TRUYỀN VÀ BẢO MẬT THÔNG TIN

Bài 2:

An toàn và bảo mật thông tin

VŨ THỊ TRÀ

Nội dung

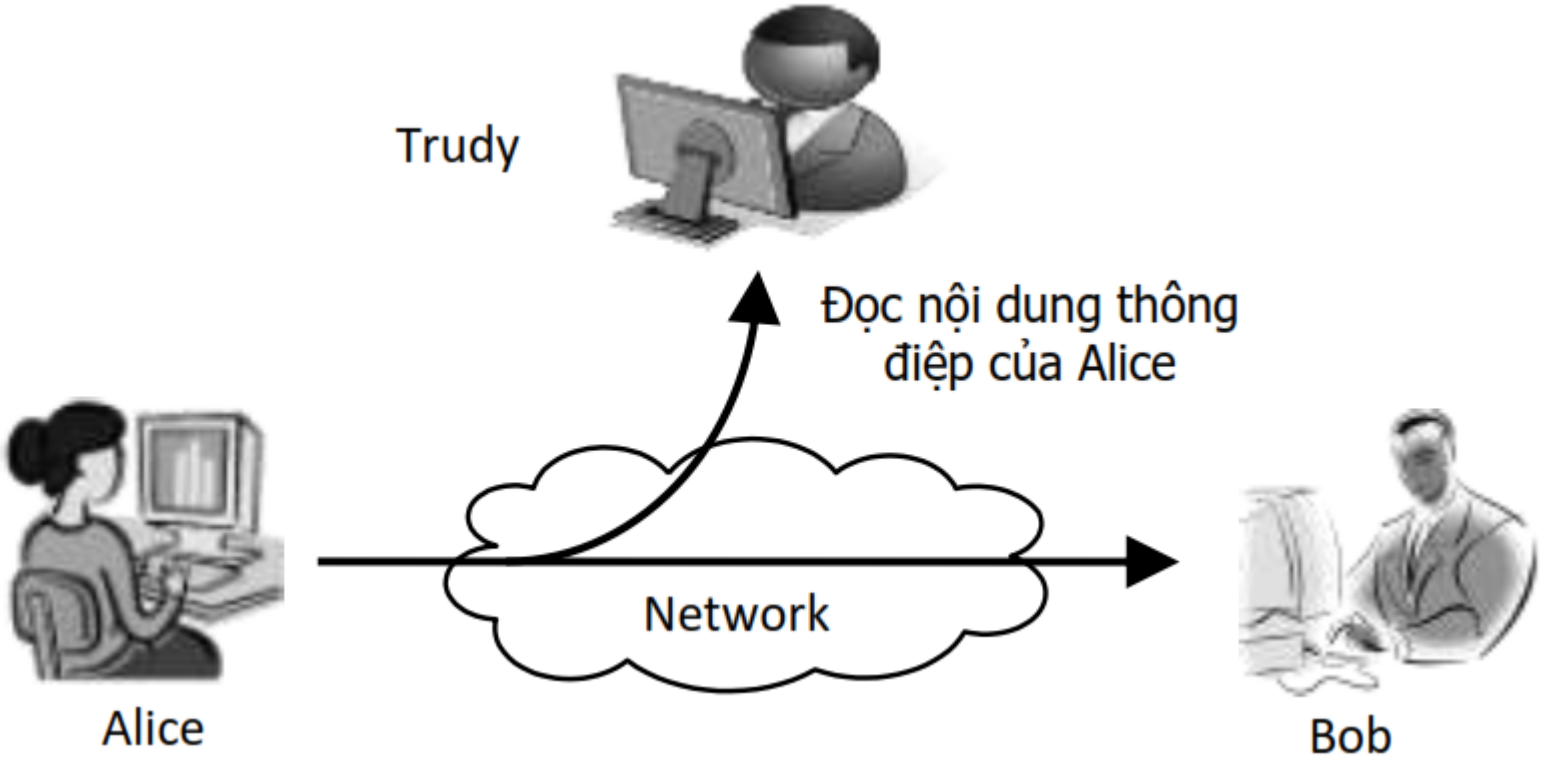
- Bảo mật thông tin
- Các loại hình tấn công
- Hệ truyền tin an toàn và bảo mật
- Mô hình bảo mật hệ truyền tin
- Vai trò của mật mã và các giao thức
- Mô hình chống xâm nhập hệ thống

