TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ ĐÔNG Á
EAST ASIA UNIVERSITY OF TECHNOLOGY

Chương 5. Network Sercurity

Overview

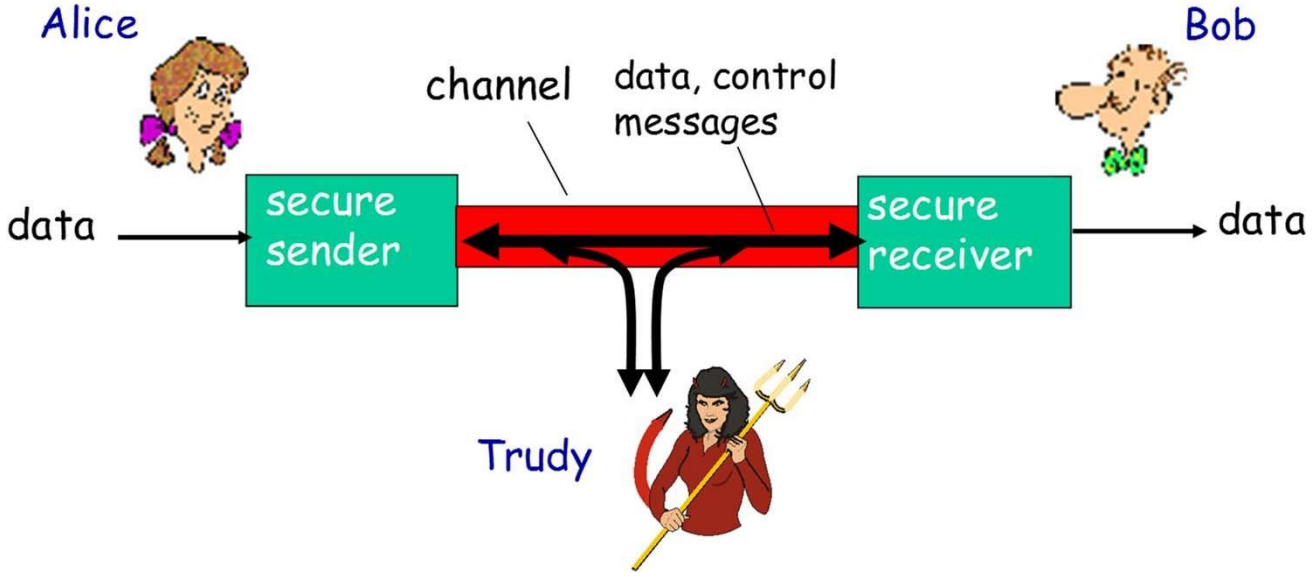
Giới thiệu nội dung

- Nội dung:
  - Tổng quan về an ninh mạng.
  - Một số kiểu tấn công mạng phổ biến.
  - Biện pháp đảm bảo an ninh mạng
- Tài liệu tham khảo:
  - Network and Internetwork Security
  - Introduction to Cryptography – PGP
  - Cryptography: Theory and Practice

Tổng quan về an ninh mạng

Mục tiêu

- Xác định các khả năng, nguy cơ xâm phạm mạng
- Đánh giá nguy cơ tấn công của Hacker, sự phát tán virus...
- Xác định cấp độ an ninh cần thiết cho việc điều khiển hệ thống và các thành phần mạng
- Sử dụng hiệu quả các công cụ bảo mật và những biện pháp, chính sách cụ thể chặt chẽ



