CMC UNIVERSITY
Aspire to Inspire the Digital World

INFORMATION SECURITY
An toàn thông tin

PGS.TS. Hoàng Trọng Minh

Hà Nội, ngày … tháng … năm 2025

CMC UNIVERSITY
Aspire to Inspire the Digital World

Chương 1: Tổng quan về an toàn thông tin

Mục lục

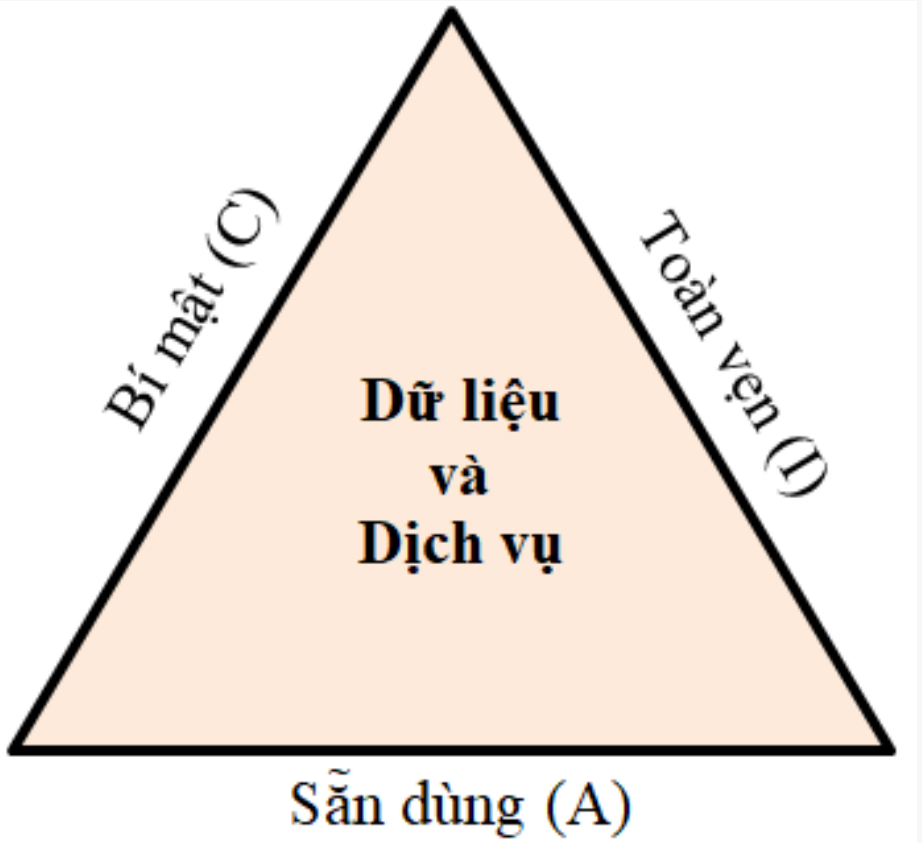
1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

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

- An toàn thông tin là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép.

- An toàn thông tin là việc bảo vệ các thuộc tính bí mật (Confidentiality), tính toàn vẹn (Integrity) và tính sẵn dùng (Availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải



1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ **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). Trong đó dữ liệu thông tin từ hệ thống gốc được sao lưu ra các thiết bị lưu trữ vật lý đặt ở một vị trí khác

1.1 Khái niệm về an toàn thông tin

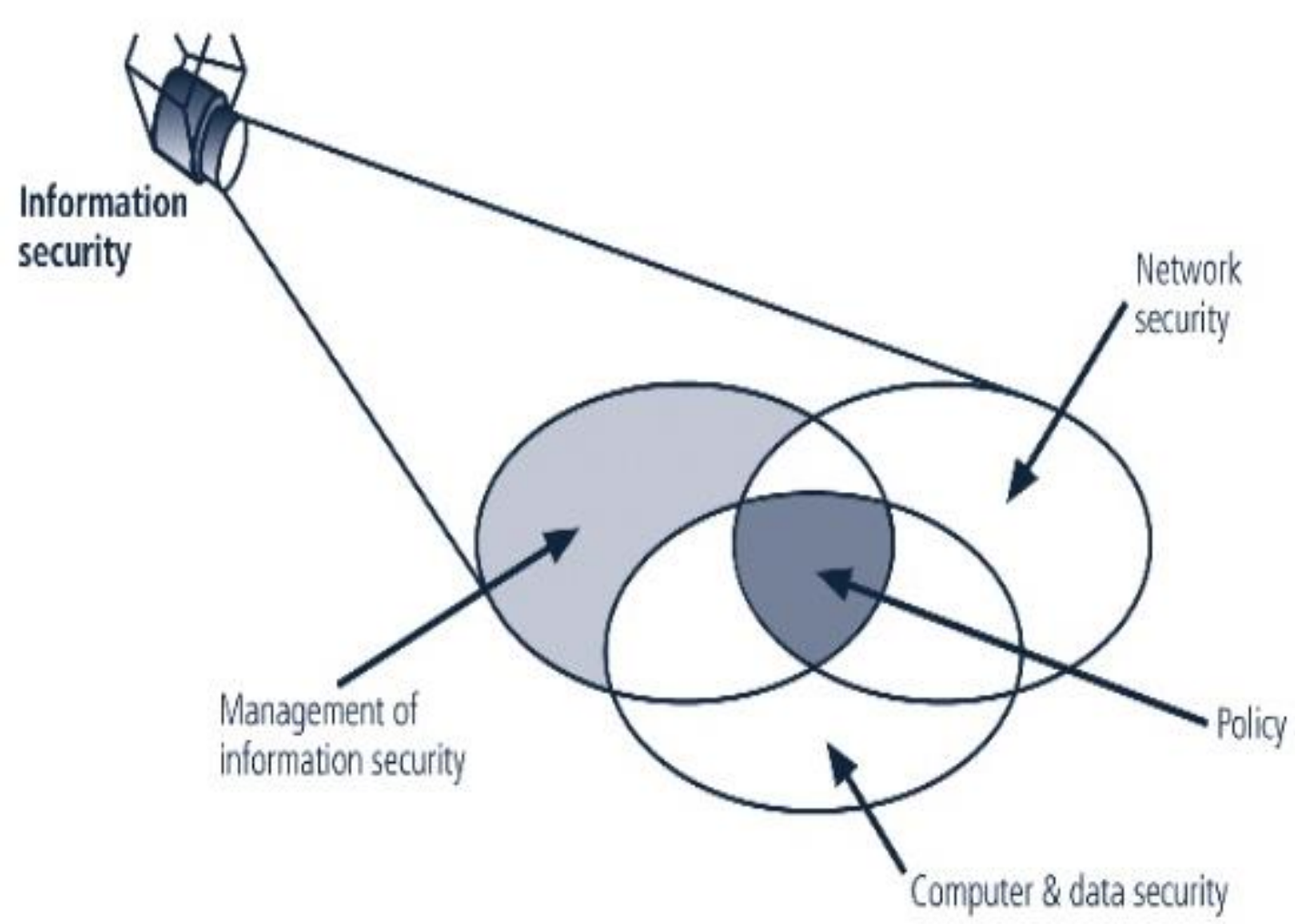
➢ Các thành phần của ATTT:

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

1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

Các thành phần của ATTT:



1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- **An toàn máy tính và dữ liệu** là việc đảm bảo an toàn cho hệ thống phần cứng, phần mềm và dữ liệu trên máy tính; đảm bảo cho máy tính có thể vận hành an toàn, đáp ứng các yêu cầu của người sử dụng. Bao gồm:
  - ✓ Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ;
  - ✓ Vấn đề kiểm soát truy cập;
  - ✓ 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.

1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- **An toàn mạng** là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các tấn công, xâm nhập trái phép. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:
  - ✓ Các tường lửa, proxy cho lọc gói tin và kiểm soát truy cập;
  - ✓ 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.

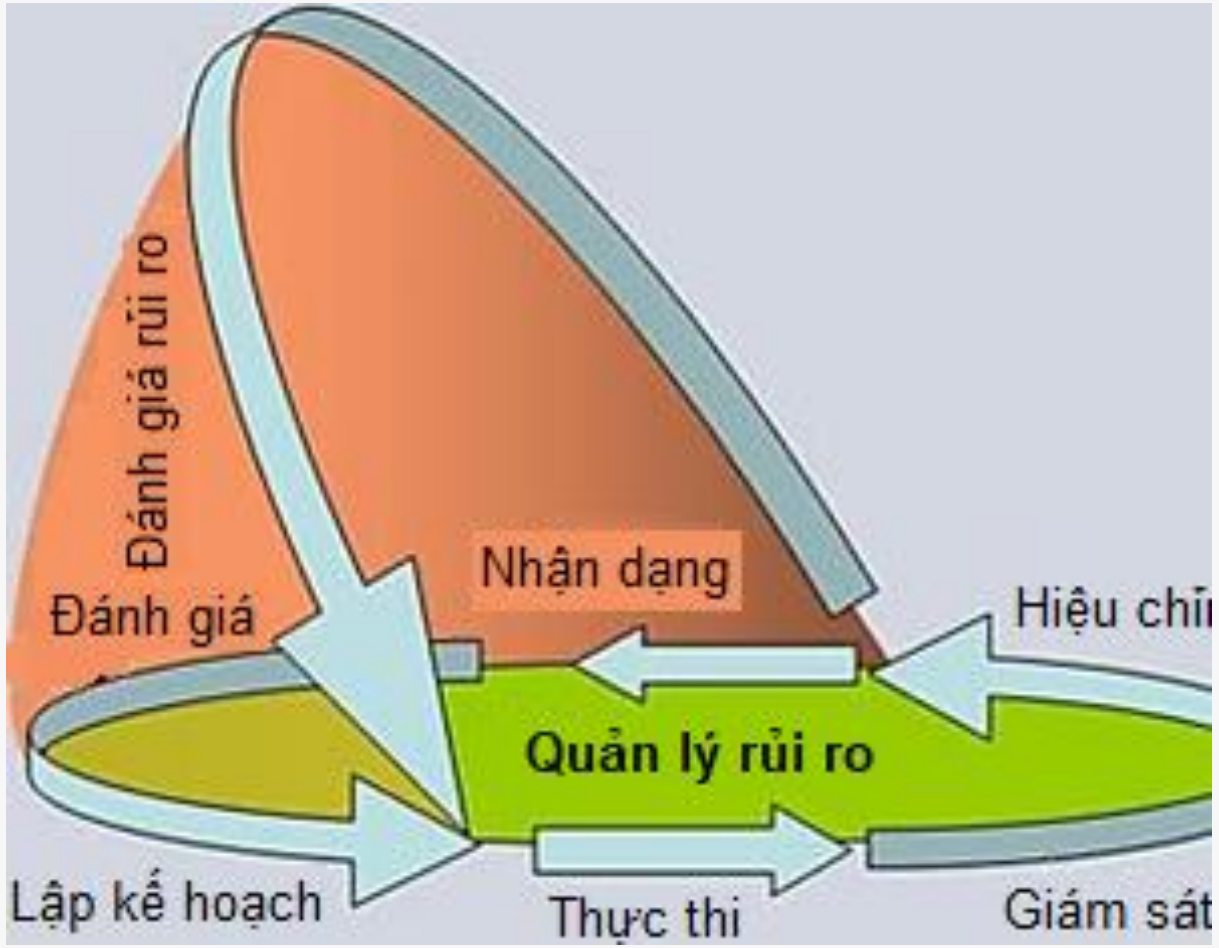
1.1 Khái niệm về an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- **Quản lý an toàn thông tin** là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Bao gồm các nội dung:
  - ✓ Quản lý các rủi ro (Risk management) là nội dung cốt lõi, trong đó quan trọng là việc nhận dạng và đánh giá rủi ro (Risk assessment).
  - ✓ Các chuẩn an toàn thông tin, chính sách an toàn thông tin và
  - ✓ Vấn đề đào tạo, nâng cao ý thức an toàn thông tin của người dùng.
  - ✓ Chu trình quản lý an toàn thông tin: Lập kế hoạch (Plan), Thực thi kế hoạch (Implement), Giám sát kết quả thực hiện (Monitor) và Hiệu chỉnh kiểm soát (Control)

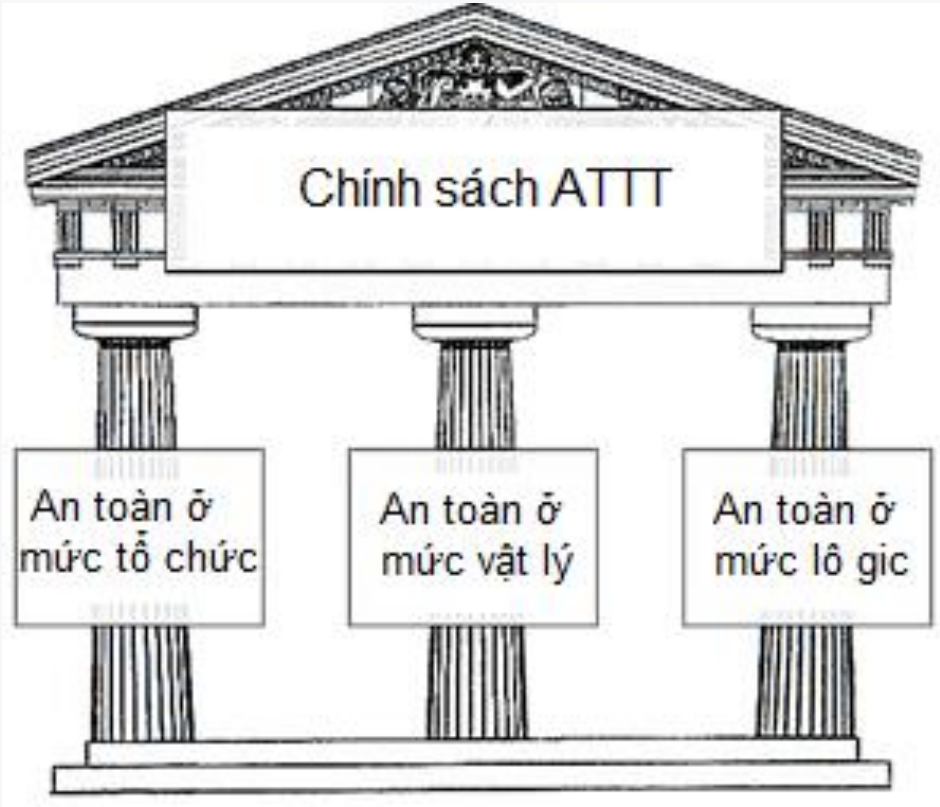
1.1 Khái niệm về an toàn thông tin

Chu trình quản lý an toàn thông tin



1.1 Khái niệm về an toàn thông tin

- **Chính sách an toàn thông tin (Information security policy)** là các nội quy, quy định của tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ. Chính sách an toàn thông tin gồm 3 thành phần:
  - ✓ 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).

