AN TOÀN THÔNG TIN

Giảng viên: Th.s Nguyễn Thu Hiền

Email: nthien@uneti.edu.vn

Tổ Mạng Máy Tính và Công Nghệ Đa Phương Tiện

Khoa Công nghệ Thông tin

GIỚI THIỆU MÔN HỌC

- Học phần trang bị cho sinh viên kiến thức cơ bản về lĩnh vực an toàn thông tin, an toàn mạng.
  - Nguyên lý hoạt động của các giải thuật mã hóa đối xứng hiện đại và sơ đồ mã hóa khối tổng quát Feistel.
  - Các phương thức mã hóa liên hợp nhiều khối và cách thức chung quản lý các khóa bí mật.
  - Các ứng dụng bảo mật, chữ ký số, và trao đổi khóa bí mật của mật mã khóa công khai.
  - Các cơ chế xác thực thông báo và tác giả của thông báo.
  - Các ứng dụng của các phương pháp mật mã, xác thực và chữ ký số trong lĩnh vực an toàn mạng.

MỤC TIÊU MÔN HỌC

- Kiến thức:
  - Hiểu được các khái niệm cơ bản về an toàn truyền thông trên mạng Internet.
  - Nắm được phương pháp mã hóa đối xứng và mã hóa khóa công khai, các kỹ thuật xác thực và chữ ký số.
  - Biết một số phương thức chủ yếu đảm bảo an toàn thư điện tử, cơ chế an toàn mạng ở mức IP và an toàn cho các giao tác trên Web.

MỤC TIÊU MÔN HỌC (t)

- Kỹ năng:
  - Sử dụng các giải thuật mã hóa, mã xác thực thông báo, và băm.
  - Vận dụng suy luận toán học đánh giá độ an toàn hệ thống.
  - Phân tích phát hiện các yếu điểm của các hệ thống mạng và các hiểm họa tấn công.
  - Áp dụng một cách thích hợp các kỹ thuật an toàn mạng thông dụng.
  - Đề xuất và xây dựng các giải pháp đảm bảo an toàn truyền thông.

TÀI LIỆU THAM KHẢO

- Tài liệu tham khảo:
  - Bài giảng An toàn thông tin – Khoa CNTT – trường ĐH KTKTCN.
  - William Stallings. Cryptography and Network Security: Principles and Practice, Sixth Edition. Prentice Hall, 2014.
  - Charlie Kaufman, Radia Perlman, and Mike Speciner. Network Security: Private Communication in a Public World, Second Edition. Prentice Hall, 2002.

NỘI DUNG

1. GIỚI THIỆU
2. MÃ HÓA ĐỐI XỨNG CỔ ĐIỂN
3. MÃ HÓA ĐỐI XỨNG HIỆN ĐẠI
4. MẬT MÃ KHÓA CÔNG KHAI
5. XÁC THỰC VÀ CHỮ KÝ SỐ
6. CÁC ỨNG DỤNG XÁC THỰC
7. AN TOÀN THƯ ĐIỆN TỬ
8. AN TOÀN IP
9. AN TOÀN WEB

