TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HCM

MẠNG MÁY TÍNH
(Computer Networks)

Giảng viên: Vũ Đức Thịnh
Email: thinhvd@hufi.edu.vn

NỘI DUNG MÔN HỌC

Chương 1: Tổng quan về mạng máy tính

Chương 2: Kiến trúc phân tầng và mô hình OSI

Chương 3: Mô hình TCP/IP và mạng Internet

Chương 4: Phương tiện truyền dẫn và các thiết bị mạng

Chương 5: Mạng cục bộ LAN

Chương 6: Mạng diện rộng WAN

Chương 7: ATTT mạng máy tính

CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

Giới thiệu một số kỹ thuật tấn công phổ biến

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

MỤC ĐÍCH – YÊU CẦU

Mục đích:

Trình bày được các vấn đề của ATTT.

Nhận biết được các kỹ thuật tấn công cơ bản.

Trình bày được các cơ chế mã hóa, bảo mật.

Trình bày được các giao thức an toàn trên mạng Internet

Yêu cầu:

Học viên tham gia học tập đầy đủ.

Nghiên cứu trước các nội dung có liên quan đến bài giảng

CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

Giới thiệu một số kỹ thuật tấn công phổ biến

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

Tổng quan ATTT

Sự cấn thiết phải có an ninh mạng

Các yếu tố đảm bảo an toàn thông tin

Mối đe dọa an ninh mạng (Threat)

Lỗ hổng hệ thống (Vulnerable)

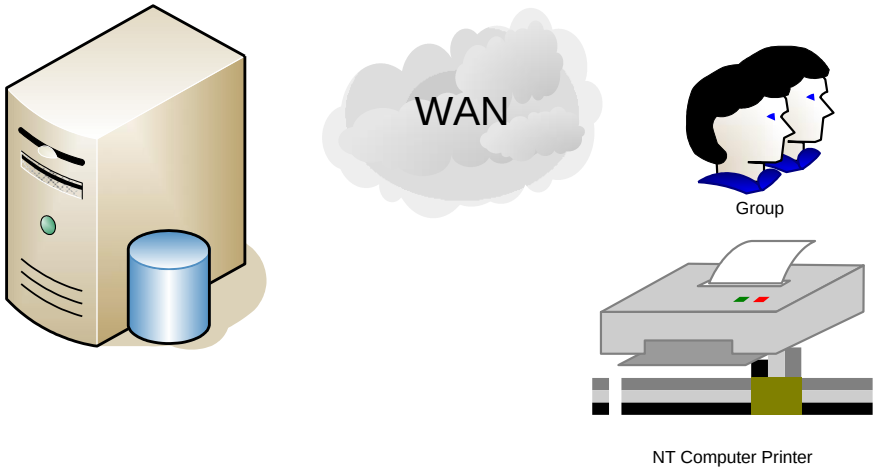
Nguy cơ hệ thống (Risk)

Đánh giá nguy cơ hệ thống

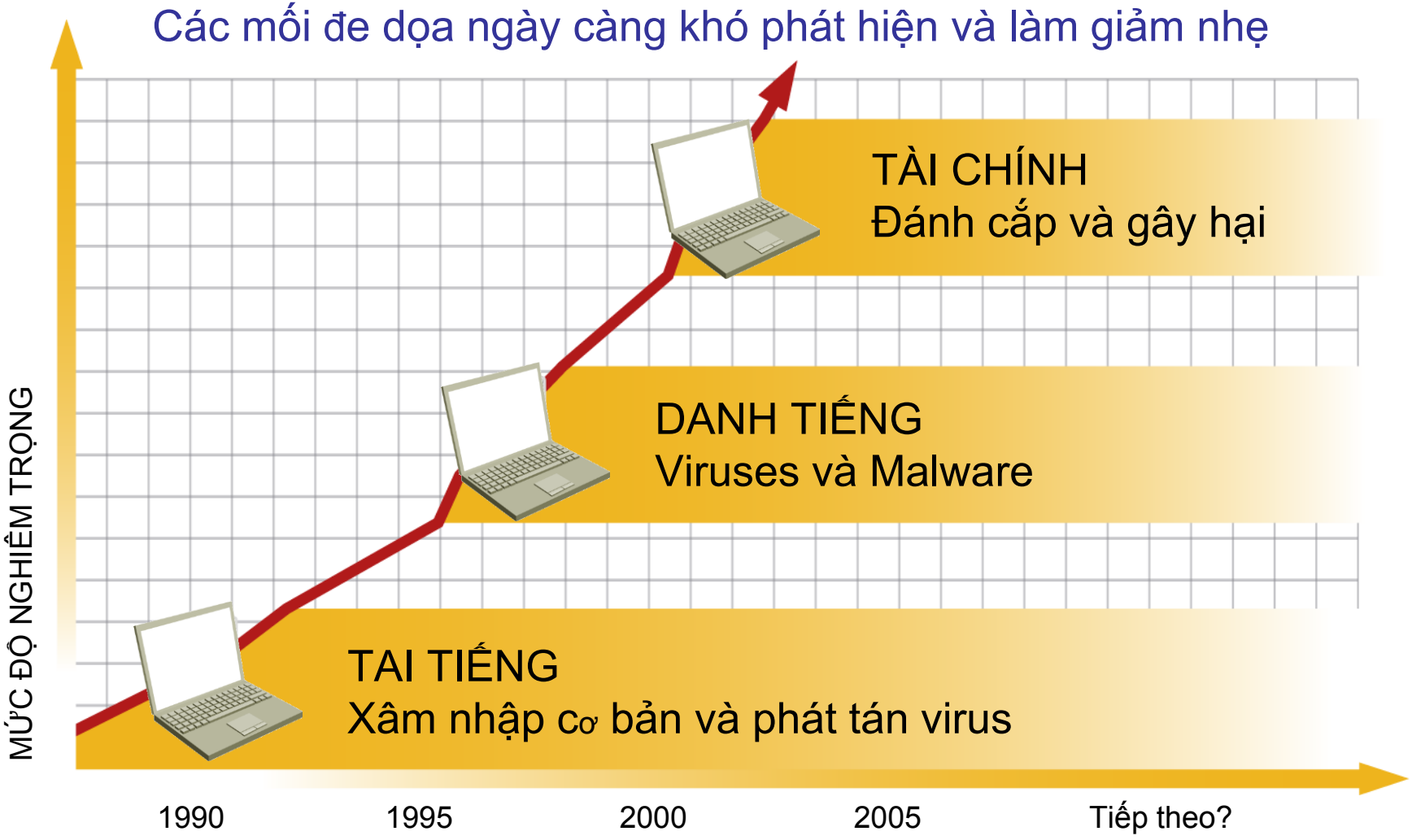
Sự cần thiết phải có an ninh mạng

Các yếu tố cần bảo vệ

- Dữ liệu
- Tài nguyên: con người, hệ thống, đường truyền
- Danh tiếng



Sự cần thiết phải có an ninh mạng



Sự cần thiết phải có an ninh mạng

Tác hại đến doanh nghiệp

- Tốn kém chi phí
- Tốn kém thời gian
- Ảnh hưởng đến tài nguyên hệ thống
- Ảnh hưởng danh dự, uy tín doanh nghiệp
- Mất cơ hội kinh doanh

Sự cần thiết phải có an ninh mạng

Cân nhắc

- Khả năng truy cập và khả năng bảo mật hệ thống tỉ lệ nghịch với nhau.

Các yếu tố đảm bảo an toàn thông tin

Bảo mật thông tin (Secrecy): đảm bảo thông tin được giữ bí mật.

Toàn vẹn thông tin (Integrity): bảo đảm tính toàn vẹn thông tin trong liên lạc hoặc giúp phát hiện rằng thông tin đã bị sửa đổi.

Xác thực (Authentication): xác thực các đối tác trong liên lạc và xác thực nội dung thông tin trong liên lạc.

Chống lại sự thoái thác trách nhiệm (Non-repudiation): đảm bảo một đối tác bất kỳ trong hệ thống không thể từ chối trách nhiệm về hành động mà mình đã thực hiện.

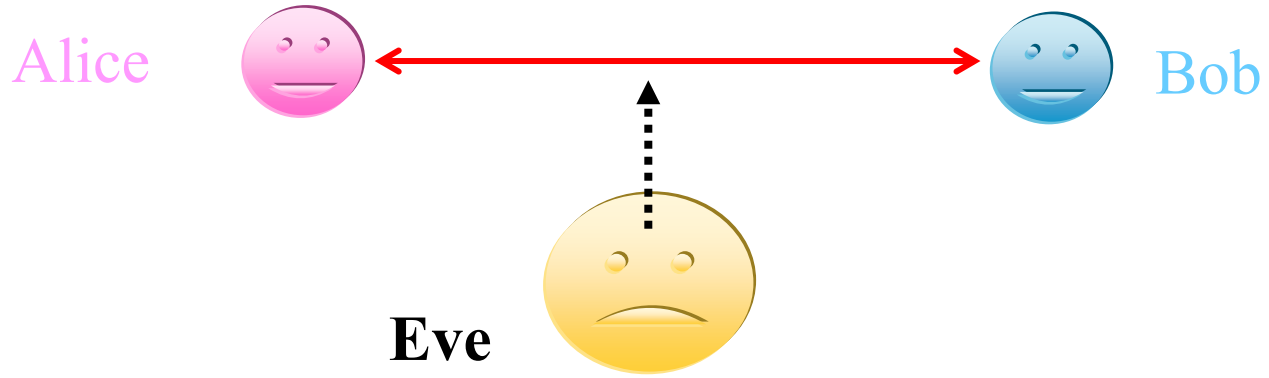
Tính sẵn sàng: Thông tin phải luôn sẵn sàng để tiếp cận, để phục vụ theo đúng mục đích và đúng cách.

Xác thực (Authentication)

Ví dụ:

- Bob chờ Alice "xác nhận" khi đến thời điểm thực hiện công việc
- Cần đảm bảo rằng Eve không can thiệp để tạo "xác nhận" giả

Xác thực (Authentication), Định danh (identification)

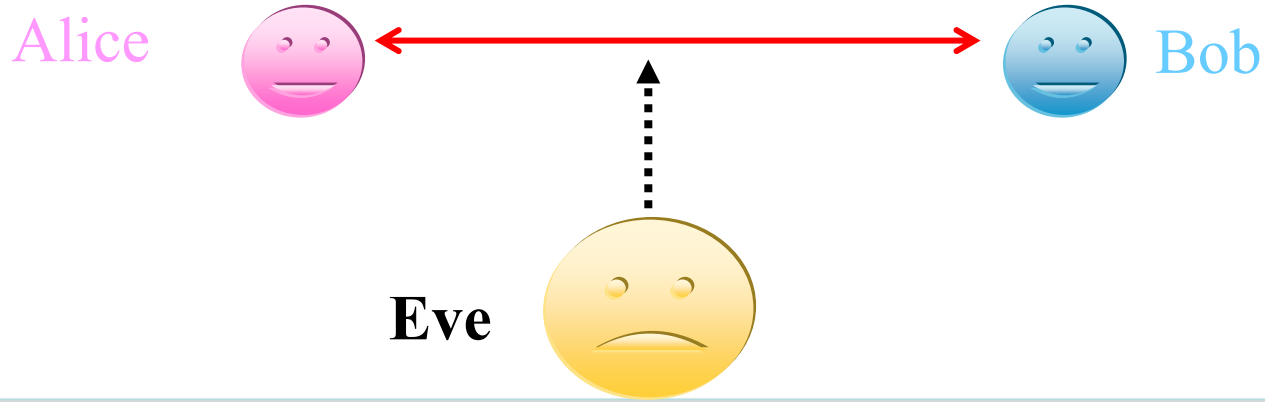


Tính toàn vẹn thông tin (Integrity)

Ví dụ:

- Bob cần đảm bảo là nhận chính xác nội dung mà Alice đã gửi
- Cần đảm bảo rằng Eve không can thiệp để sửa nội dung thông điệp mà Alice gửi cho Bob

Tính toàn vẹn thông tin (Integrity)



Chống lại sự thoái thác trách nhiệm

Ví dụ:

- Bob nhận được 1 thông điệp mà Alice đã gửi
- Alice không thể "chối" rằng không gửi thông điệp này cho Bob

Chống lại sự thoái thác trách nhiệm (Non-repudiation)

Các mối đe dọa (threat)

Các mối đe dọa (threat) đến an toàn hệ thống là các hành động hoặc các sự kiện/hành vi có khả năng xâm hại đến độ an toàn của một hệ thống thông tin

- Mục tiêu đe dọa tấn công.
- Đối tượng đe dọa tấn công (chủ thể tấn công)
- Hành vi đe dọa tấn công

Các mối đe dọa (threat)-2

Mục tiêu đe dọa tấn công (Target): chủ yếu là các dịch vụ an ninh (dịch vụ www, dns, …)

- Khả năng bảo mật thông tin: sẽ bị đe dọa nếu thông tin không được bảo mật
- Tính toàn vẹn của thông tin: đe dọa thay đổi cấu trúc thông tin
- Tính chính xác của thông tin: đe dọa thay đổi nội dung thông tin
- Khả năng cung cấp dịch vụ của hệ thống: làm cho hệ thống không thể cung cấp được dịch vụ (tính sẵn sàng)
- Khả năng thống kê tài nguyên hệ thống

Các mối đe dọa (threat)-3

Đối tượng đe dọa tấn công (Agent) là chủ thể gây hại đến hệ thống

- Khả năng đe dọa tấn công của đối tượng: khả năng truy cập để khai thác các lỗ hổng hệ thống tạo ra mối đe dọa trực tiếp
- Sự hiểu biết của đối tượng về mục tiêu đe dọa tấn công: user ID, file mật khẩu, vị trí file, địa chỉ mạng,…
- Động cơ tấn công của đối tượng: chinh phục, lợi ích cá nhân, cố tình

Các mối đe dọa (threat)-4

Hành vi đe dọa tấn công

- Lợi dụng quyền truy nhập thông tin hệ thống
- Cố tình hoặc vô tình thay đổi thông tin hệ thống
- Truy cập thông tin bất hợp pháp
- Cố tình hoặc vô tình phá hủy thông tin hoặc hệ thống
- Nghe lén thông tin
- Ăn cắp phần mềm hoặc phần cứng
- .....