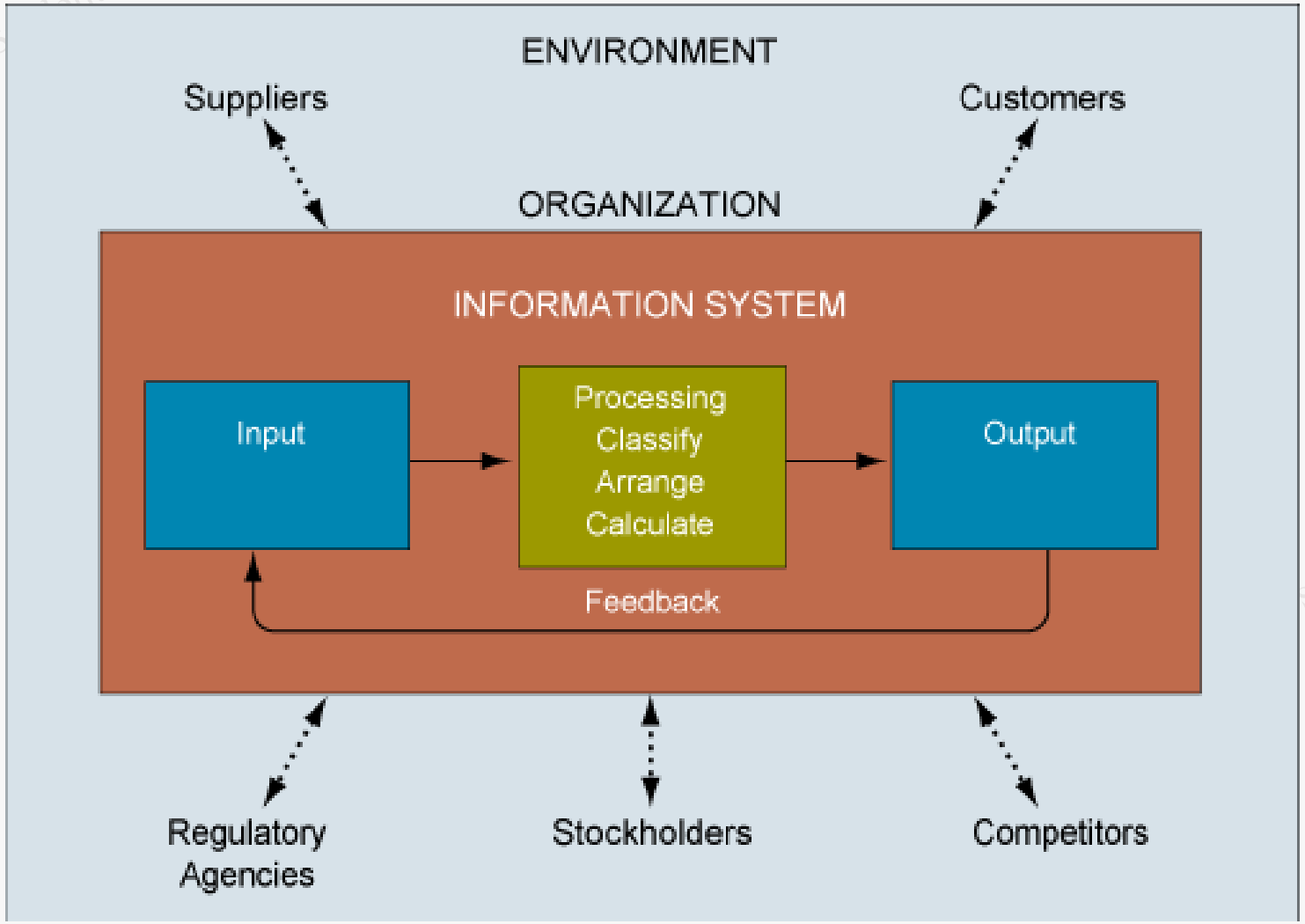


1.2 Khái niệm về an toàn hệ thống thông tin

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

1.2 Khái niệm về an toàn hệ thống thông tin

Sơ đồ hệ thống thông tin

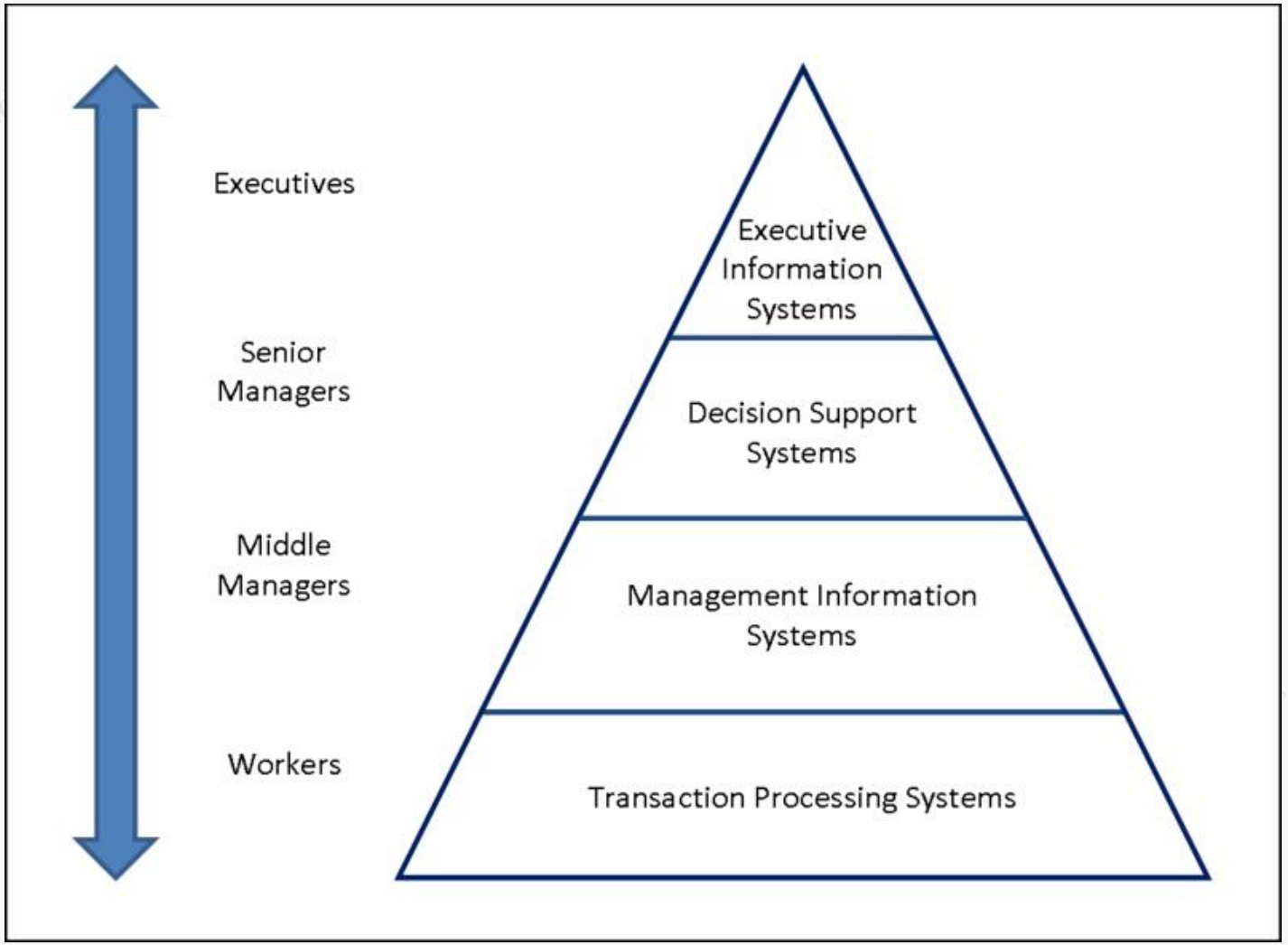


1.2 Khái niệm về an toàn hệ thống thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- 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).

1.2 Khái niệm về an toàn hệ thống thông tin



Các loại hệ thống thông tin (mô hình tháp)

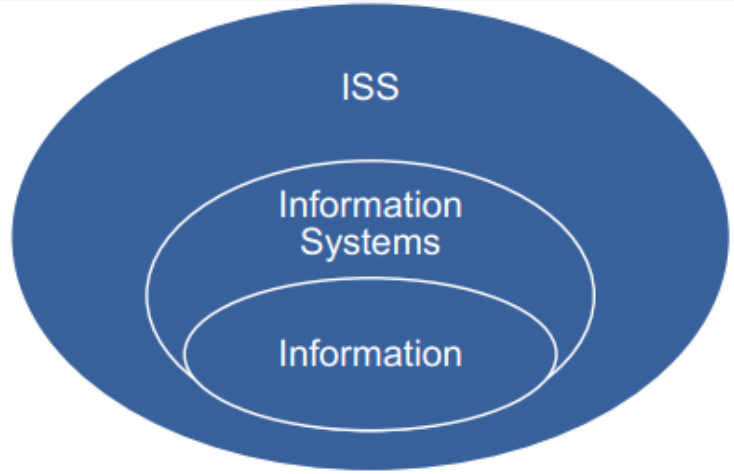
1.2 Khái niệm về an toàn hệ thống thông tin

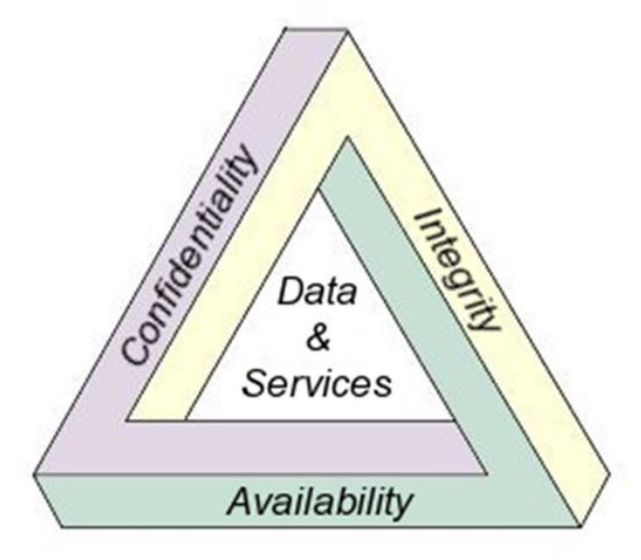
- Một hệ thống thông tin dựa trên máy tính (Computer-Based Information System) là một hệ thống thông tin sử dụng công nghệ máy tính để thực thi các nhiệm vụ.
- Các thành phần của hệ thống thông tin dựa trên máy tính:
  - ✓ Hardware: phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu
  - ✓ Software: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

1.2 Khái niệm về an toàn hệ thống thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- An toàn hệ thống thông tin (ISS - Information Systems Security): là việc đảm bảo các thuộc tính an ninh an toàn của hệ thống thông tin:
  - ✓ Bí mật (Confidentiality)
  - ✓ Toàn vẹn (Integrity)
  - ✓ Sẵn dùng (Availability)

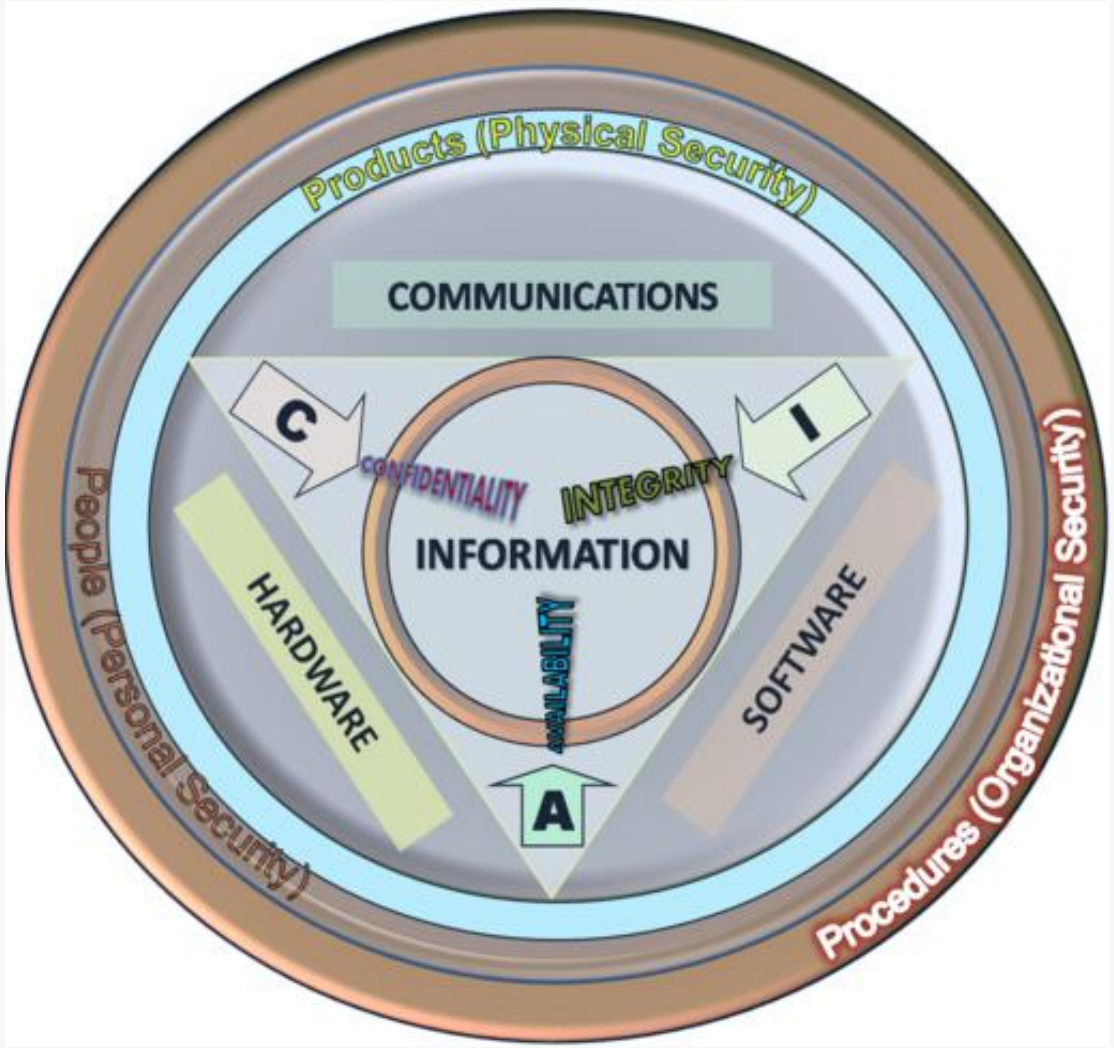




1.2 Khái niệm về an toàn hệ thống thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ An toàn hệ thống thông tin (ISS)



1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

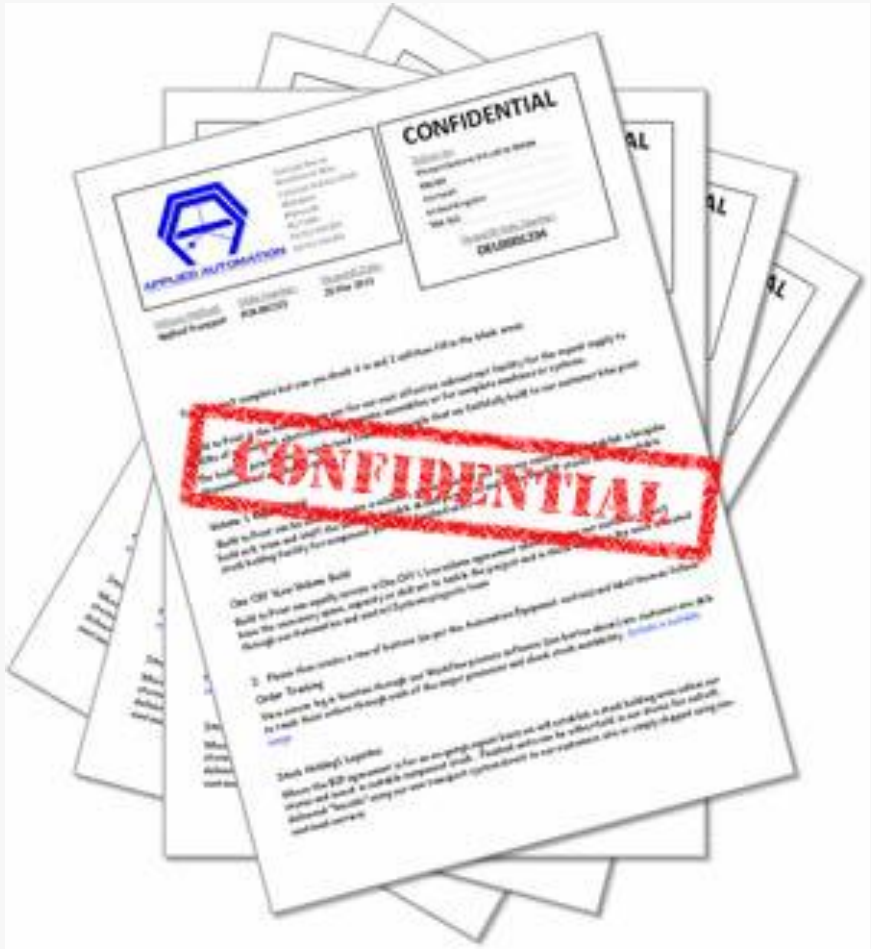
- Việc đảm bảo an toàn thông tin, hoặc hệ thống thông tin là việc đảm bảo ba thuộc tính quan trọng của thông tin, hoặc hệ thống, bao gồm:
  - ✓ Tính Bí mật,
  - ✓ Tính Toàn vẹn,
  - ✓ Tính Sẵn dùng.