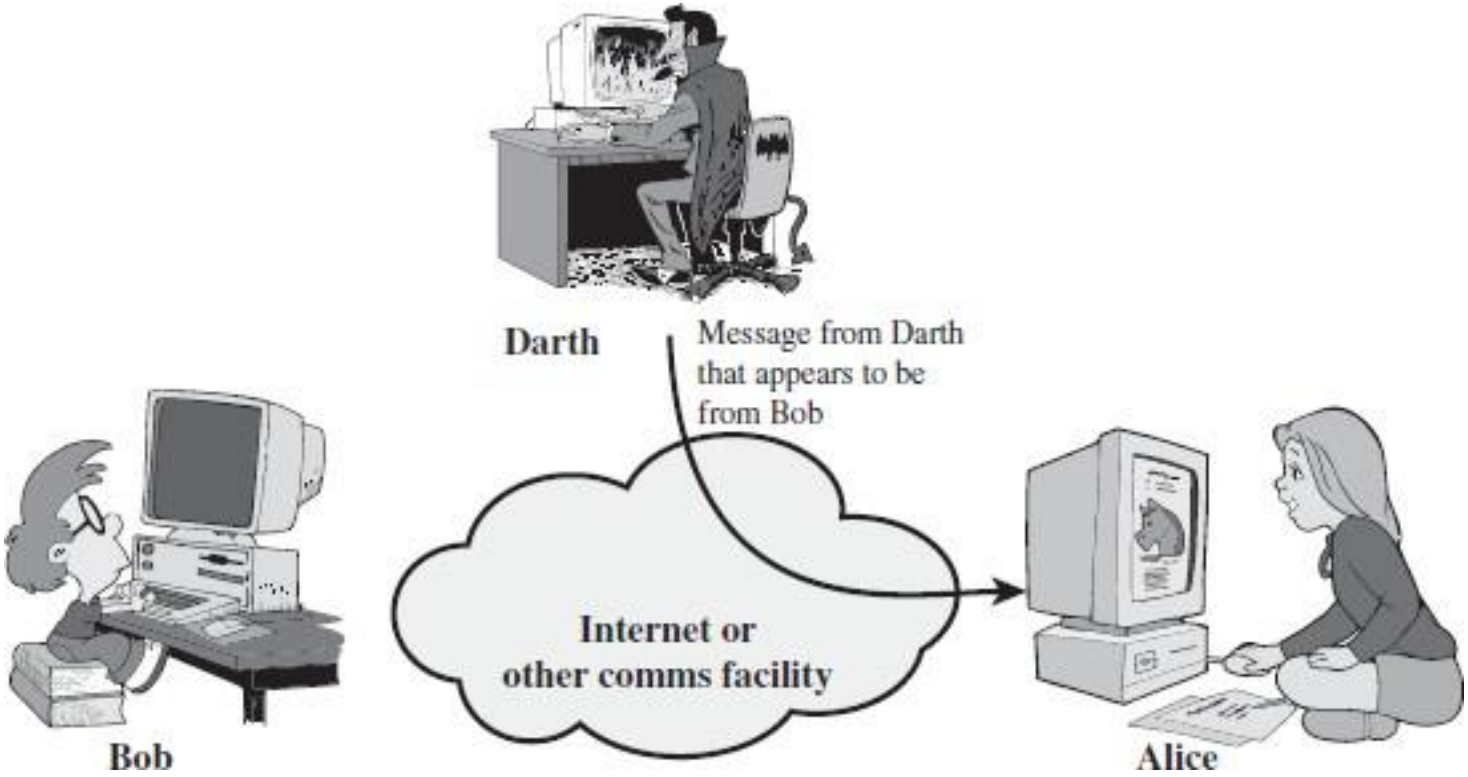
Các dạng tấn công

- Tấn công thụ động:
  - Nhằm mục đích nắm bắt được thông tin
    - Phát tán nội dung thông điệp (release of message contents)
    - Phân tích tải (traffic analysis)
  - Các hành động tấn công thụ động thường khó có thể phát hiện nhưng có thể ngăn chặn hiệu quả
- Tấn công chủ động
  - Thực hiện sự biến đổi thông điệp, xoá bỏ hoặc thêm thông tin ngoại lai (dữ liệu giả) để làm sai lệch thông tin gốc nhằm mục đích phá hoại, phủ nhận dịch vụ
    - Giả danh (masquerade)
    - Phát lại (replay)
    - Thay đổi thông điệp (modification of message).
    - Phủ nhận dịch vụ (denial of service):
  - Tấn công chủ động dễ phát hiện nhưng lại khó ngăn chặn tuyệt đối

Các dạng tấn công

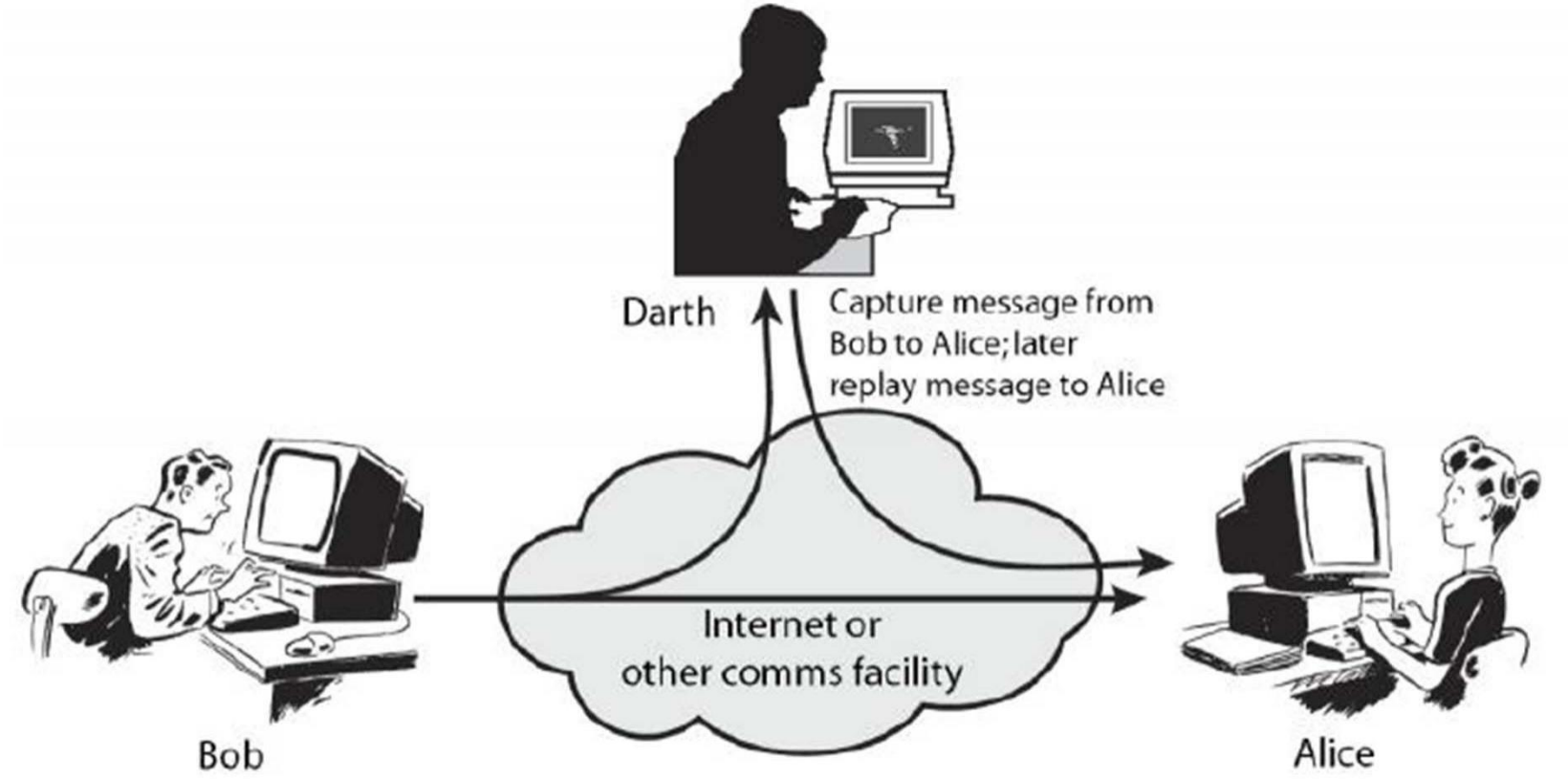
- Mạo danh (Masquerade)
  - Đối phương giả mạo một đối tượng được ủy quyền

