AN TOÀN VÀ AN NINH MẠNG

TS. Nguyễn Đại Thọ
Trường Đại học Công nghệ
Đại học Quốc gia Hà Nội

Chương 1

GIỚI THIỆU

Bối cảnh xã hội

- Thế giới đứng trước thách thức của các tấn công khủng bố với an ninh được thắt chặt
- Công nghệ thông tin cũng là nạn nhân của một số lượng lớn chưa từng có các tấn công
- An toàn thông tin là một thành phần cốt lõi của công nghệ thông tin
  - Bảo vệ thông tin điện tử có giá trị
- Nhu cầu về các chuyên gia CNTT biết bảo vệ an toàn mạng và máy tính là rất lớn

Bối cảnh công nghệ

- Hai biến đổi lớn trong yêu cầu về an toàn thông tin thời gian gần đây
  - Trước đây an toàn thông tin được đảm bảo bằng các biện pháp vật lý và hành chính
  - Sử dụng máy tính tạo yêu cầu về các công cụ tự động để bảo vệ file và các thông tin lưu trữ khác
  - Sử dụng mạng và các phương tiện truyền thông tạo yêu cầu về các biện pháp bảo vệ dữ liệu trong khi truyền

Làm rõ khái niệm an toàn thông tin

- An toàn
  - Trạng thái không bị nguy hiểm hoặc rủi ro
    - Trạng thái hay điều kiện đó tồn tại vì các biện pháp bảo vệ được thiết lập và duy trì
- An toàn thông tin
  - Mô tả nhiệm vụ bảo vệ thông tin ở khuôn dạng số
- An toàn thông tin có thể được hiểu thông qua xem xét mục tiêu và cách thức thực hiện

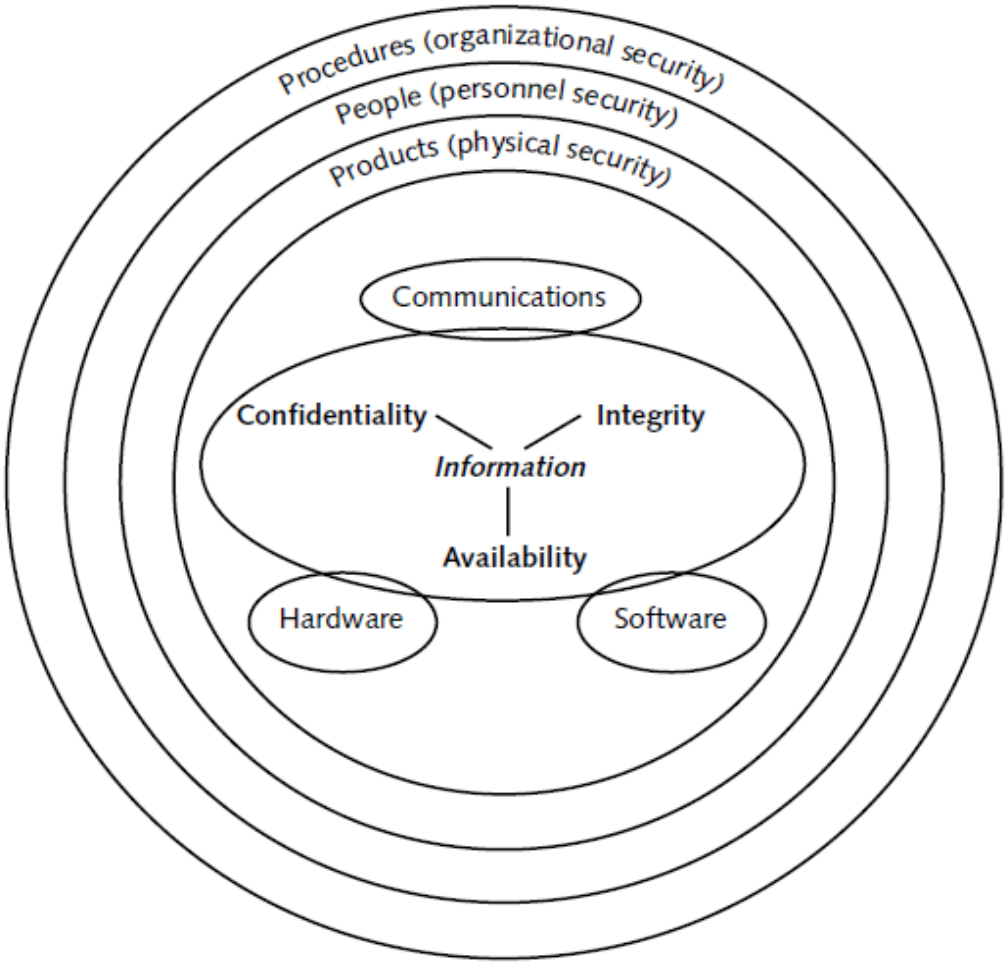
Mục tiêu của an toàn thông tin

- Đảm bảo các biện pháp bảo vệ được thực hiện một cách thích hợp
- Bảo vệ thông tin có giá trị đối với con người hoặc tổ chức
  - Giá trị ở các đặc tính **bảo mật**, **toàn vẹn**, và **khả dụng**
- Bảo vệ các đặc tính của thông tin trên các thiết bị lưu trữ, thao tác, và truyền thông tin