- Ngoài ra một thuộc tính mở rộng quan trọng khác là tính xác thực.

1.3 Các khía cạnh cơ bản của an toàn thông tin

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

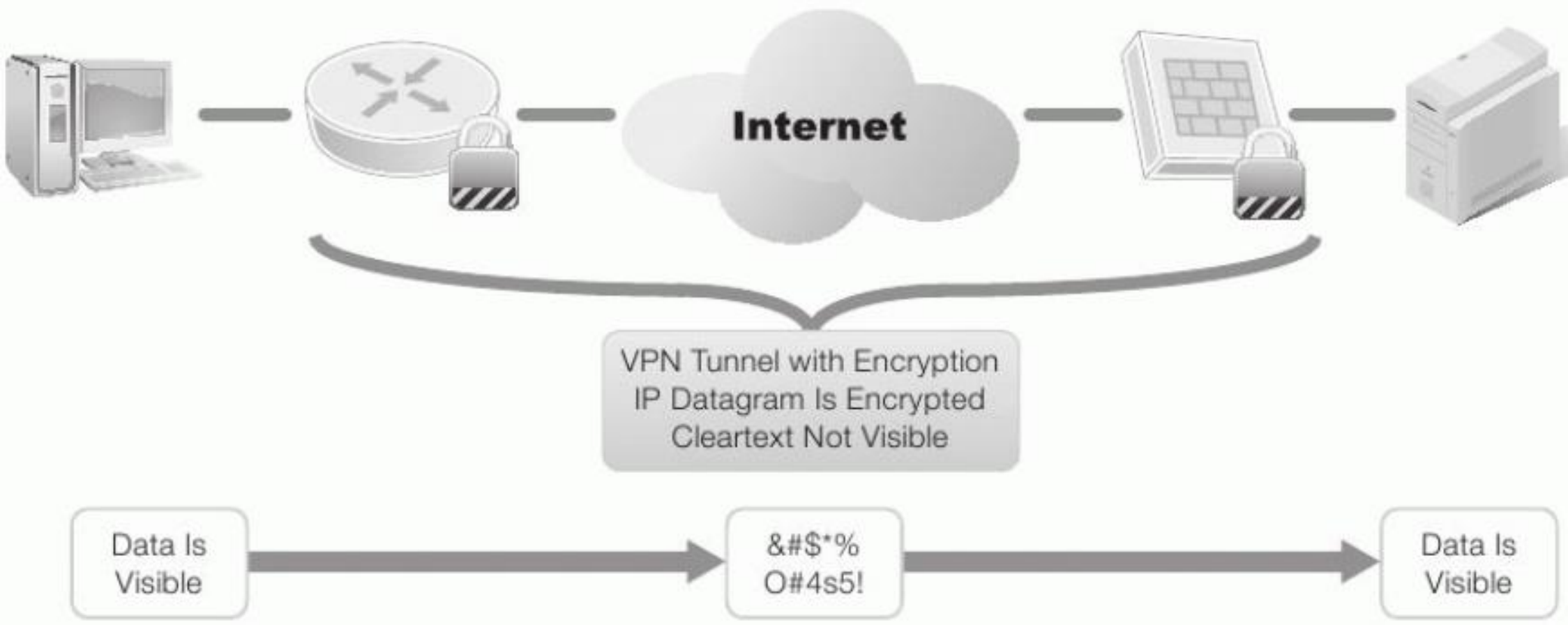
- Các thông tin bí mật có thể gồm:
  - ✓ Dữ liệu riêng của cá nhân;
  - ✓ Các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan/tổ chức;
  - ✓ Các thông tin có liên quan đến an ninh quốc gia.



1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ Tính bí mật được đảm bảo bằng kênh mã hóa VPN

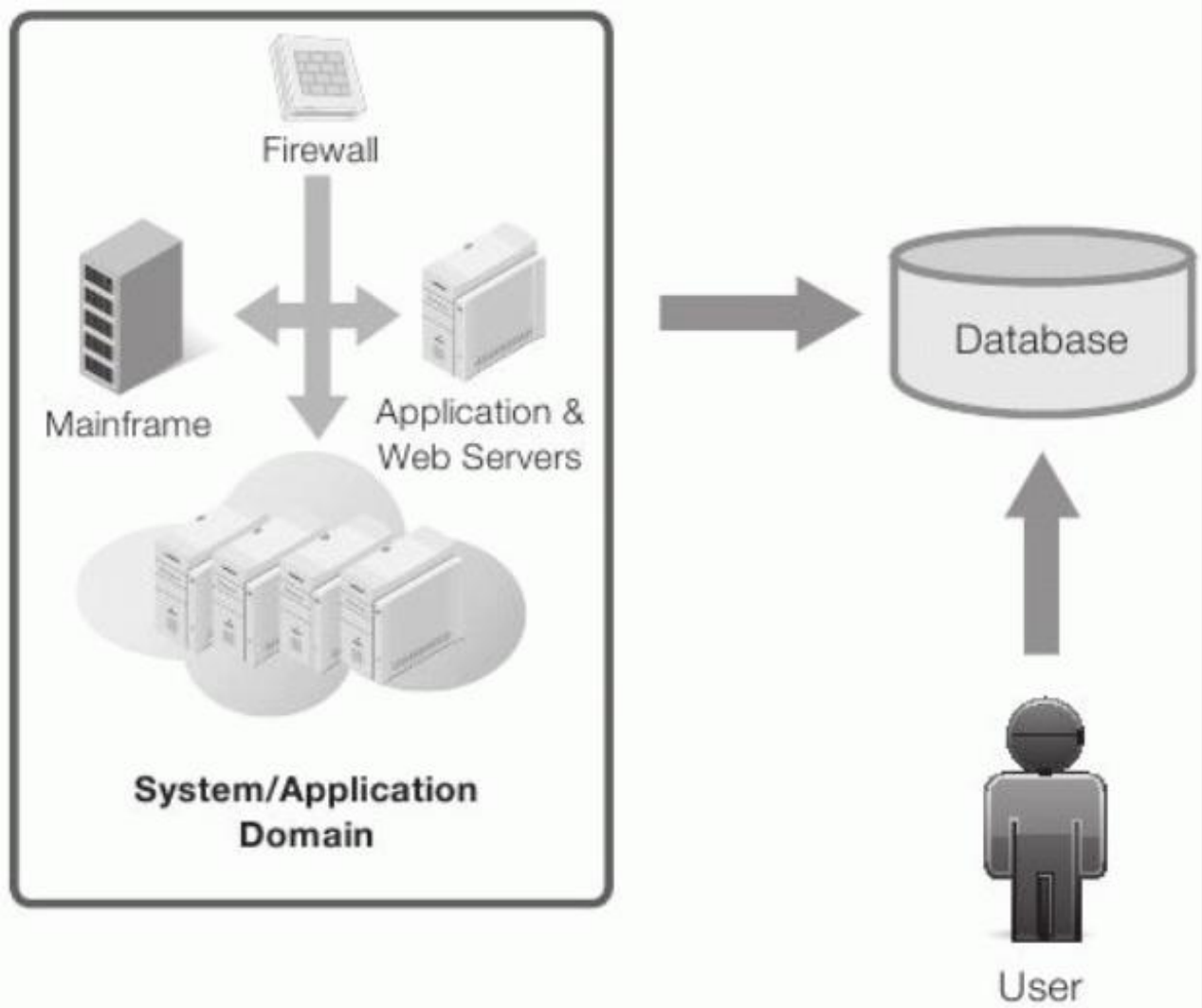


1.3 Các khía cạnh cơ bản của an toàn thông tin

- Tính toàn vẹn (Integrity): thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền.
- Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu.
  - ✓ Trong nhiều tổ chức, thông tin có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế;
  - ✓ Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin.
- Dữ liệu là toàn vẹn nếu:
  - ✓ Dữ liệu không bị thay đổi;
  - ✓ Dữ liệu hợp lệ;
  - ✓ Dữ liệu chính xác.

1.3 Các khía cạnh cơ bản của an toàn thông tin

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



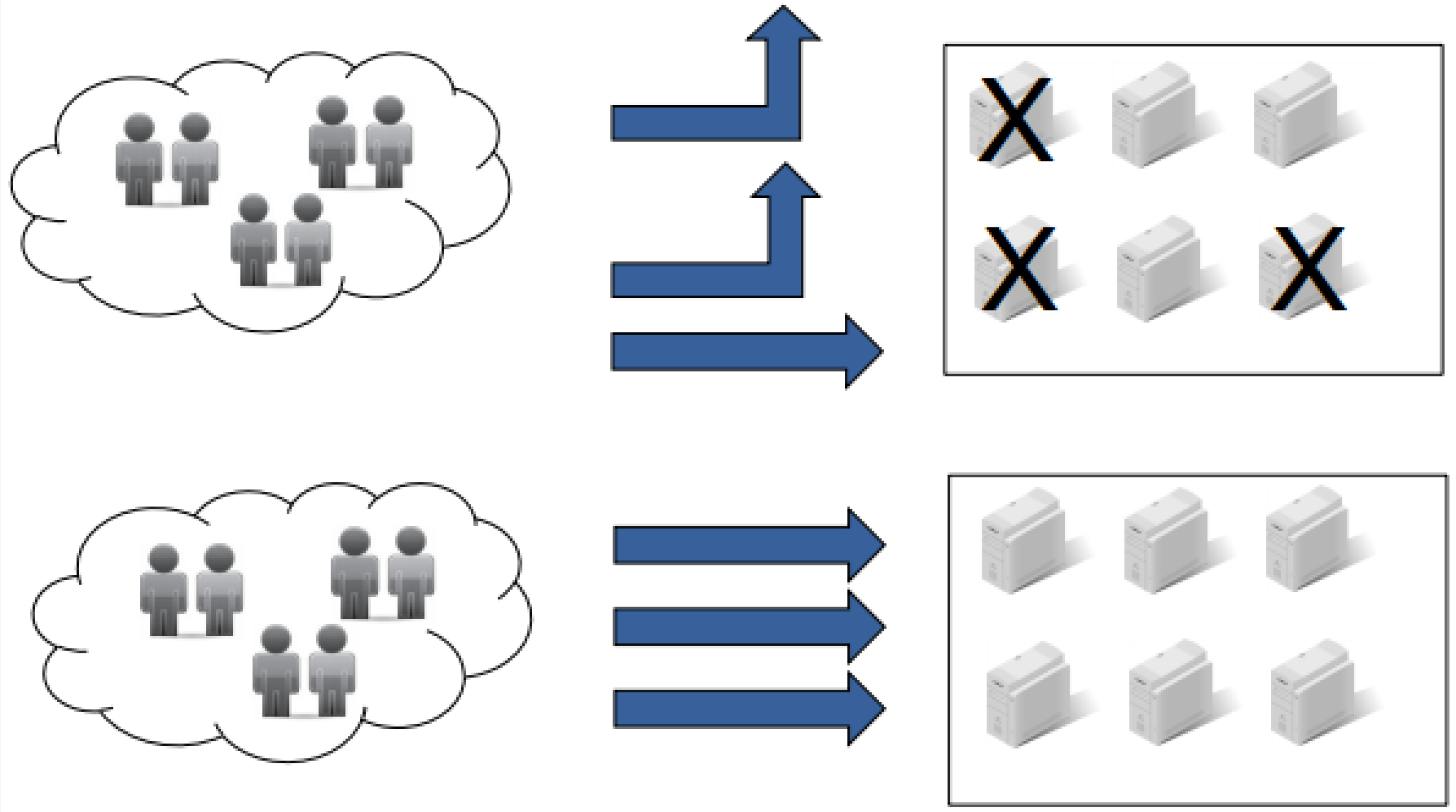
1.3 Các khía cạnh cơ bản của an toàn thông tin

- 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 = (Uptime)/(Uptime + Downtime);
  - ✓ Thời gian trung bình giữa các sự cố;
  - ✓ Thời gian trung bình ngừng để sửa chữa;
  - ✓ Thời gian khôi phục sau sự cố.

1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ Tính sẵn dùng



1.3 Các khía cạnh cơ bản của an toàn thông tin

- Tính xác thực (Authenticity): đảm bảo rằng thông tin, hệ thống và người dùng đều là thật, không bị giả mạo hoặc thay thế. Việc xác thực giúp khẳng định danh tính của người truy cập, độ tin cậy của nguồn dữ liệu và tính chính danh của hệ thống.
- Các tình huống cần đảm bảo tính xác thực gồm:
  - ✓ Xác minh danh tính người dùng khi đăng nhập hệ thống (ví dụ: sử dụng mật khẩu, mã OTP, xác thực đa yếu tố);
  - ✓ Kiểm tra tính hợp lệ và nguồn gốc của dữ liệu (ví dụ: sử dụng chữ ký số hoặc chứng chỉ số);
  - ✓ Đảm bảo rằng phần mềm hoặc bản cập nhật là do nhà phát triển hợp pháp cung cấp, không bị chèn mã độc.