CHƯƠNG 1: GIỚI THIỆU

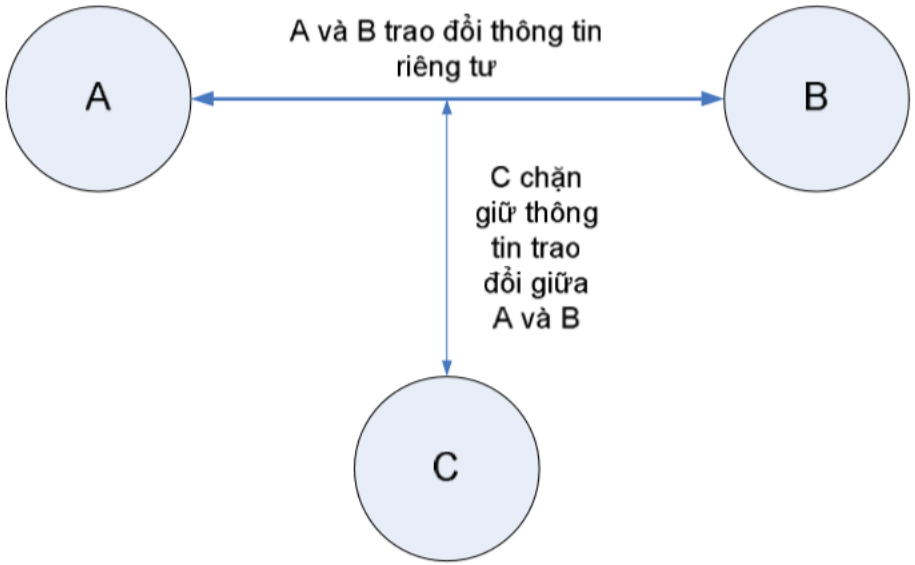
1.1. Khái niệm an toàn mạng.

1.2. Các yếu tố xác lập an toàn thông tin.

1.3. Mô hình an toàn mạng.

Một số ví dụ về an toàn Mạng

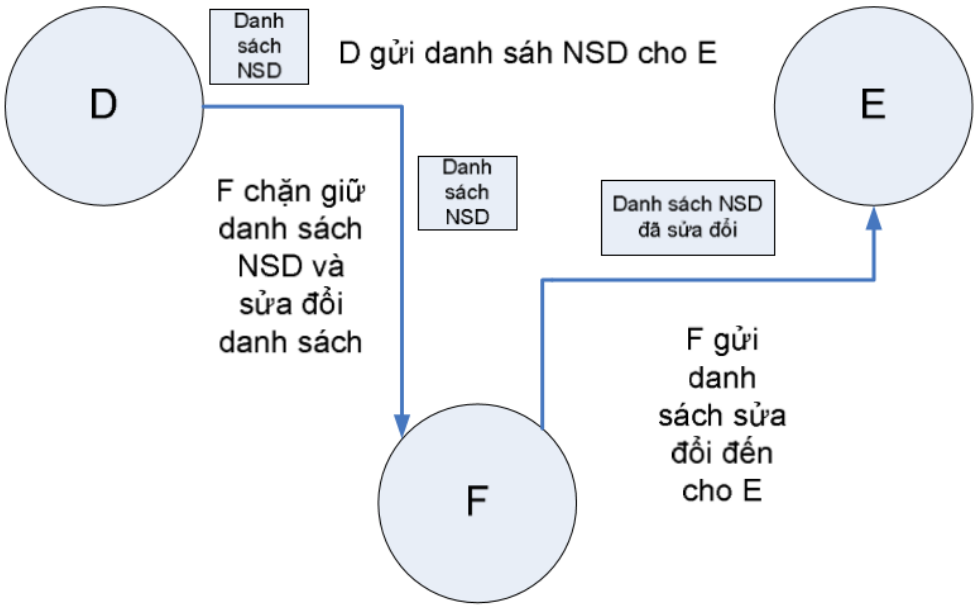
- Truyền file
  - A truyền file cho B;
  - Trong file chứa những thông tin bí mật;
  - C không được phép đọc file nhưng có thể theo dõi được quá trình truyền file và sao chép file trong quá trình truyền.