Cách thức thực hiện ATTT

- Thông qua kết hợp 3 thực thể
  - Phần cứng, phần mềm, và truyền thông
- Ba lớp bảo vệ
  - Sản phẩm
    - An ninh vật lý xung quanh dữ liệu
  - Con người
    - Những người cài đặt và sử dụng các sản phẩm an ninh
  - Thủ tục
    - Kế hoạch và chính sách đảm bảo sử dụng đúng đắn các sản phẩm

Các thành phần an toàn thông tin



Định nghĩa an toàn thông tin

- Một định nghĩa hoàn chỉnh hơn về an toàn thông tin
  - *Là thứ bảo vệ tính toàn vẹn, tính bảo mật, và tính khả dụng của thông tin trên các thiết bị lưu trữ, thao tác, và truyền dẫn thông tin thông qua các sản phẩm, con người, và các thủ tục*

Các khái niệm an toàn thông tin (1)

- Tính bảo mật
  - Bảo vệ những hạn chế cho phép về truy nhập và tiết lộ thông tin
    - Bao gồm các biện pháp bảo vệ tính riêng tư cá nhân và thông tin độc quyền
- Tính toàn vẹn
  - Bảo vệ thông tin khỏi bị sửa đổi hoặc triệt tiêu một cách không thích hợp
    - Bao gồm đảm bảo tính không thể chối bỏ và tính xác thực của thông tin

Các khái niệm an toàn thông tin (2)

- Tính khả dụng
  - Đảm bảo truy nhập và sử dụng thông tin một cách kịp thời và đáng tin cậy
- Tính xác thực
  - Tính chân thật và có thể kiểm tra và tin cậy được
- Tính chịu trách nhiệm
  - Mục tiêu an ninh quy định các hành động của một thực thể phải được quy một cách duy nhất về thực thể đó

Các thuật ngữ an toàn thông tin (1)

- Tài sản
  - Một thứ có giá trị
- Mối đe dọa
  - Một tiềm năng vi phạm an toàn tồn tại khi có một tình huống, một khả năng, một hành động, hay một sự kiện có thể phá vỡ an toàn và gây hại
    - Một mối đe dọa là một nguy hiểm tiềm tàng có thể khai thác một điểm nhạy cảm

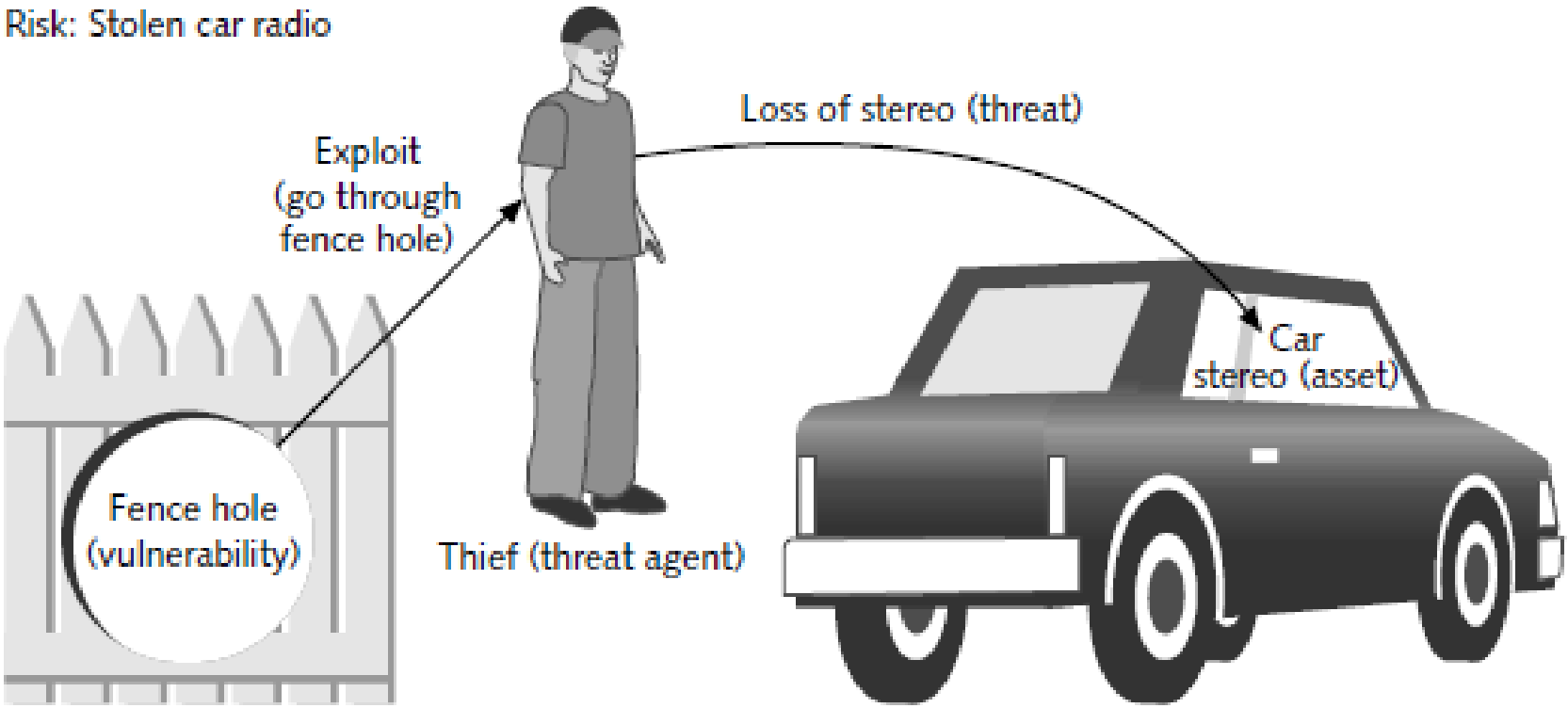
Các thuật ngữ an toàn thông tin (2)