Các mối đe dọa (threat)-5

Phân loại các mối đe dọa

- Có mục đích
- Không có mục đích
- Từ bên ngoài
- Từ bên trong

Lỗ hổng hệ thống (Vulnerable)

Lỗ hổng hệ thống: là nơi mà đối tượng tấn công có thể khai thác để thực hiện các hành vi tấn công hệ thống. Lỗ hổng hệ thống có thể tồn tại trong hệ thống mạng hoặc trong thủ tục quản trị mạng.

- Lỗ hổng lập trình (back-door)
- Lỗ hổng Hệ điều hành
- Lỗ hổng ứng dụng
- Lỗ hổng vật lý
- Lỗ hổng trong thủ tục quản lý (mật khẩu, chia sẽ,...)

Nguy cơ hệ thống (Risk)

Nguy cơ hệ thống: được hình thành bởi sự kết hợp giữa lỗ hổng hệ thống và các mối đe dọa đến hệ thống

Nguy cơ = Mối đe dọa + Lỗ hổng hệ thống

Nguy cơ hệ thống (Risk)

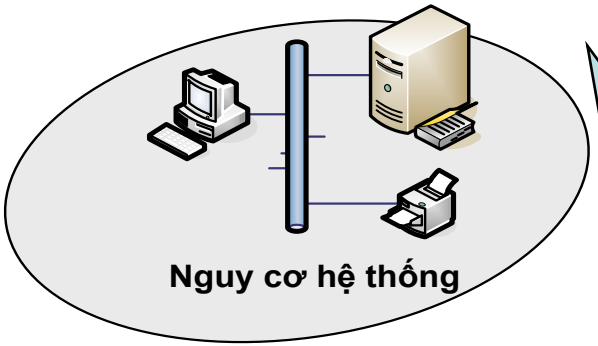
Các cấp độ nguy cơ

- Nguy cơ cao
- Nguy cơ trung bình
- Nguy cơ thấp

Đánh giá nguy cơ hệ thống

Xác định lỗ hổng hệ thống

Xác định các mối đe dọa đến hệ thống



Các biện pháp an toàn hệ thống hiện có

Đánh giá nguy cơ hệ thống (2)

Xác định các lỗ hổng hệ thống: việc xác định các lỗ hổng hệ thống được bắt đầu từ các điểm truy cập vào hệ thống như:

- Kết nối mạng Internet
- Các điểm kết nối từ xa
- Kết nối đến các tổ chức khác

- Các môi trường truy cập vật lý đến hệ thống
- Các điểm truy cập người dùng
- Các điểm truy cập không dây

Ở mỗi điểm truy cập, ta phải xác định được các thông tin có thể truy cập và mức độ truy cập vào hệ thống

Đánh giá nguy cơ hệ thống (3)

Xác định các mối đe dọa

- Đây là một công việc khó khăn vì các mối đe dọa thường không xuất hiện rõ ràng (ẩn)
  - Các hình thức và kỹ thuật tấn công đa dạng:
    - DoS/DDoS, BackDoor, Tràn bộ đệm,...
    - Virus, Trojan Horse, Worm
    - Social Engineering
  - Thời điểm tấn công không biết trước
  - Qui mô tấn công không biết trước

Đánh giá nguy cơ hệ thống (3)

Kiểm tra các biện pháp an ninh mạng

– Các biện pháp an ninh gồm các loại sau:

- Bức tường lửa - Firewall
- Phần mềm diệt virus
- Điều khiển truy nhập
-Hệ thống chứng thực (mật khẩu, sinh trắc học, thẻ nhận dạng,…)
- Mã hóa dữ liệu
- Hệ thống dò xâm nhập IDS
-Các kỹ thuật khác: AD, VPN, NAT

- Ý thức người sử dụng
- Hệ thống chính sách bảo

Mật và tự động vá lỗi hệ thống

Đánh giá nguy cơ hệ thống (4)

Xác định mức độ nguy cơ

– Sau khi xác định được các lỗ hổng hệ thống, các mối đe dọa và các biện pháp an ninh hiện có, ta có thể xác định được mức độ nguy cơ hệ thống như sau:

- Tại một điểm truy cập cho trước với các biện pháp an ninh hiện có, xác định các tác động của các mối đe dọa đến hệ thống: khả năng bảo mật, tính bảo toàn dữ liệu, khả năng đáp ứng dịch vụ, khả năng phục hồi dữ liệu thông qua điểm truy cập đó.

Đánh giá nguy cơ hệ thống (4)

Xác định mức độ nguy cơ (tt)

- Căn cứ vào 5 tiêu chí đánh giá (Chi phí, Thời gian, Danh dự, Tài nguyên hệ thống, Cơ hội kinh doanh) ta có thể phân nguy cơ an toàn mạng ở một trong các mức: cao, trung bình, thấp.
- Nếu hệ thống kết nối vật lý không an toàn thì hệ thống cũng ở mức nguy cơ cao

CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

Giới thiệu một số kỹ thuật tấn công phổ biến

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

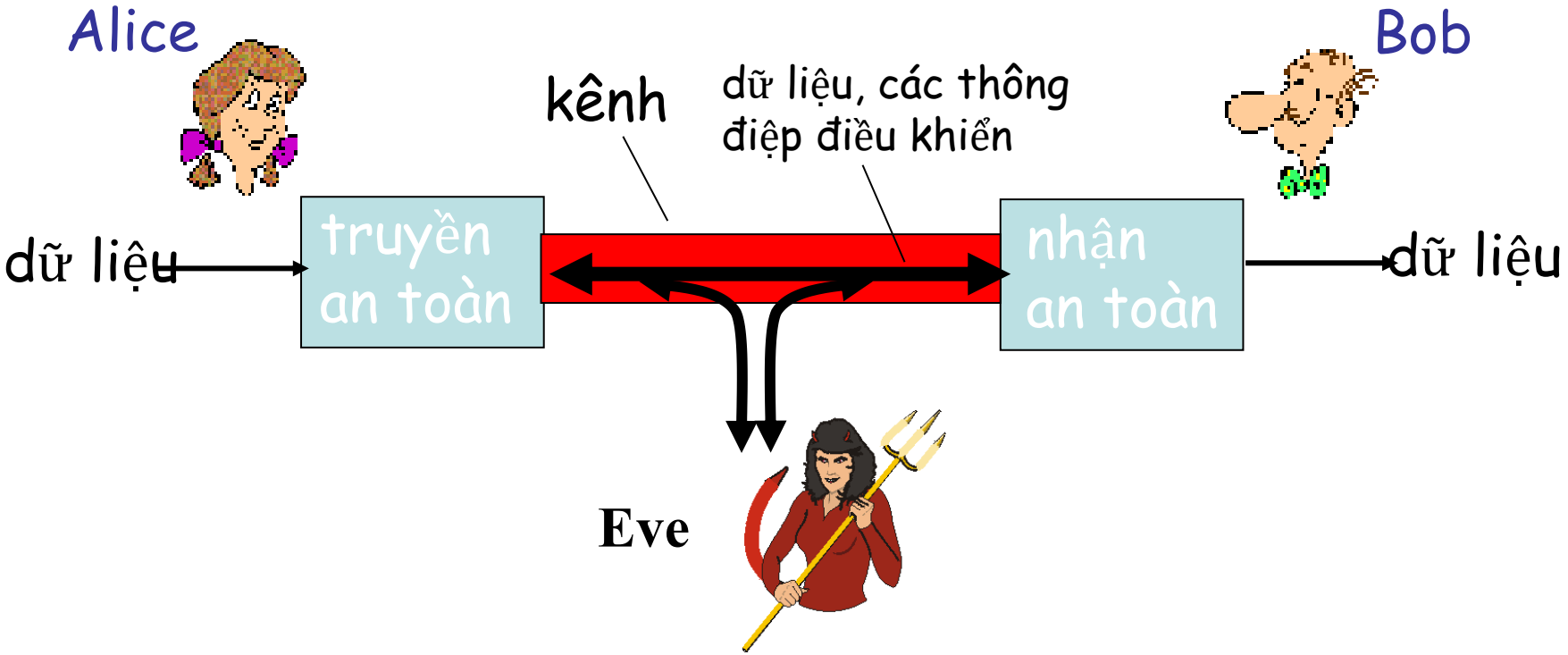
Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

Giới thiệu một số kỹ thuật tấn công phổ biến

Bob, Alice (bạn bè) muốn truyền thông "an toàn"

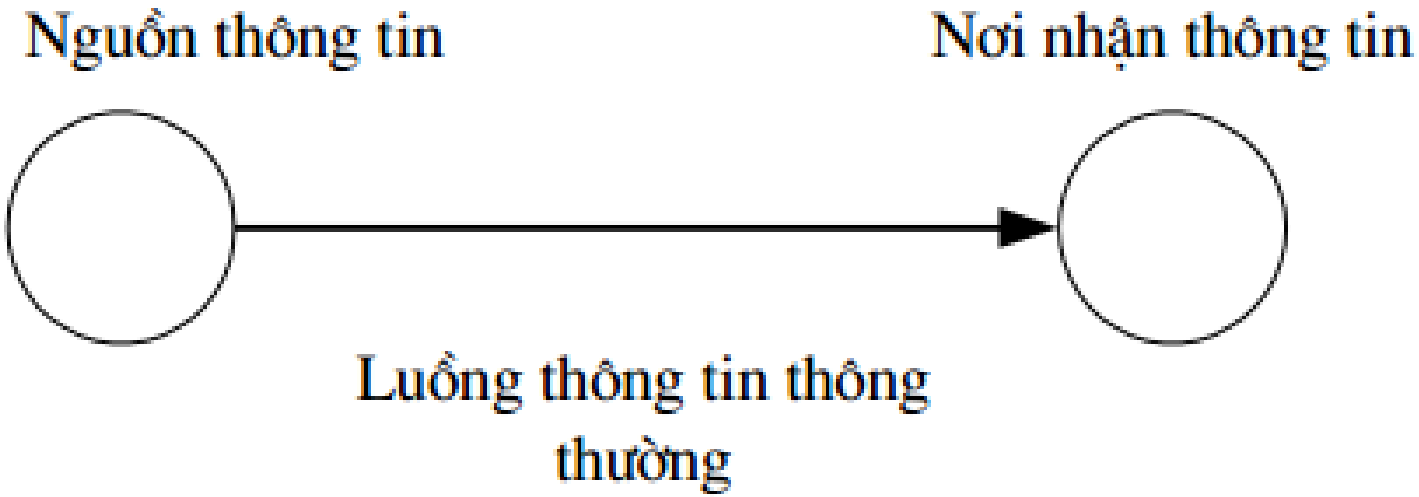
Eve (kẻ xâm nhập) có thể ngăn chặn, xóa, thêm các thông điệp