Một số ví dụ về an toàn Mạng

Trao đổi thông điệp

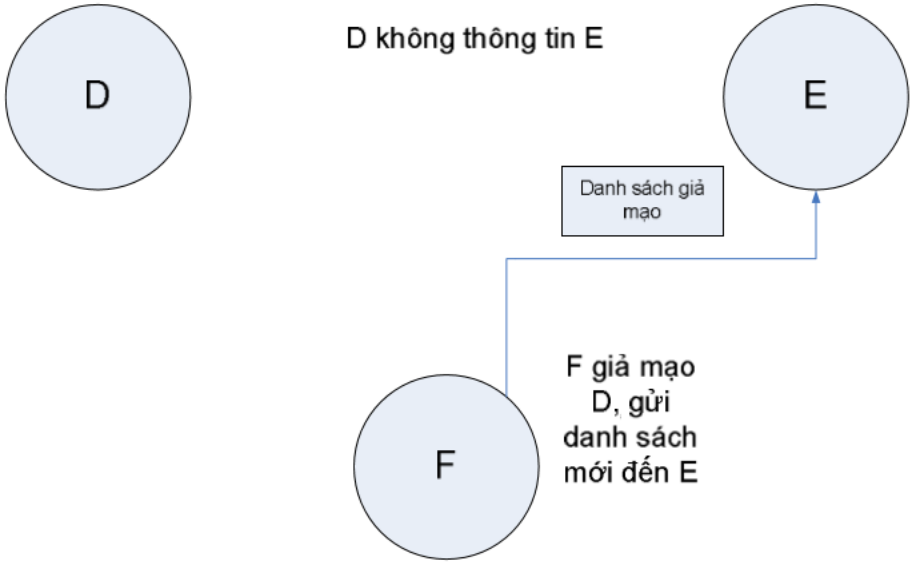
- Quản trị mạng D gửi thông điệp đến máy tính chịu sự quản trị E;
- Thông điệp chứa những thông tin về danh sách những người sử dụng mới.
- Người sử dụng F bắt thông điệp;
- F thêm các user mới vào nội dung thông điệp, rồi gửi tiếp cho E;
- E nhận thông điệp, không biết là đã bị F thay đổi, vẫn tưởng là do D gửi tới và thay đổi danh sách user của mình.



Một số ví dụ về an toàn Mạng

Giả mạo:

- Kịch bản giống trường hợp trước;
- F tạo một thông điệp của riêng mình, chứa những thông tin riêng có lợi cho F và gửi cho E.
- E nhận được thông tin từ F, cho rằng thông tin đó do D gửi và cập nhật những thông tin giả mạo vào CSDL



1.1 Khái niệm an toàn mạng

- Khái niệm cơ bản về an toàn thông tin (security).
  - Bảo mật hay an toàn thông tin là mức độ bảo vệ thông tin trước các mối đe rọa về “thông tịn lộ”, “thông tin không còn toàn vẹn” và “thông tin không sẵn sàng”.
  - Bảo mật hay an toàn thông tin là mức độ bảo vệ chống lại các nguy cơ về mất an toàn thông tin như “nguy hiểm”, “thiệt hại”, “mất mát” và các tội phạm khác.
  - Mức độ bảo vệ thông tin bao gồm “cấu trúc” và “quá trình xử lý” để nâng cao bảo mật.

1.1 Khái niệm an toàn mạng (t)

- 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.

1.2 Các yếu tố xác lập an toàn thông tin

- Các dịch vụ an toàn:
  - 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).

Bảo mật 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 riêng tư: bảo vệ luồng thông tin trao đổi khỏi các thao tác phân tích.
  - Yêu cầu: phía tấn công không thể phát hiện được các đặc điểm của quá trình truyền tin: nguồn và đích của thông tin, tần suất, độ dài, ...

Bảo mật riêng tư (t)

- Tương ứng với hình thức phát hiện nội dung thông điệp có một vài phương pháp bảo vệ đường truyền:
  - Bảo vệ mọi dữ liệu được truyền giữa hai người sử dụng tại mọi thời điểm: thiết lập đường truyền ảo giữa hai hệ thống và ngăn chặn mọi hình thức phát hiện nội dung thông điệp.
  - Bảo vệ các thông điệp đơn lẻ hoặc một số trường hợp đơn lẻ: không thực sự hữu ích, trong nhiều trường hợp khá phức tạp, chi phí lớn.

Xác thực

- Khẳng định các bên tham gia vào quá trình truyền tin được xác thực và đáng tin cậy.
- Đối với các thông điệp đơn lẻ:
  - Các thông báo, báo hiệu: dịch vụ xác thực đảm bảo cho bên nhận rằng các thông điệp được đưa ra từ những nguồn đáng tin cậy.
- Đối với những liên kết trực tuyến:
  - Tại thời điểm khởi tạo kết nối, hai thực thể tham gia vào trao đổi thông tin phải được ủy quyền.
  - Dịch vụ cần khẳng định rằng kết nối không bị can thiệp bởi một bên thứ ba.