- Tác nhân đe dọa
  - Một người hoặc vật có khả năng thực hiện một mối đe dọa
- Tấn công
  - Một công phá vào an toàn hệ thống bắt nguồn từ một mối đe dọa hay một hành động thông minh
    - Một nỗ lực có chủ ý vượt qua các dịch vụ an ninh và vi phạm chính sách an ninh của một hệ thống
  - Thường được dùng cùng nghĩa như mối đe dọa

Các thuật ngữ an toàn thông tin (3)

- Điểm nhạy cảm
  - Điểm yếu cho phép một tác nhân đe dọa vượt qua an ninh
- Rủi ro
  - Khả năng một tác nhân đe dọa sẽ khai thác một điểm nhạy cảm
  - Thực tế không loại trừ được hoàn toàn rủi ro
  - Ba phương án đối phó với rủi ro
    - Chấp nhận rủi ro, giảm thiểu rủi ro, chuyển giao rủi ro

Ví dụ các thuật ngữ an ninh



Các định nghĩa về an toàn

- An toàn máy tính
  - Tên chung cho tập các công cụ được thiết kế để bảo vệ dữ liệu và chống lại tin tặc
- An toàn mạng
  - Các biện pháp bảo vệ dữ liệu khi truyền dẫn
- An toàn liên mạng
  - Các biện pháp bảo vệ dữ liệu khi truyền dẫn qua một tập các mạng kết nối với nhau

Các thách thức an toàn máy tính (1)

- Không đơn giản như lầm tưởng ban đầu
- Luôn phải xem xét các tấn công tiềm tàng vào các tính năng an ninh muốn phát triển
- Các thủ tục an ninh thường trái với trực quan
- Phải quyết định triển khai các cơ chế an ninh ở đâu
- Bao hàm nhiều hơn một giải thuật hay giao thức và cần tới thông tin bí mật

Các thách thức an toàn máy tính (2)

- Cuộc đấu trí giữa kẻ tấn công và người thiết kế hay quản trị
- Không thấy là có lợi cho đến khi bị phá hoại
- Yêu cầu giám sát đều đặn thậm chí thường xuyên
- Quá thường xuyên là giải pháp tích hợp sau khi hoàn thành thiết kế
- Bị coi là trở ngại đối với việc sử dụng hiệu quả và thân thiện hệ thống hoặc thông tin

Các mẫu kẻ tấn công (1)

- Tin tặc
  - Những người với kiến thức đặc biệt về các hệ thống máy tính
  - Tin tặc mũ đen
    - Chế ngự các hệ thống tính toán vì lợi ích cá nhân
  - Tin tặc mũ trắng
    - Chế ngự để tìm lỗ hổng và phát triển giải pháp
  - Tin tặc mũ xám
    - Thường đội mũ trắng nhưng cũng có thể đội mũ đen

Các mẫu kẻ tấn công (2)

- Trẻ dùng tập lệnh
  - Những người sử dụng các tập lệnh và chương trình phát triển bởi tin tặc mũ đen để tấn công các hệ thống tính toán
  - Họ không biết cách viết các công cụ chế ngự hay hiểu cách một công cụ chế ngự có sẵn hoạt động, nhưng có thể gây ra nhiều thiệt hại
- Gián điệp mạng
  - Thu thập tin tình báo thông qua các trao đổi trên mạng chặn nghe được

Các mẫu kẻ tấn công (3)

- Nhân viên bất mãn
  - Những người cố tình chọc thủng an ninh để gây hại cho giới chủ
- Khủng bố mạng
  - Những kẻ khủng bố sử dụng các công nghệ máy tính và mạng để thực hiện tấn công và làm hoảng sợ công cộng
- Kẻ tấn công giả định
  - Tất cả các mẫu kẻ tấn công trừ khủng bố mạng

Kiến trúc an ninh OSI

- Mục tiêu
  - Ước định một cách có hiệu quả các nhu cầu an ninh
  - Đánh giá và lựa chọn các sản phẩm và chính sách an ninh thích hợp
- "Kiến trúc an ninh cho OSI" của ITU-T X.800
- Một cách thức có hệ thống định nghĩa và đáp ứng các nhu cầu an ninh
- Cung cấp một tổng quan hữu ích mặc dù trừu tượng về các khái niệm sẽ nghiên cứu