Giới thiệu một số kỹ thuật tấn công phổ biến

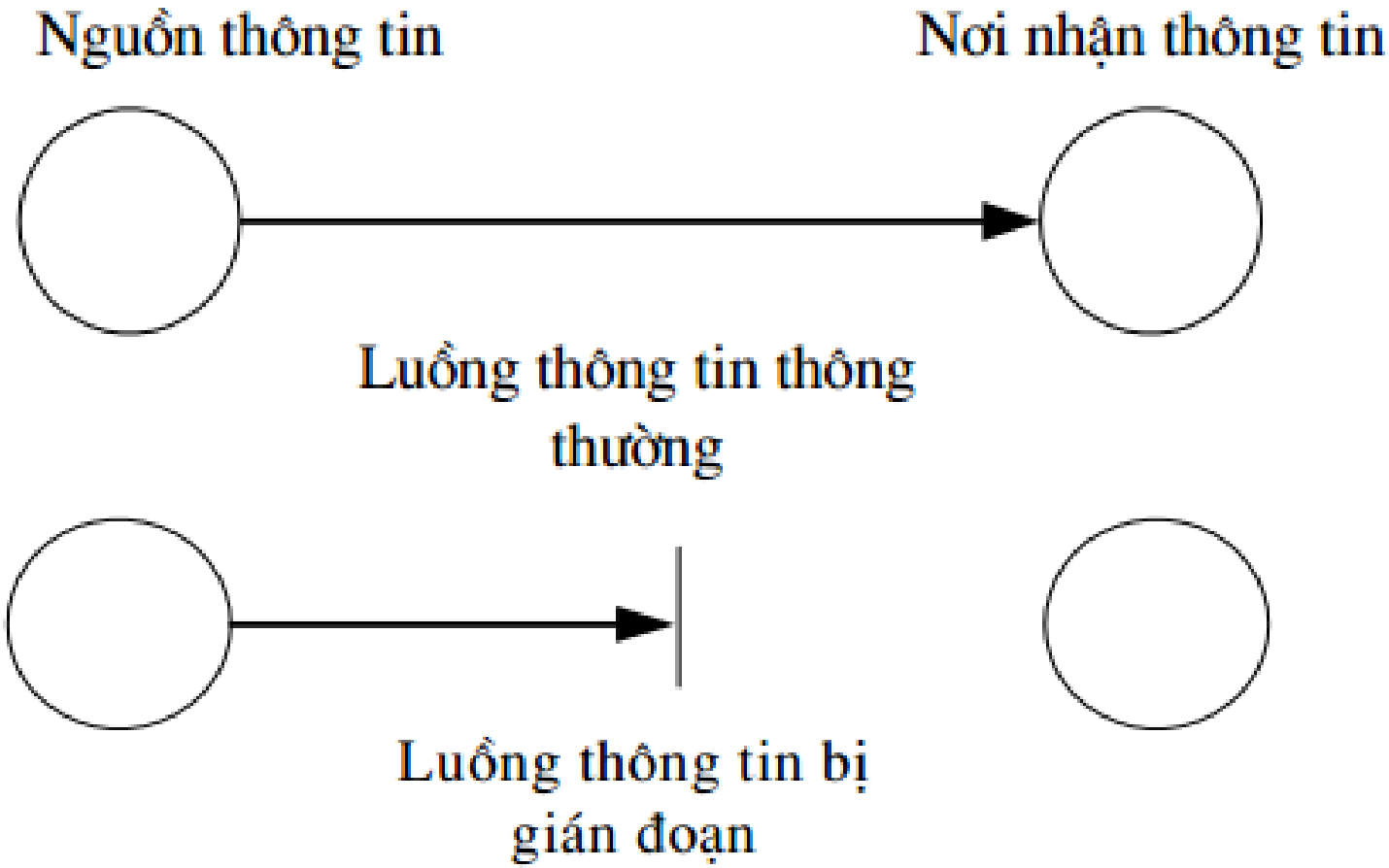
Các dạng tấn công

- Truy nhập thông tin bất hợp pháp
- Sửa đổi thông tin bất hợp pháp
- v.v và v.v ...



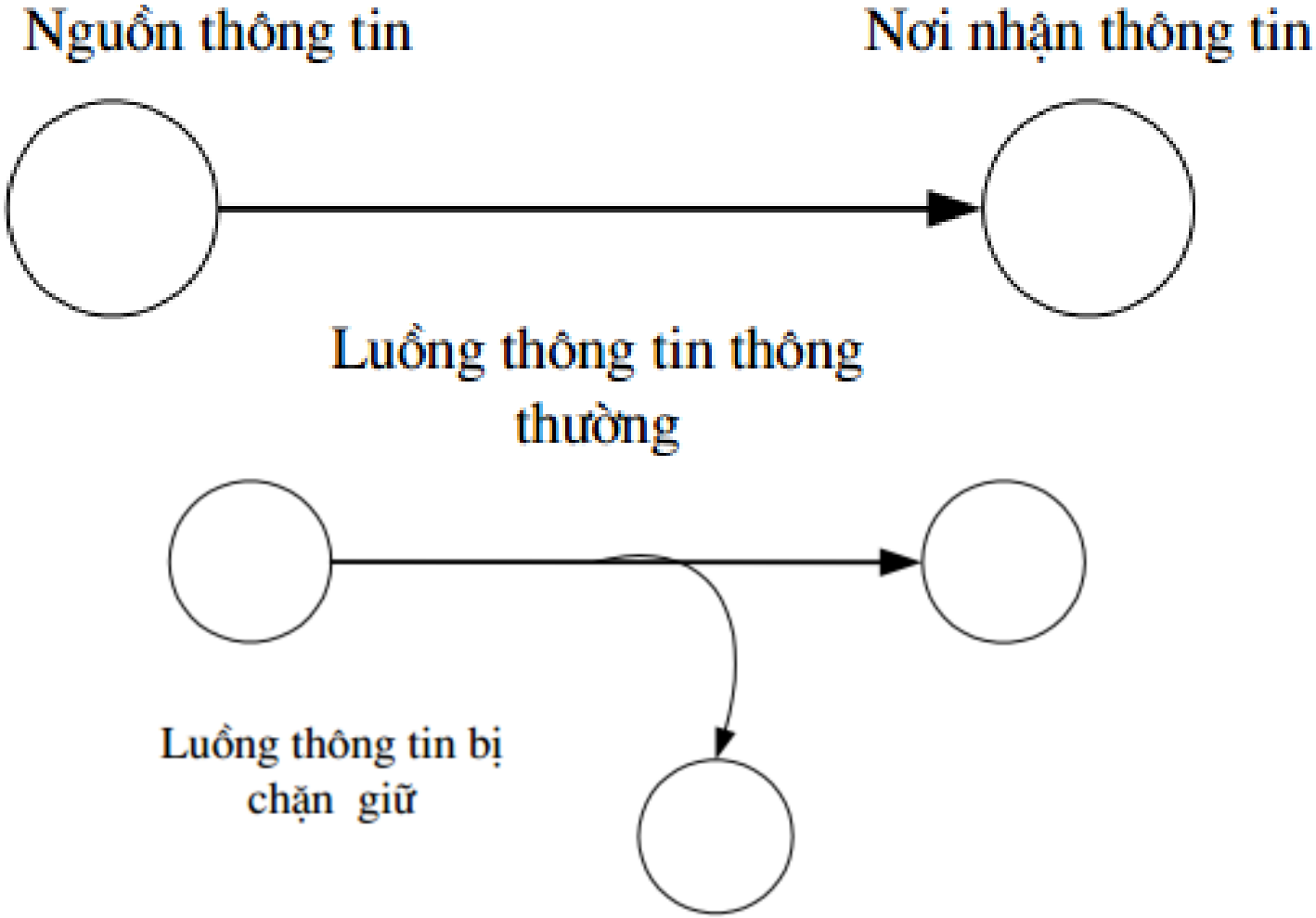
Giới thiệu một số kỹ thuật tấn công phổ biến

Gián đoạn truyền tin (interruption)



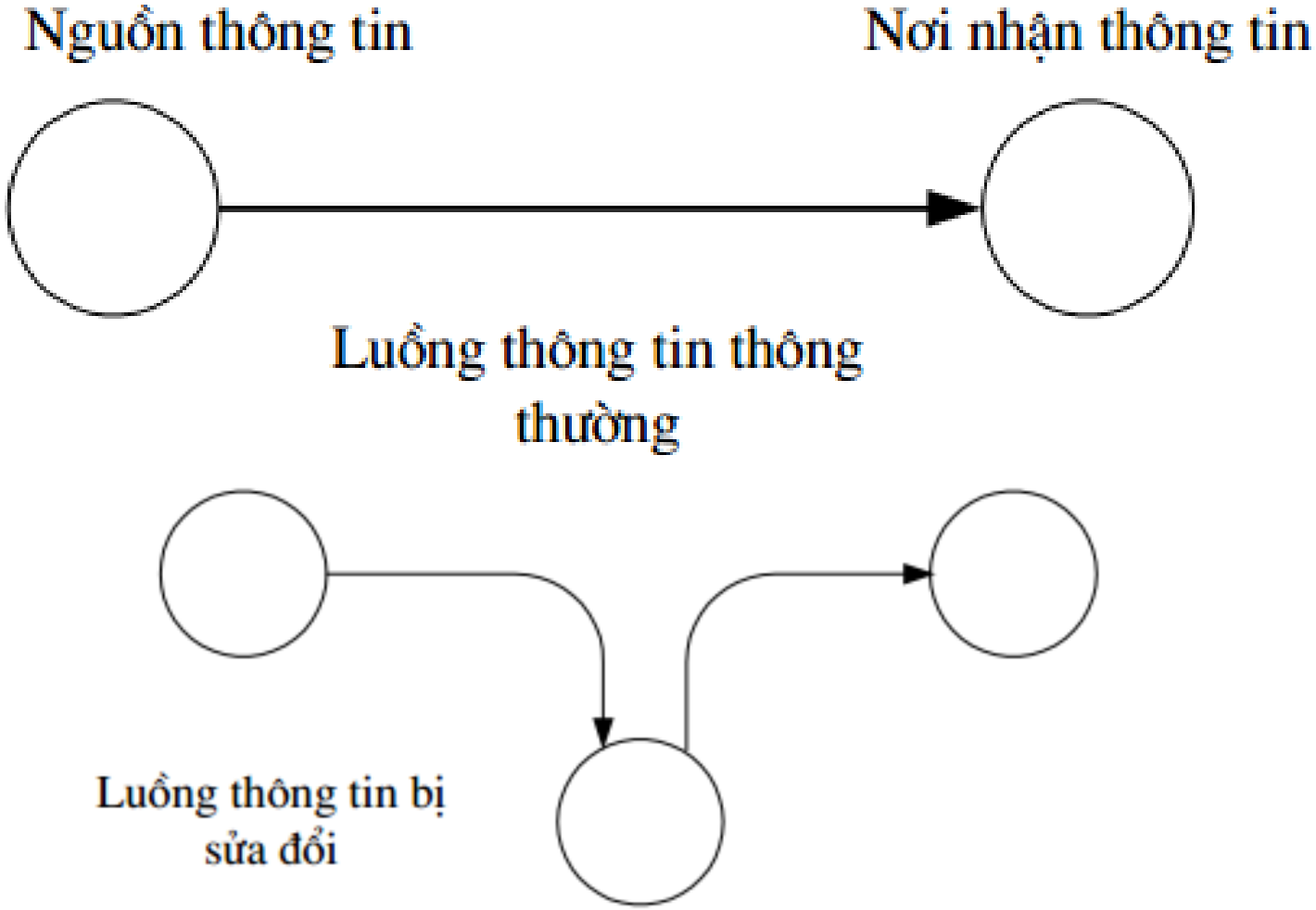
Giới thiệu một số kỹ thuật tấn công phổ biến

Chặn giữ thông tin (interception)



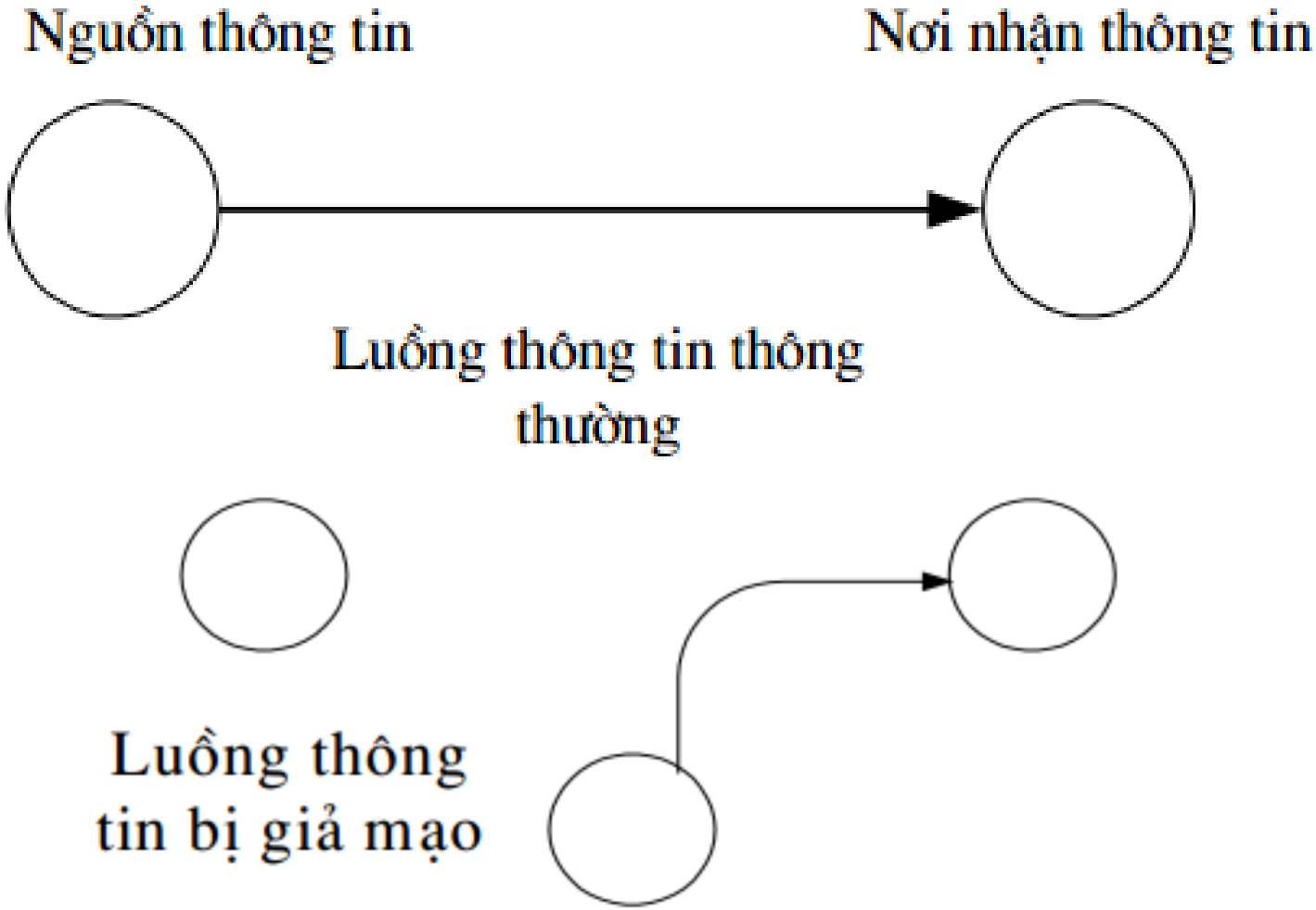
Giới thiệu một số kỹ thuật tấn công phổ biến