  → Entity Authentification



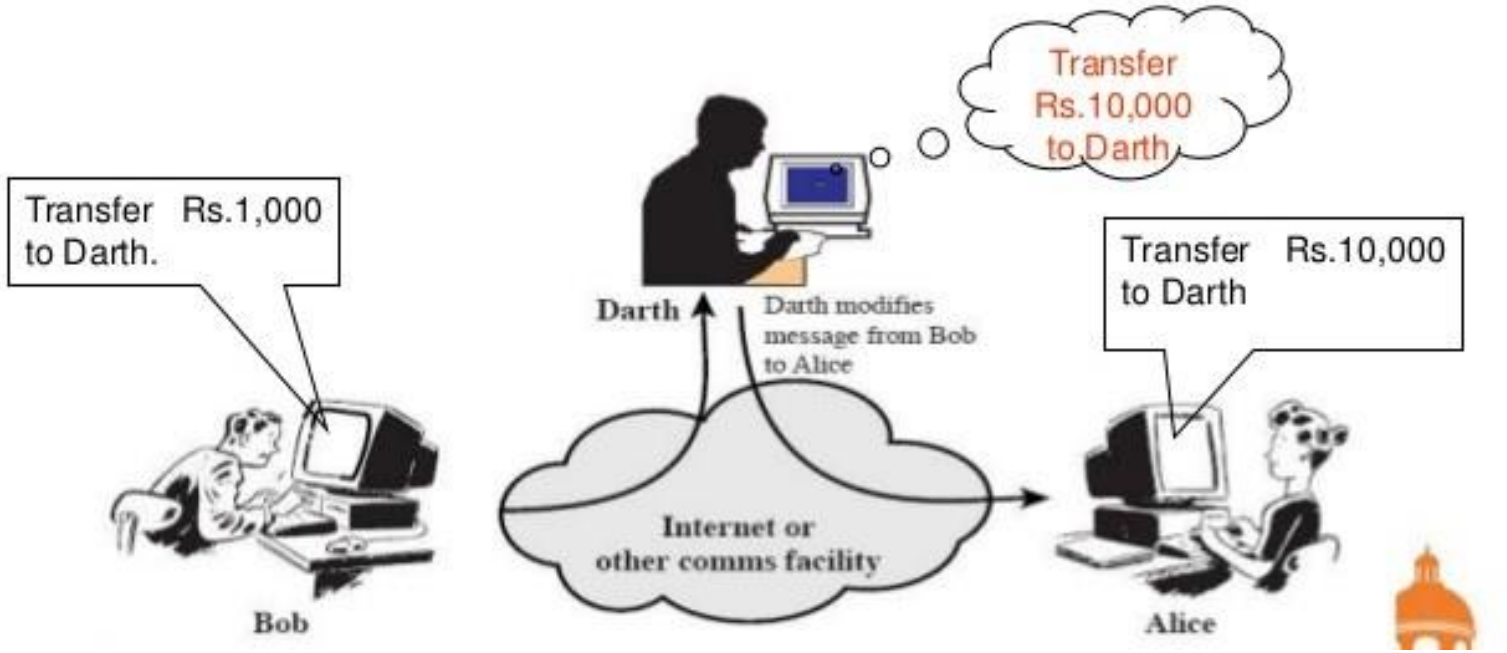
Các dạng tấn công

- Phát lại (replay)
  - Đối phương chặn bắt các đơn vị dữ liệu và phát lại chúng tạo lên các hiệu ứng không được ủy quyền