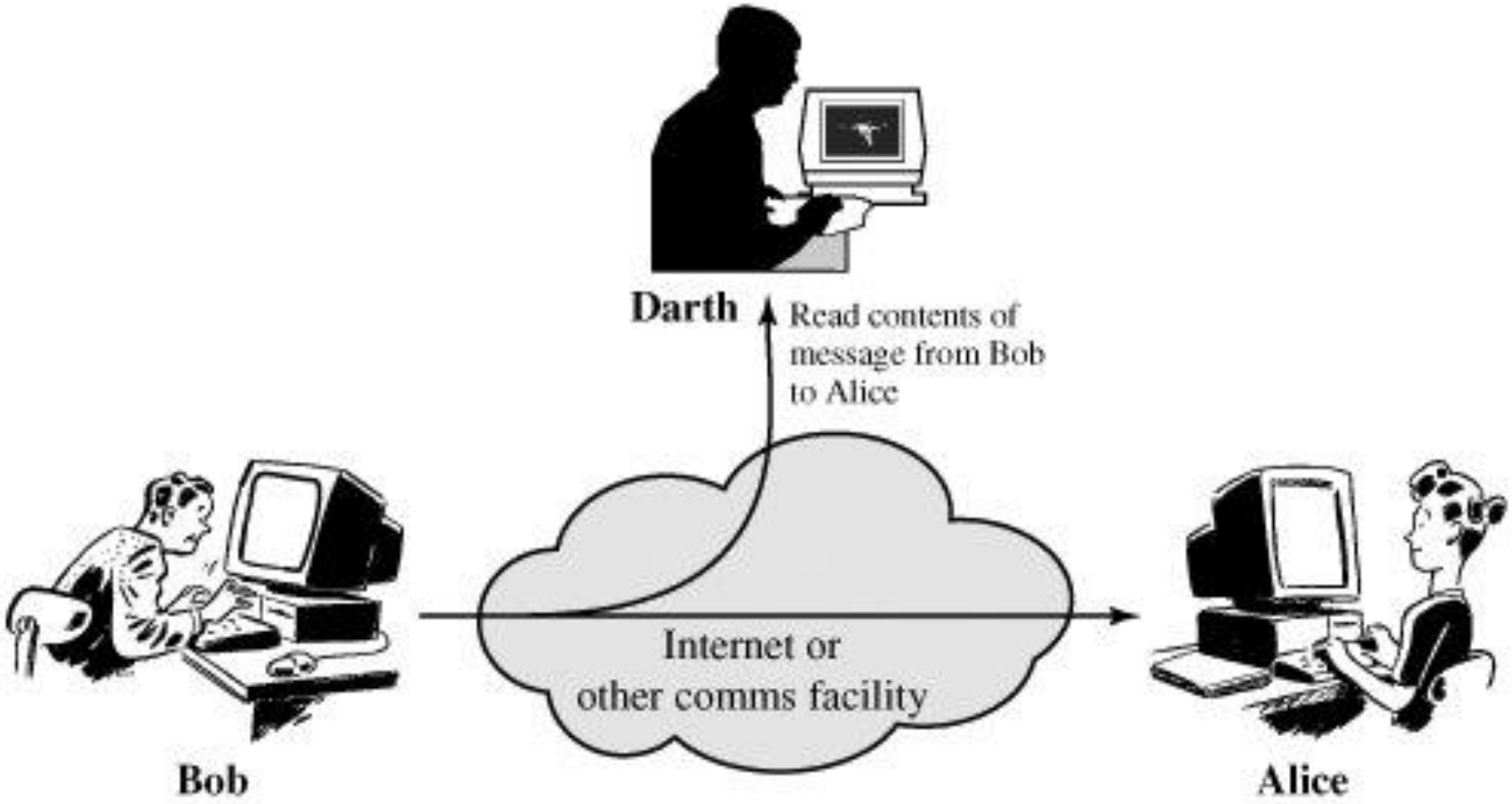
Các khía cạnh an ninh

- Tấn công an ninh
  - Hành động làm tổn hại an toàn thông tin
- Cơ chế an ninh
  - Quá trình được thiết kế để phát hiện, ngăn ngừa hoặc khôi phục từ một tấn công an ninh
- Dịch vụ an ninh
  - Dịch vụ tăng cường an ninh của các hệ thống xử lý dữ liệu và các chuyển giao thông tin