Sửa đổi thông tin (modification)



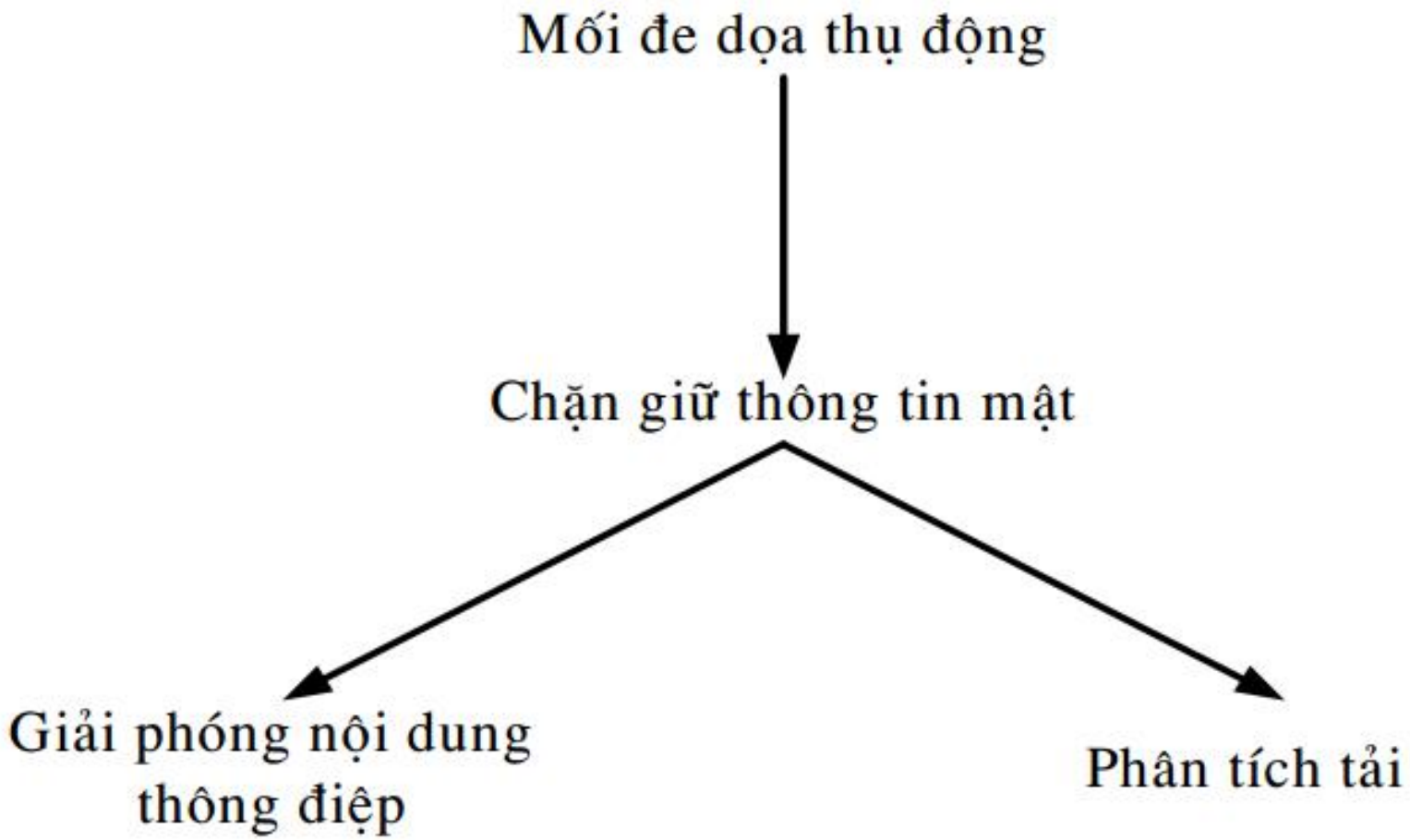
Giới thiệu một số kỹ thuật tấn công phổ biến

Giả mạo thông tin (fabrication)



Giới thiệu một số kỹ thuật tấn công phổ biến

Tấn công thụ động



Giới thiệu một số kỹ thuật tấn công phổ biến

Các dạng tấn công thụ động

- Giải phóng nội dung thông điệp (release of message contents).
  - Ngăn chặn đối phương thu và tìm hiểu được nội dung của thông tin truyền tải.

Phân tích tải (traffic analysis).

- Đối phương có thể xác định:
  - Vị trí của các máy tham gia vào quá trình truyền tin,
  - Tần suất và kích thước bản tin.

Giới thiệu một số kỹ thuật tấn công phổ biến

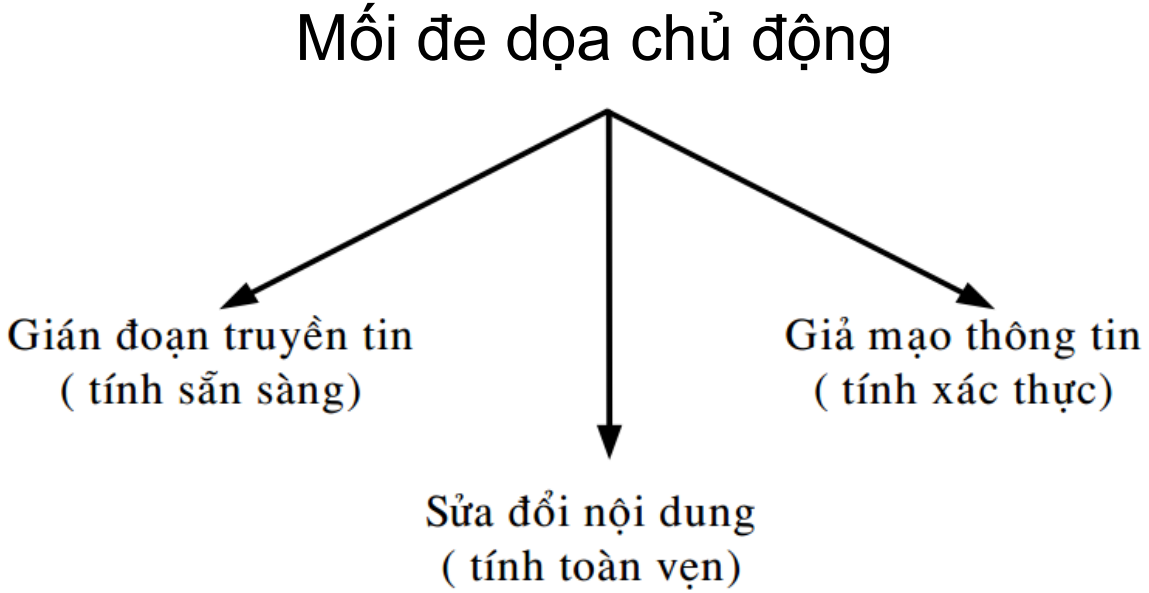
Dạng tấn công thụ động rất khó bị phát hiện vì không làm thay đổi dữ liệu.

Với dạng tấn công thụ động, nhấn mạnh vấn đề ngăn chặn hơn là vấn đề phát hiện.

Giới thiệu một số kỹ thuật tấn công phổ biến

Dạng tấn công chủ động

– Dạng tấn công chủ động bao gồm: sửa các dòng dữ liệu, đưa những dữ liệu giả, giả danh, phát lại, thay đổi thông điệp, phủ nhận dịch vụ



Giới thiệu một số kỹ thuật tấn công phổ biến

Dạng tấn công chủ động

- Giả danh (masquerade): khi đối phương giả mạo một đối tượng được uỷ quyền.
- Phát lại (replay): dạng tấn công khi đối phương chặn bắt các đơn vị dữ liệu và phát lại chúng tạo nên các hiệu ứng không được uỷ quyền;
- Thay đổi thông điệp (modification of message): một phần của thông điệp hợp pháp bị sửa đổi, bị làm chậm lại hoặc bị sắp xếp lại và tạo ra những hiệu ứng không được uỷ quyền.

Giới thiệu một số kỹ thuật tấn công phổ biến

Dạng tấn công chủ động

- Từ chối dịch vụ (denial of service): dạng tấn công đưa đến việc cấm hoặc ngăn chặn sử dụng các dịch vụ, các khả năng truyền thông.
- Dạng tấn công chủ động rất khó có thể ngăn chặn tuyệt đối. Điều đó yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm.
- Mục tiêu an toàn: phát hiện và phục hồi lại thông tin từ mọi trường hợp bị phá huỷ và làm trễ

CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

Giới thiệu một số kỹ thuật tấn công phổ biến

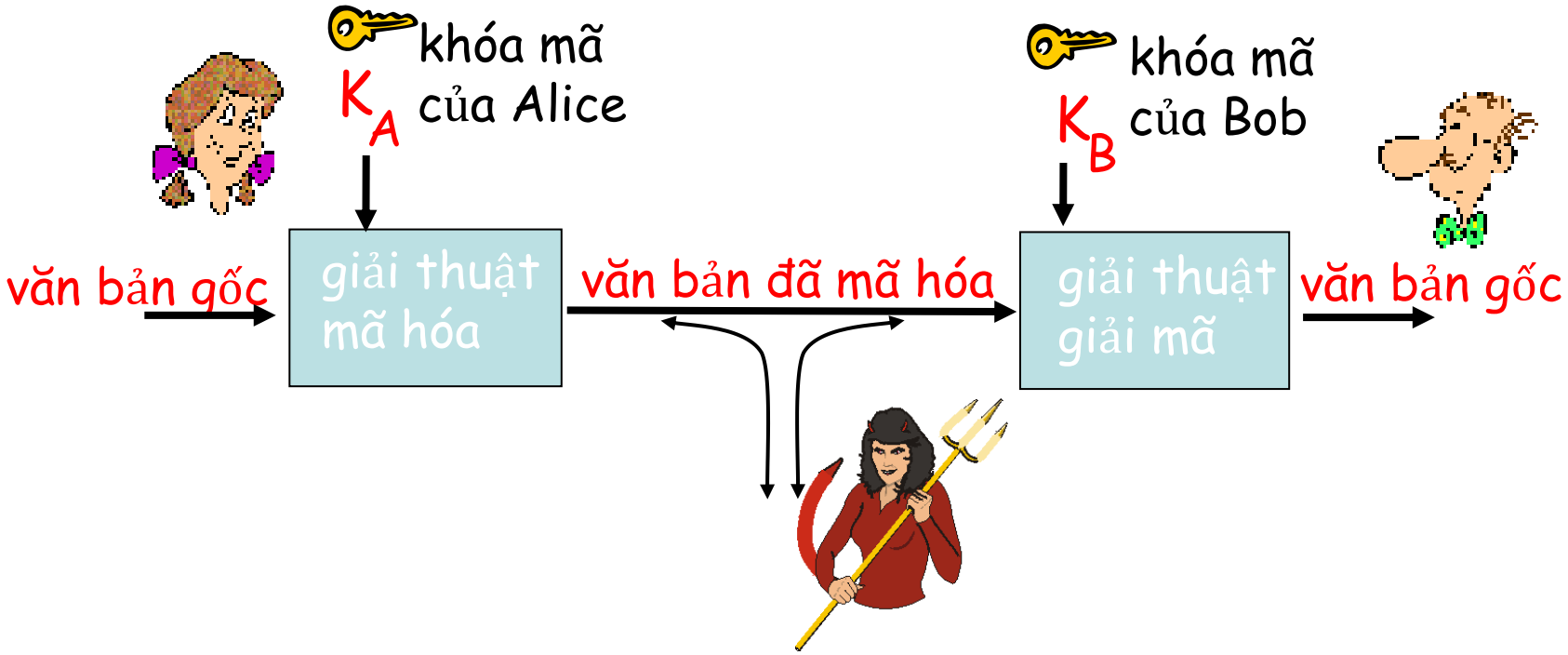
Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