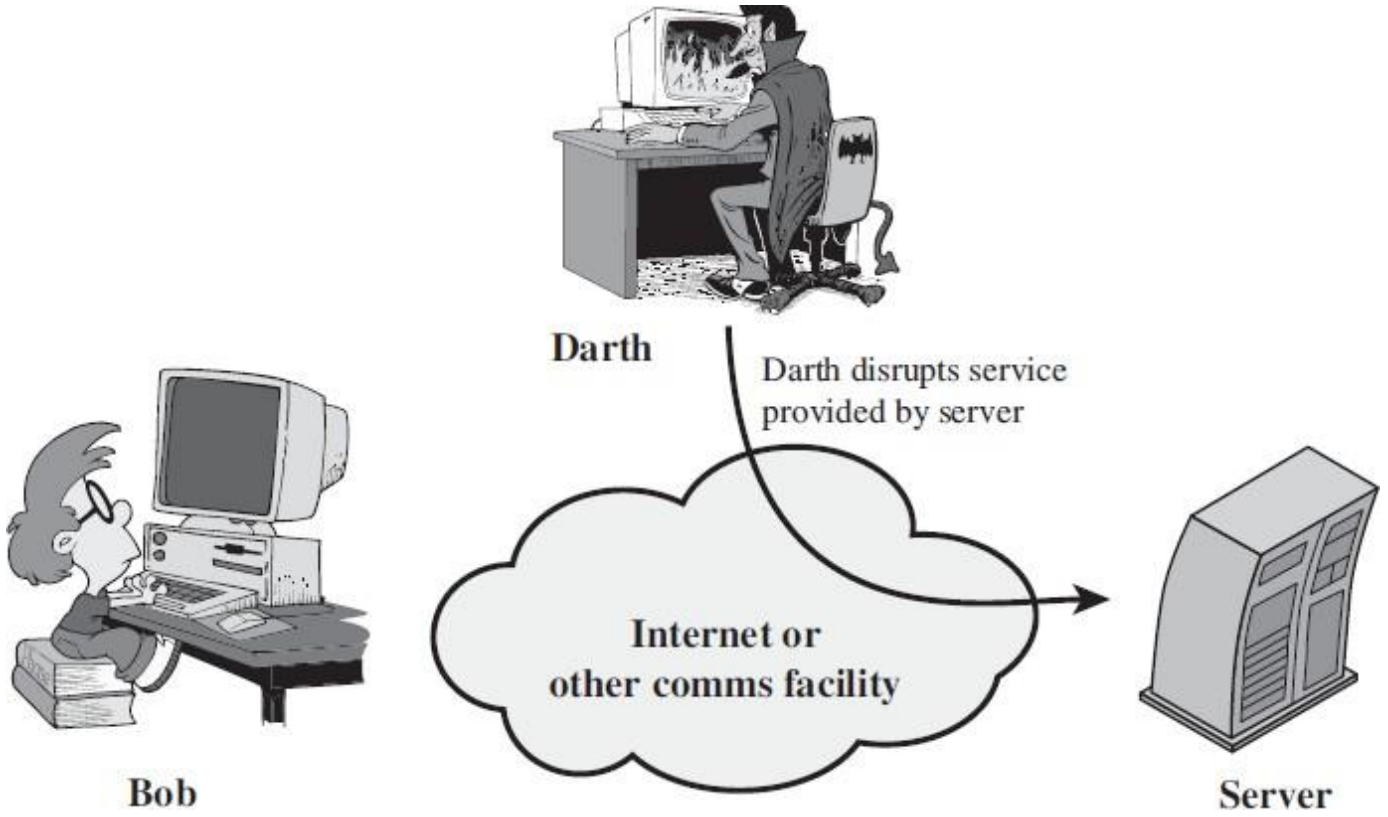
Các dạng tấn công

- Thay đổi thông điệp (modification of message)
  - Một phần của thông điệp hợp pháp bị sửa đổi, bị làm chậm, hoặc bị sắp xếp lại tạo ra các hiệu ứng không được ủy quyền



Các dạng tấn công

- Phủ nhận dịch vụ (denial of service)
  - dạng tấn công đưa đến việc cấm hoặc ngăn chặn khả năng sử dụng các dịch vụ, các khả năng truyền thông