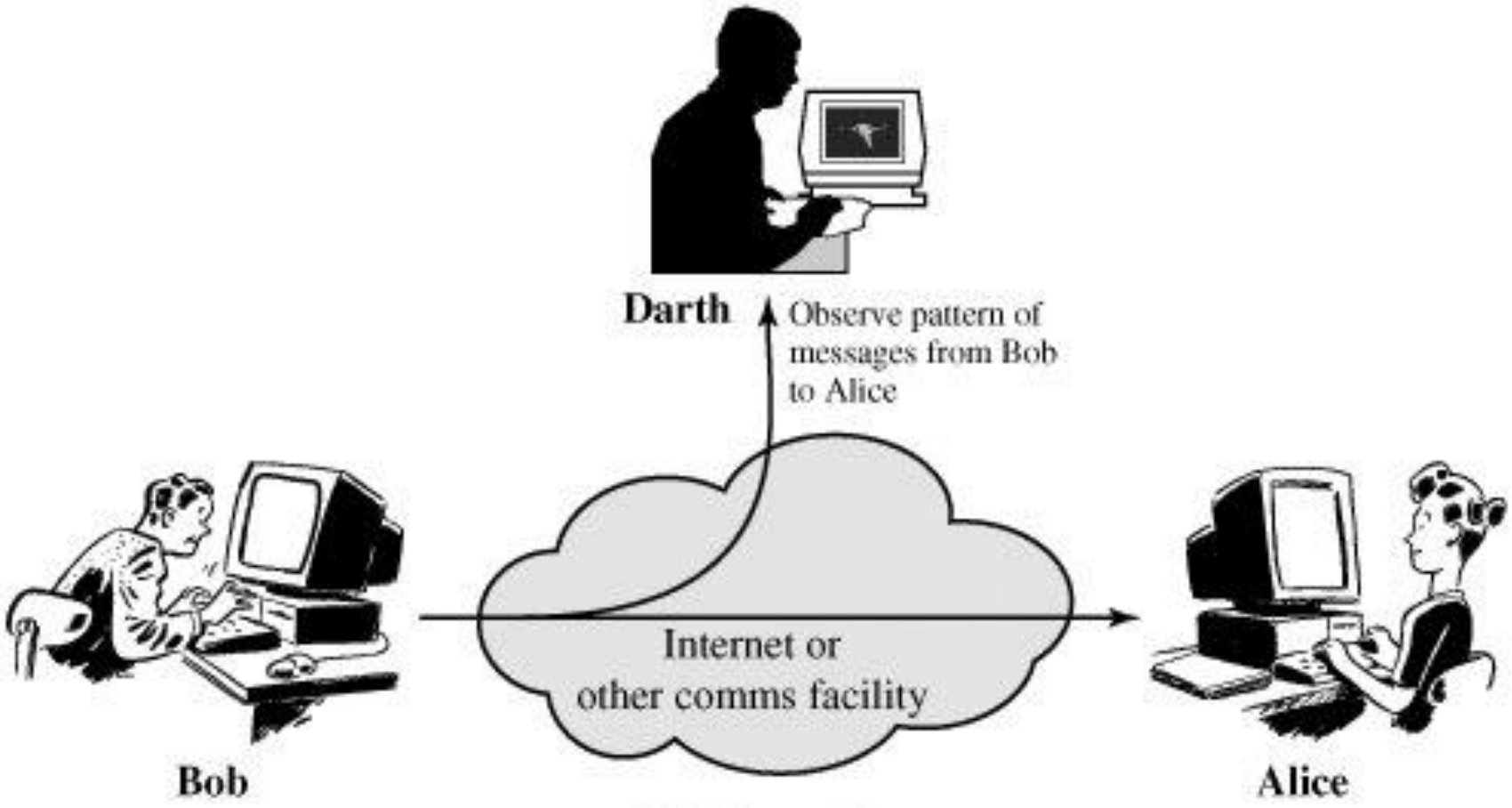
Tấn công thụ động

- Tìm cách nắm bắt và sử dụng thông tin nhưng không tác động đến tài nguyên hệ thống
  - Không bao hàm bất kỳ sửa đổi nào trên dữ liệu
- Hai kiểu
  - Làm lộ nội dung thông báo
  - Phân tích lưu lượng
- Chú trọng ngăn ngừa thay vì phát hiện
  - Thường bằng các biện pháp mã hóa