Bảo mật thông tin (Information Security)

- **Khi chưa có máy tính**: thông tin được trao đổi hay cất giữ dưới
  - Đóng dấu và ký niêm phong
  - Dùng mật mã mã hóa thông điệp
  - Lưu trữ tài liệu mật trong các két sắt có khóa
- **CNTT và Internet:** xuất hiện nhu cầu
  - Bảo vệ thông tin trong quá trình truyền tin trên mạng (Network Security)
  - Bảo vệ hệ thống máy tính, mạng máy tính khỏi sự xâm nhập phá hoại từ bên ngoài (System Security)

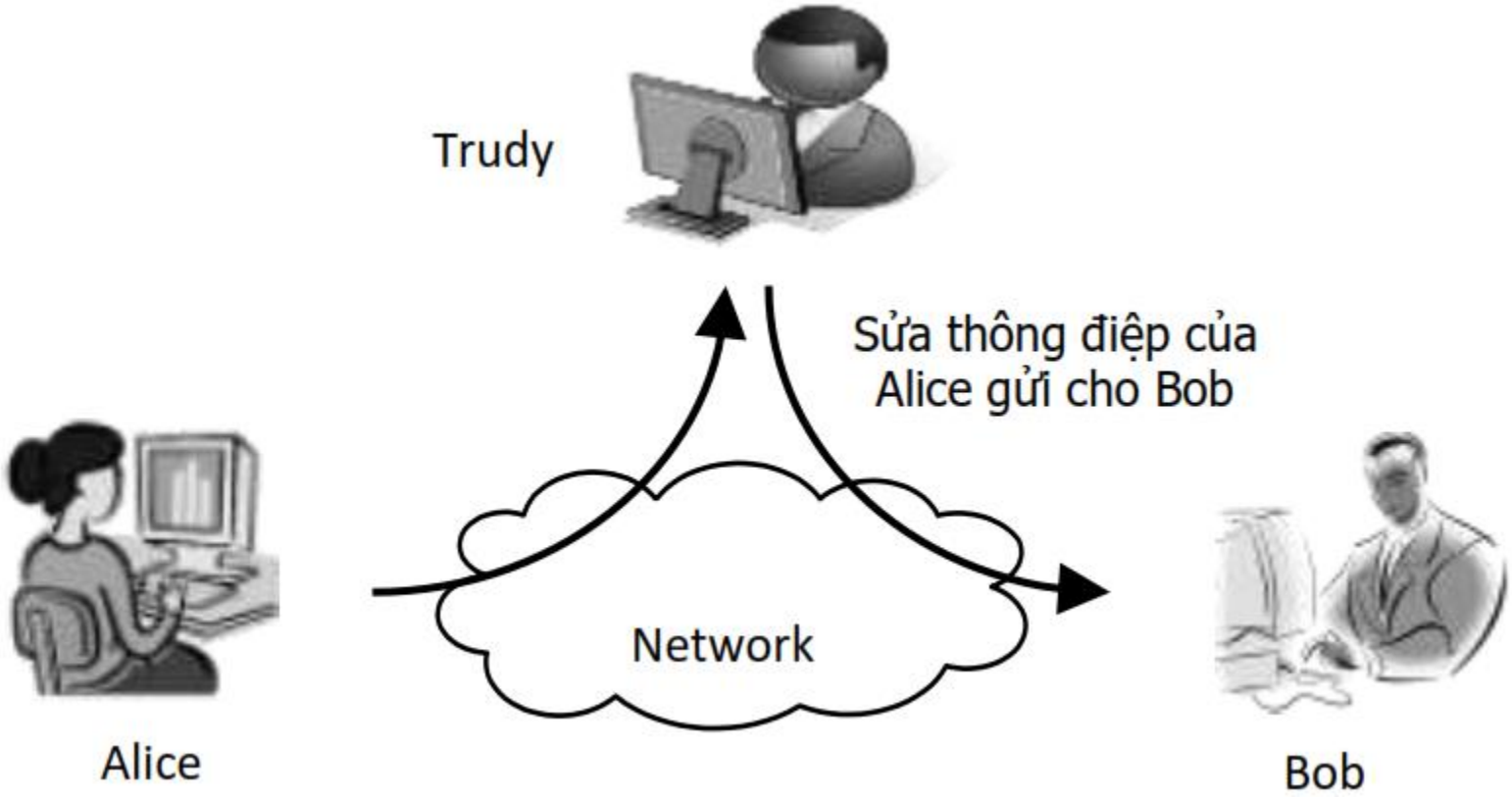
Các loại hình tấn công trên kênh truyền

1. **Xem trộm thông tin (*Release of Message Content*)**



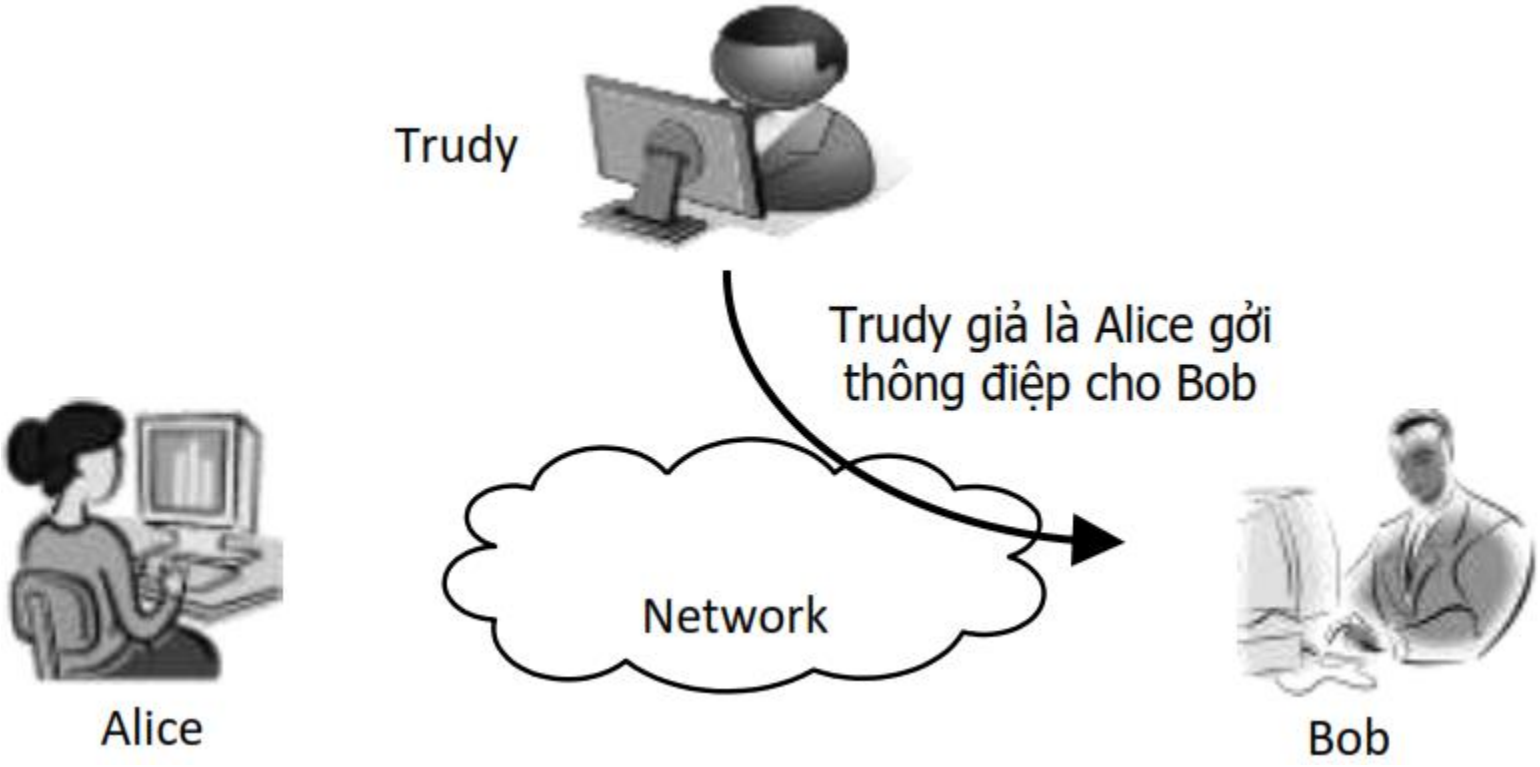
Các loại hình tấn công trên kênh truyền