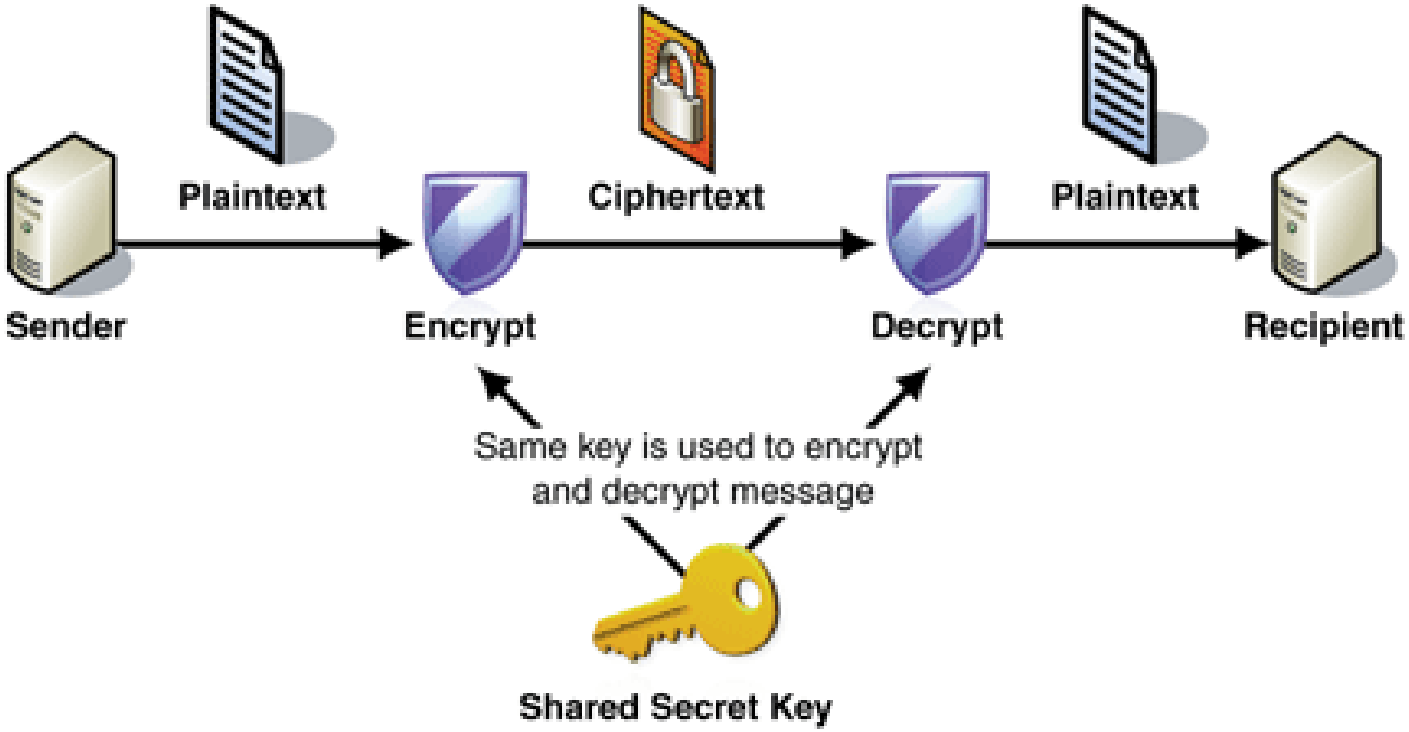


Các đặc trưng kỹ thuật của an ninh mạng

- Tính bảo mật, riêng tư (Confidentiality)
- Tính toàn vẹn (Integrity)
- Tính khả dụng (Availability)
- Xác thực (Authentication)
- Kiểm soát truy cập (Access control)
- Chống phủ định (Nonreputation)

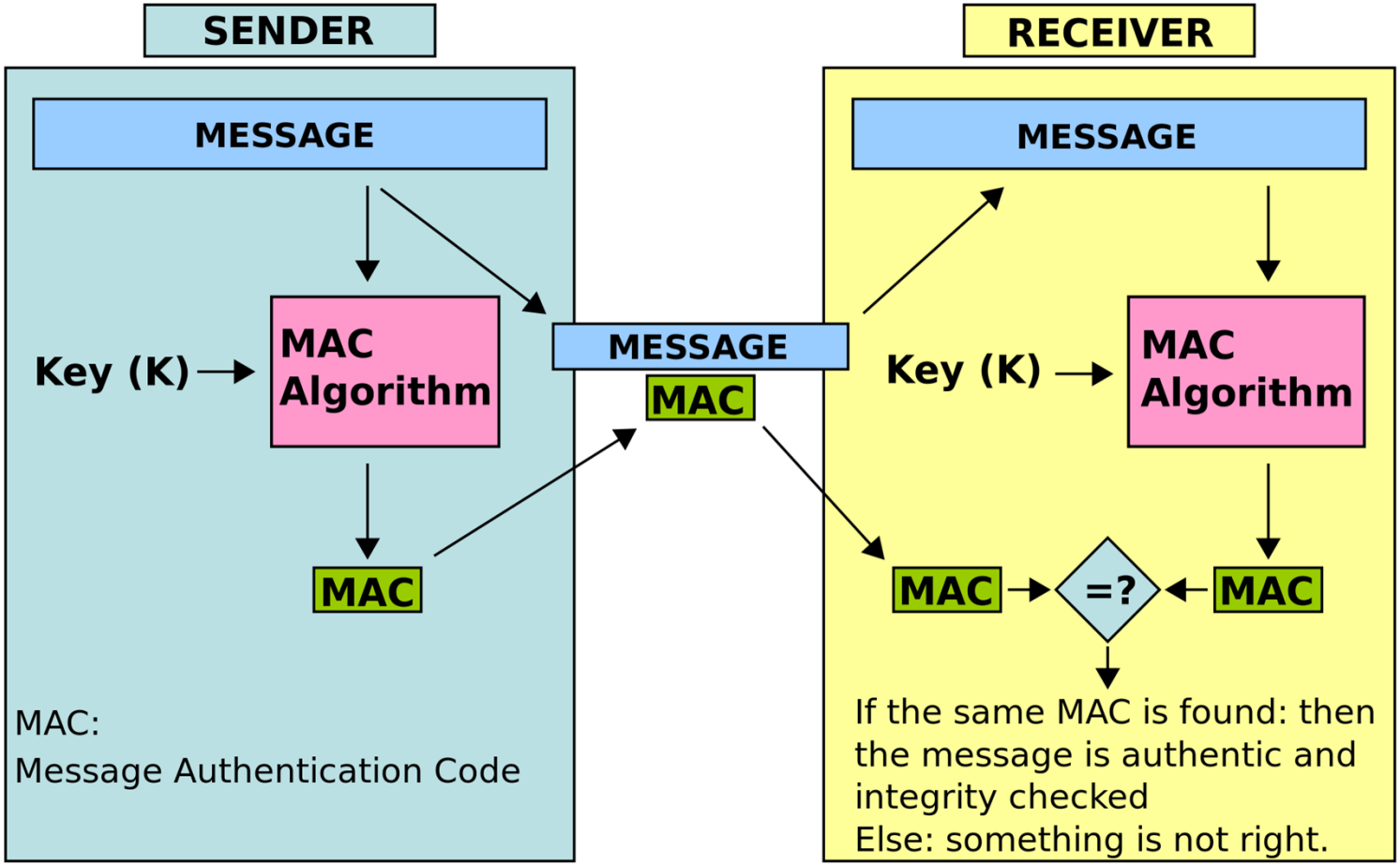
Các đặc trưng kỹ thuật của an ninh mạng

- Tính bảo mật, riêng tư (**C**onfidentiality)
  - Khoá mật mã, bảo mật vật lý
  - Thiết lập đường truyền ảo (e.g., VPN)
  - Bảo vệ luồng thông tin khỏi các thao tác phân tích luồng thông tin