Làm lộ nội dung thông báo



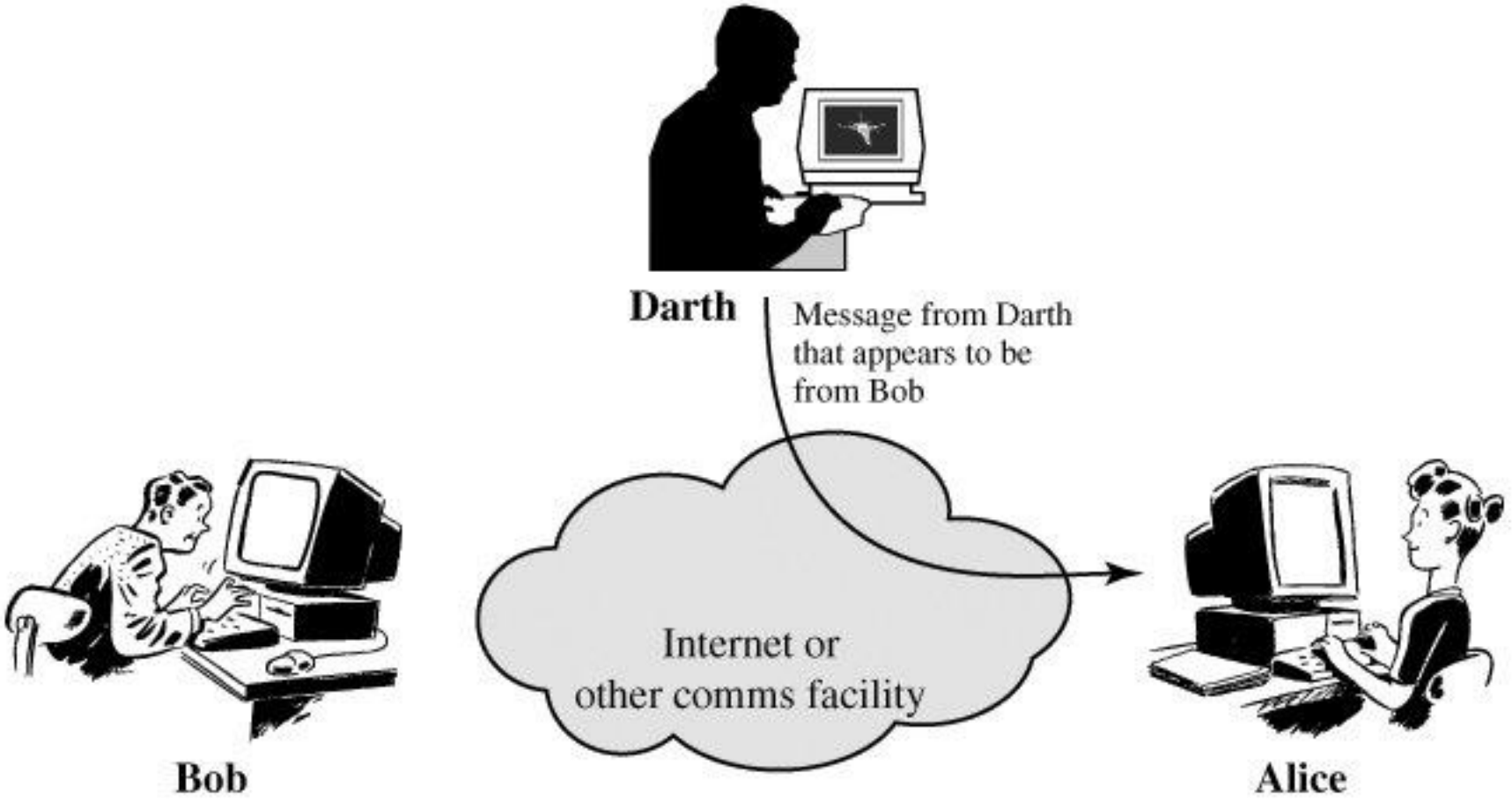
Phân tích lưu lượng



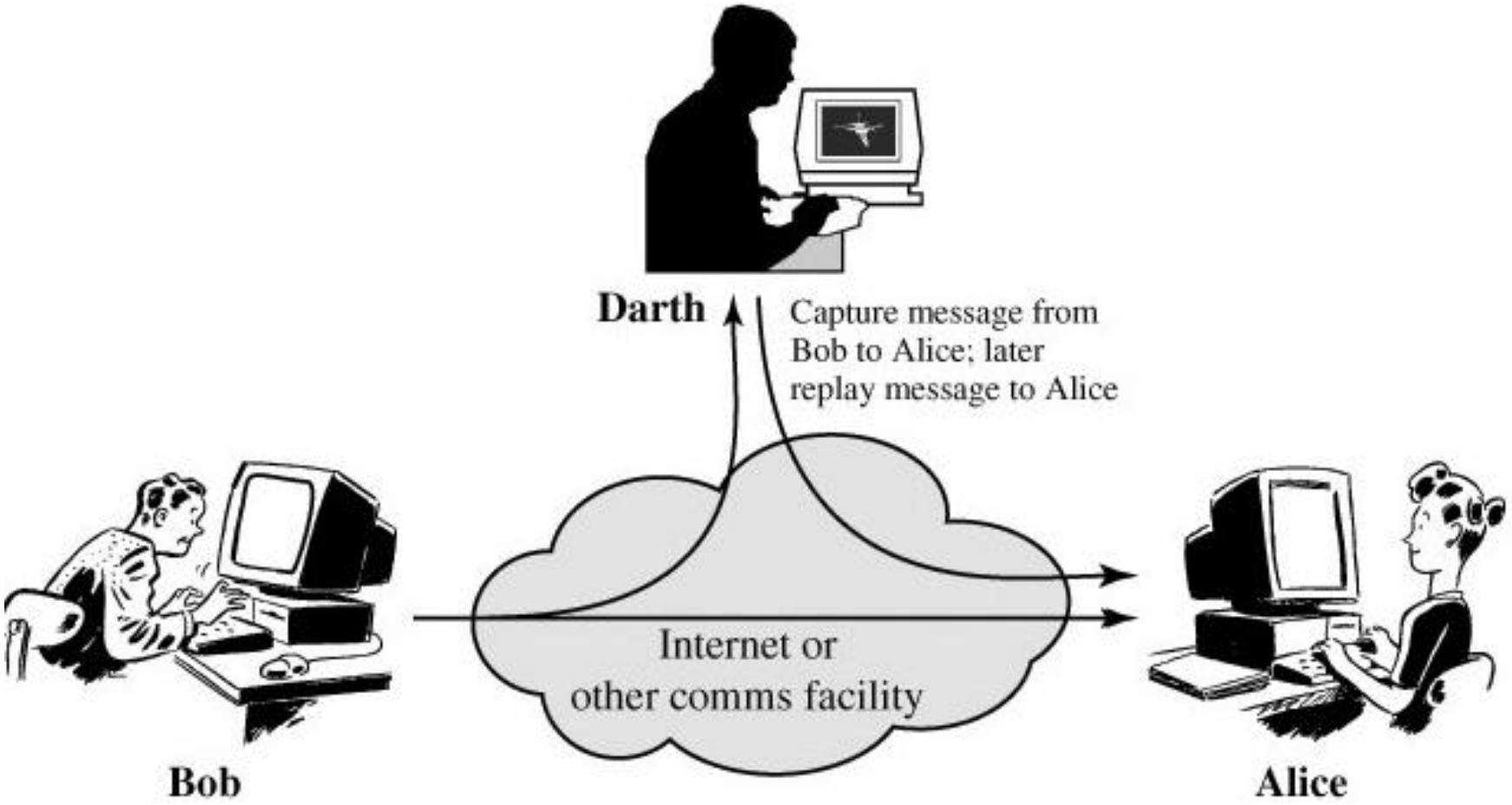
Tấn công chủ động

- Bao hàm việc sửa đổi luồng dữ liệu hoặc tạo ra luồng dữ liệu giả
- Bốn kiểu
  - Giả mạo
  - Lặp lại
  - Sửa đổi thông báo