2. Thay đổi thông điệp (*Modification of Message*)



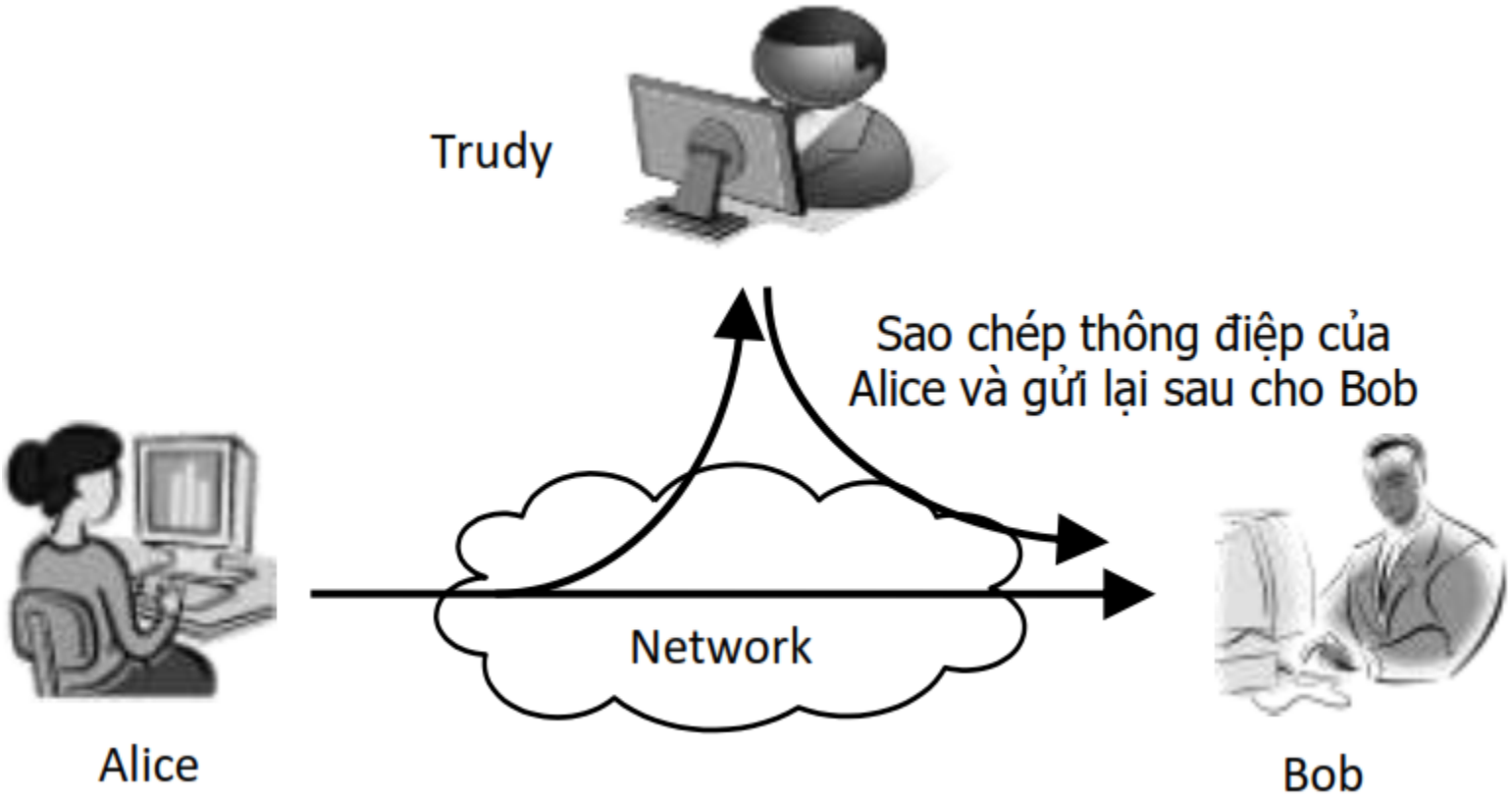
Các loại hình tấn công trên kênh truyền

3. Mạo danh (*Masquerade*)



Các loại hình tấn công trên kênh truyền

4. **Phát lại thông điệp (*Replay*)**

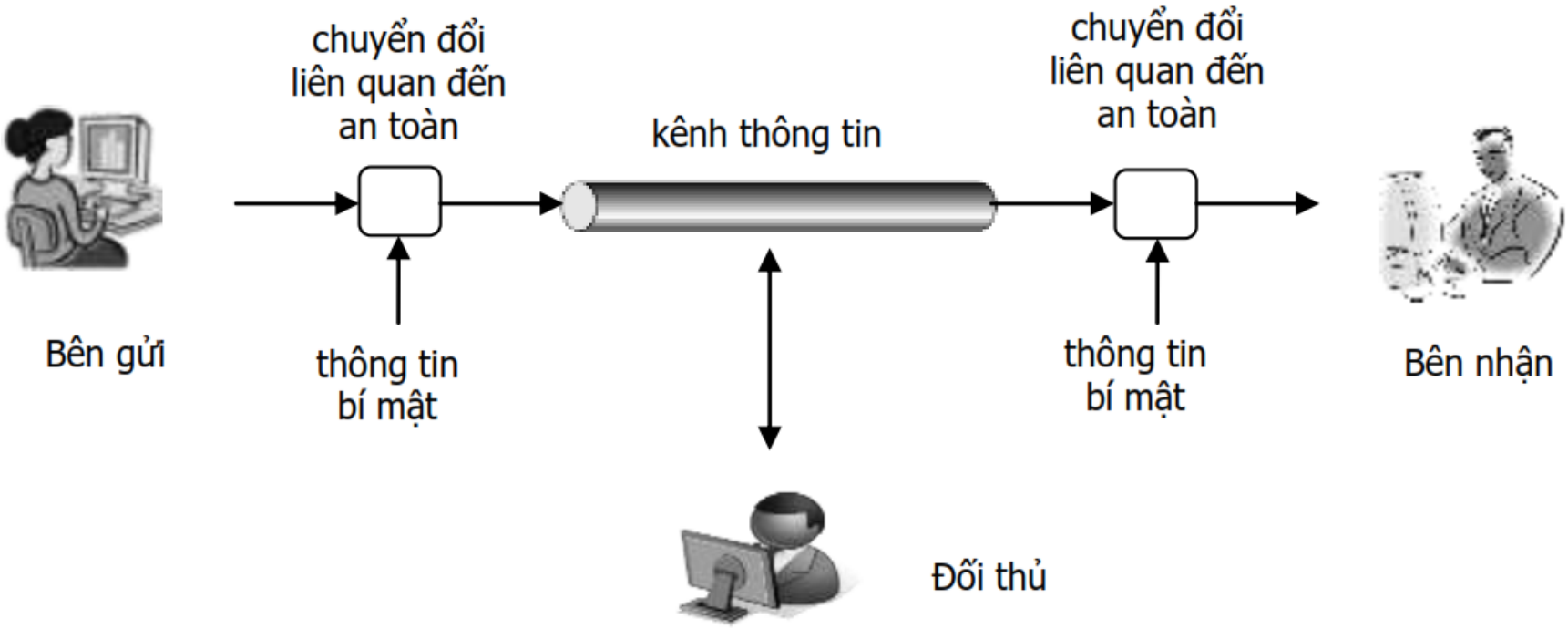


Hệ truyền tin an toàn và bảo mật

- **Tính bảo mật (*Confidentiality*)**
  - ✓ ngăn chặn trộm thông điệp
- **Tính chứng thực (*Authentication*)**
  - ✓ ngăn chặn việc sửa thông điệp, mạo danh, phát lại thông điệp
- **Tính không từ chối (*Non-repudiation*)**
  - ✓ Bod có cơ chế để xác định chính Alice là người gửi mà Alice không thể chối bỏ trách nhiệm

