

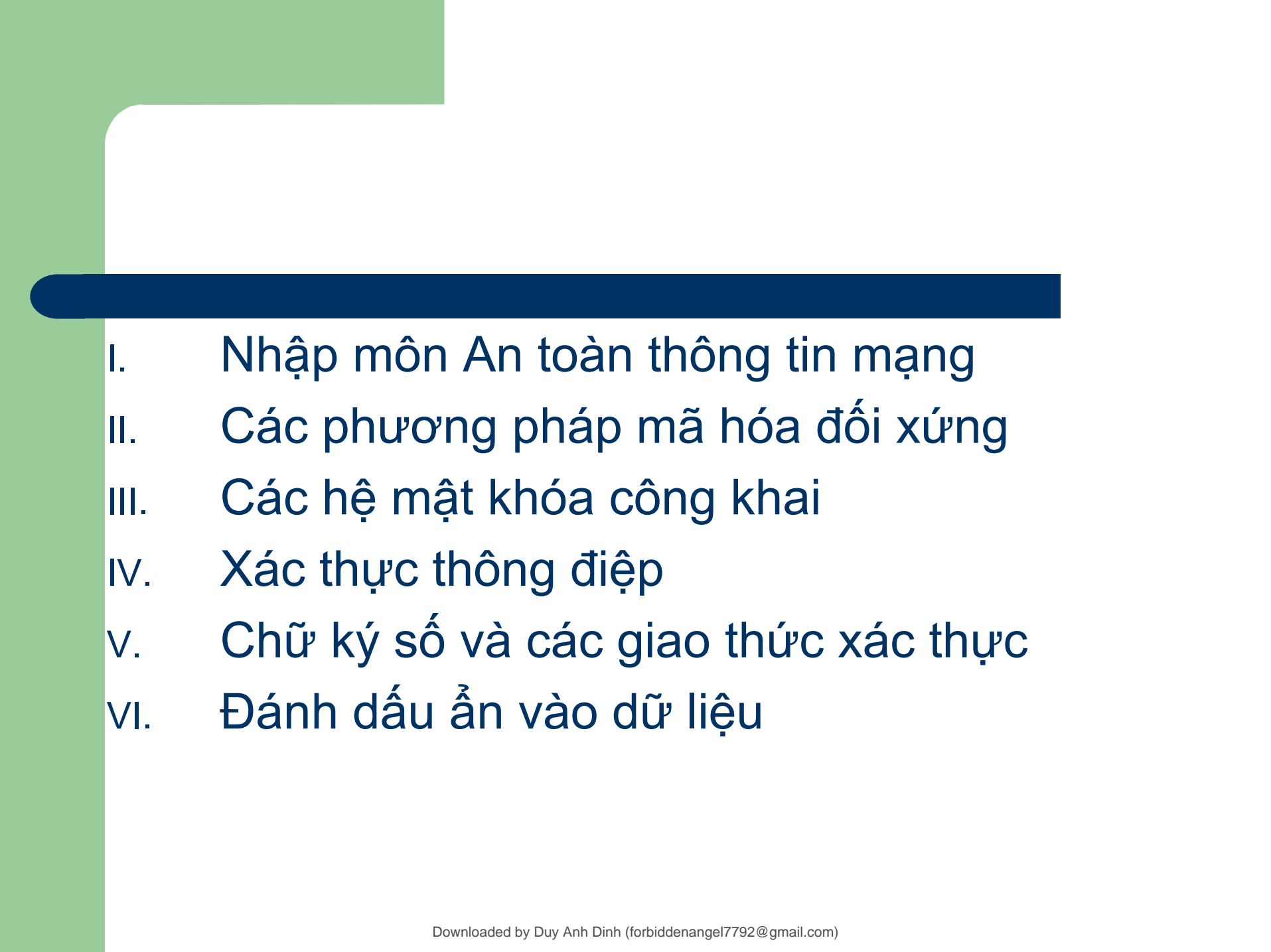


## An toàn và bảo mật thông tin tài liệu lý thuyết

Lý thuyết thông tin (Trường Đại học Bách khoa Hà Nội)

# An toàn và An ninh thông tin

Nguyễn Linh Giang.  
Bộ môn Truyền thông  
và Mạng máy tính.