1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

- Xác thực đa yếu tố

1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

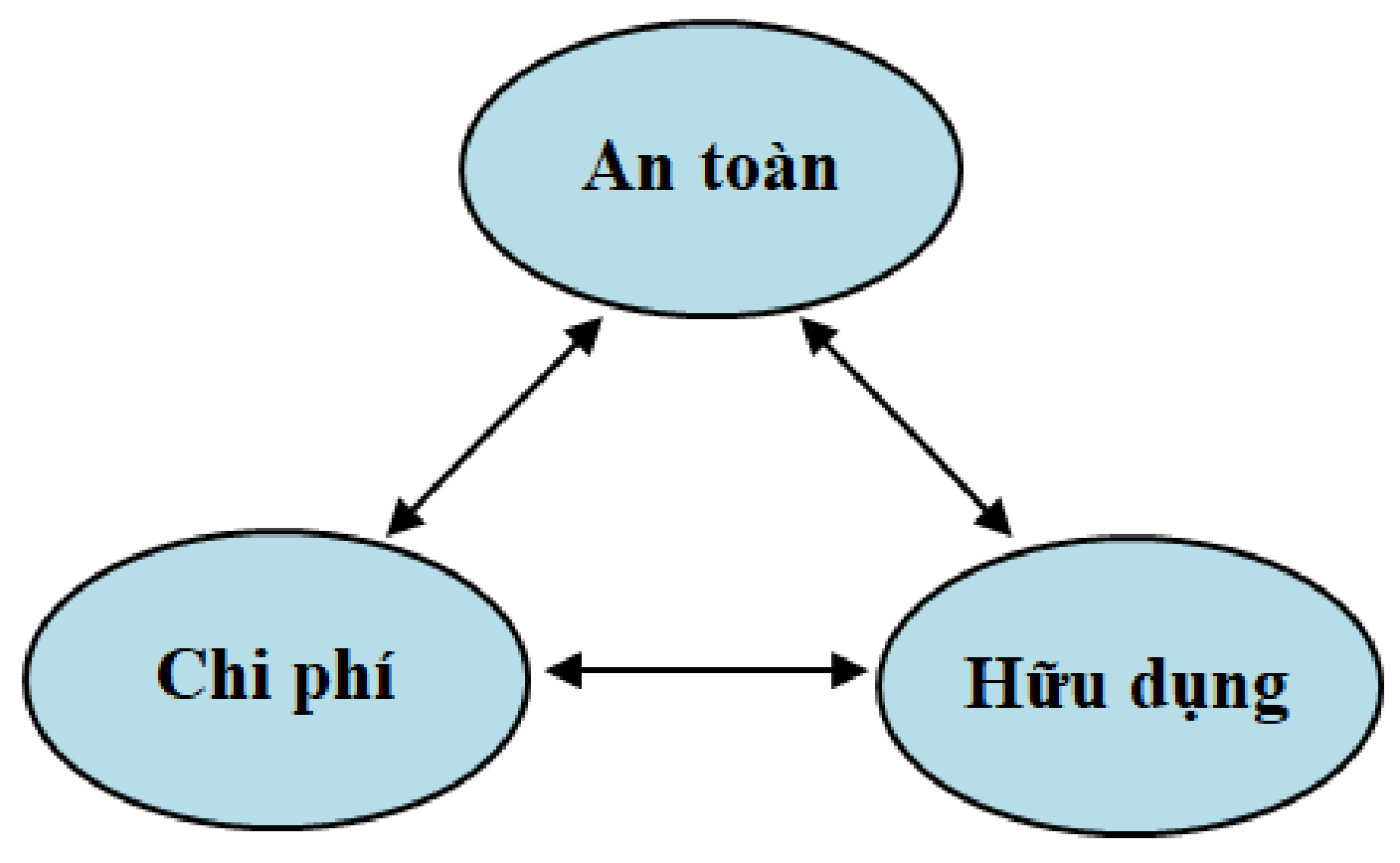
❑ **Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng:**

- ➢ 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 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 an toàn, tính hữu dụng và chi phí đảm bảo an toàn.

1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

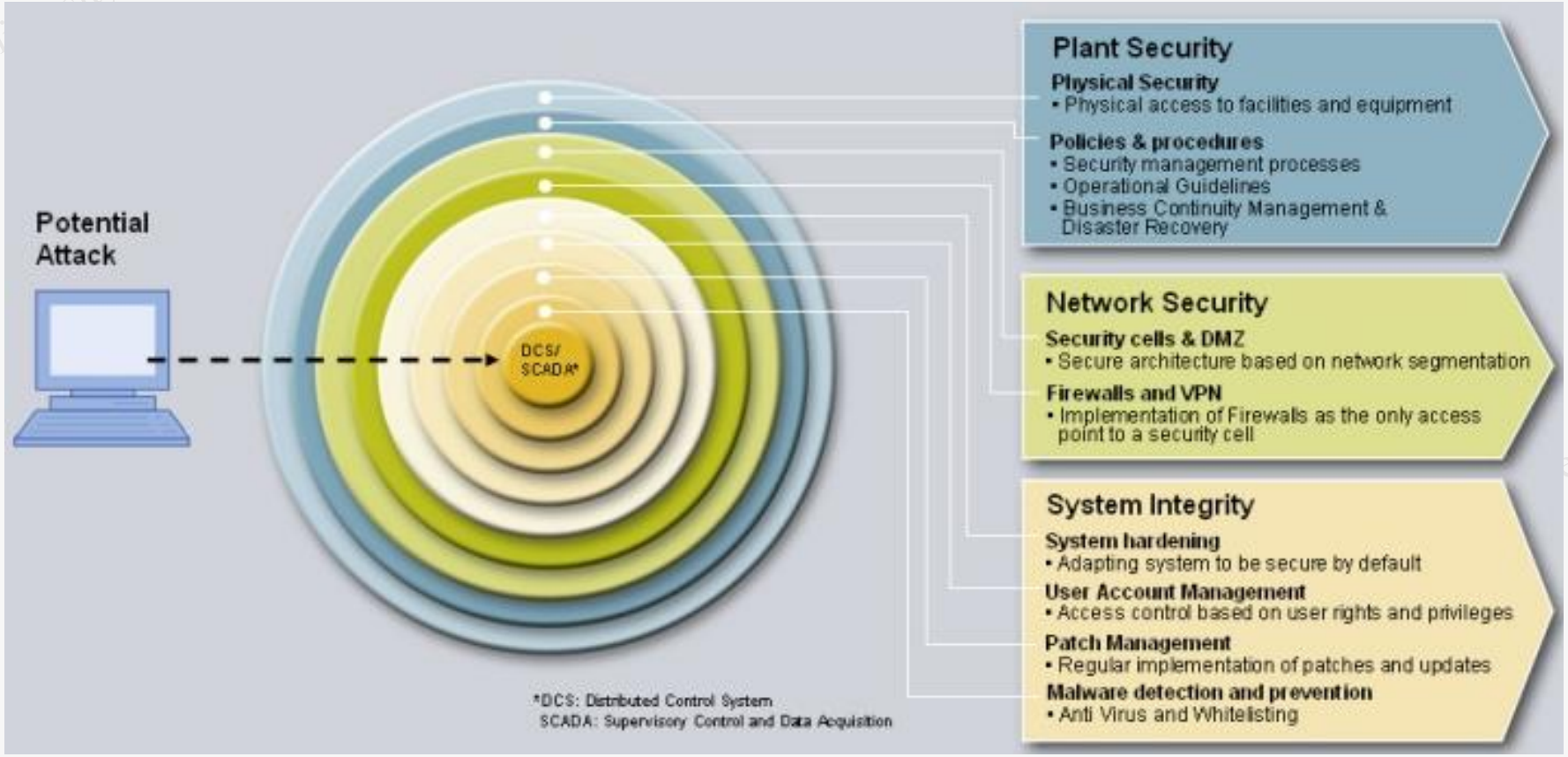
- Cần cân bằng giữa Usability (Tính hữu dụng), Cost (chi phí) và Security (an toàn)



1.3 Các khía cạnh cơ bản của an toàn thông tin

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ Mô hình đảm bảo an toàn thông tin với ba lớp chính



1.4 Các kỹ thuật tấn công

1.4.1. Tấn công bị động

1.4.2. Tấn công chủ động

1.4.3. Các dạng tấn công thường gặp

1.4 Các kỹ thuật 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.

1.4 Các kỹ thuật 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.

1.4 Các kỹ thuật 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 trong hệ thống;
  - ✓ Tấn công = Mối đe dọa + Lỗ hổng.

1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

- 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.

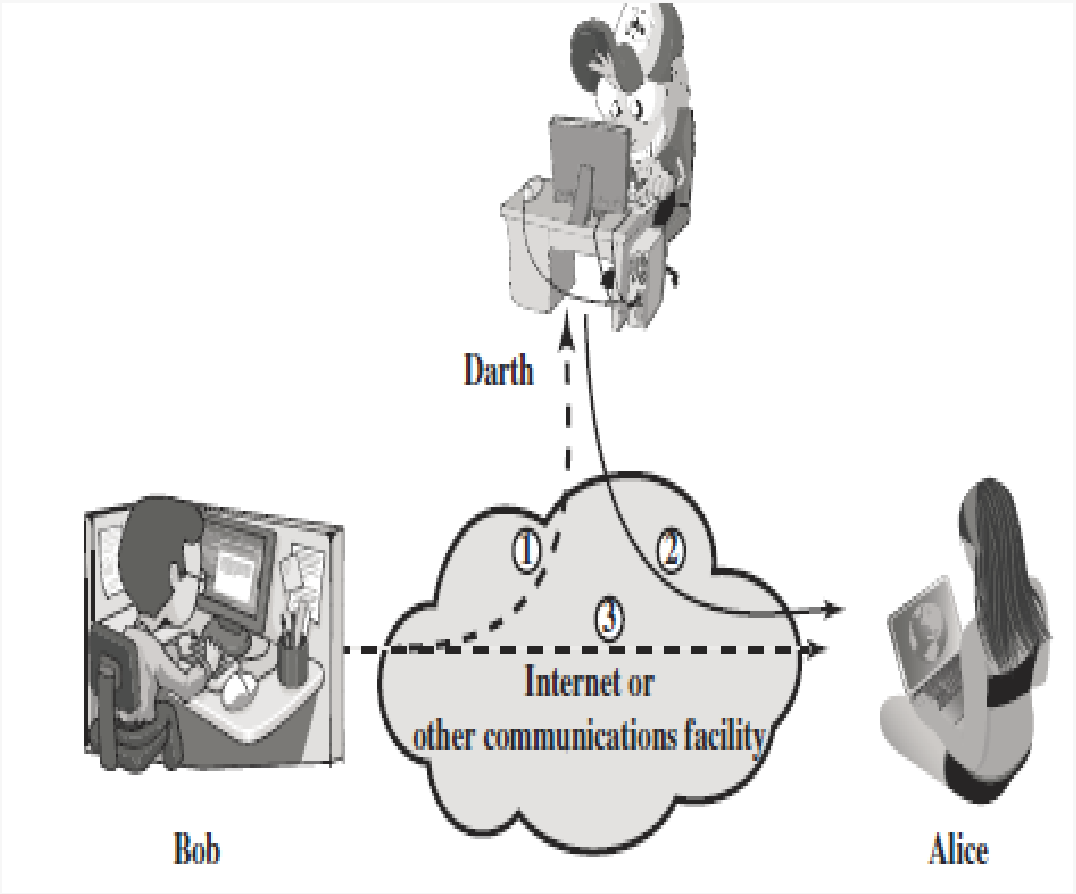
1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

- Hai kiểu tấn công:
  - ✓ Tấn công chủ động (Active attacks)
  - ✓ Tấn công thụ động (Passive attacks)

1.4 Các kỹ thuật tấn công

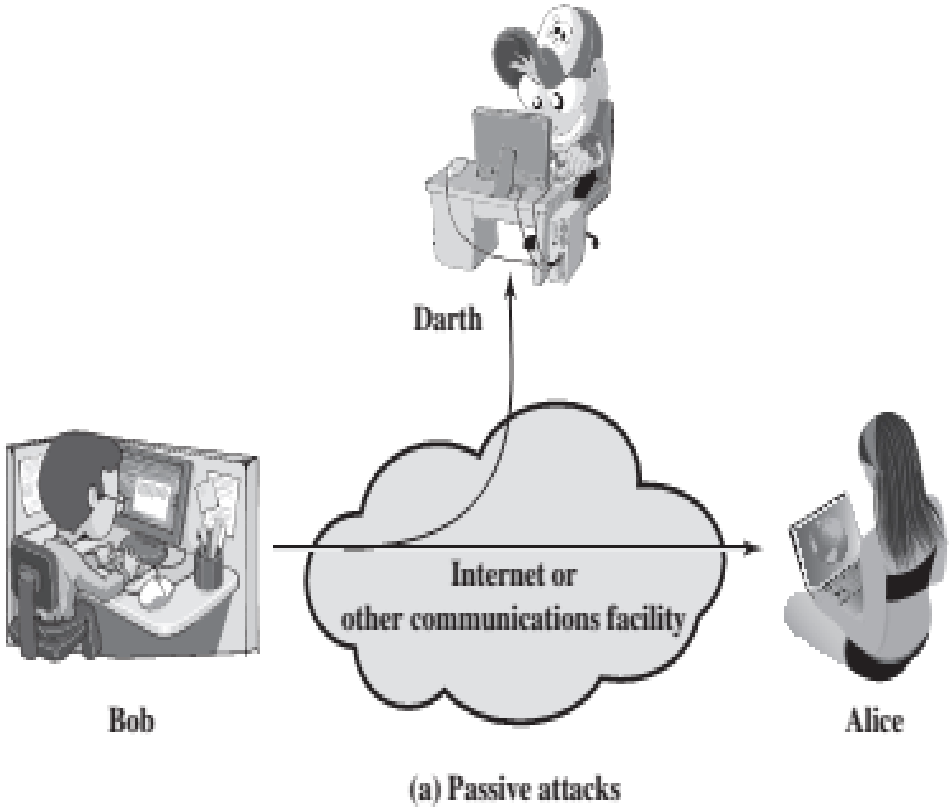
- Tấn công chủ động (Active attacks):
  - ✓ Sửa đổi dữ liệu trên đường truyền
  - ✓ Sửa đổi dữ liệu trong file
  - ✓ Giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng
  - ✓ Tấn công chủ động là một đột nhập (intrusion) về mặt vật lý.



1.4 Các kỹ thuật tấn công

- Tấn công thụ động (Passive attacks):
  - ✓ Không gây ra thay đổi trên hệ thống,
  - ✓ Nghe lén,
  - ✓ Giám sát lưu lượng trên đường truyền.

- Trên thực tế, tấn công thụ động thường là giai đoạn đầu của tấn công chủ động



(a) Passive attacks

1.4 Các kỹ thuật 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 trộm
  - ✓ 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.

1.4 Các kỹ thuật tấn công

- 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.

1.4 Các kỹ thuật tấn công

❖ 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.