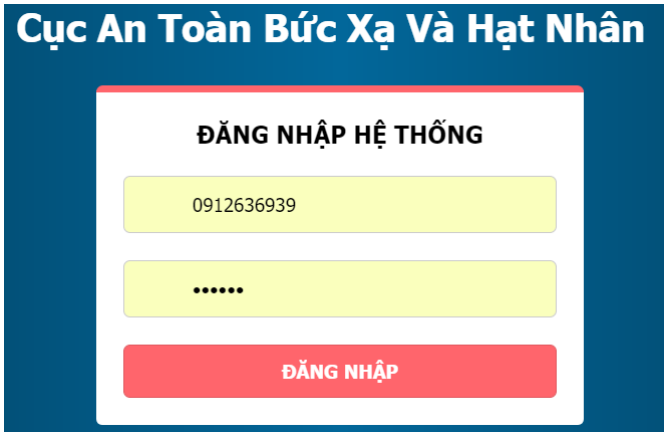
Các đặc trưng kỹ thuật của an ninh mạng

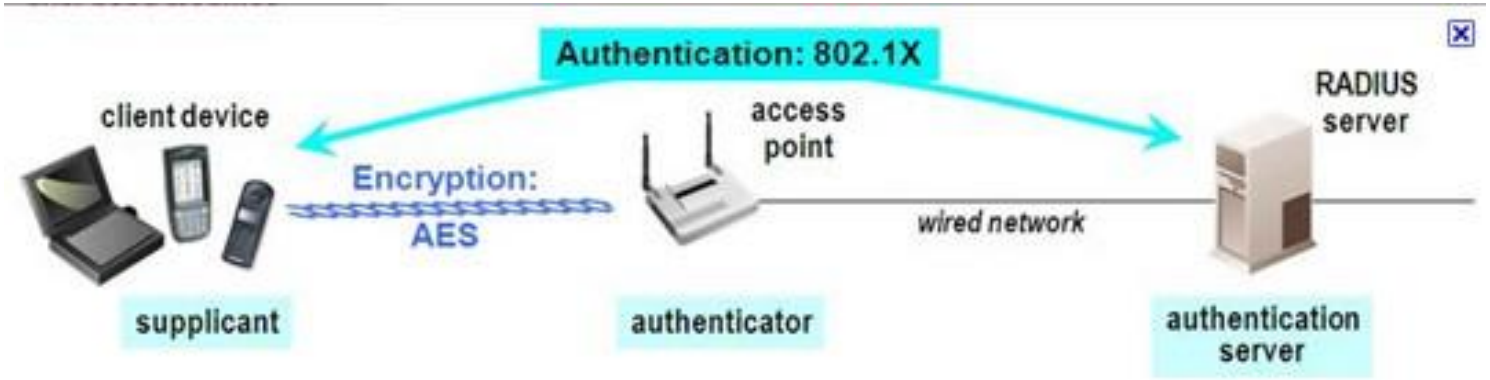
- Tính toàn vẹn (Integrity)



Các đặc trưng kỹ thuật của an ninh mạng

- Xác thực (**A**uthentication)