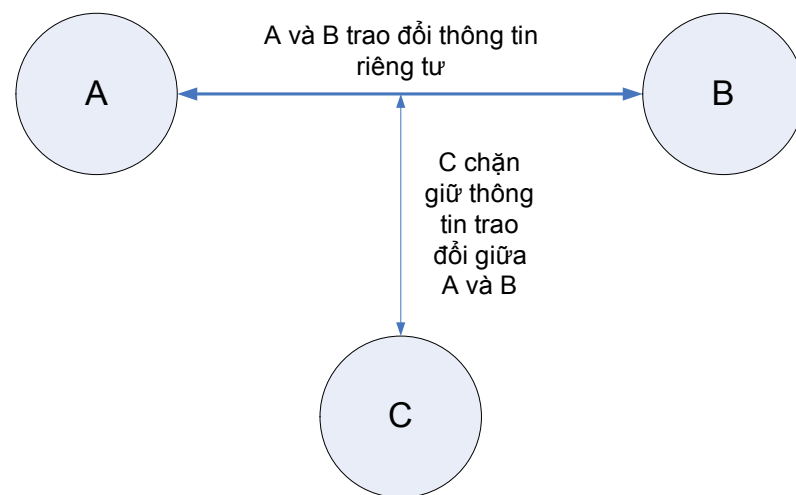
- 
- I. Nhập môn An toàn thông tin mạng
  - II. Các phương pháp mã hóa đối xứng
  - III. Các hệ mật khóa công khai
  - IV. Xác thực thông điệp
  - V. Chữ ký số và các giao thức xác thực
  - VI. Đánh dấu ẩn vào dữ liệu

# Chương I. Nhập môn

1. Nhập môn
2. Các dịch vụ, cơ chế an toàn an ninh thông tin và các dạng tấn công vào hệ thống mạng
3. Các dạng tấn công
4. Các dịch vụ an toàn an ninh
5. Các mô hình an toàn an ninh mạng