1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

❖ 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 về mặt tính toán hơn “abc12345”.
- ➢ 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
- ➢ John the Ripper

1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

❖ 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)

✓ Tấn công lợi dụng lỗi không kiểm tra đầu vào:

- Tấn công chèn mã SQL (SQL Injection)
- Tấn công script kiểu XSS, CSRF

➢ Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại

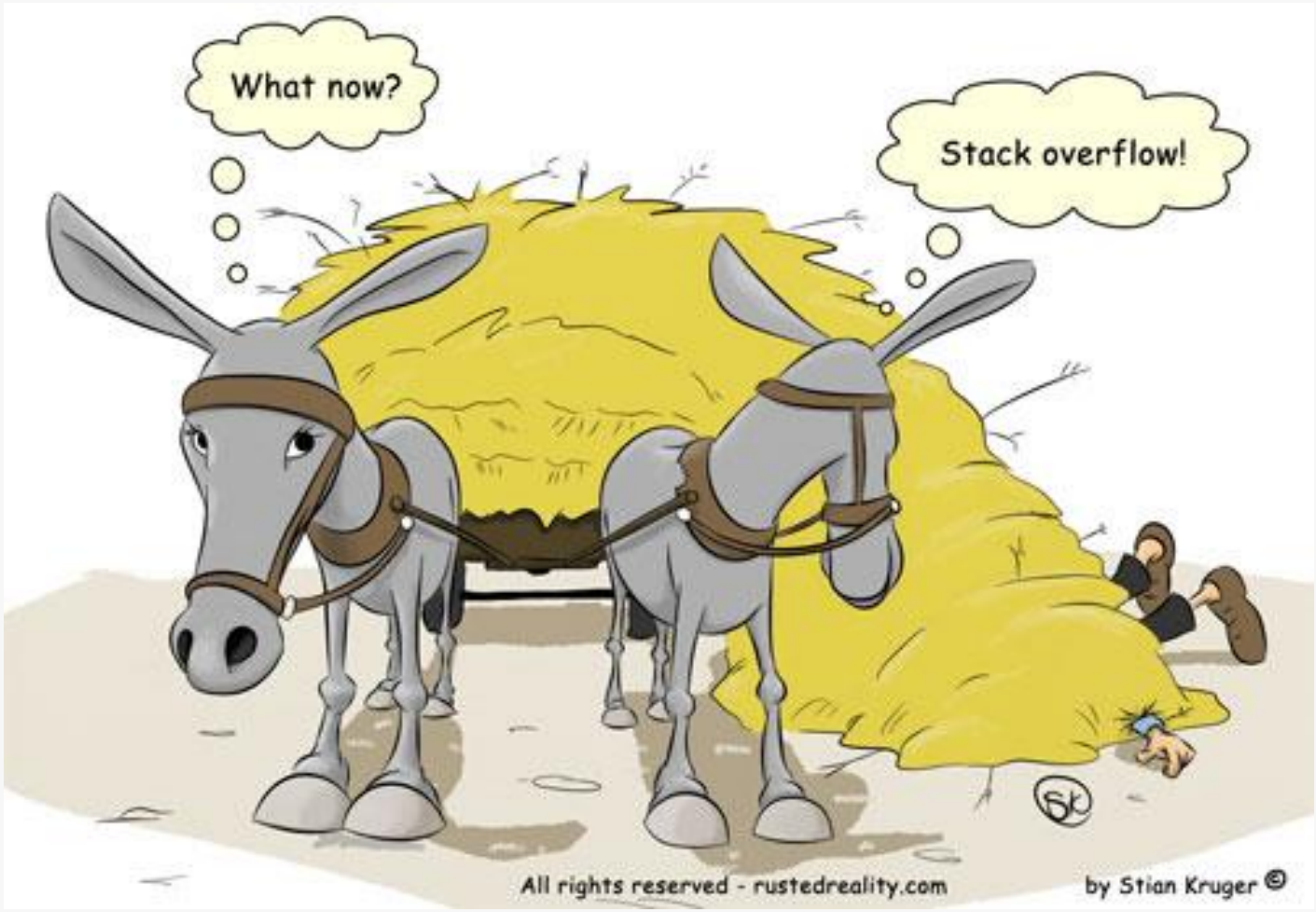
✓ Các phần mềm Adware, Spyware

✓ Virus

✓ Trojan

1.4 Các kỹ thuật tấn công

- 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);



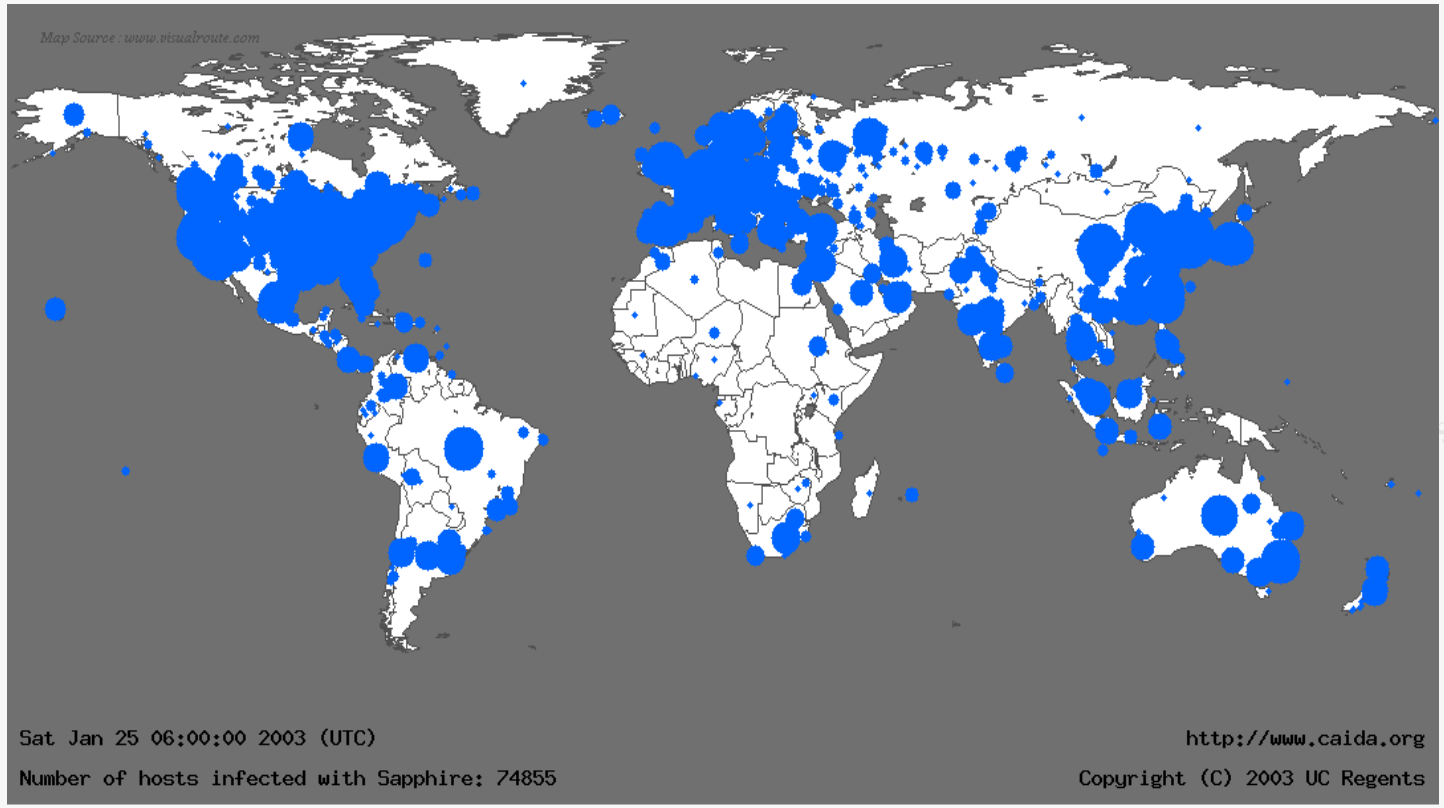
1.4 Các kỹ thuật tấn công

- 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 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.

1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

- **Ví dụ về khai thác lỗi tràn bộ đệm**
  - ✓ Sâu SQL Slammer (một số tài liệu gọi là sâu Sapphire) được phát hiện ngày 25/1/2003 lúc 5h30 (UTC) là sâu có tốc độ lây lan nhanh nhất lúc bấy giờ: nó lây nhiễm 36 ra khoảng 75.000 máy chủ chỉ trong khoảng 30 phút



➢ Ví dụ về khai thác lỗi tràn bộ đệm

- ✓ Sâu SQL Slammer (một số tài liệu gọi là sâu Sapphire) được phát hiện ngày 25/1/2003 lúc 5h30 (UTC) là sâu có tốc độ lây lan nhanh nhất lúc bấy giờ: nó lây nhiễm 36 ra khoảng 75.000 máy chủ chỉ trong khoảng 30 phút
- ✓ Sâu Slammer khai thác lỗi tràn bộ đệm trong thành phần Microsoft SQL Server Resolution Service của hệ quản trị cơ sở dữ liệu Microsoft SQL Server 2000.
- ✓ Sâu sử dụng giao thức UDP với kích thước gói tin 376 byte và vòng lặp chính của sâu chỉ gồm 22 lệnh hợp ngữ. Chu trình hoạt động của sâu SQL Slammer gồm:
  - Sinh tự động địa chỉ IP;
  - Quét tìm các máy có lỗi với IP tự sinh trên cổng dịch vụ 1434;
  - Nếu tìm được, gửi một bản sao của sâu đến máy có lỗi;
  - Mã của sâu gây tràn bộ đệm, thực thi mã của sâu và quá trình lặp lại

1.4 Các kỹ thuật tấn công

- ✓ SQL Slammer là sâu "lành tính" vì nó không can thiệp vào hệ thống file, không thực hiện việc phá hoại hay đánh cắp thông tin ở hệ thống bị lây nhiễm. Tuy nhiên, sâu tạo ra lưu lượng mạng khổng lồ trong quá trình lây nhiễm, gây tê liệt đường truyền mạng Internet trên nhiều vùng của thế giới.
- ✓ Do mã của SQL Slammer chỉ được lưu trong bộ nhớ nó gây tràn mà không được lưu vào hệ thống file, nên chỉ cần khởi động lại máy là có thể tạm thời xóa được sâu khỏi hệ thống. Tuy nhiên, hệ thống chứa lỗ hổng có thể bị lây nhiễm lại nếu nó ở gần một máy khác bị nhiễm sâu.
- ✓ Các biện pháp phòng chống triệt để khác là cập nhật bản vá cho bộ phần mềm Microsoft SQL Server 2000.

1.4 Các kỹ thuật tấn công

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ **Các biện pháp phòng chống lỗi tràn bộ đệm:**

✓ Kiểm tra mã nguồn bằng tay để tìm và vá 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;

✓ Sử dụng các cơ chế bảo vệ Stack:

- Thêm một số ngẫu nhiên (canary) phía trước địa chỉ trở về;
- Kiểm tra số ngẫu nhiên này trước khi trở về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trở về.

✓ Sử dụng các thư viện an toàn hoặc các ngôn ngữ không tràn, như Java, nền tảng .net.

1.4 Các kỹ thuật tấn công: Tấn công lợi dụng lỗi không kiểm tra đầu vào

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ 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 điển 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 để khai thác.

1.4 Các kỹ thuật tấn công: Tấn công lợi dụng lỗi không kiểm tra đầu vào

CMC UNIVERSITY
Aspire to Inspire the Digital World

- **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:

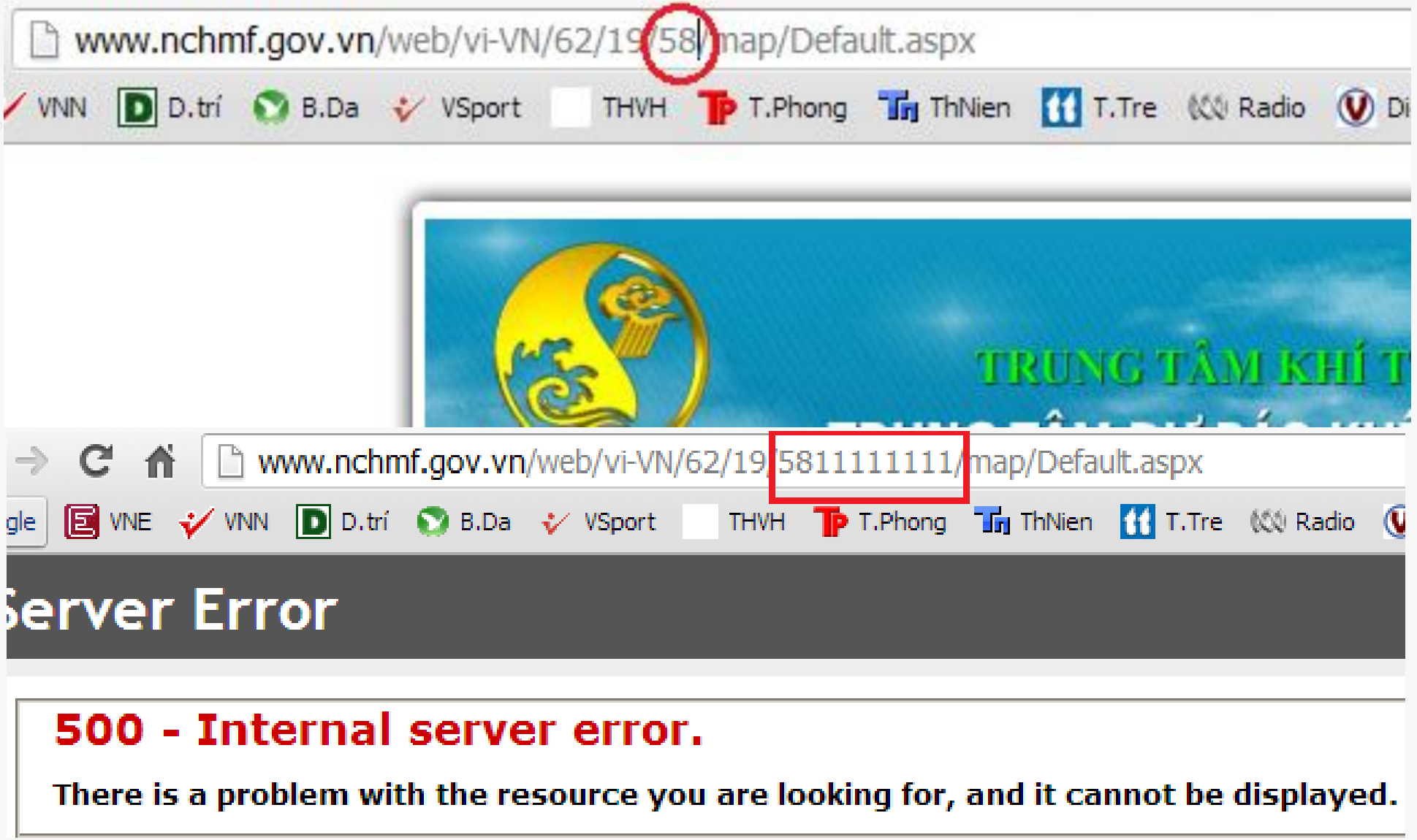
- Gây lỗi ứng dụng/dịch vụ, có thể làm ứng dụng ngừng hoạt động.

✓ Chèn mã khai thác vào dữ liệu đầu vào để thực hiện trên hệ thống của nạn nhân, nhằm đánh cắp dữ liệu nhạy cảm hoặc thực hiện các hành vi phá hoại

1.4 Các kỹ thuật tấn công: Tấn công lợi dụng lỗi không kiểm tra đầu vào

CMC UNIVERSITY
Aspire to Inspire the Digital World

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



1.4 Các kỹ thuật tấn công: SQL Injection

CMC UNIVERSITY
Aspire to Inspire the Digital World

- ✓ 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 ra câu lệnh SQL hoàn chỉnh.
- ✓ Tùy 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;

1.4 Các kỹ thuật tấn công: SQL Injection

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ 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.

1.4 Các kỹ thuật tấn công: SQL Injection

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ 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.

1.4 Các kỹ thuật tấn công: SQL Injection

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ Công cụ kiểm tra và tấn công

- ✓ Sử dụng các công cụ rà quét để chủ động tìm lỗi SQL injection tồn tại trong hệ thống;
- ✓ SQLmap (có thể tải từ trang sqlmap.org) là 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.