Tính toàn vẹn

- Đảm bảo tính toàn vẹn cũng có thể áp dụng cho luồng thông điệp hoặc một thông điệp.
- Phương pháp hữu ích nhất là trực tiếp bảo vệ luồng thông điệp.
- Đảm bảo tính toàn vẹn:
  - Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết.
  - Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết.

Tính toàn vẹn (t)

- Dịch vụ bảo đảm tính toàn vẹn dữ liệu hướng liên kết:
  - Tác động lên luồng thông điệp, đảm bảo rằng thông điệp được nhận hoàn toàn giống khi được gửi (không bị sao chép, sửa đổi, thêm bớt).
  - Các dữ liệu bị phá huỷ cũng được khôi phục bằng dịch vụ này.
- Dịch vụ bảo đảm tính toàn vẹn hướng không liên kết:
  - Chỉ xử lý một thông điệp đơn lẻ.
  - Chỉ tập trung vào ngăn chặn sửa đổi nội dung thông điệp.

Chống phủ định

- Dịch vụ chống phủ định ngăn chặn người nhận và người gửi từ chối thông điệp được truyền tải.
- Khi thông điệp được gửi đi, người nhận có thể khẳng định rằng thông điệp đích thực được gửi tới từ người được uỷ quyền.
- Khi thông điệp được nhận, người gửi có thể khẳng định rằng thông điệp thực sự tới đích.

Kiểm soát truy cập

- Dịch vụ kiểm soát truy cập cung cấp khả năng giới hạn và kiểm soát truy cập tới máy chủ hoặc các ứng dụng thông qua đường truyền tin.
- Để đạt được sự kiểm soát này, mỗi đối tượng khi truy nhập vào mạng, phải được nhận biết hoặc được xác thực, sao cho quyền truy cập sẽ được gắn với từng cá nhân.

Tính sẵn sàng

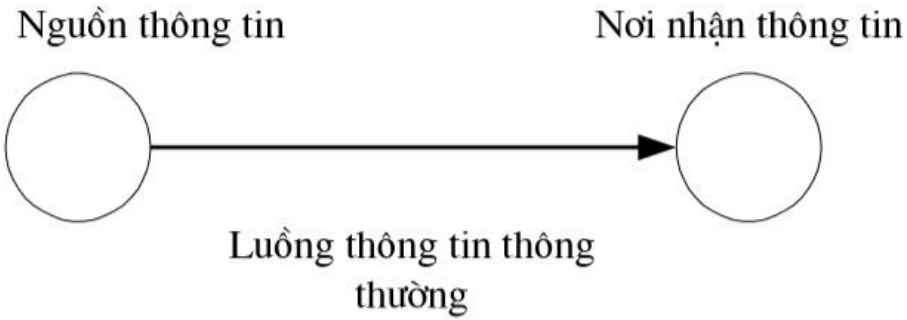
- Khi có sự tấn công phá hủy tính sẵn sàng của hệ thống, thực hiện các thao tác vật lý tác động lên hệ thống.
- Dịch vụ đảm bảo tín sẵn sàng phải:
  - Ngăn chặn các ảnh hưởng lên thông tin trong hệ thống.
  - Phục hồi khả năng phục vụ của các phần tử hệ thống trong thời gian nhanh nhất.