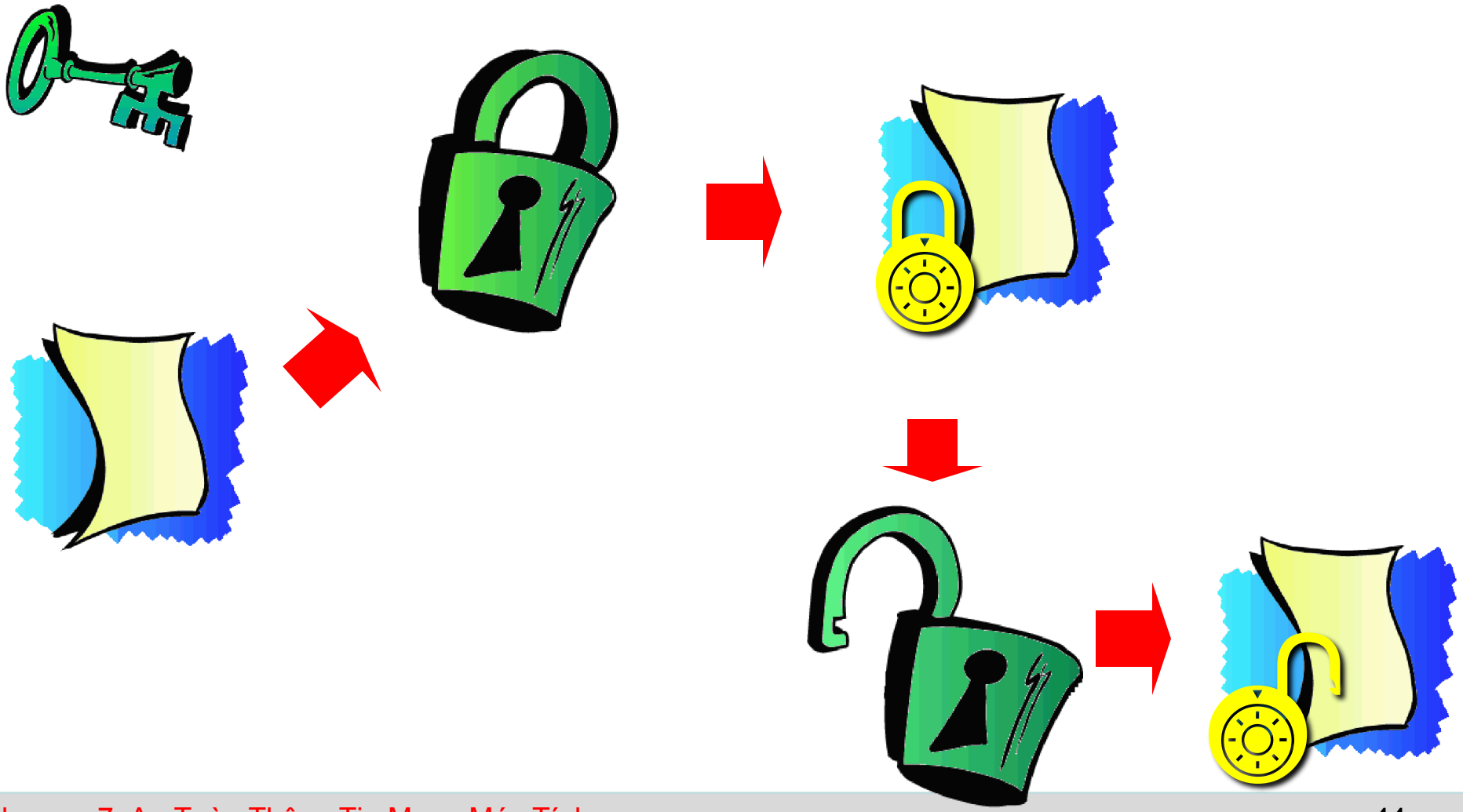
Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Ngôn ngữ mã hóa



Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Hệ thống mã hóa đối xứng



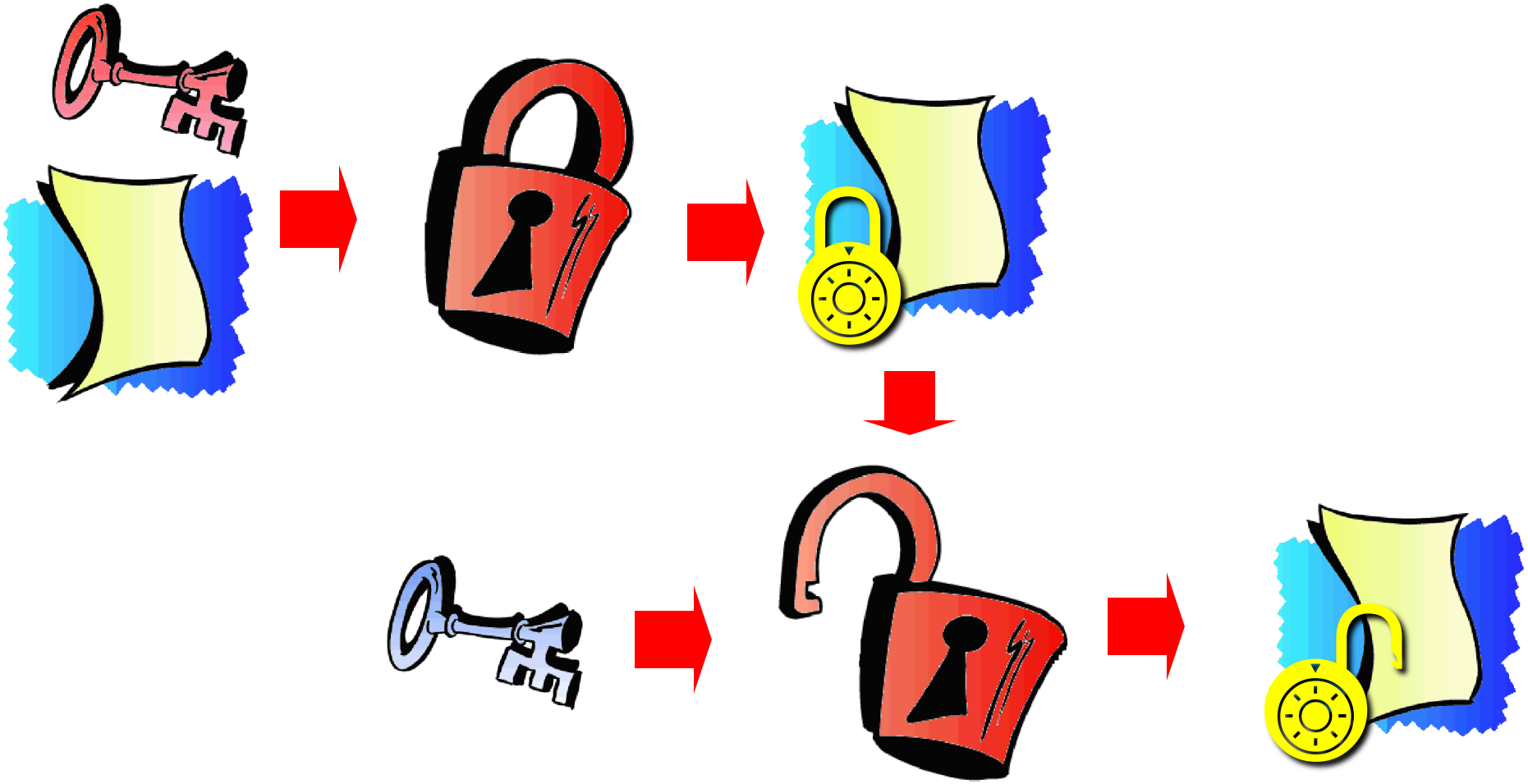
Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Mã đối xứng

- DES: Data Encryption Standard
  - Chuẩn mã hóa của hoa kỳ [NIST 1993]
  - Khóa đối xứng 56-bit, văn bản gốc vào 64-bit
- AES: Advanced Encryption Standard
  - Chuẩn NIST khóa đối xứng (tháng 11-2001) thay thế cho DES
  - Dữ liệu xử lý từng khối 128 bit
  - Các khóa 128, 192, hoặc 256 bit
  - Giải mã brute force (thử sai) tốn 1s với DES, tốn 149 tỷ tỷ năm với AES

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

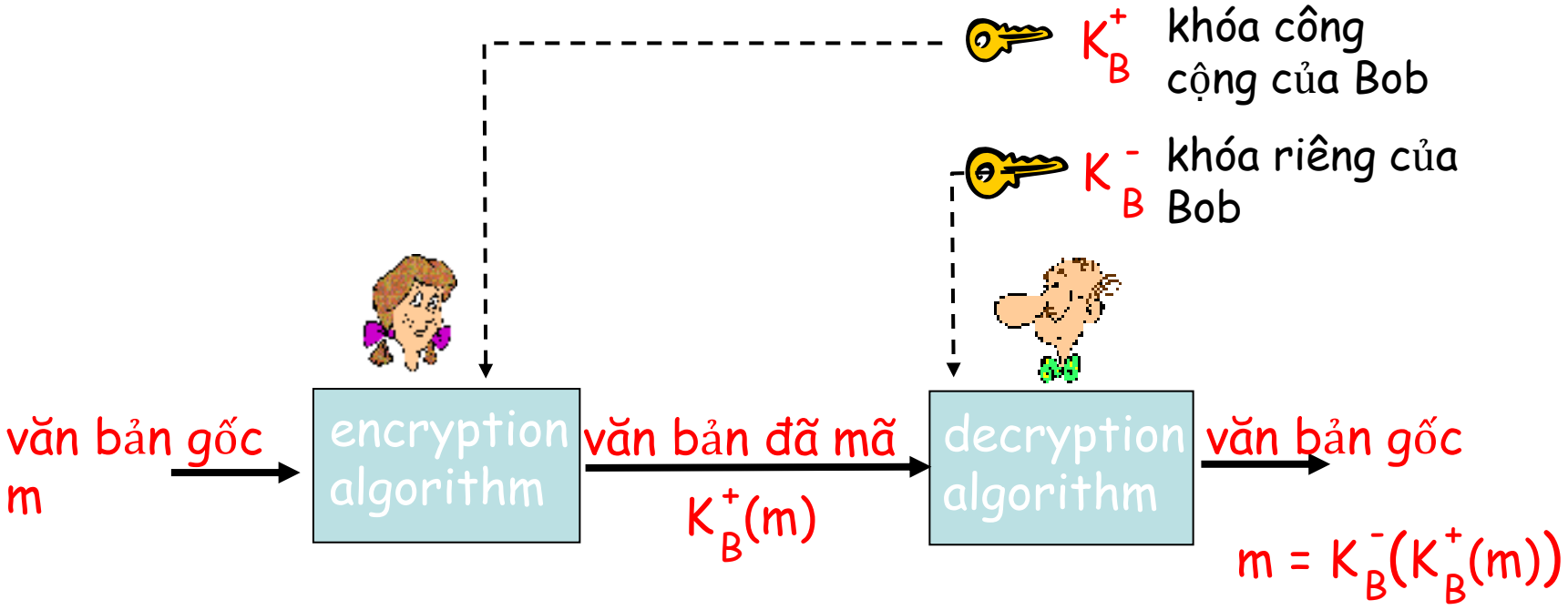
Mã hóa khóa công cộng



Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Mã hóa khóa công cộng (Mã bất đối xứng)

- Giải thuật RSA: Rivest, Shamir, Adelson



Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Mã đối xứng VS mã bất đối xứng

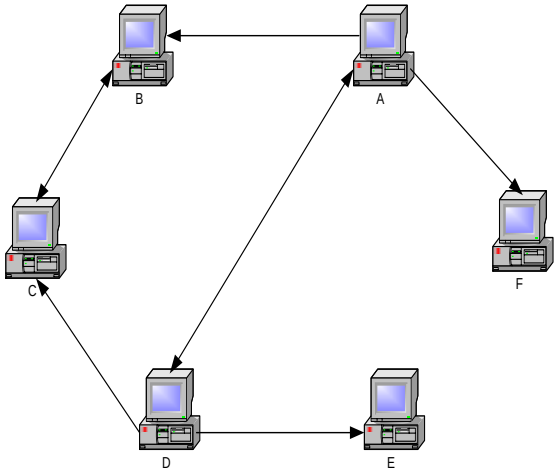
- Tốc độ xử lý nhanh
- Mã khóa ngắn
- Khó trao đổi mã khóa