1.4 Các kỹ thuật tấn công: Tấn công từ chối dịch vụ (DoS)

CMC UNIVERSITY
Aspire to Inspire the Digital World

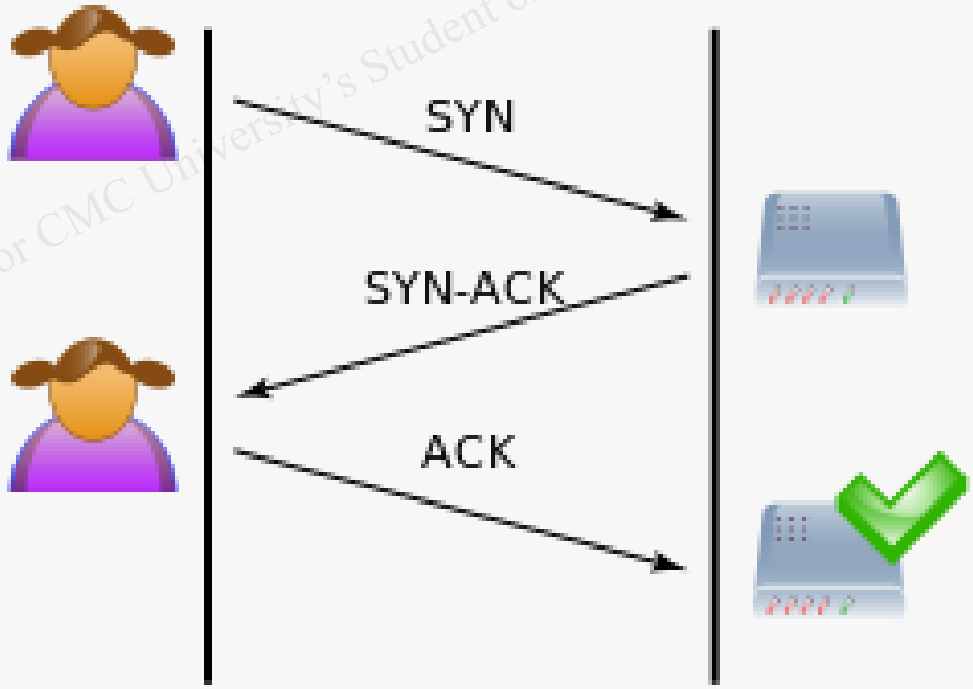
- Tấn công từ chối dịch vụ (DoS - Denial of Service Attacks) là dạng tấn công cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống;
- Hai loại tấn công DoS:
  - ✓ Tấn công logic (Logic attacks): tấn công dựa vào các lỗi phần mềm làm dịch vụ ngừng hoạt động hoặc làm giảm hiệu năng hệ thống.
    - 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.
- Hai kỹ thuật tấn công gây ngập lụt:
  - ✓ SYN floods
  - ✓ Smurf

1.4 Các kỹ thuật tấn công: Tấn công từ chối dịch vụ (DoS) – SYN floods

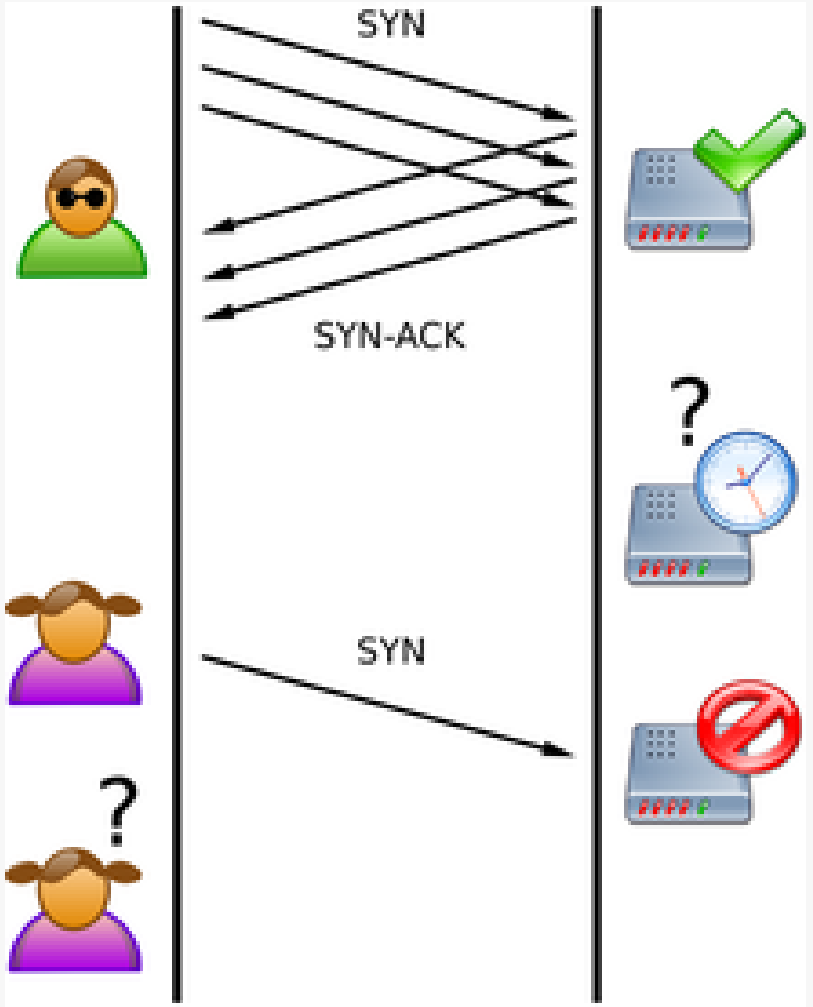
CMC UNIVERSITY
Aspire to Inspire the Digital World

- SYN floods là kỹ thuật gây ngập lụt các gói tin TCP.
- ✓ SYN là bít điều khiển của TCP dùng để đồng bộ số trình tự gói.
- 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 khi nó timed-out.

1.4 Các kỹ thuật tấn công: Tấn công từ chối dịch vụ (DoS) – SYN floods



Normal TCP three-way handshake



SYN Floods Attack

1.4 Các kỹ thuật tấn công: Tấn công DDoS

CMC UNIVERSITY
Aspire to Inspire the Digital World

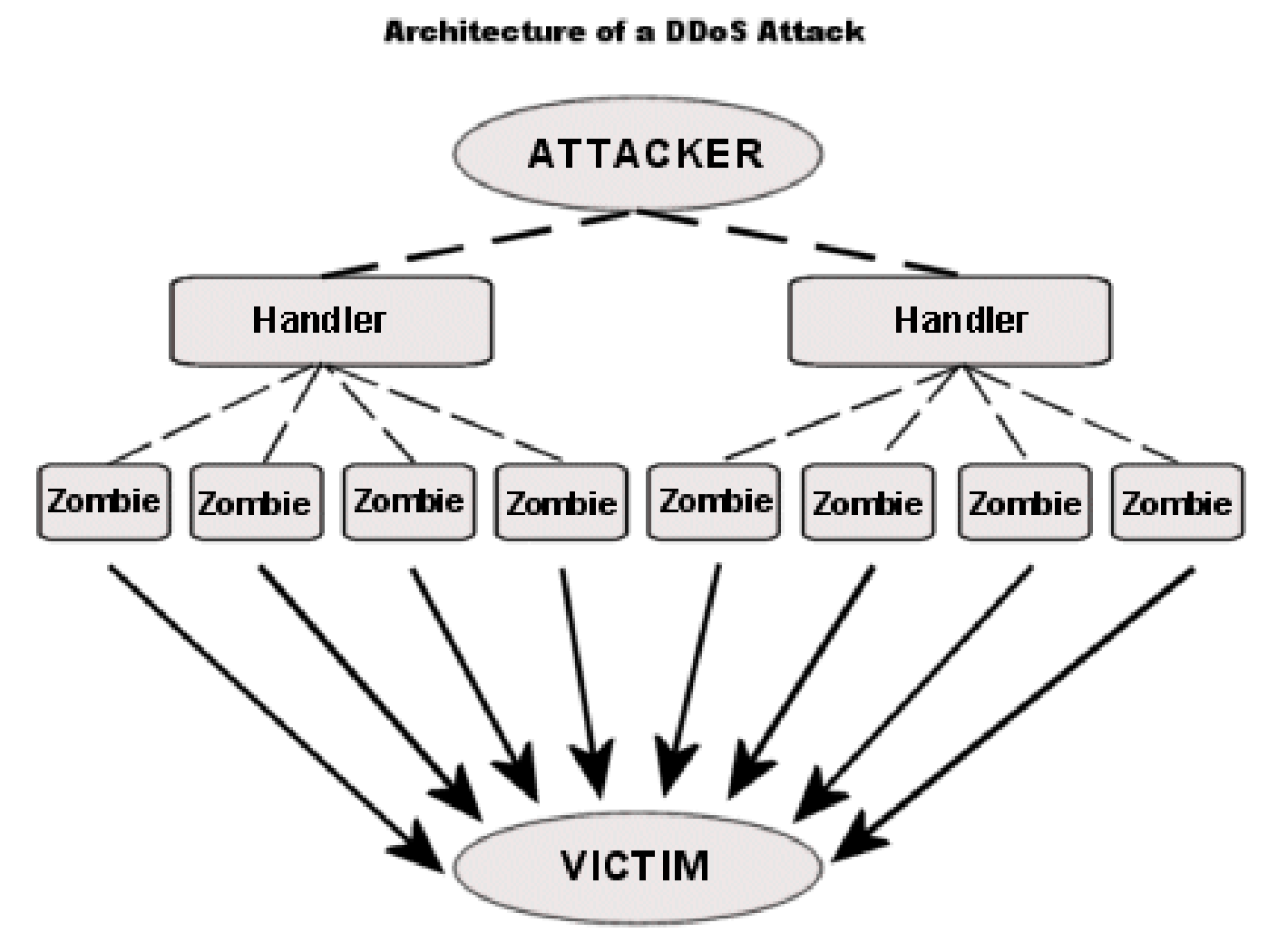
- Tấn công DDoS (Distributed Denial of Service Attacks) là một loại tấn công DoS:
- ✓ Liên quan đến gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo;
- ✓ DDoS khác DoS ở phạm vi tấn công (số lượng host tham gia);
  - Số host tham gia tấn công DoS thường giới hạn trong 1 hoặc 1 số máy
  - Số host tham gia tấn công DDoS có thể hàng chục ngàn và nằm phân tán trên mạng Internet.

1.4 Các kỹ thuật tấn công: Tấn công DDoS

CMC UNIVERSITY
Aspire to Inspire the Digital World

- 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;
  - ✓ Sau đó, 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.