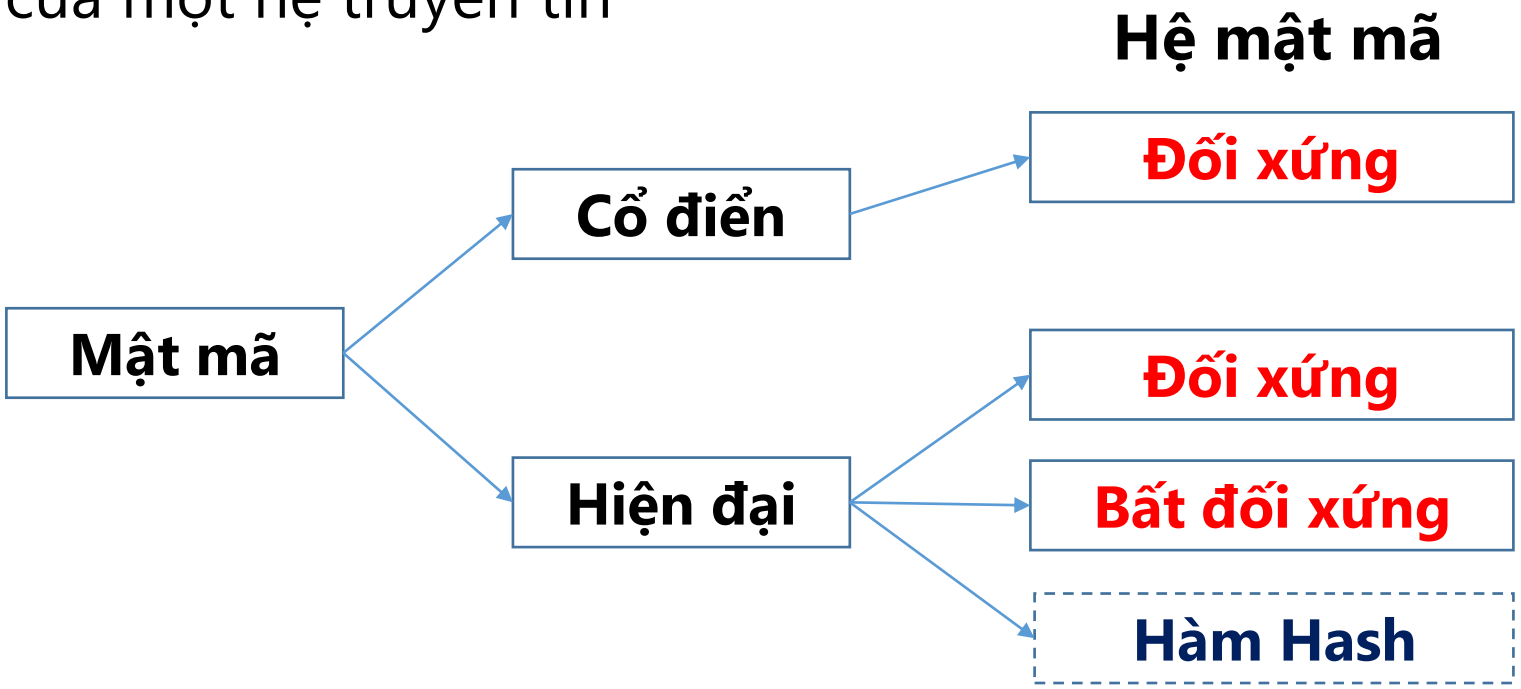
→ Ví dụ ?