1.2 Các yếu tố xác lập an toàn thông tin

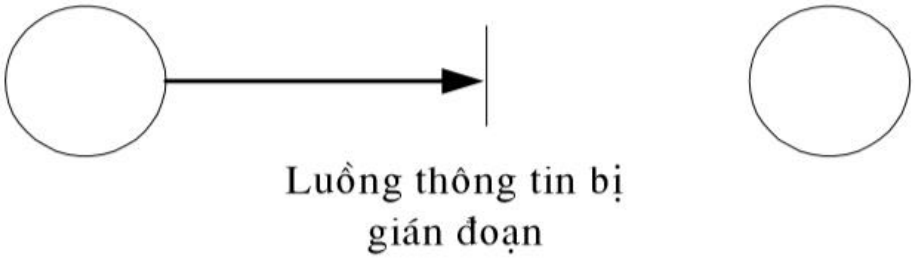
- Các cơ chế an toàn
  - Không tồn tại một cơ chế duy nhất.
  - Sử dụng các kỹ thuật mật mã.
- Các hình thức tấn công
  - Truy nhập thông tin bất hợp pháp.
  - Sửa đổi thông tin bất hợp pháp…

Một số dạng tấn công

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

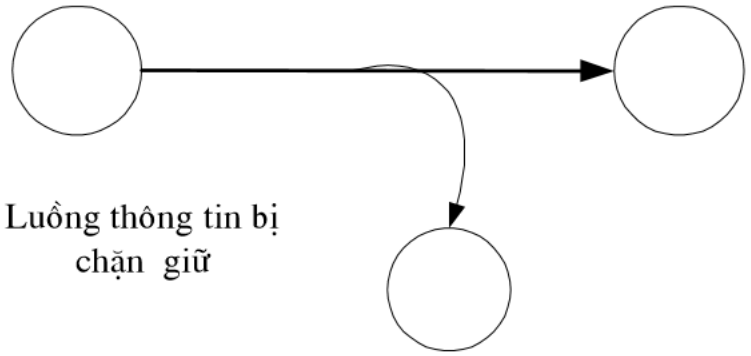


  - Gián đoạn truyền tin (interruption):

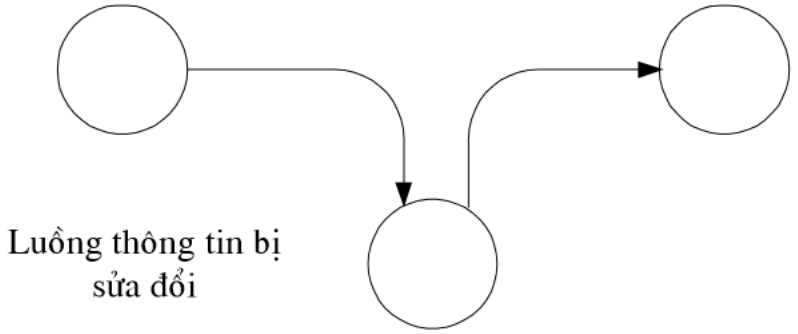


Một số dạng tấn công (t)

- Chặn giữ thông tin (interception):

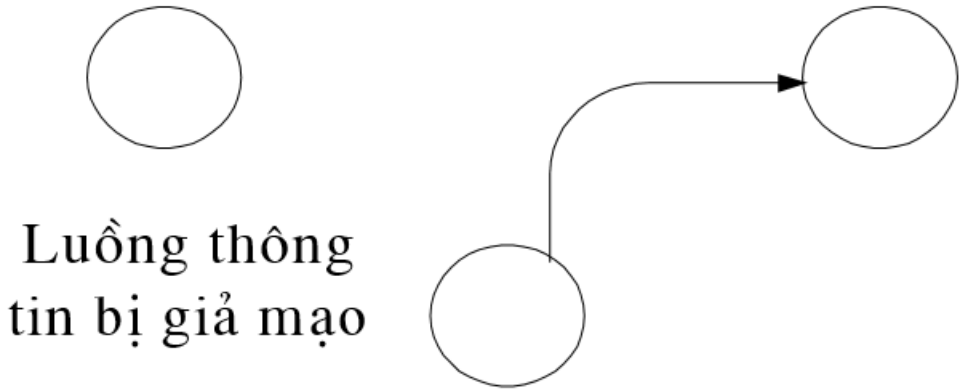


- Sửa đổi thông tin (modification):