- Tốc độ xử lý chậm
- Mã khóa dài
- Trao đổi mã khóa dễ dàng

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

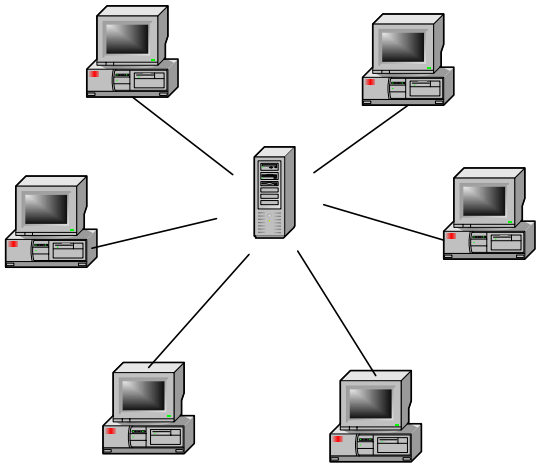
Chữ ký điện tử

Chứng nhận khóa công & Tổ chức chứng nhận khóa công (*Digital Certificate* &*Certificate Authority*)

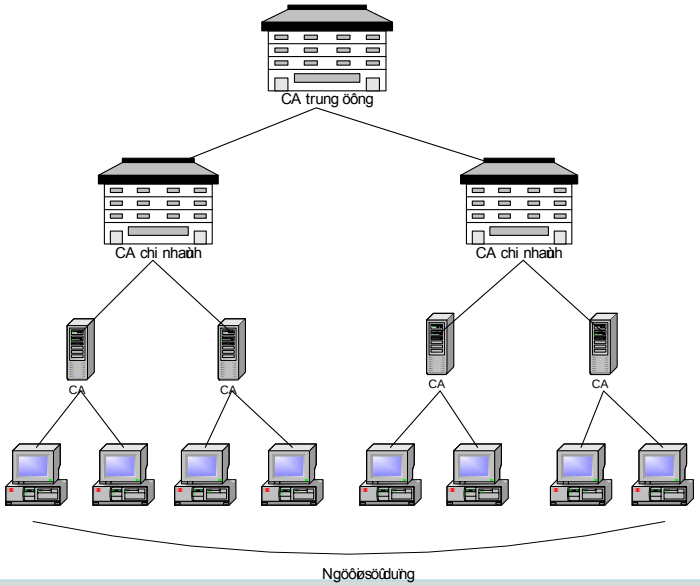


Web of Trust

Mô hình tập trung



Mô hình phân cấp



CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

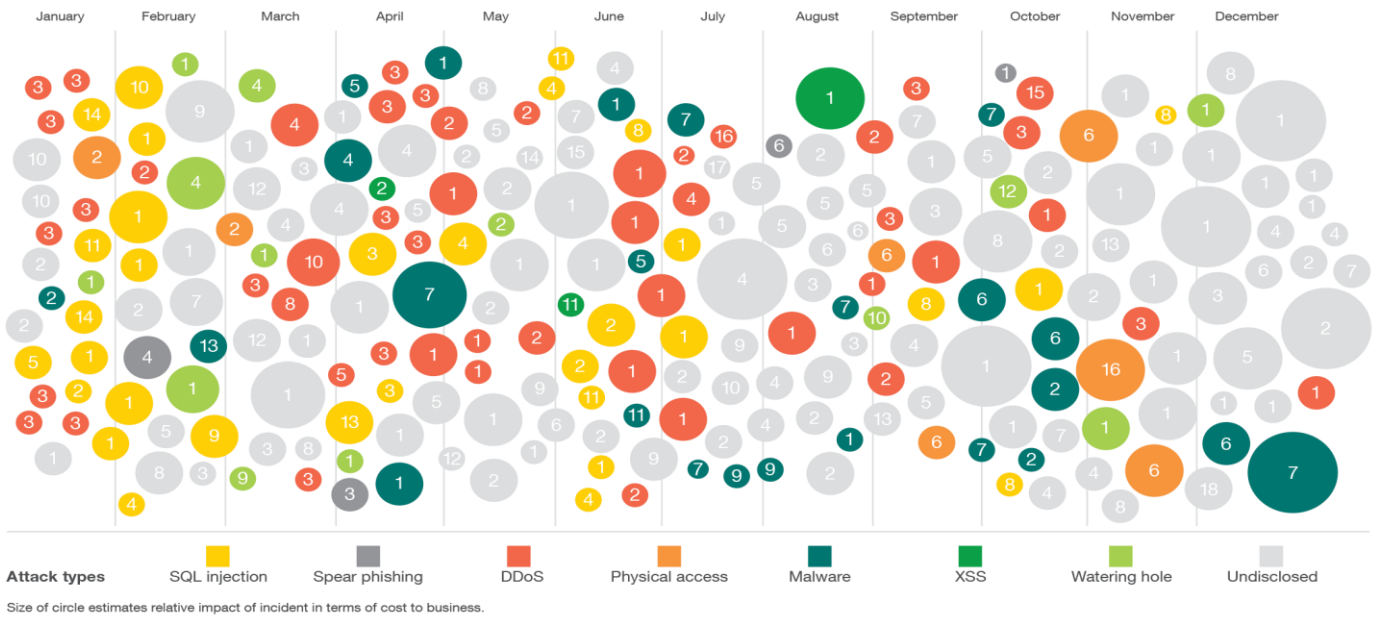
Giới thiệu một số kỹ thuật tấn công phổ biến

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

Giới thiệu các giao thức Bảo mật Web



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types

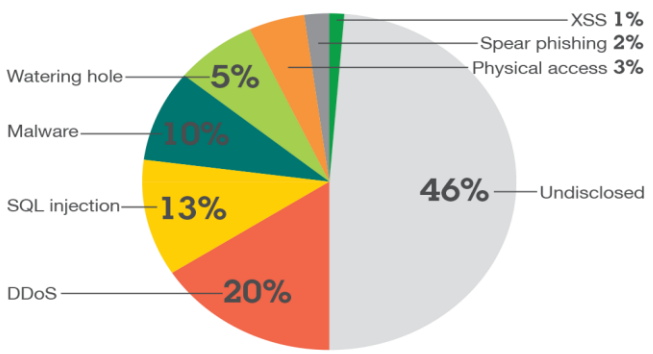


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

Giới thiệu các giao thức Bảo mật Web

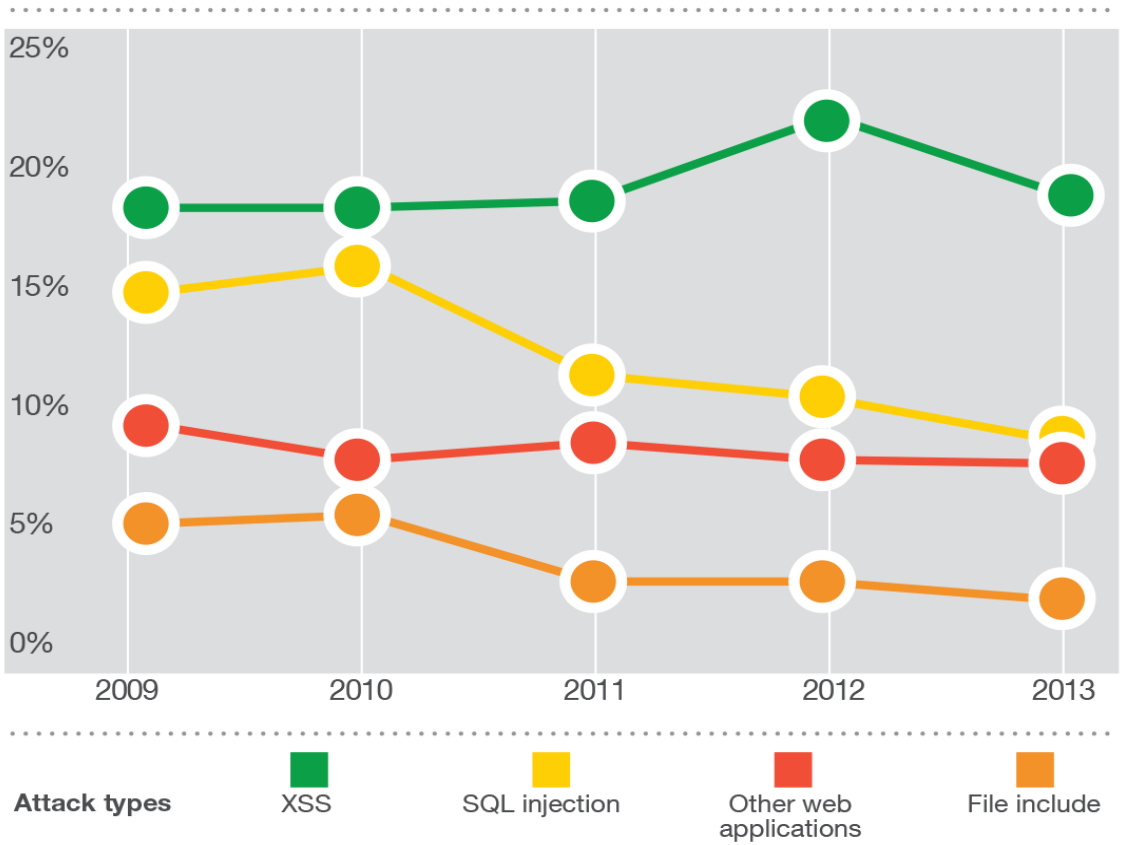
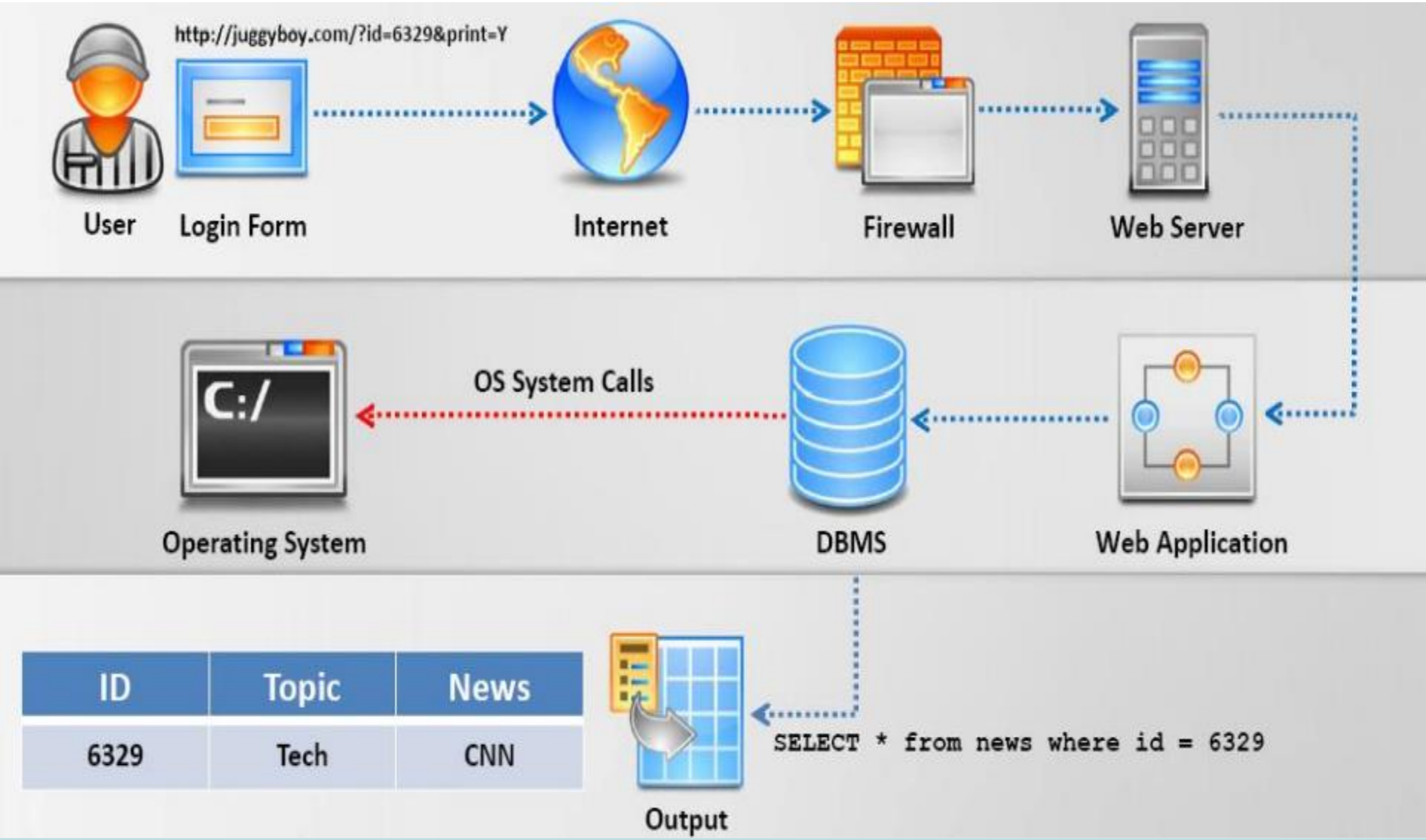