  - Từ chối dịch vụ
- Mục tiêu là phát hiện tấn công chủ động và khôi phục khỏi ngưng trệ hay chậm trễ
  - Phát hiện có thể góp phần ngăn ngừa

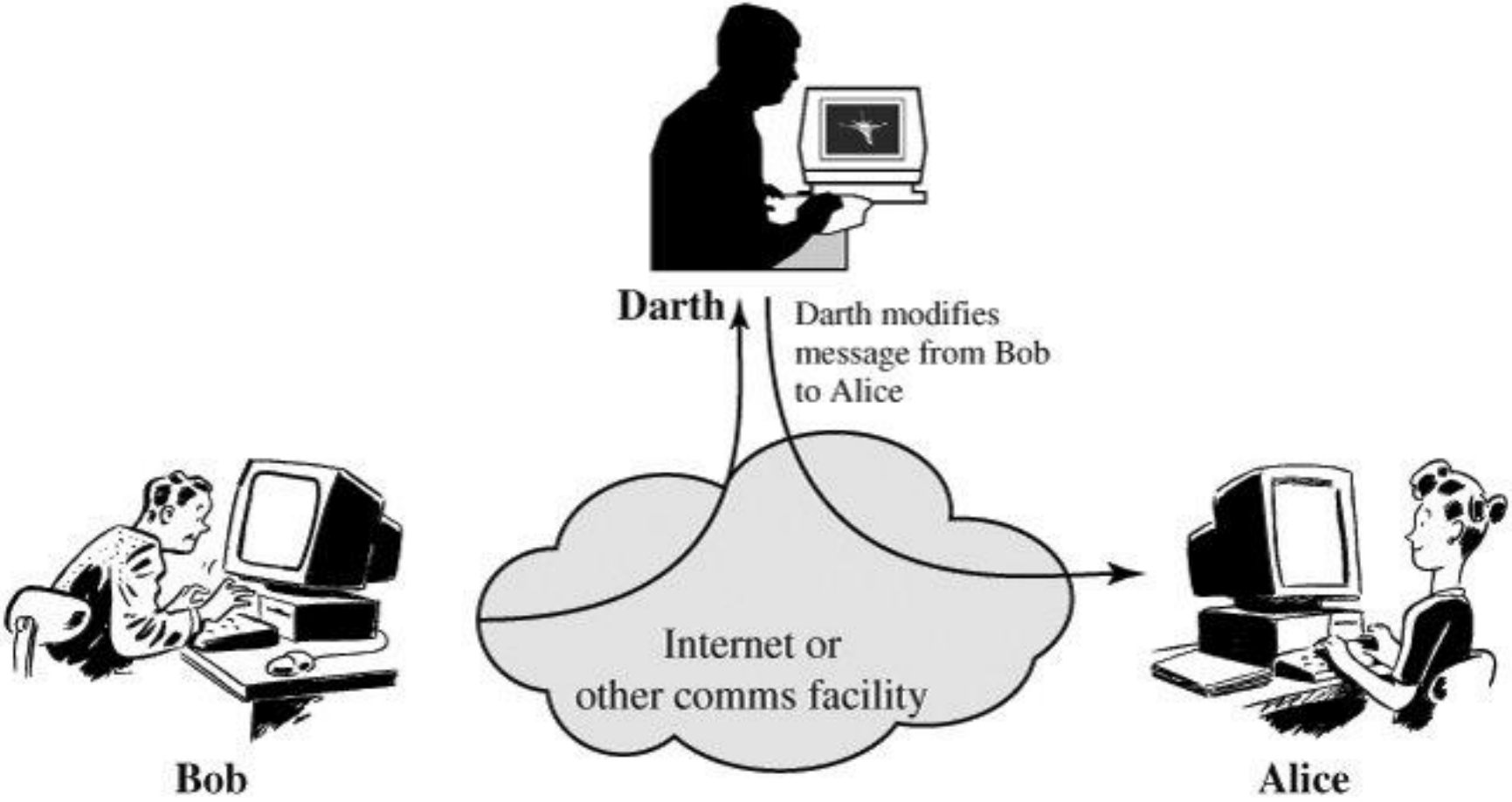
Giả mạo


Darth
Message from Darth
that appears to be
from Bob
Internet or
other comms facility
Bob
Alice