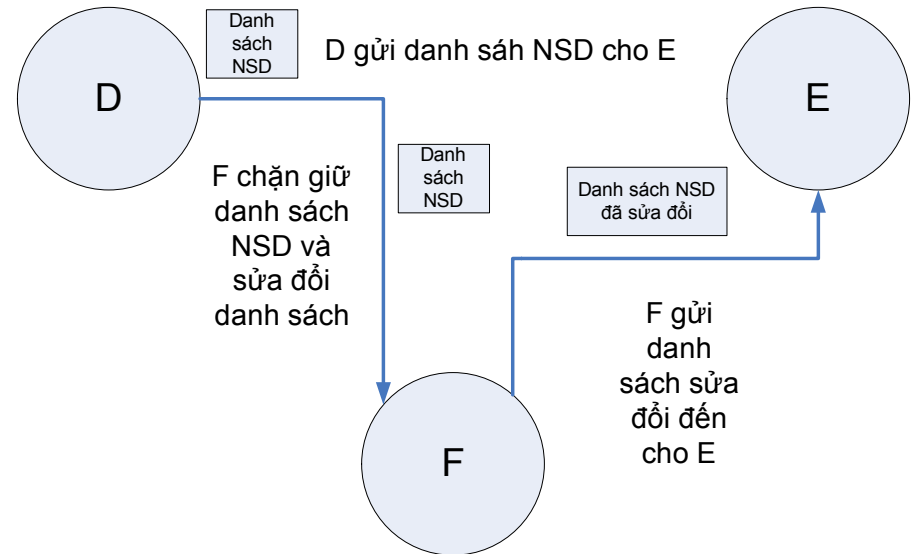
# Nhập môn

- Một số ví dụ về vấn đề bảo vệ an toàn thông tin:
  - Truyền file



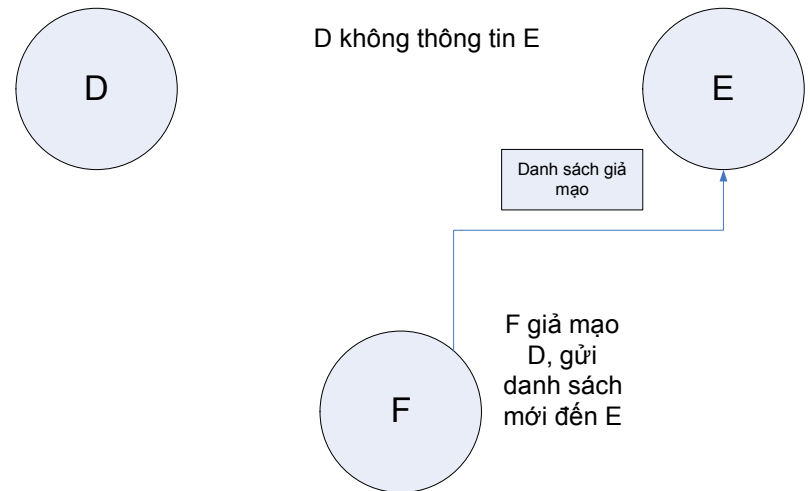
# Nhập môn

- Trao đổi thông điệp:



# Nhập môn

- Giả mạo:



# Nhập môn

- Sự phức tạp trong bài toán Bảo mật liên mạng:
  - Không tồn tại phương pháp thích hợp cho mọi trường hợp.
  - Các cơ chế bảo mật luôn đi đôi với các biện pháp đối phó.
  - Lựa chọn những giải pháp thích hợp với từng ngữ cảnh sử dụng.



# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Ba khía cạnh an toàn an ninh thông tin:
  - Tấn công vào an ninh thông tin
  - Các cơ chế an toàn an ninh
  - Các dịch vụ an toàn an ninh thông tin

# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Phân loại các dịch vụ an toàn an ninh:
  - Bảo mật riêng tư ( confidentiality )
  - Xác thực ( authentication )
  - Toàn vẹn thông tin ( integrity )
  - Chống phủ định ( nonrepudiation )
  - Kiểm soát truy cập ( access control )
  - Tính sẵn sàng ( availability )

# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Các cơ chế an toàn an ninh
  - Không tồn tại một cơ chế duy nhất;
  - Sử dụng **các kỹ thuật mật mã.**

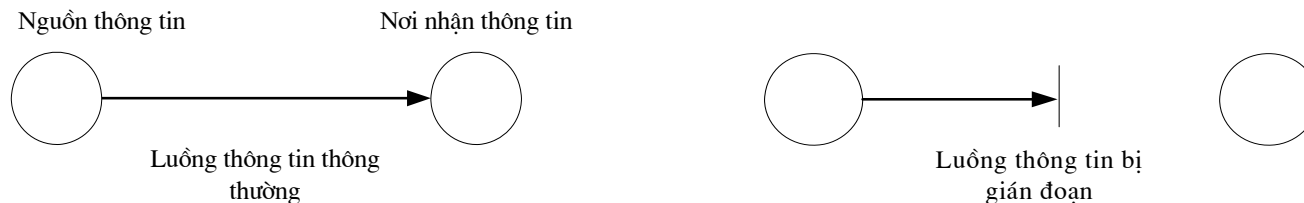
# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Các dạng tấn công.
  - Truy nhập thông tin bất hợp pháp;
  - Sửa đổi thông tin bất hợp pháp;
  - v.v và v.v ...