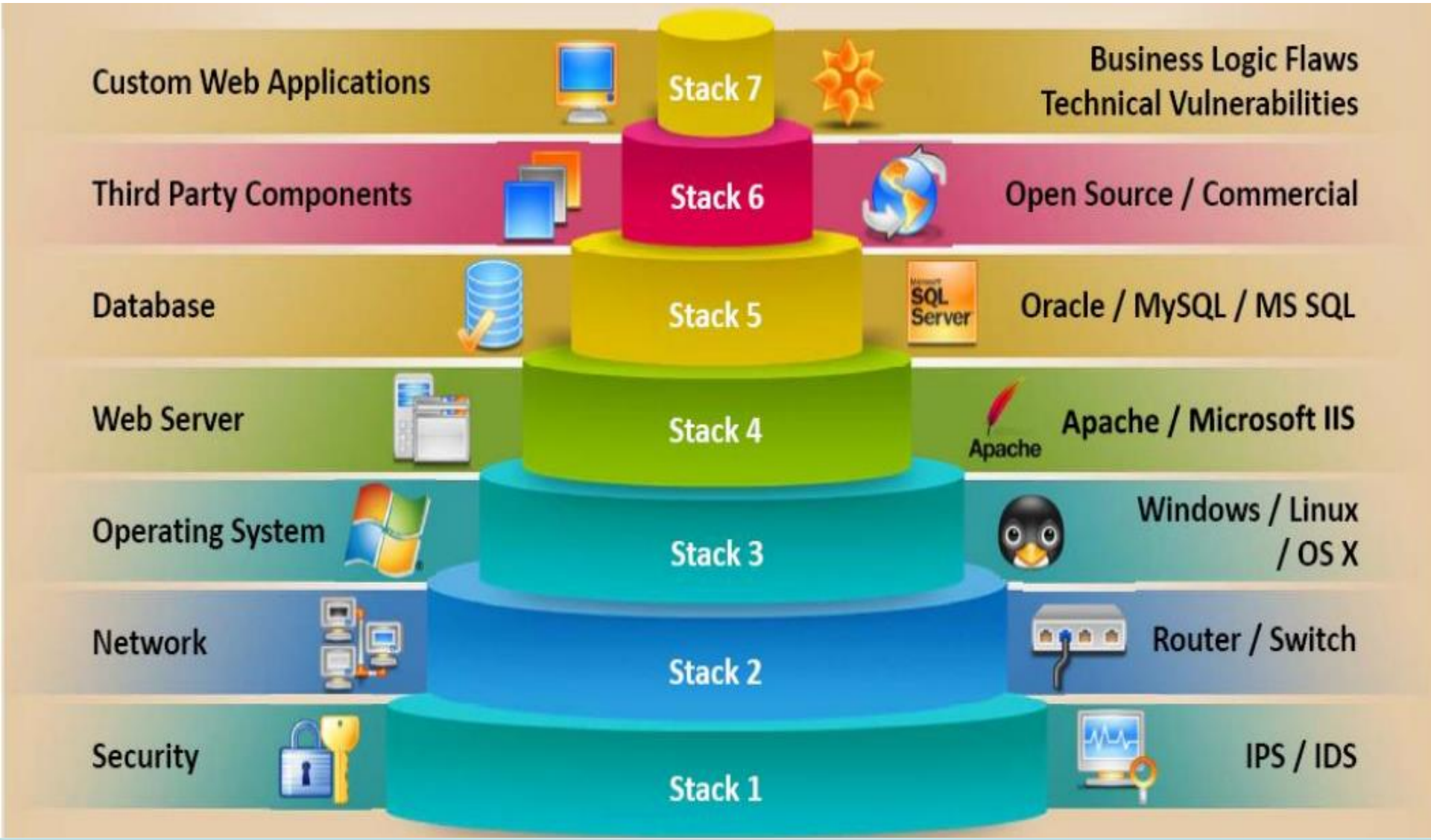
Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Source: IBM X-Force® Research and Development

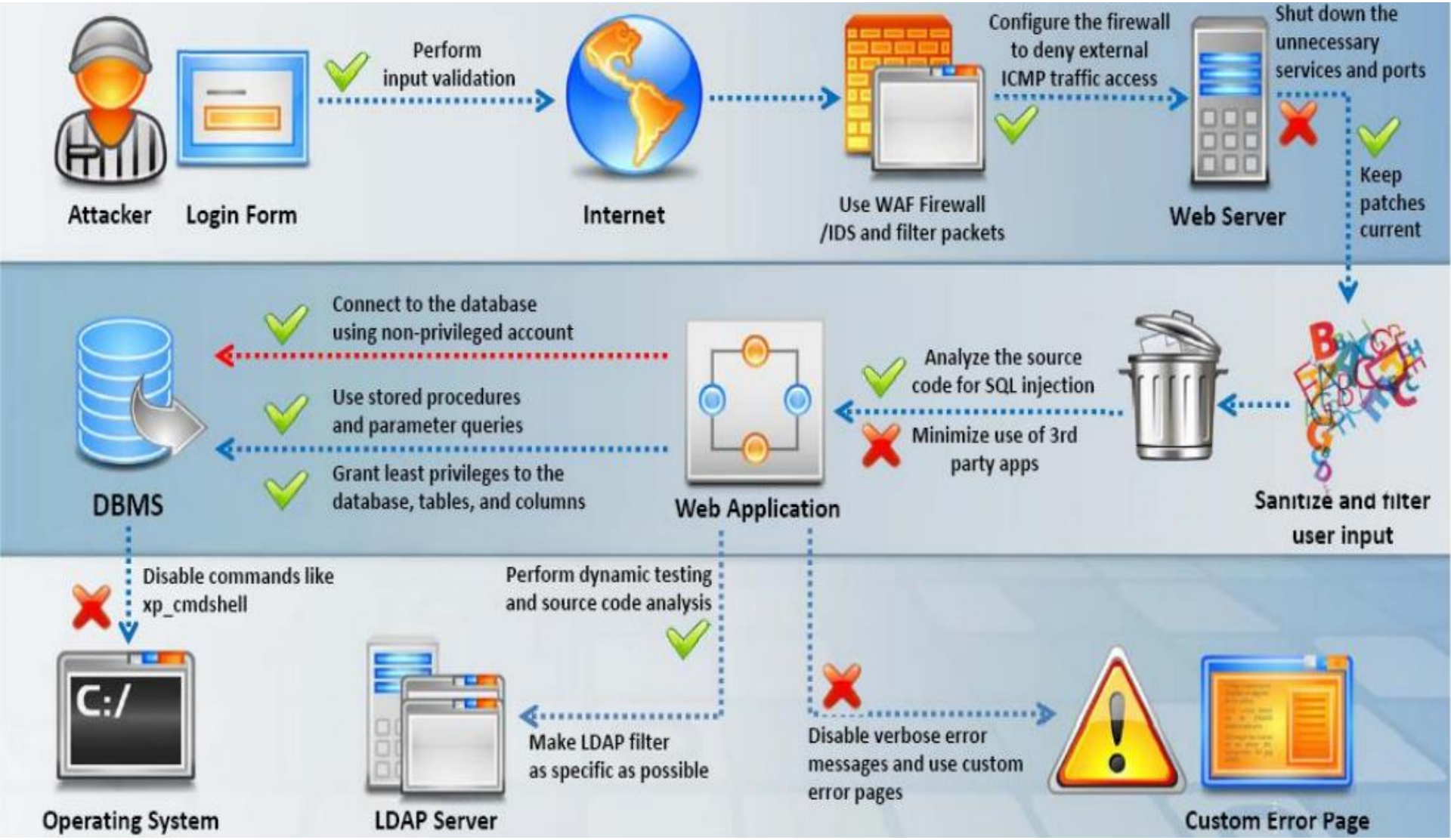
Giới thiệu các giao thức Bảo mật Web



Giới thiệu các giao thức Bảo mật Web

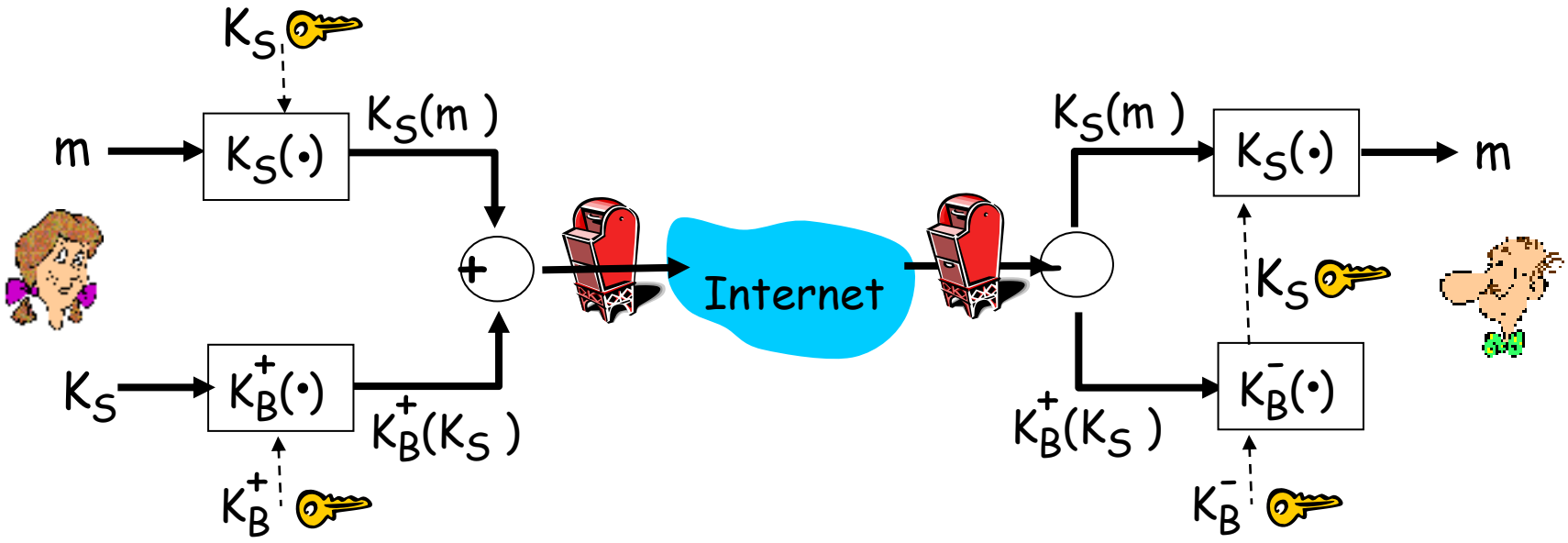


Giới thiệu các giao thức Bảo mật Web



Giới thiệu các giao thức Bảo mật Mail

- Alice muốn gửi 1 e-mail bí mật, m, đến Bob.

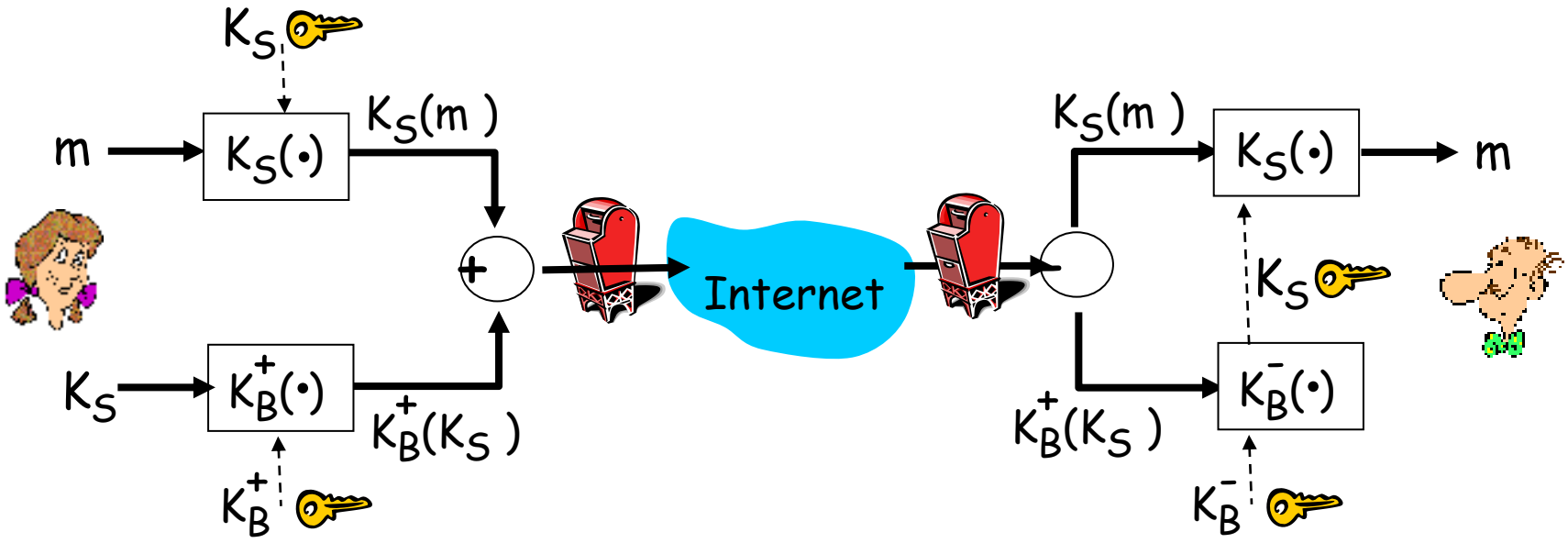


Alice:

- sinh ra khóa riêng đối xứng ngẫu nhiên, K_S.
- mã hóa thông điệp với K_S
- cũng mã hóa K_S với khóa công cộng của Bob.
- gửi cả $K_S(m)$ và $K_B(K_S)$ cho Bob.