Các đặc trưng kỹ thuật của an ninh mạng

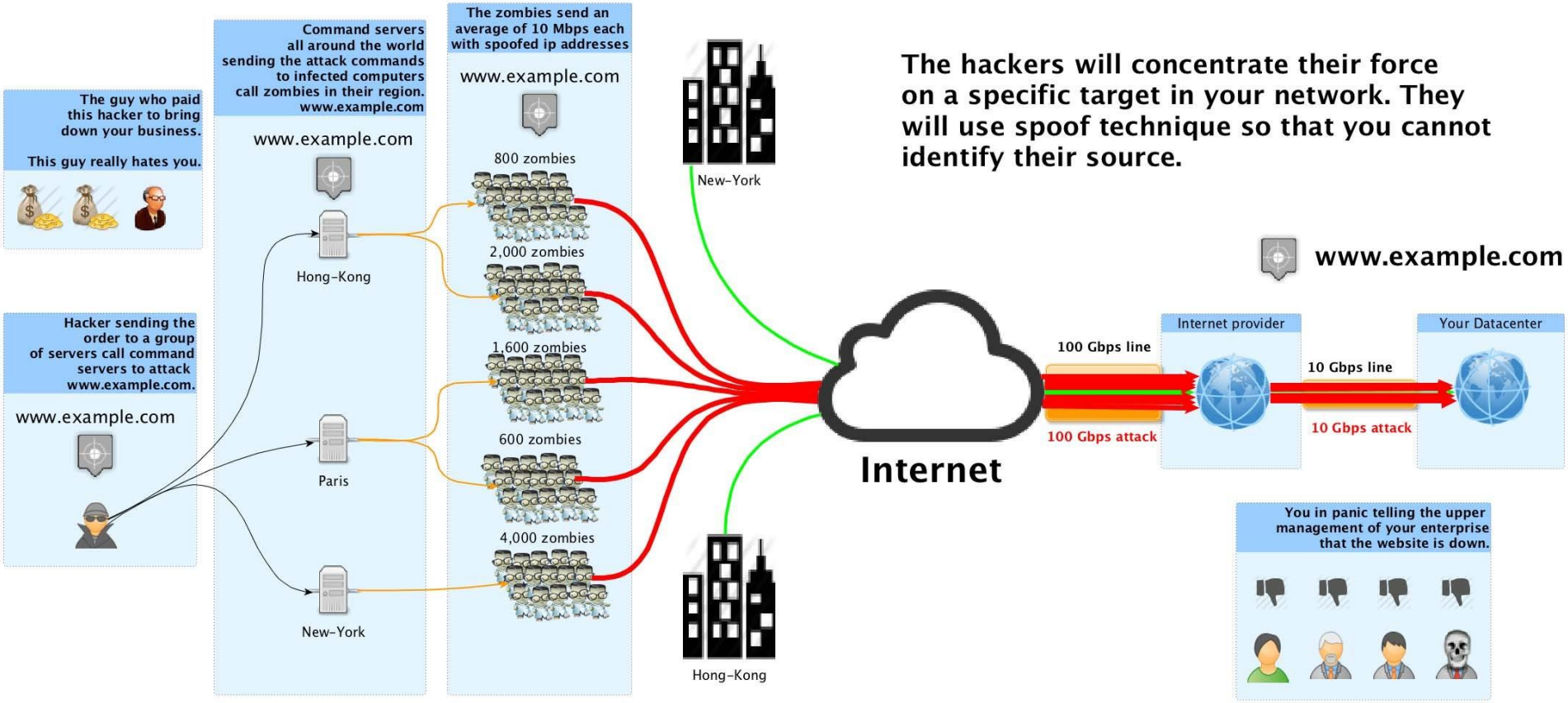
- Tính khả dụng (Availability)
- Kiểm soát truy cập (Access control)
- Chống phủ định (Nonreputation)

Lỗ hổng bảo mật và điểm yếu của mạng

- Lỗ hổng bảo mật
  - là tất cả những đặc tính của phần mềm hay phần cứng cho phép người dùng không hợp lệ có thể truy cập hoặc tăng quyền mà không cần xác thực
- Lỗ hổng loại C:
  - Cho phép thực hiện các phương thức tấn công theo kiểu từ chối dịch vụ DoS
  - Mức nguy hiểm thấp, chỉ ảnh hưởng chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống, không phá hỏng dữ liệu hoặc chiếm quyền truy nhập
  - Ví dụ:
    - Bandwidth/Throughput Attacks
    - Protocol Attacks
    - Software Vulnerability Attacks

Lỗ hổng bảo mật và điểm yếu của mạng

- Lỗ hổng loại C
  - DDoS Attacks

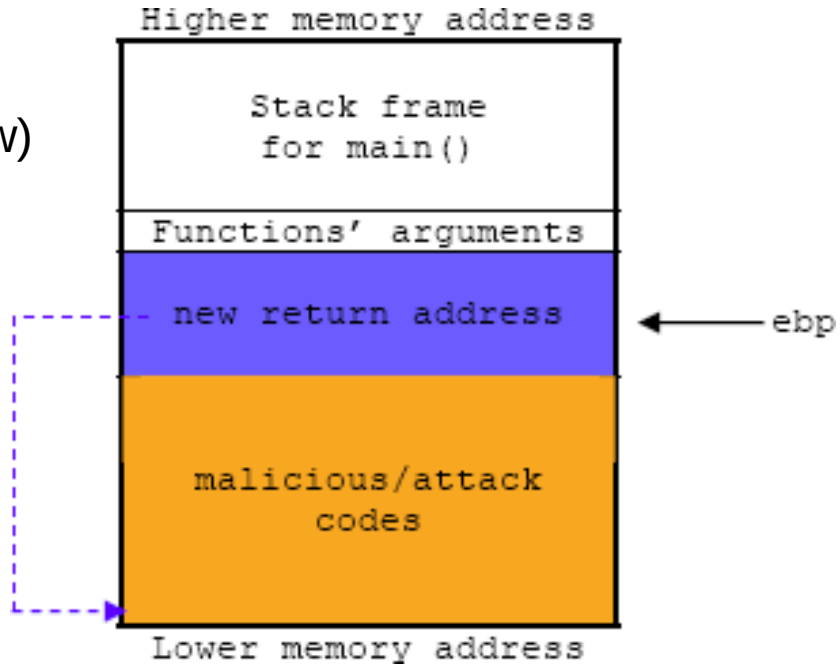


Lỗ hổng bảo mật và điểm yếu của mạng

- Lổ hổng loại B:
  - Cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ
  - Mức độ nguy hiểm trung bình, có thể dẫn đến lộ thông tin cần bảo mật

Lỗ hổng bảo mật và điểm yếu của mạng

- Lỗ hổng loại A:
  - Cho phép user có thể truy nhập bất hợp pháp vào hệ thống
  - Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống
  - Ví dụ: Lỗi tràn đệm:
    - Tràn stack (stack-based)
    - Tràn heap (heap-based)
    - Tràn số nguyên (integer overflow)