# Các dạng tấn công vào hệ thống

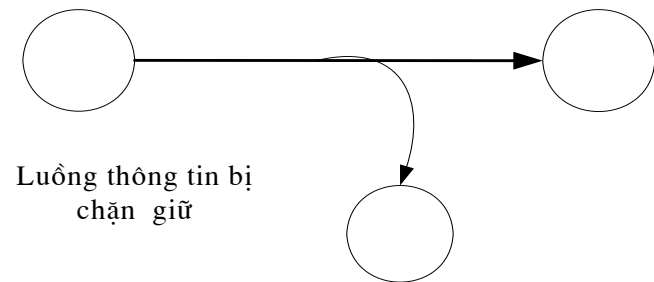
- Các dạng tấn công vào hệ thống máy tính và mạng:



- Gián đoạn truyền tin ( interruption ):

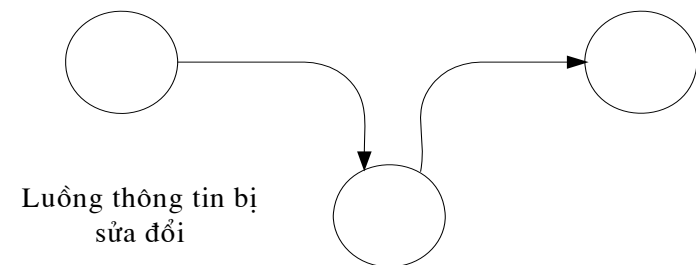
# Các dạng tấn công vào hệ thống

- Chặn giữ thông tin (interception):



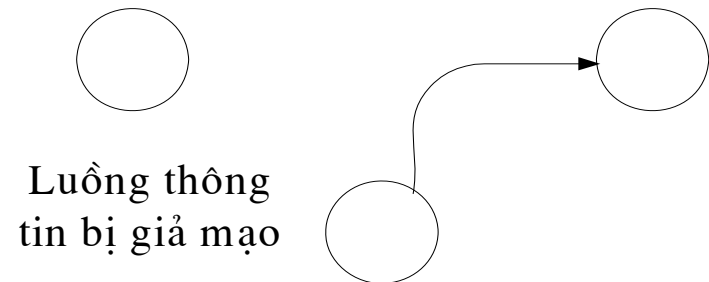
# Các dạng tấn công vào hệ thống

- Sửa đổi thông tin ( modification ):



# Các dạng tấn công vào hệ thống

- Làm giả thông tin ( fabrication ).