1.4 Các kỹ thuật tấn công: Tấn công DDoS

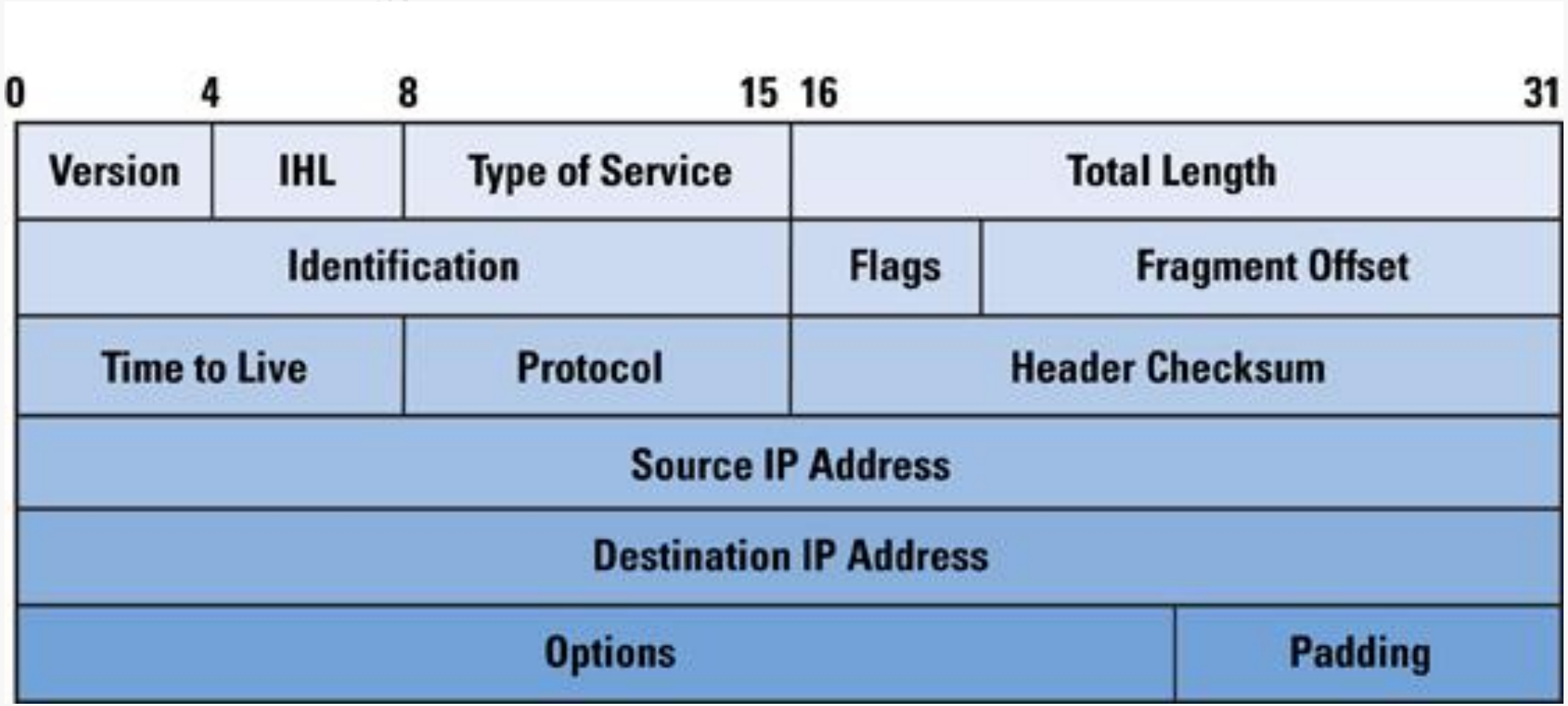


1.4 Các kỹ thuật tấn công: IP Spoofing

CMC UNIVERSITY
Aspire to Inspire the Digital World

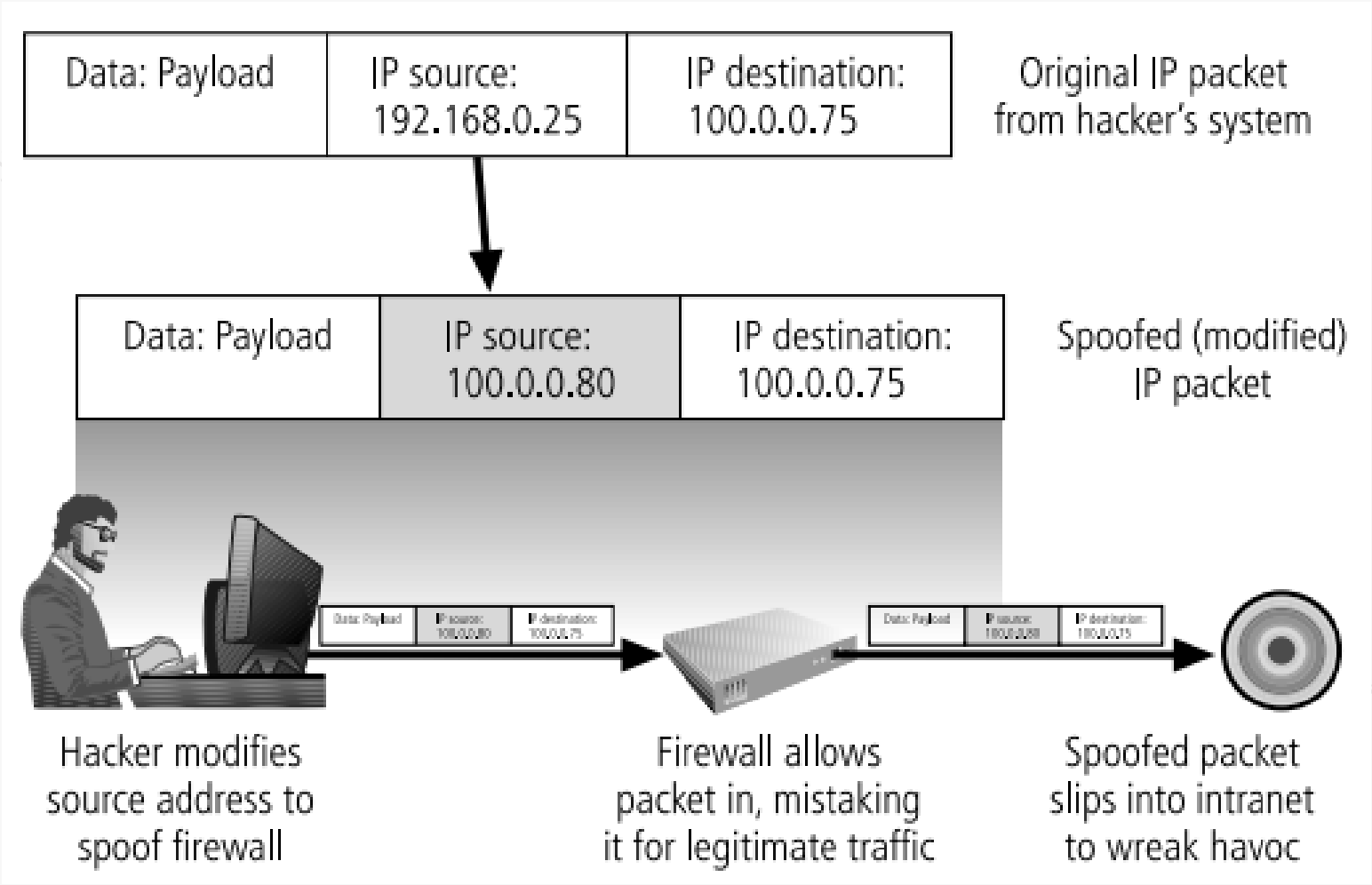
- Tấn công giả mạo địa chỉ IP (IP Spoofing) :
  - ✓ Là dạng tấn công trong đó kẻ tấn công sử dụng địa chỉ IP giả, thường để đánh lừa máy nạn nhân để vượt qua các hàng rào kiểm soát an ninh;
  - ✓ Nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội đột nhập vào các 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.

1.4 Các kỹ thuật tấn công: IP Spoofing



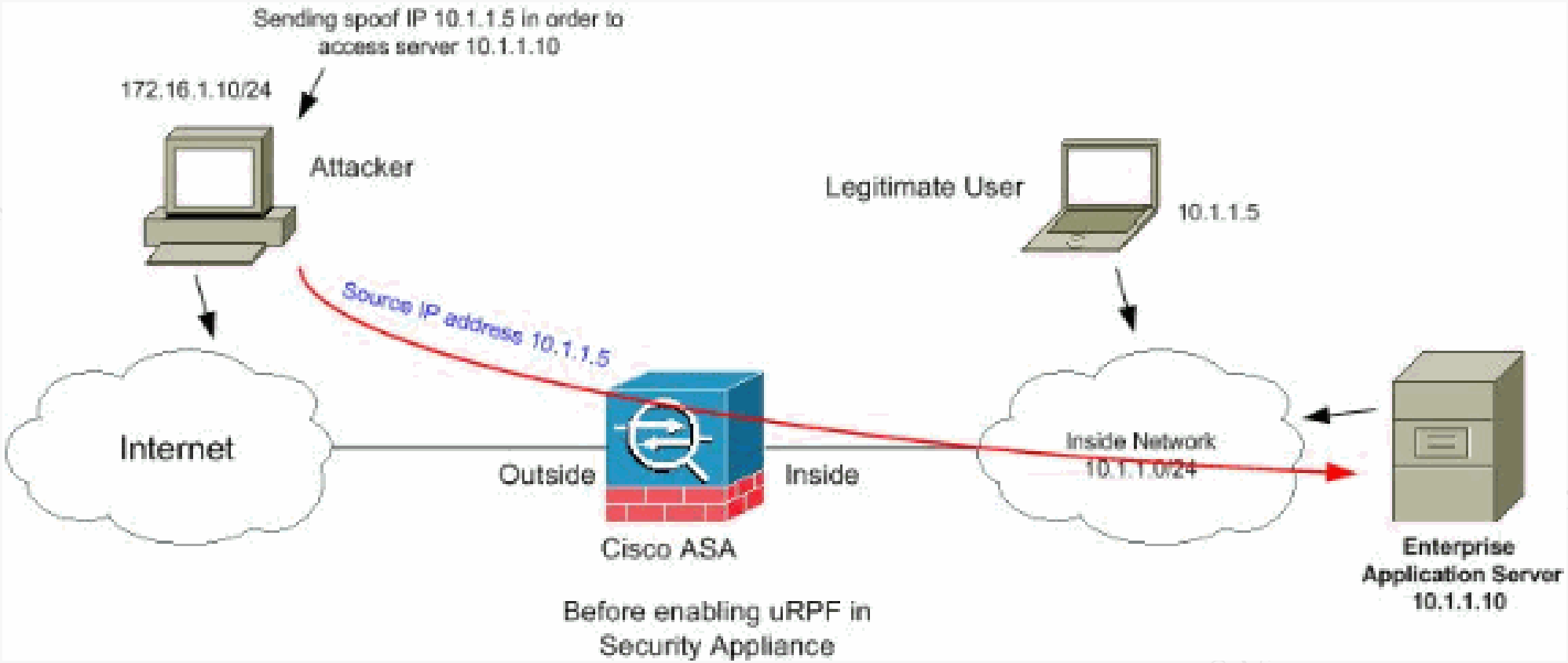
Định dạng gói tin IPv4

1.4 Các kỹ thuật tấn công: IP Spoofing



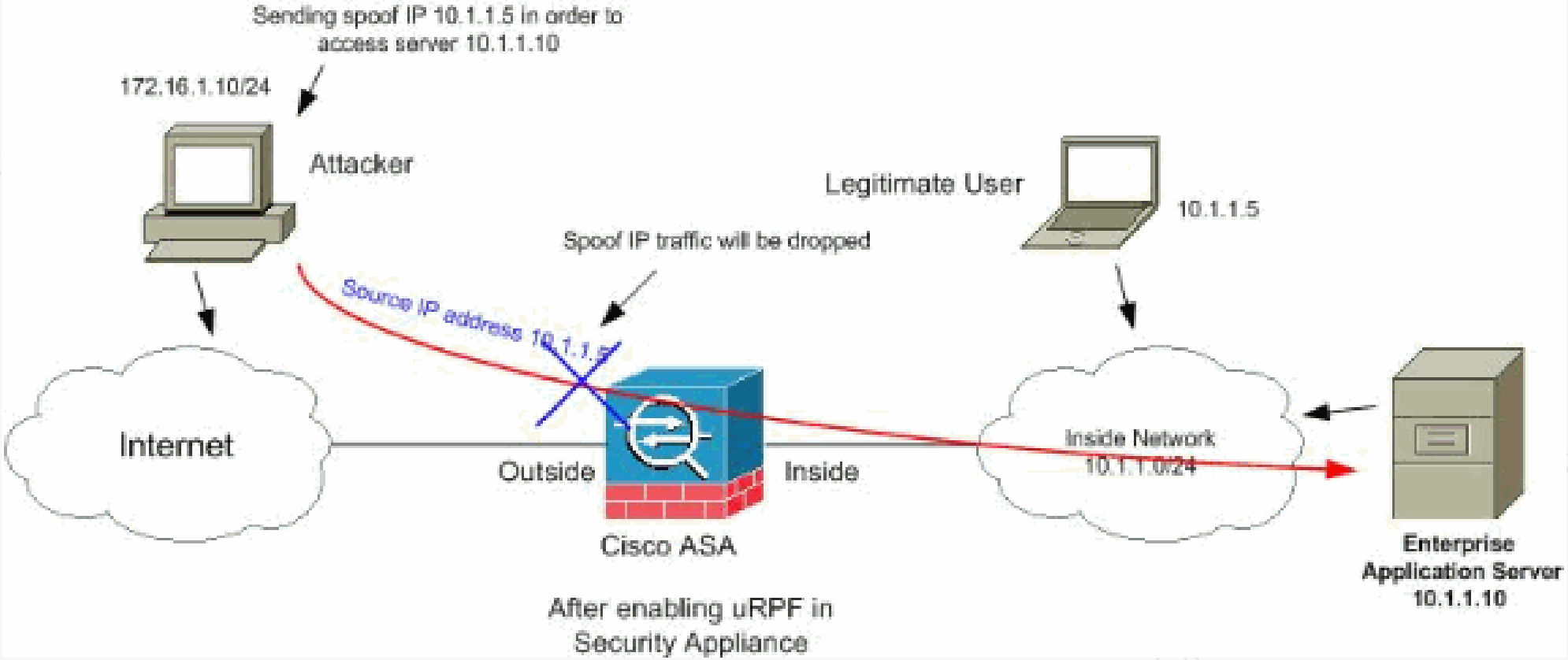
Tấn công giả mạo địa chỉ IP

1.4 Các kỹ thuật tấn công: IP Spoofing



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

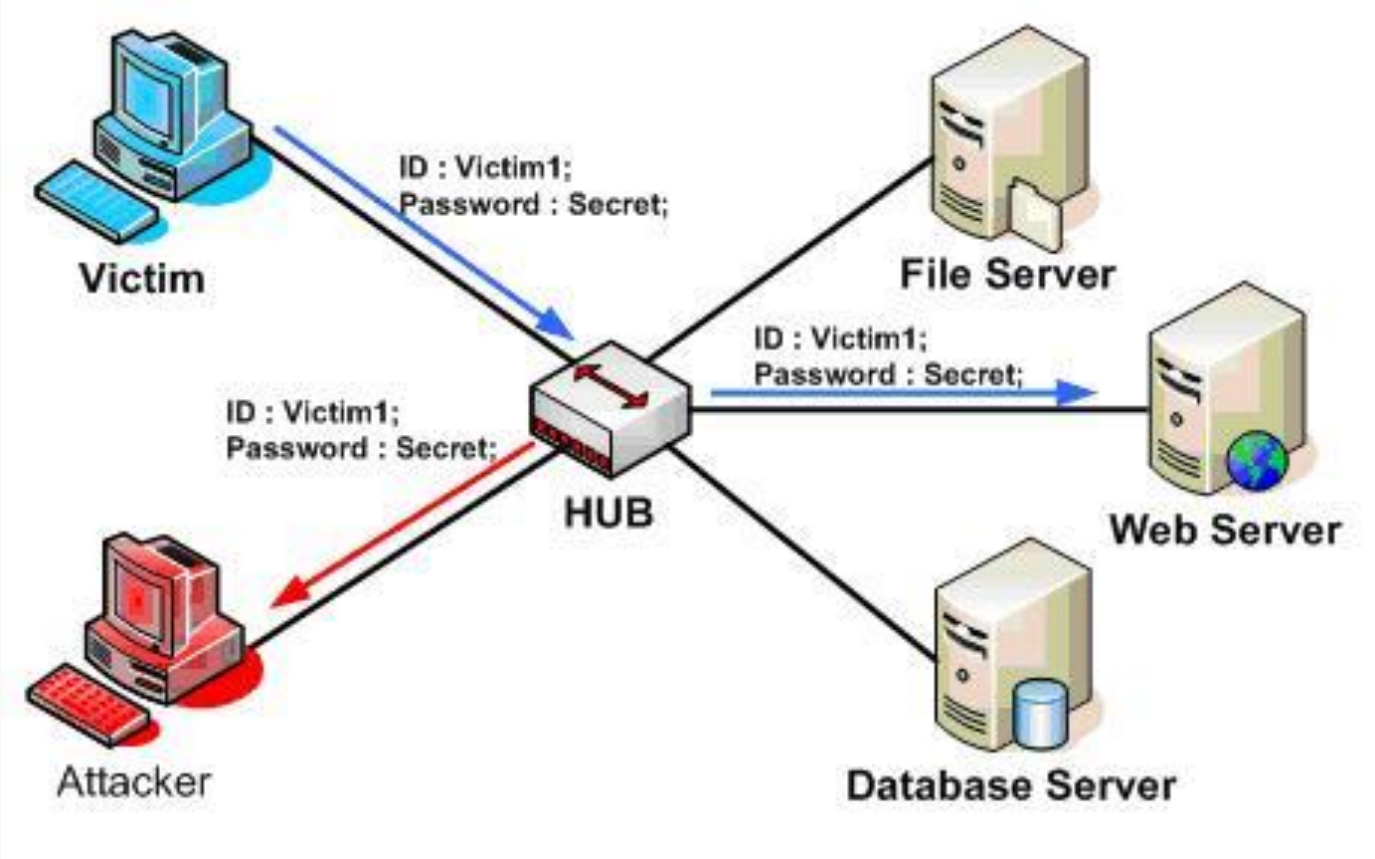
1.4 Các kỹ thuật tấn công: IP Spoofing



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

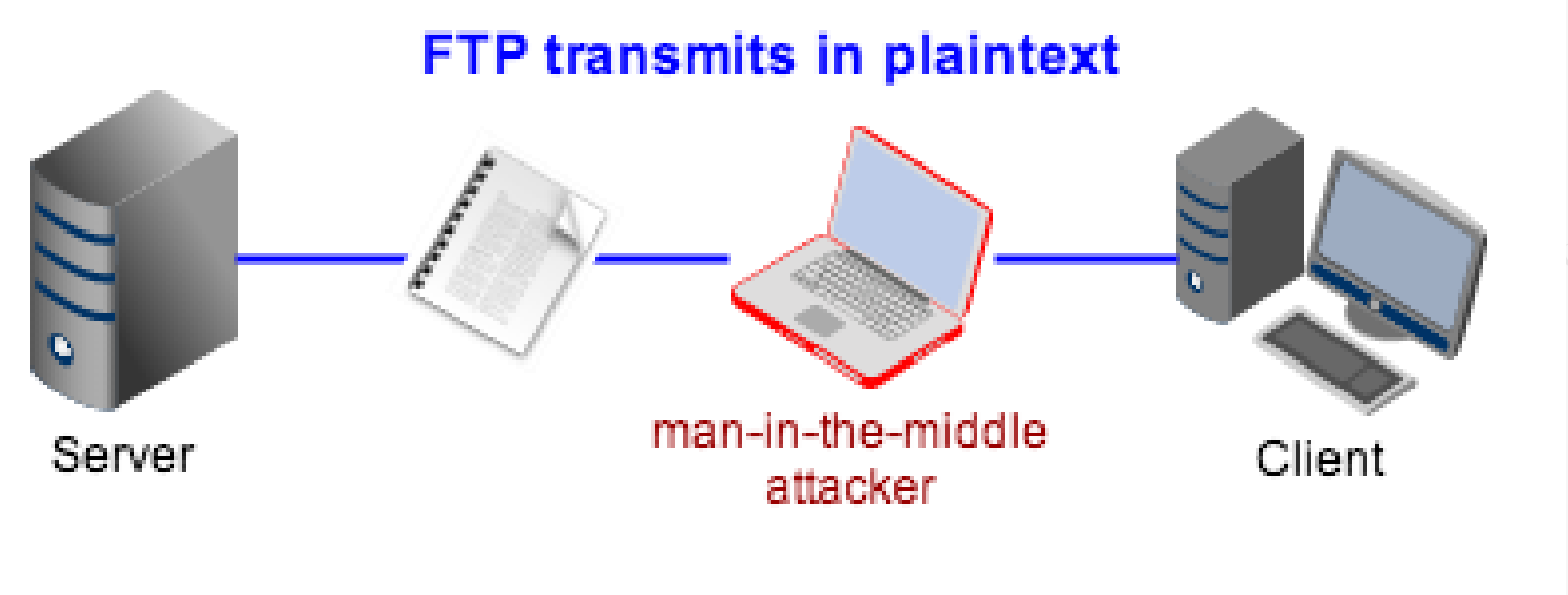
1.4 Các kỹ thuật tấn công: Sniffing/Eavesdropping

- Tấn công nghe lén (Sniffing/Eavesdropping):
- ✓ Là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub hoặc router để bắt các gói tin dùng cho phân tích về sau.

