ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

AN NINH MẠNG

TS. Nguyễn Đại Thọ

Bộ môn Mạng & Truyền thông Máy tính
Khoa Công nghệ Thông tin

thond_cn@vnu.edu.vn

Năm học 2007-2008

Chương 1

Giới thiệu

Bối cảnh

- Nhu cầu đảm bảo an ninh thông tin có những biến đổi lớn
  - Trước đây
    - Chỉ cần các phương tiện vật lý và hành chính
  - Từ khi có máy tính
    - Cần các công cụ tự động bảo vệ tệp tin và các thông tin khác lưu trữ trong máy tính
  - Từ khi có các phương tiện truyền thông và mạng
    - Cần các biện pháp bảo vệ dữ liệu truyền trên mạng

Các khái niệm

- An ninh thông tin
  - Liên quan đến các yếu tố tài nguyên, nguy cơ, hành động tấn công, yếu điểm, và điều khiển
- An ninh máy tính
  - Các công cụ bảo vệ dữ liệu và phòng chống tin tặc
- An ninh mạng
  - Các biện pháp bảo vệ dữ liệu truyền trên mạng
- An ninh liên mạng
  - Các biện pháp bảo vệ dữ liệu truyền trên một tập hợp các mạng kết nối với nhau

Mục tiêu môn học

- Chú trọng an ninh liên mạng
- Nghiên cứu các biện pháp ngăn cản, phòng chống, phát hiện và khắc phục các vi phạm an ninh liên quan đến truyền tải thông tin

Đảm bảo an ninh thông tin

- Để thực hiện có hiệu quả cần đề ra một phương thức chung cho việc xác định các nhu cầu về an ninh thông tin
- Phương thức đưa ra sẽ xét theo 3 mặt
  - Hành động tấn công
  - Cơ chế an ninh
  - Dịch vụ an ninh

Dịch vụ an ninh

- Là một dịch vụ nâng cao độ an ninh của các hệ thống xử lý thông tin và các cuộc truyền dữ liệu trong một tổ chức
- Nhằm phòng chống các hành động tấn công
- Sử dụng một hay nhiều cơ chế an ninh
- Có các chức năng tương tự như đảm bảo an ninh tài liệu vật lý
- Một số đặc trưng của tài liệu điện tử khiến việc cung cấp các chức năng đảm bảo an ninh khó khăn hơn

Cơ chế an ninh

- Là cơ chế định ra để phát hiện, ngăn ngừa và khắc phục một hành động tấn công
- Không một cơ chế đơn lẻ nào có thể hỗ trợ tất cả các chức năng đảm bảo an ninh thông tin
- Có một yếu tố đặc biệt hậu thuẫn nhiều cơ chế an ninh sử dụng hiện nay là các kỹ thuật mật mã
- Môn học sẽ chú trọng lĩnh vực mật mã

Hành động tấn công

- Là hành động phá hoại an ninh thông tin của một tổ chức
- An ninh thông tin là những cách thức ngăn ngừa các hành động tấn công, nếu không được thì phát hiện và khắc phục hậu quả
- Các hành động tấn công có nhiều và đa dạng
- Chỉ cần tập trung vào những thể loại chung nhất
- Lưu ý : nguy cơ tấn công và hành động tấn công thường được dùng đồng nghĩa với nhau

Kiến trúc an ninh OSI

- Kiến trúc an ninh cho OSI theo khuyến nghị X.800 của ITU-T
- Định ra một phương thức chung cho việc xác định các nhu cầu về an ninh thông tin
- Cung cấp một cái nhìn tổng quan về các khái niệm môn học sẽ đề cập đến
- Chú trọng đến các dịch vụ an ninh, các cơ chế an ninh và các hành động tấn công

Các dịch vụ an ninh

- Theo X.800
  - Dịch vụ an ninh là dịch vụ cung cấp bởi một tầng giao thức của các hệ thống mở kết nối nhằm đảm bảo an ninh cho các hệ thống và các cuộc truyền dữ liệu
  - Có 5 loại hình
- Theo RFC 2828
  - Dịch vụ an ninh là dịch vụ xử lý hoặc truyền thông cung cấp bởi một hệ thống để bảo vệ tài nguyên theo một cách thức nhất định

Các dịch vụ an ninh X.800

- Xác thực
  - Đảm bảo thực thể truyền thông đúng là nó
- Điều khiển truy nhập
  - Ngăn không cho sử dụng trái phép tài nguyên
- Bảo mật dữ liệu
  - Bảo vệ dữ liệu khỏi bị tiết lộ trái phép
- Toàn vẹn dữ liệu
  - Đảm bảo nhận dữ liệu đúng như khi gửi
- Chống chối bỏ
  - Ngăn không cho bên liên quan phủ nhận hành động