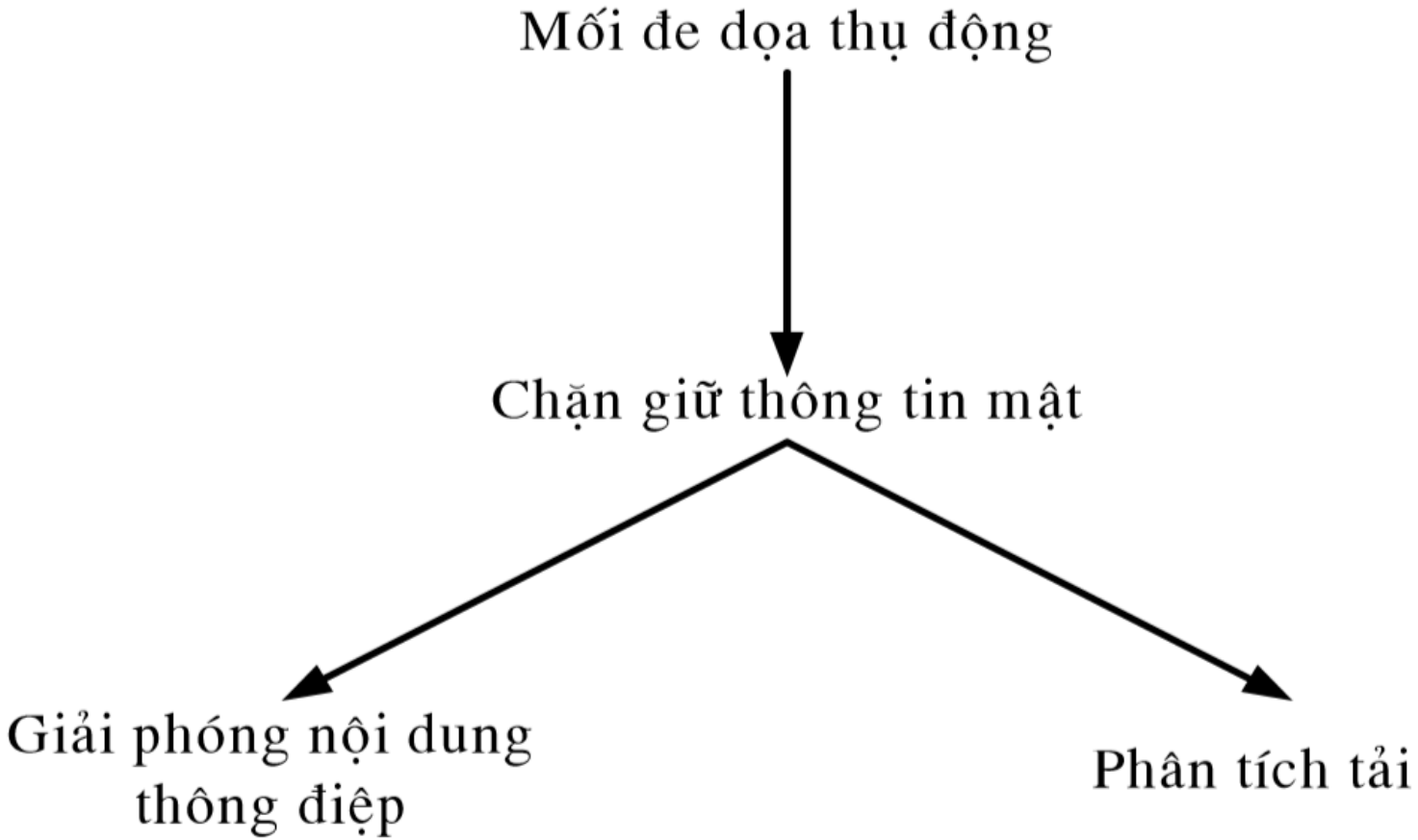
Một số dạng tấn công (t)

- Giả mạo thông tin (fabrication).