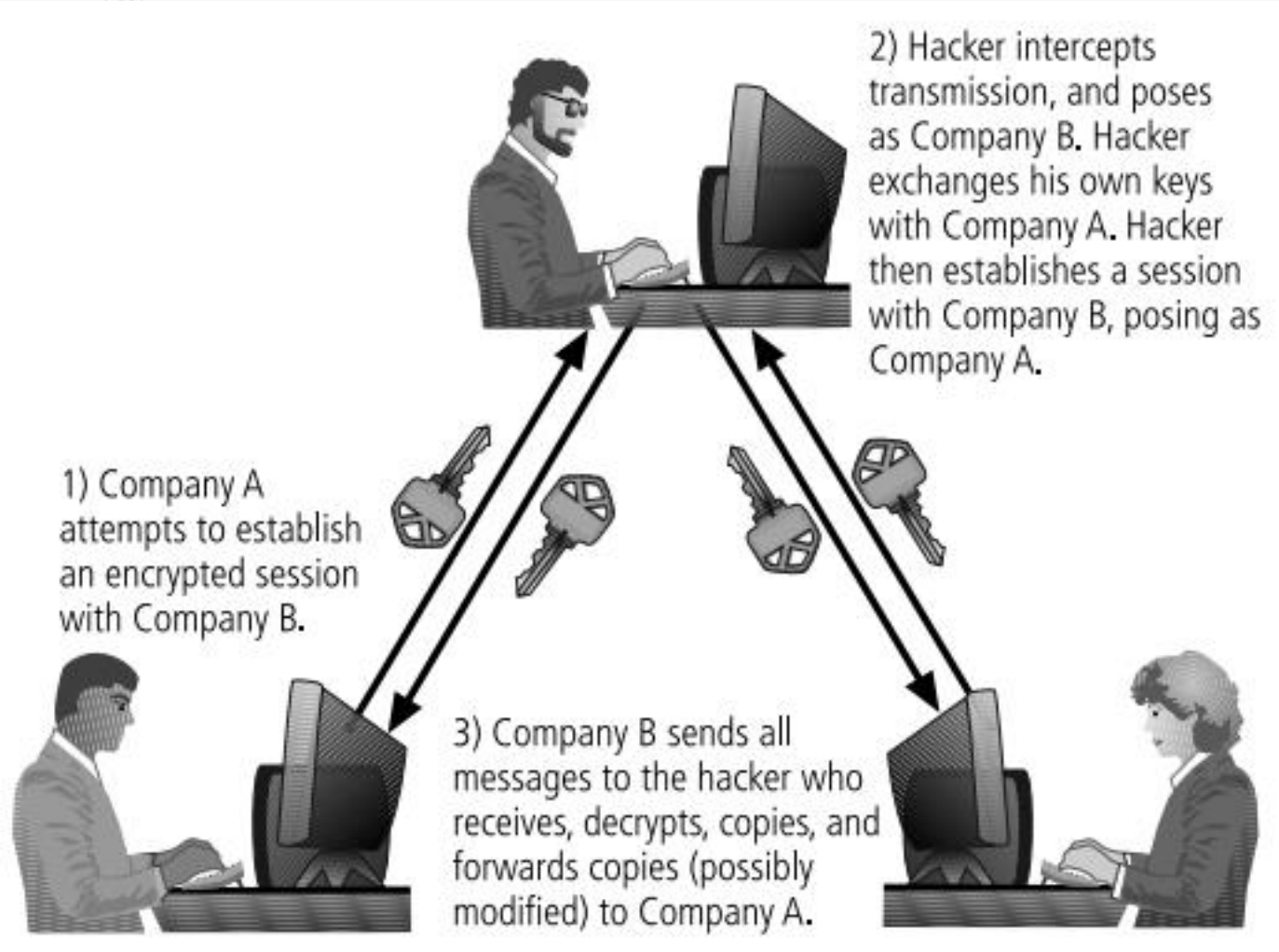


1.4 Các kỹ thuật tấn công: Man in the middle

- 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 và chuyển thông điệp lại cho bên kia.
  - ✓ Thường được sử dụng để đánh cắp thông tin.



1.4 Các kỹ thuật tấn công: Man in the middle



1.4 Các kỹ thuật tấn công: Bom thư và thư rác

CMC UNIVERSITY
Aspire to Inspire the Digital World

➢ 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 nhưng 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.

1.4 Các kỹ thuật tấn công: Social Engineering

CMC UNIVERSITY
Aspire to Inspire the Digital World

- Tấn công kiểu Social Engineering là dạng tấn công sử dụng các kỹ thuật xã hội đã 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,…

1.4 Các kỹ thuật tấn công: Social Engineering

CMC UNIVERSITY
Aspire to Inspire the Digital World

- 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.

1.4 Các kỹ thuật tấn công: 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.

1.4 Các kỹ thuật tấn công: Phishing

From: CustomerSecurity@royalbank.com[1]
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder[2]

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 time[4] now and, as a security measure, we must to suspend your online account.[5] If you would like to continue to use the online banking facilty[6] offered by Royal Bank, please click the link below and renew your security details[7] 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 facilty:
https://customerbankingrenewal.royalbank.com/[9]

We are sorry for any convenience[10] caused and hope you continue to use our online banking facilty.

The Royal Bank Online Security Team[11]

Link: http://customerbankingrenewal.royaibank.com/

1.4 Các kỹ thuật tấn công: Pharming

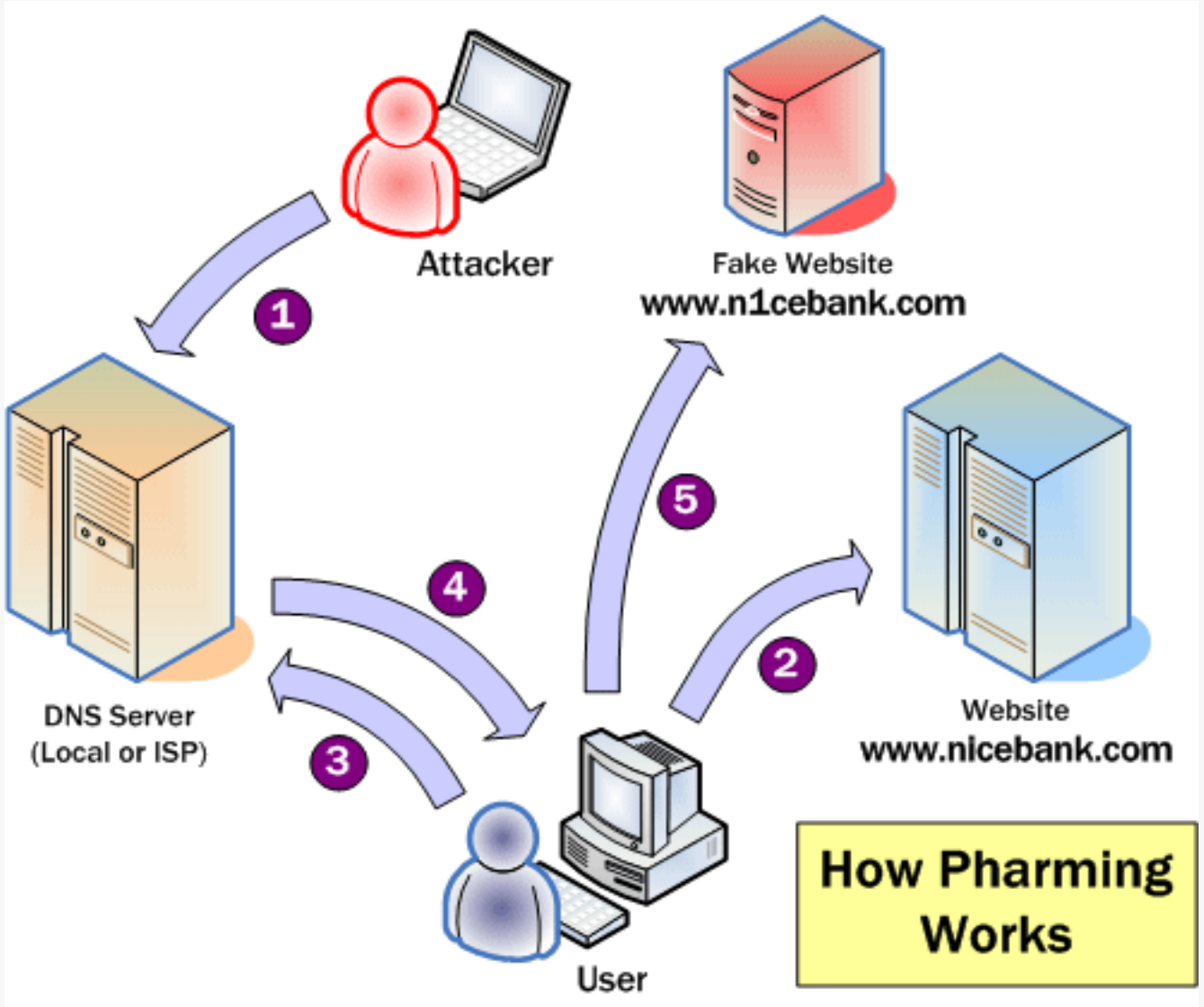
- Pharming là kiểu tấn công vào trình duyệt người dùng:
  - ✓ Người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu 1 website khác (độc hại);
  - ✓ Kẻ tấn công thường sử dụng sâu, virus hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng;
  - ✓ Kẻ tấn công cũng có thể 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.

1.4 Các kỹ thuật tấn công: Pharming

Cài đặt malware để điều khiển trình duyệt của người dùng

1.4 Các kỹ thuật tấn công: Pharming

Tấn công vào hệ thống DNS để chuyển hướng website



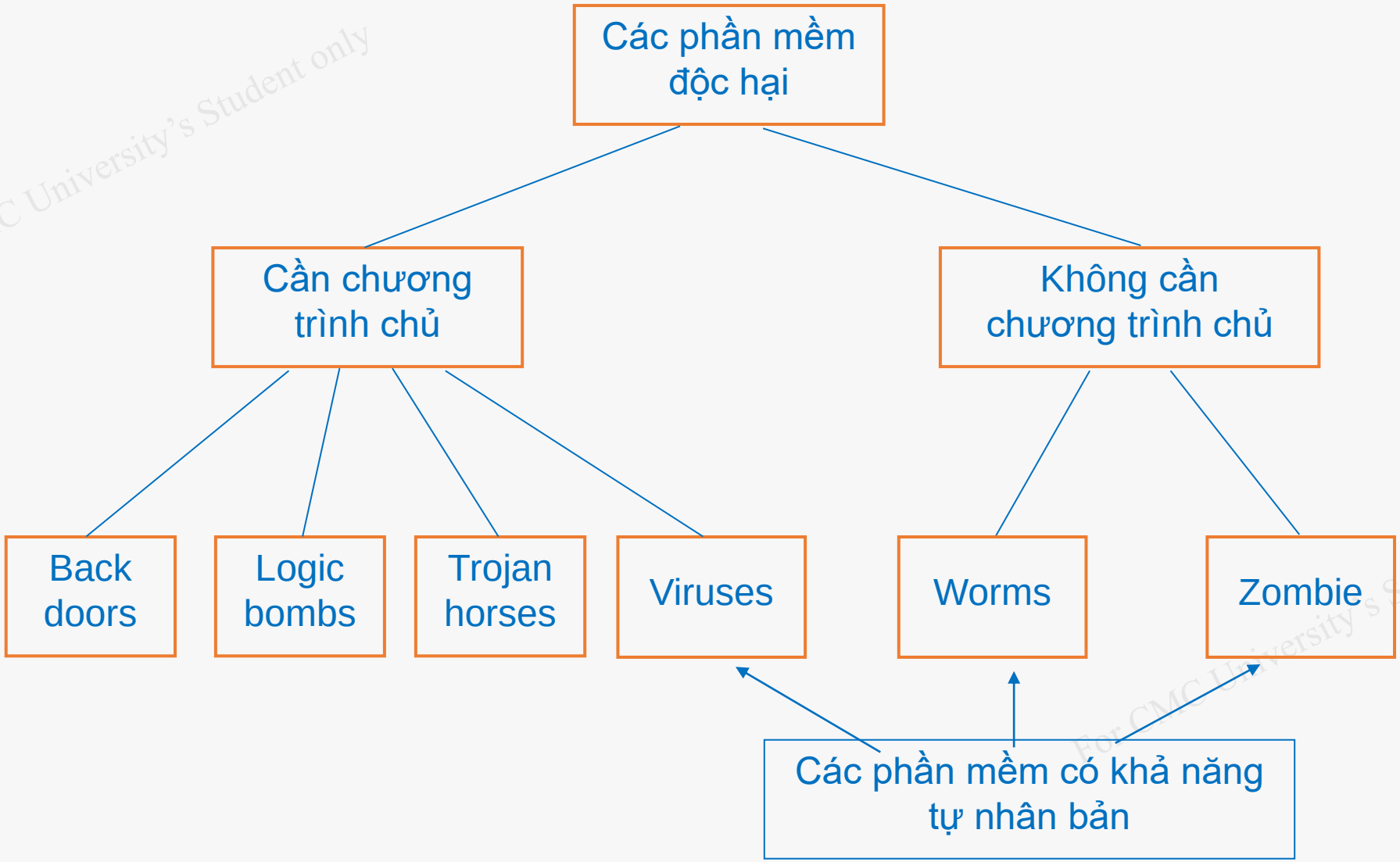
1.4 Các kỹ thuật tấn công: APT

- 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:
  - ✓ Tiên tiến, hay cao cấp (Advanced): các kỹ thuật tiên tiến được sử dụng để tấn công vào hệ thống mục tiêu một cách bài bản.
  - ✓ Kiên trì, dai dẳng (Persistent): mục tiêu được xác định rất cụ thể để thực hiện tấn công, ẩn mình và khai thác theo từng giai đoạn

1.4 Các kỹ thuật tấn công: APT

- Các giai đoạn điển hình của một cuộc tấn công APT:
  - ✓ 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.

1.4 Các kỹ thuật tấn công: Các dạng phần mềm độc hại phục vụ tấn công



CMC UNIVERSITY
Aspire to Inspire the Digital World

THANK YOU