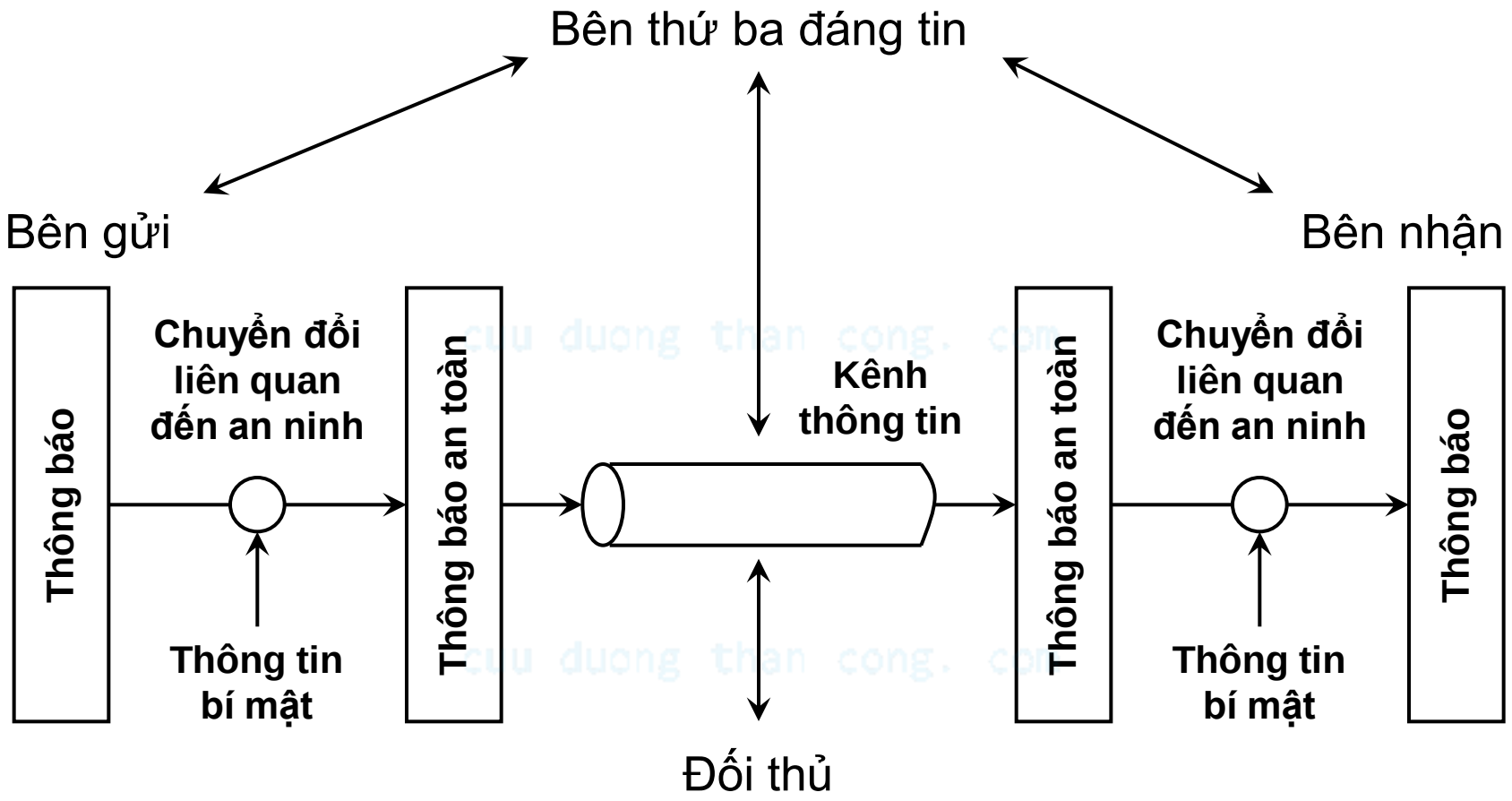
Các cơ chế an ninh X.800

- Các cơ chế an ninh chuyên dụng
  - Mã hóa, chữ ký số, điều khiển truy nhập, toàn vẹn dữ liệu, trao đổi xác thực, độn tin truyền, điều khiển định tuyến, công chứng
- Các cơ chế an ninh phổ quát
  - Tính năng đáng tin, nhãn an ninh, phát hiện sự kiện, dấu vết kiểm tra an ninh, khôi phục an ninh

Các hành động tấn công

- Các hành động tấn công thụ động
  - Nghe trộm nội dung thông tin truyền tải
  - Giám sát và phân tích luồng thông tin lưu chuyển
- Các hành động tấn công chủ động
  - Giả danh một thực thể khác
  - Phát lại các thông báo trước đó
  - Sửa đổi các thông báo đang lưu chuyển
  - Từ chối dịch vụ

Mô hình an ninh mạng



Mô hình an ninh mạng

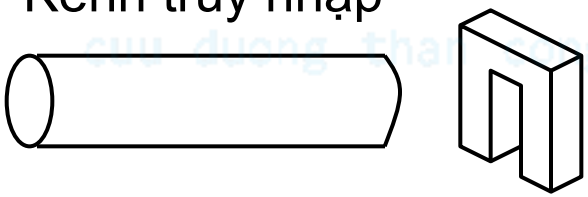
- Yêu cầu
  - Thiết kế một giải thuật thích hợp cho việc chuyển đổi liên quan đến an ninh
  - Tạo ra thông tin bí mật (khóa) đi kèm với giải thuật
  - Phát triển các phương pháp phân bổ và chia sẻ thông tin bí mật
  - Đặc tả một giao thức sử dụng bởi hai bên gửi và nhận dựa trên giải thuật an ninh và thông tin bí mật, làm cơ sở cho một dịch vụ an ninh

Mô hình an ninh truy nhập mạng

Đối thủ

- **Con người**
- **Phần mềm**

Kênh truy nhập



Chức năng gác cổng

Các tài nguyên tính toán (bộ xử lý, bộ nhớ, ngoại vi)

Dữ liệu

Các tiến trình

Phần mềm

Các điều khiển an ninh bên trong

Mô hình an ninh truy nhập mạng

- Yêu cầu
  - Lựa chọn các chức năng gác cổng thích hợp để định danh người dùng
  - Cài đặt các điều khiển an ninh để đảm bảo chỉ những người dùng được phép mới có thể truy nhập được vào các thông tin và tài nguyên tương ứng
- Các hệ thống máy tính đáng tin cậy có thể dùng để cài đặt mô hinh này