Một số dạng tấn công (t)

- Tấn công thụ động

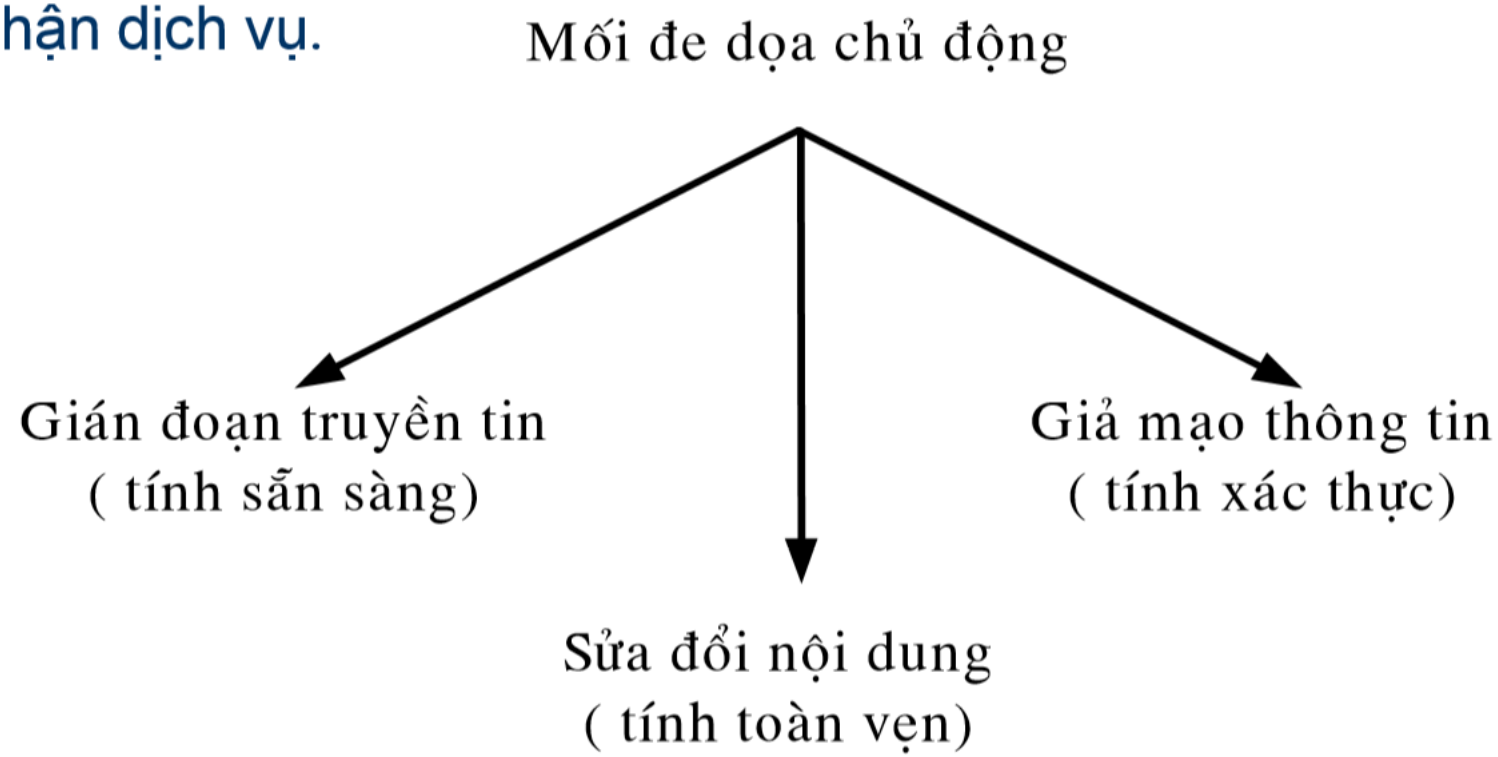


Một số dạng tấn công (t)

- Các dạng tấn công thụ động:
  - Giải phóng nội dung thông điệp: ngăn chặn đối phương thu và tìm hiểu được nội dung của thông tin truyền tải.
  - Phân tích tải: 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.
- 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 “ngăn chặn” hơn “phát hiện”.

Một số dạng tấn công (t)

- 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.