Giới thiệu các giao thức Bảo mật Mail

- Alice muốn gửi 1 e-mail bí mật, m, đến Bob.

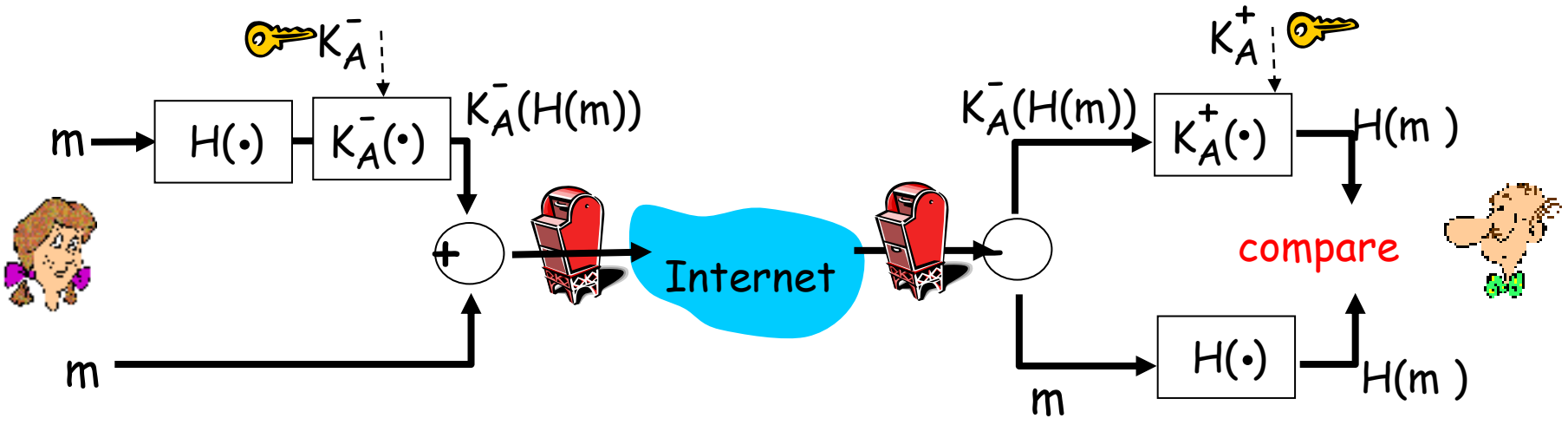


Bob:

- dùng khóa riêng của anh ấy để giải mã và phục hồi K_S
- dùng K_S để giải mã $K_S(m)$ và phục hồi m

Giới thiệu các giao thức Bảo mật Mail

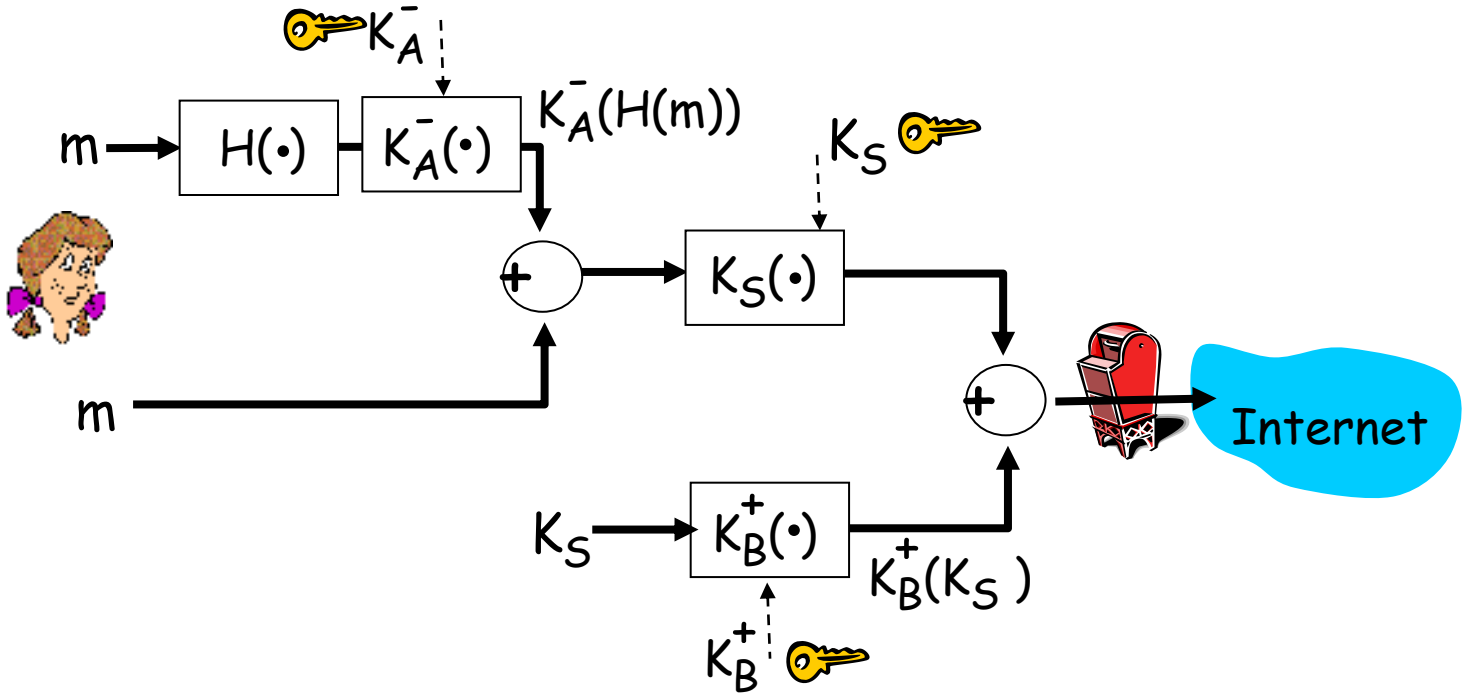
- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi.



- Alice ký số trên thông điệp.
- gửi cả thông điệp (dạng rõ ràng) và chữ ký số.

Giới thiệu các giao thức Bảo mật Mail

- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi, sự bí mật



Alice dùng 3 khóa: khóa riêng của cô ấy, khóa công cộng của Bob, khóa đối xứng vừa mới tạo

Giới thiệu các giao thức Bảo mật Mail

Pretty Good Privacy (PGP)

Chuẩn trên thực tế, là lược đồ mã hóa email internet.

Dùng mã hóa khóa đối xứng, khóa công cộng, hàm băm và chữ ký số

Hỗ trợ đồng nhất, chứng thực người gửi, sự bí mật

Người phát minh: phil zimmerman.

A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Giới thiệu các giao thức Bảo mật Mail

Secure sockets layer (SSL)

Ipsec

Giao thức AH

Giao thức ESP

...

CHƯƠNG 7: ATTT MẠNG MÁY TÍNH

Tổng quan ATTT

Giới thiệu một số kỹ thuật tấn công phổ biến

Giới thiệu các kỹ thuật mã hóa, bảo mật và xác thực

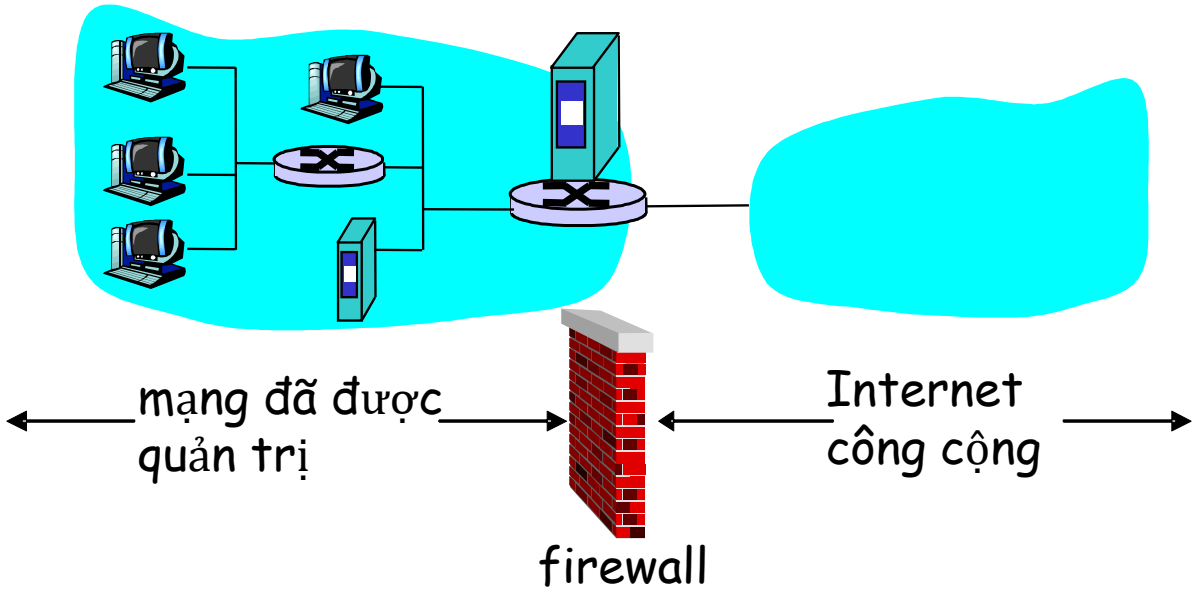
Giới thiệu các giao thức Bảo mật Web, Mail

Tường lửa và Kỹ thuật mạng riêng ảo

Tường lửa (Firewall)

firewall

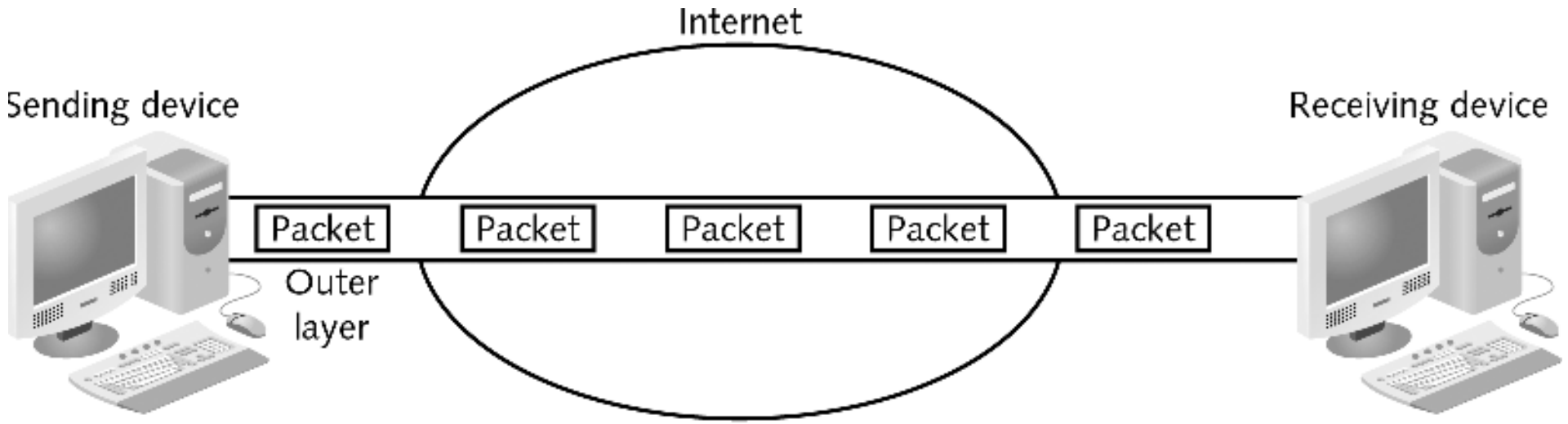
cô lập mạng nội bộ của tổ chức với Internet, cho phép một số gói được truyền qua, ngăn chặn các gói khác



Kỹ thuật mạng riêng ảo (VPN)

Tunneling Protocols

– Đây là kỹ thuật đóng gói một gói tin dữ liệu bên trong một gói tin khác để tạo ra một kênh truyền an toàn.



Kỹ thuật mạng riêng ảo (VPN)

Các công nghệ VPN

- Point-to-point Tunneling Protocol – PPTP
- Layer 2 Forwarding – L2F
- Layer 2 Tunneling Protocol - L2TP
- Layer 2 Security Protocol (L2Sec)
- IP Security – IPSec
- Secure Socket Layer/ Transport Socket Layer - SSL/ TLS

References

Một số nội dung môn học được tham khảo từ:

Jim Kurose, Keith Ross, *Computer Networking: A Top Down Approach 6th edition*, Addison-Wesley, March 2012.

Dương Anh Đức, Trần Minh Triết, *Mã hóa và Ứng dụng*, NXB Đại học Quốc gia (2005).

IBM X-Force 1Q2014-Graphics Package

CEH, EC-Council

Q & A

Câu hỏi ?

Ý kiến ?

Đề xuất ?