Mô hình bảo mật truyền tin



Vai trò của mật mã trong hệ truyền tin

- **Mật mã *(cryptography)*** là công cụ cơ bản thiết yếu của bảo mật thông tin
- Mật mã đáp ứng được 3 nhu cầu về an toàn và bảo mật của một hệ truyền tin



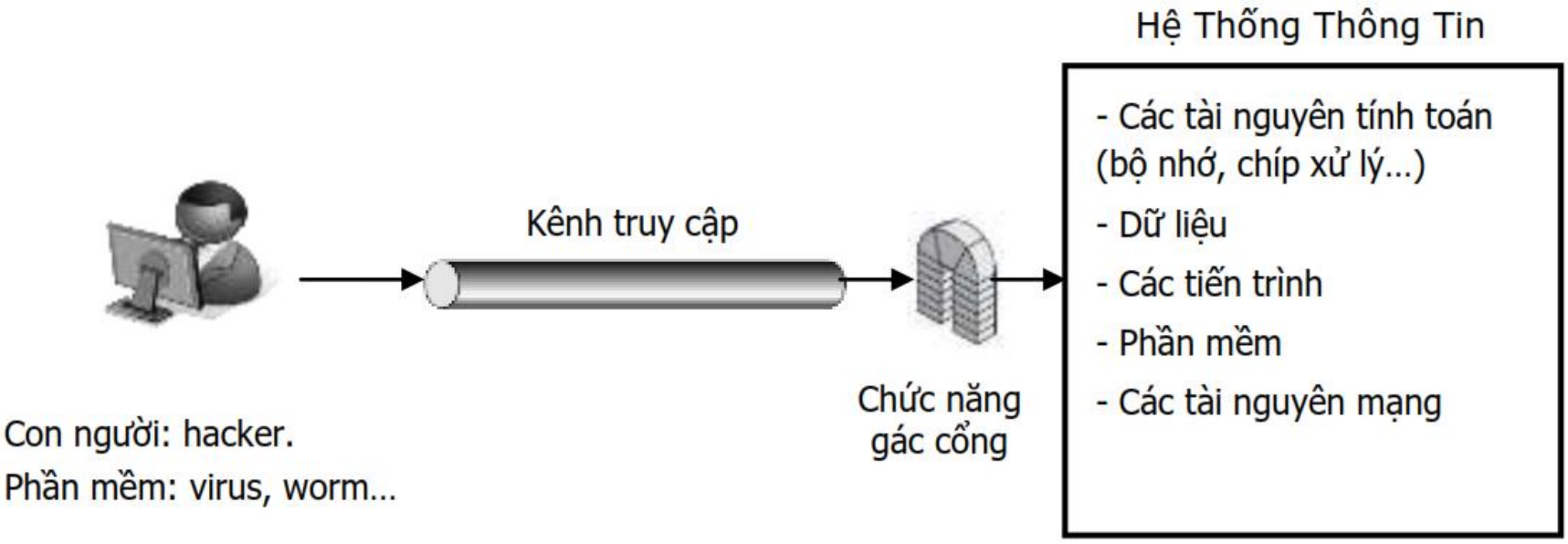
Các giao thức (protocol) bảo mật

- **Keberos**: là giao thức dùng để chứng thực dựa trên mã hóa đối xứng.
- **Chuẩn chứng thực X509**: dùng trong mã hóa khóa công khai.
- **Secure Socket Layer (SSL):** là giao thức bảo mật Web, được sử dụng phổ biến trong Web &thương mại điện tử.
- **PGP và S/MIME**: bảo mật thư điện tử.

Bảo vệ hệ thống khỏi sự xâm nhập

- **Kiểm soát truy cập (*Access Control*)**
  - ✓ **Chứng thực truy cập** (*Authentication*): xác nhận rằng đối tượng (con người hay chương trình máy tính) được cấp phép truy cập vào hệ thống
  - ✓ **Phân quyền** (*Authorization*): các hành động được phép thực hiện sau khi đã truy cập vào hệ thống
- **Kẻ phá hoại** tìm cách phá bỏ 2 cơ chế trên bằng cách:
  - ✓ **Dùng các đoạn mã phá hoại** (*Malware*): như virus, worm, trojan, backdoor…
  - ✓ **Thực hiện các hành vi xâm phạm** (*Intrusion*): việc thiết kế các phần mềm có nhiều lỗ hổng, dẫn đến các hacker lợi dụng để thực hiện những lệnh phá hoại.

Mô hình chống xâm nhập hệ thống



Q&A

1. Làm thế nào là hạn chế tối đa các lỗ hổng bảo mật?