt động có liên quan đến ATTT.
- ❖ Luật ATTT mạng gồm 8 chương với 54 điều:
 - Chương I: NHỮNG QUY ĐỊNH CHUNG
 - Chương II: BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG
 - Chương III: MẬT MÃ DÂN SỰ
 - Chương IV: TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT ATTT MẠNG
 - Chương V: KINH DOANH TRONG LĨNH VỰC ATTT MẠNG
 - Chương VI: PHÁT TRIỂN NGUỒN NHÂN LỰC ATTT MẠNG
 - Chương VII: QUẢN LÝ NHÀ NƯỚC VỀ ATTT MẠNG
 - Chương VIII: ĐIỀU KHOẢN THI HÀNH

Luật Việt Nam về ATTT

- ❖ Luật An ninh mạng của Việt Nam được Quốc hội thông qua vào tháng 6 năm 2018 và có hiệu lực từ 1/1/2019:
 - Quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật trên không gian mạng.

Luật Việt Nam về ATTT

❖ Một số văn bản khác có liên quan đến ATTT:

- Luật CNTT số 67/2006/QH11 của Quốc hội, ngày 12/07/2006
- Nghị định số 90/2008/NĐ-CP của Chính Phủ "Về chống thư rác", ngày 13/08/2008.
- Quyết định số 59/2008/QĐ-BTTTT của Bộ Thông tin và Truyền thông "Ban hành Danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số", ngày 31/12/2008.
- Quyết định 63/QĐ-TTg của Thủ tướng CP "Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020", ngày 13/01/2010.
- Chỉ thị số 897/CT-TTg của Thủ tướng CP "V/v tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số", 10/06/2011.

Luật Việt Nam về ATTT

❖ Một số văn bản khác có liên quan đến ATTT:

- Thông tư số 23/2011/TT-BTTTT của Bộ TT&TT "Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước", ngày 11/08/2011.
- Nghị định số 77/2012/NĐ-CP của Chính Phủ "Sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 của Chính phủ về chống thư rác", ngày 05/10/2012.
- Nghị định 72/2013/NĐ-CP của Chính Phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng; quy định về việc chia sẻ thông tin trên các trang mạng xã hội.
- Dự thảo Luật An ninh mạng được đưa ra lấy ý kiến Quốc hội và các chuyên gia trong năm 2017. Dự kiến thông qua trong năm 2018.

6.4 Vấn đề đạo đức ATTT

- ❖ Nhiều tổ chức xã hội nghề nghiệp đã ban hành các quy tắc ứng xử (Code of Conduct) bắt buộc tại nơi làm việc:
 - Luật sư, bác sĩ nếu vi phạm nghiêm trọng các quy tắc ứng xử có thể bị cấm hành nghề.
 - Các vận động viên thể thao vi phạm bộ quy tắc ứng xử có thể bị cấm thi đấu có thời hạn hoặc vĩnh viễn.

6.4 Vấn đề đạo đức ATTT

❖ CNTT và ATTT không có bộ quy tắc ứng xử bắt buộc;

- Một số tổ chức nghề nghiệp như ACM (Association for Computing Machinery) và ISSA (Information Systems Security Association) hợp tác để đề ra các quy tắc ứng xử trong ATTT;
- Tuy nhiên, các quy tắc ứng xử trong ATTT chỉ có tính khuyến nghị mà các tổ chức trên không có thẩm quyền buộc phải thực hiện;
- Hiệp hội ATTT Việt Nam đã công bố Bộ Qui tắc ứng xử ATTT vào đầu năm 2015, đưa ra một số quy tắc và khuyến nghị về những việc không được làm cho các thành viên và các nhân viên của các tổ chức hoạt động trong lĩnh vực ATTT.

Vấn đề đạo đức ATTT

❖ Bộ Quy tắc ứng xử 10 điểm (Ten Commandments of Computer Ethics) đề xuất bởi Viện đạo đức máy tính (Mỹ):

1. Không được sử dụng máy tính để gây hại cho người khác;
2. Không được can thiệp vào công việc của người khác trên máy tính;
3. Không trộm cắp các files trên máy tính của người khác;
4. Không được sử dụng máy tính để trộm cắp;
5. Không được sử dụng máy tính để tạo bằng chứng giả;
6. Không sao chép hoặc sử dụng phần mềm không có bản quyền;
7. Không sử dụng các tài nguyên máy tính của người khác khi không được phép hoặc không có bồi thường thỏa đáng;
8. Không chiếm đoạt tài sản trí tuệ của người khác;
9. Nên suy nghĩ về các hậu quả xã hội của chương trình mình đang xây dựng hoặc hệ thống đang thiết kế;
10. Nên sử dụng máy tính một cách có trách nhiệm, đảm bảo sự quan tâm và tôn trọng đến đồng bào của mình.

Vấn đề đạo đức ATTT

❖ Sự khác biệt về vấn đề đạo đức giữa các nền văn hóa:

- Nhận thức về vấn đề đạo đức trong sử dụng các tài nguyên của cơ quan, tổ chức là rất khác biệt giữa các quốc gia có nền văn hóa khác nhau;
- Trong nhiều trường hợp, hành vi được phép của một số cá nhân trong một quốc gia lại vi phạm quy tắc đạo đức của quốc gia khác;
- VD: Vấn đề vi phạm bản quyền phần mềm ở các nước tiên tiến như Mỹ và châu Âu ở mức tương đối thấp, nhưng ở mức rất cao ở các nước châu Á và châu Phi.
 - Tỷ lệ vi phạm bản quyền phần mềm ở Việt Nam khoảng 90%.

Vấn đề đạo đức ATTT

❖ Vấn đề vi phạm bản quyền phần mềm:

- Vấn đề vi phạm bản quyền phần mềm ở mức rất nghiêm trọng, đặc biệt là tại các nước đang phát triển ở châu Á và châu Phi;
- Người dùng đa số có hiểu biết về vấn đề bản quyền phần mềm, nhưng coi việc sử dụng phần mềm bất hợp pháp là bình thường vì nhiều nước chưa có quy định hoặc không xử lý nghiêm vi phạm.

Vấn đề đạo đức ATTT

❖ Vấn đề lạm dụng các tài nguyên của công ty, tổ chức:

- Một số công ty/tổ chức chưa có các quy định cấm nhân viên sử dụng các tài nguyên của công ty, tổ chức vào việc riêng. Một số có quy định nhưng chưa được thực thi chặt chẽ và chưa có chế tài xử phạt nghiêm minh;
- Các hành vi lạm dụng thường gặp:
 - In ấn tài liệu riêng;
 - Sử dụng email cá nhân cho việc riêng;
 - Tải các tài liệu/files không được phép;
 - Cài đặt và chạy các chương trình/phần mềm không được phép;
 - Sử dụng máy tính công ty làm việc riêng;
 - Sử dụng các loại phương tiện làm việc khác như điện thoại công ty quá mức vào việc riêng;