Một số dạng tấn công (t)

- Giả danh: khi đối phương giả mạo một đối tượng được uỷ quyền.
- Phát lại: 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: một phần của thông điệp hợp pháp bị sửa đổi, làm chậm hoặc sắp xếp lại => những hiệu ứng không được uỷ quyền.
- Phủ nhận dịch vụ: cấm hoặc ngăn chặn sử dụng các dịch vụ, các khả năng truyền thông.

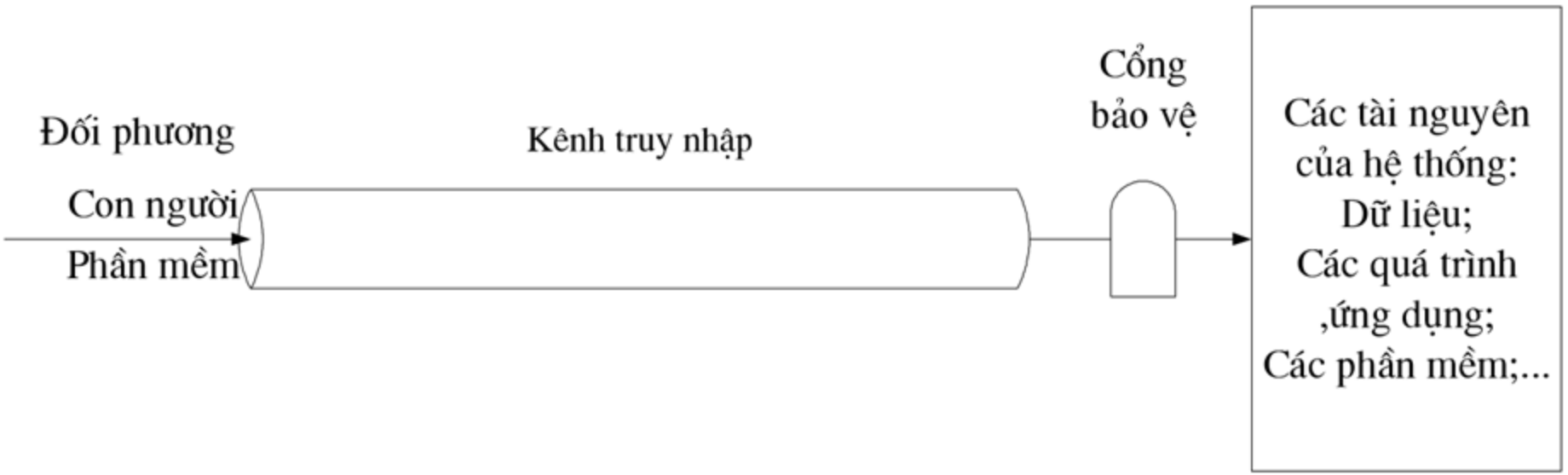
Một số dạng tấn công (t)

- Dạng tấn công chủ động rất khó có thể ngăn chặn tuyệt đối => 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.

1.3 Mô hình an toàn mạng

- Quá trình truyền tải có bảo mật thông tin được gửi.
- Một số thông tin mật sẽ được chia sẻ giữa hai bên truyền tin.
- Các thao tác cơ bản thiết kế một hệ thống an toàn
  - Thiết kế các thuật toán để thực hiện quá trình truyền tin an toàn.
  - Tạo ra những thông tin mật sẽ được xử lý bằng thuật toán trên.
  - Phát triển những phương pháp để phân phối và chia sẻ các thông tin mật
  - Đặt ra giao thức trao đổi.

1.3 Mô hình an toàn mạng (t)



TỔNG KẾT

01 An ninh mạng: phương tiện bảo vệ, chống, phát hiện, hiệu chỉnh các phá hoại an toàn khi truyền và lưu trữ thông tin.

02 Các yếu tố xác lập ATTT: bảo mật riêng tư, xác thực, toàn vẹn thông tin chống phủ định, kiểm soát truy cập, sẵn sàng.

03 Mô hình an toàn mạng