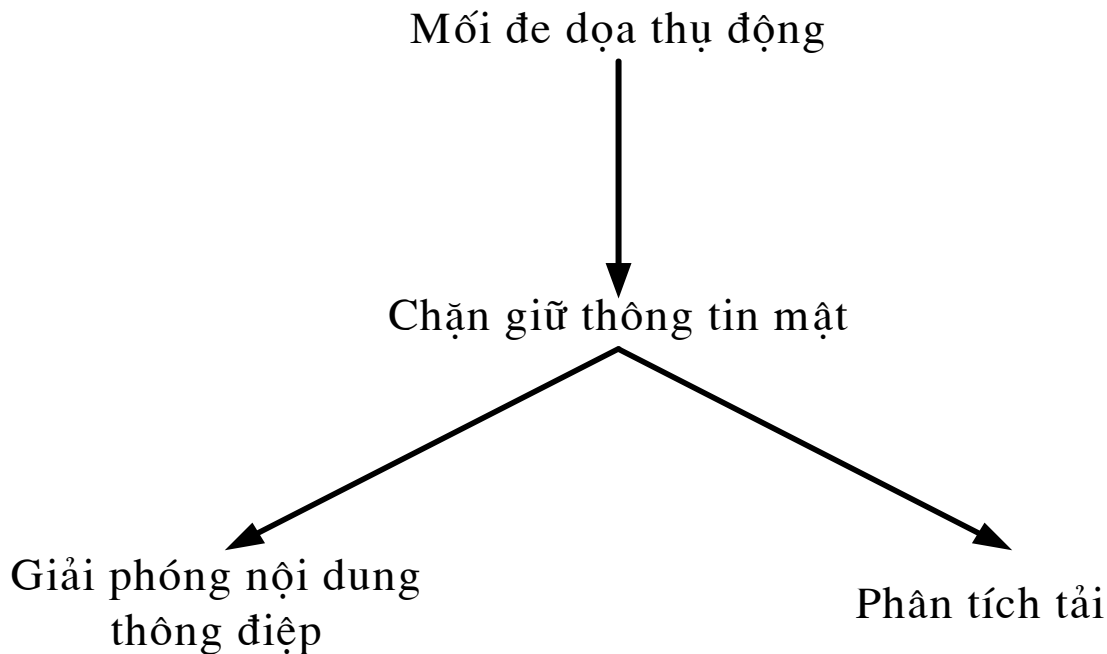




# Các dạng tấn công vào hệ thống

## Tấn công thụ động

- Tấn công thụ động



# Các dạng tấn công vào hệ thống

## Tấn công thụ động

- 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.

# Các dạng tấn công vào hệ thống

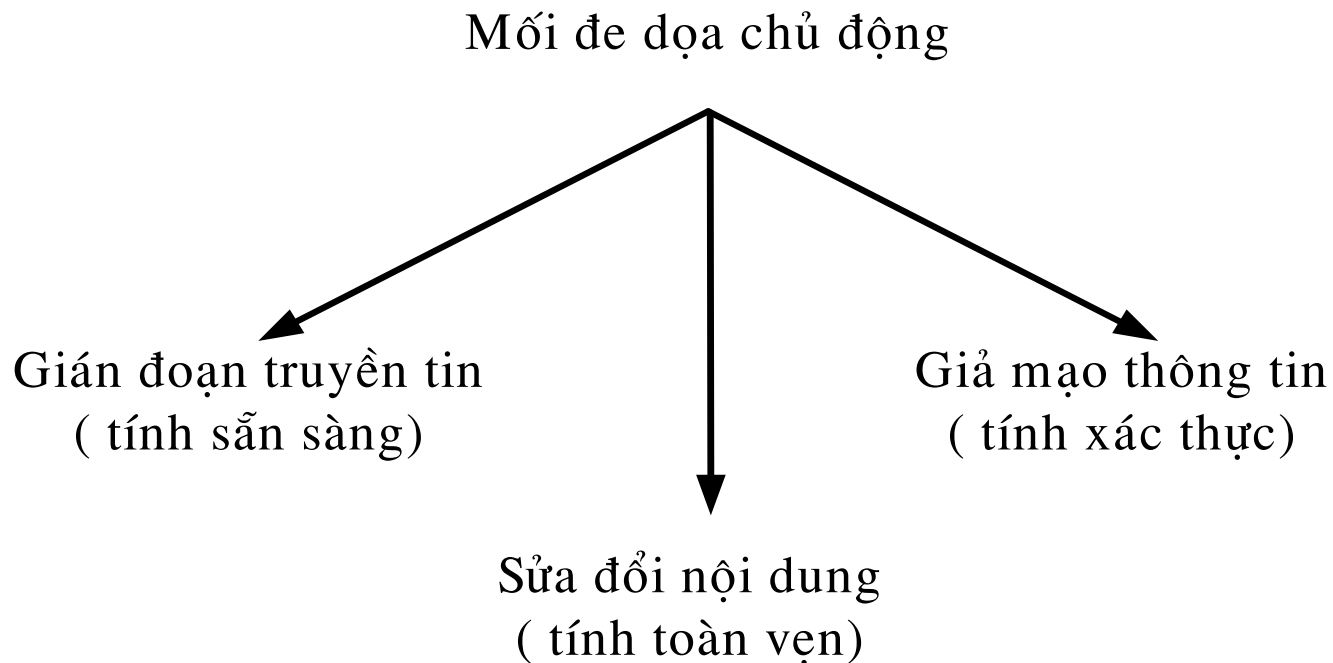
## Tấn công thụ động

- 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.

# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- Dạng tấn công chủ động.



# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- Giả danh
- Phát lại
- Thay đổi nội dung thông điệp
- Từ chối dịch vụ

# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- 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 trể.