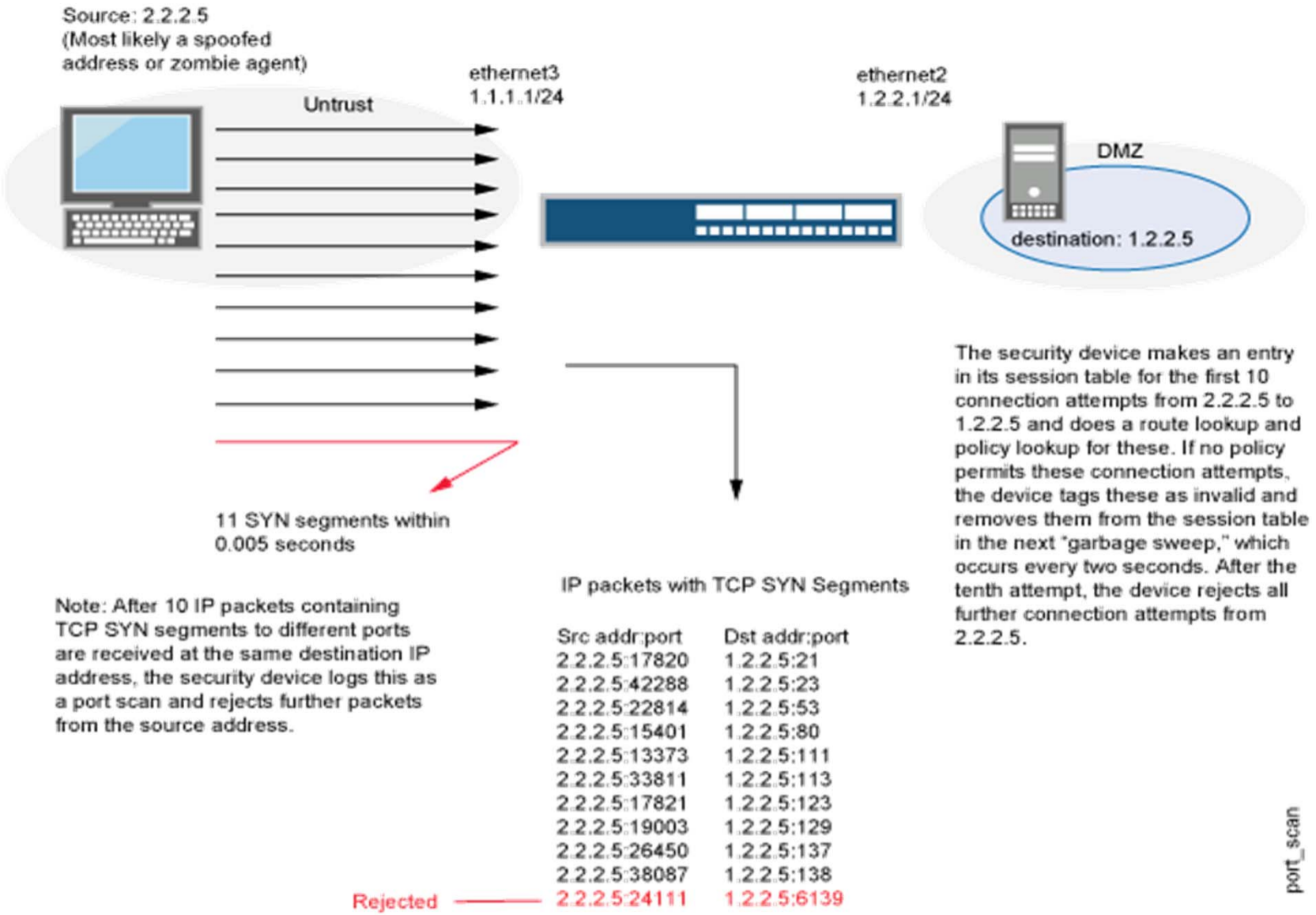
Các biện pháp phát hiện hệ thống bị tấn công

- Kiểm tra các dấu hiệu hệ thống bị tấn công
- Kiểm tra các tài khoản người dùng lạ
- Kiểm tra sự xuất hiện các tập tin lạ
- Kiểm tra thời gian thay đổi trên hệ thống
- Kiểm tra hiệu năng của hệ thống
- Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp

Một số công cụ tấn công mạng phổ biến

- Quét mạng (Scanner)
  - Quét cổng
  - Quét điểm yếu
  - Khắc phục: Sử dụng các phần mềm phát hiện quét cổng, dùng firewall hoặc IDS. Cấu hình dịch vụ hợp lý và kịp thời vá lỗ
- Bẻ khoá (Password Cracker)
  - Attack: Password Guessing
  - Khắc phục: có chính sách bảo vệ mật khẩu đúng đắn
- Trojans
  - Khắc phục: Quét virus và cập nhật virus database thường xuyên
- Sniffer
- Kiểm thử các thâm nhập
  - Sử dụng chính các kỹ thuật do đối phương sử dụng để xác định cụ thể các lỗ hổng và mức độ ảnh hưởng của chúng

Understanding TCP Port Scanning



The security device makes an entry in its session table for the first 10 connection attempts from 2.2.2.5 to 1.2.2.5 and does a route lookup and policy lookup for these. If no policy permits these connection attempts, the device tags these as invalid and removes them from the session table in the next "garbage sweep," which occurs every two seconds. After the tenth attempt, the device rejects all further connection attempts from 2.2.2.5.

Note: After 10 IP packets containing TCP SYN segments to different ports are received at the same destination IP address, the security device logs this as a port scan and rejects further packets from the source address.

port_scan


?
Q
&
&
A
!