# Các dịch vụ an toàn an ninh

- Đảm bảo tính riêng tư
  - Đảm bảo tính riêng tư của thông tin: Bảo vệ dữ liệu được truyền tải khỏi các tấn công thụ động.
- Đảm bảo tính xác thực
  - Dịch vụ đảm bảo tính xác thực:
    - Khẳng định các bên tham gia vào quá trình truyền tin được xác thực và đáng tin cậy.

# Các dịch vụ an toàn an ninh

- Đảm bảo tính sẵn sàng
  - Dịch vụ đảm bảo tính sẵn sàng phải:
    - Ngăn chặn các ảnh hưởng lên thông tin trong hệ thống;
    - Phục hồi khả năng phục vụ của các phần tử hệ thống trong thời gian nhanh nhất.
- Đảm bảo tính toàn vẹn
  - Đảm bảo tính toàn vẹn cũng có thể áp dụng cho luồng thông điệp, một thông điệp hoặc một số trường được lựa chọn của thông điệp.



# Các dịch vụ an toàn an ninh

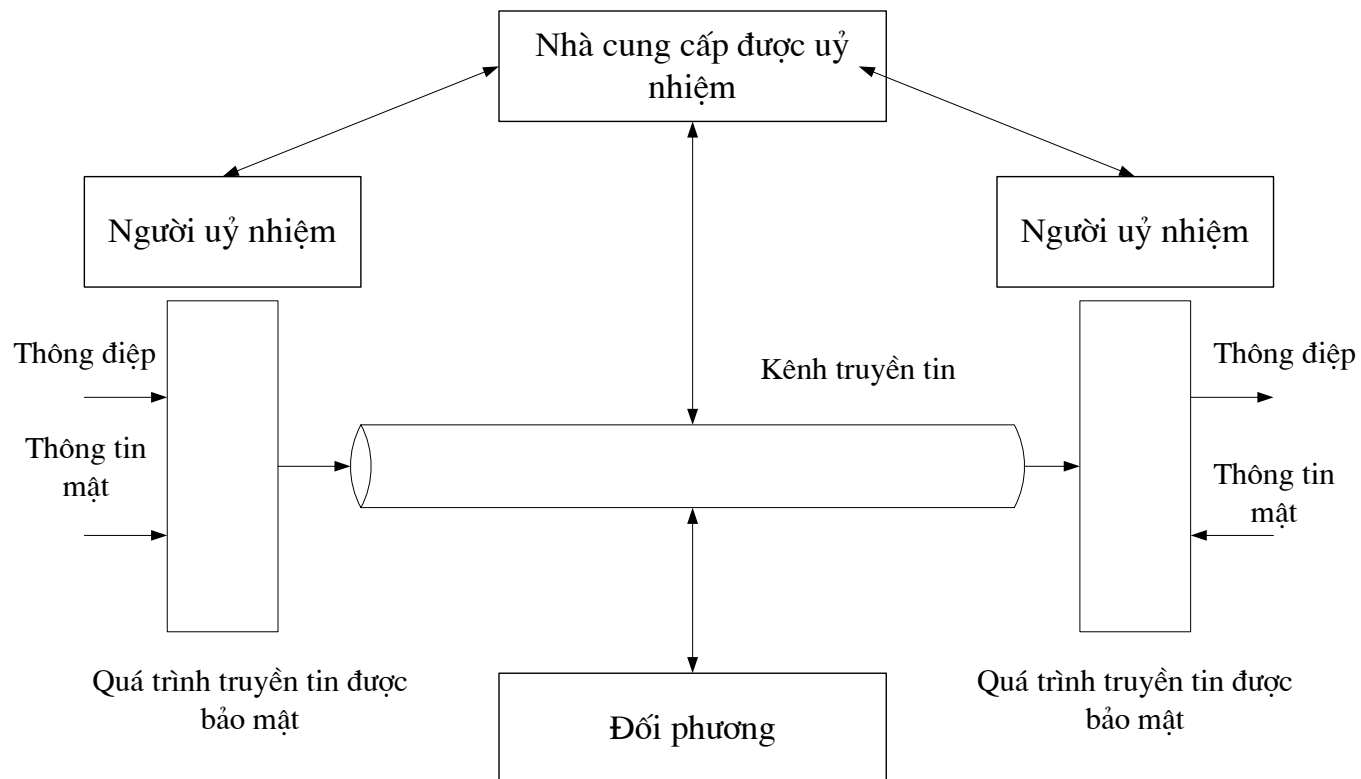
- Dịch vụ chống phủ nhận
  - Dịch vụ chống phủ nhận ngăn chặn người nhận và người gửi từ chối thông điệp được truyền tải.
- Dịch vụ kiểm soát truy nhập.
  - Dịch vụ kiểm soát truy nhập cung cấp khả năng giới hạn và kiểm soát các truy nhập tới các máy chủ hoặc các ứng dụng thông qua đường truyền tin

# Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn mạng
  - Bài toán an toàn an ninh thông tin mạng nảy sinh khi:
    - Cần thiết phải bảo vệ quá trình truyền tin khỏi các hành động truy cập trái phép;
    - Đảm bảo tính riêng tư và tính toàn vẹn;
    - Đảm bảo tính xác thực; ..vv.

© 2015 Pearson Education, Inc. or its affiliate(s). All rights reserved. Pearson Education, Inc., publishing as Pearson Benjamin Cummings, 101 Philip Drive, Assinippi Park, New York, NY 10986-1997

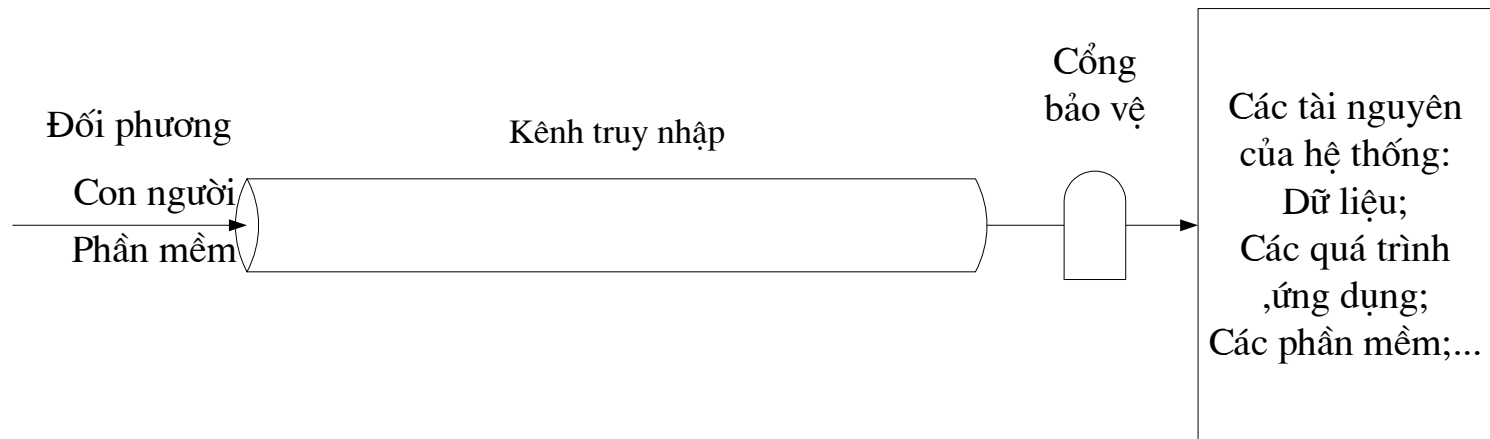
## – Mô hình truyền tin an toàn



# Các mô hình an toàn mạng và hệ thống

- Mô hình an toàn an ninh hệ thống
  - Truy nhập của các hacker;
  - Các lỗ hổng an ninh hệ thống;
  - Các tiến trình ngoại lai

# Các mô hình an toàn mạng và hệ thống



Mô hình An ninh truy nhập hệ thống Mạng