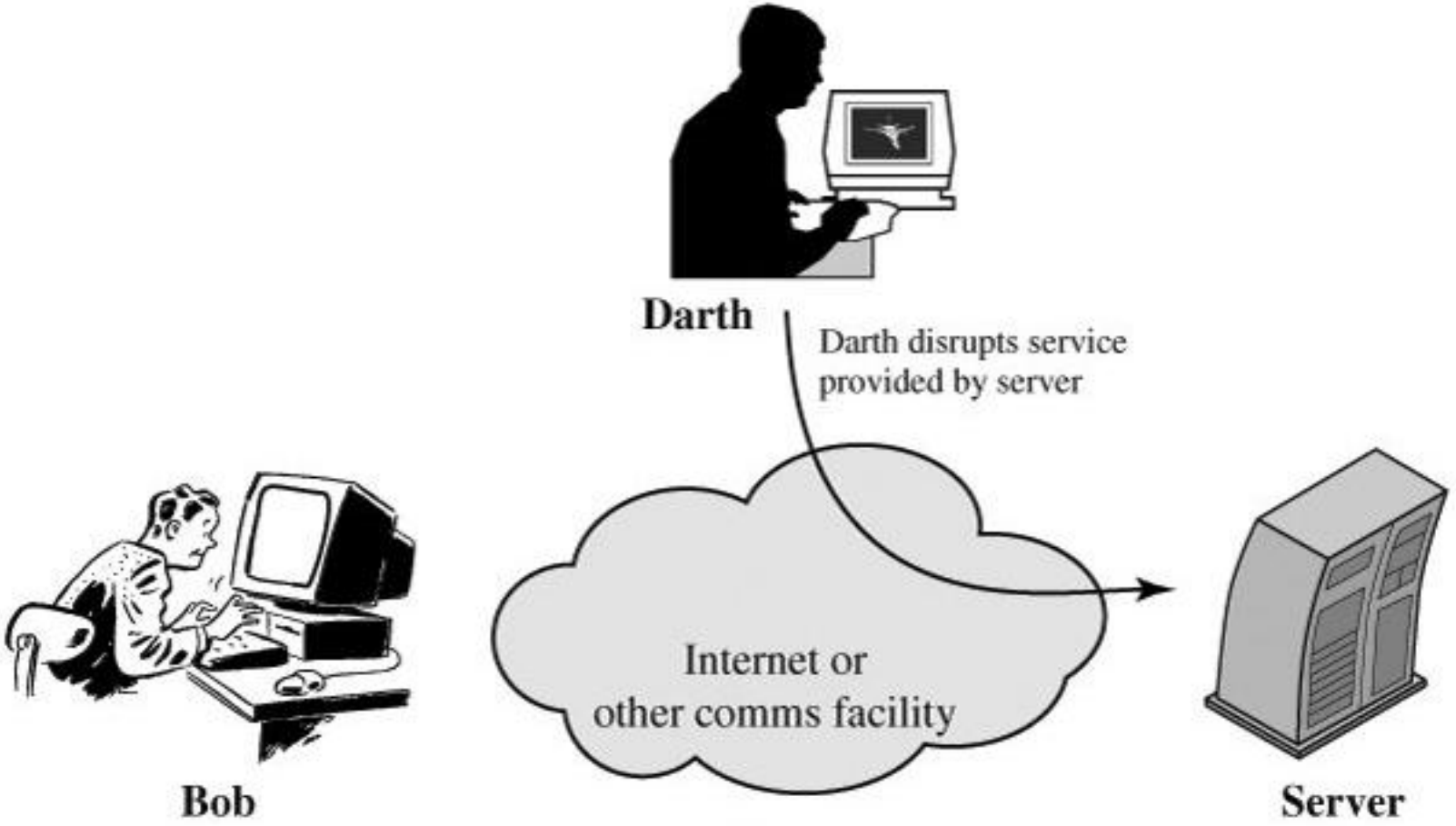
Lặp lại


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

Sửa đổi thông báo



Từ chối dịch vụ



Dịch vụ an ninh

- X.800
  - Dịch vụ cung cấp bởi một tầng giao thức trong các hệ thống mở truyền thông, đảm bảo an toàn thỏa đáng các hệ thống và các chuyển giao dữ liệu
- RFC 2828
  - Dịch vụ xử lý hoặc truyền thông cung cấp bởi một hệ thống để đem lại một loại bảo vệ nhất định cho các tài nguyên hệ thống
- Chủ định chống lại các tấn công an ninh

Các dịch vụ an ninh (X.800) (1)

- Xác thực
  - Đảm bảo thực thể truyền thông là cái nó khai nhận
- Điều khiển truy nhập
  - Ngăn ngừa sử dụng một cách trái phép tài nguyên
- Bảo mật dữ liệu
  - Bảo vệ dữ liệu khỏi bị tiết lộ một cách trái phép

Các dịch vụ an ninh (X.800) (2)

- Toàn vẹn dữ liệu
  - Đảm bảo dữ liệu nhận được đúng như khi gửi bởi một thực thể được phép
- Chống chối bỏ
  - Bảo vệ khỏi sự chối bỏ bởi một trong các thực thể tham gia truyền thông
- Khả dụng
  - Đảm bảo tài nguyên có thể truy nhập và sử dụng được

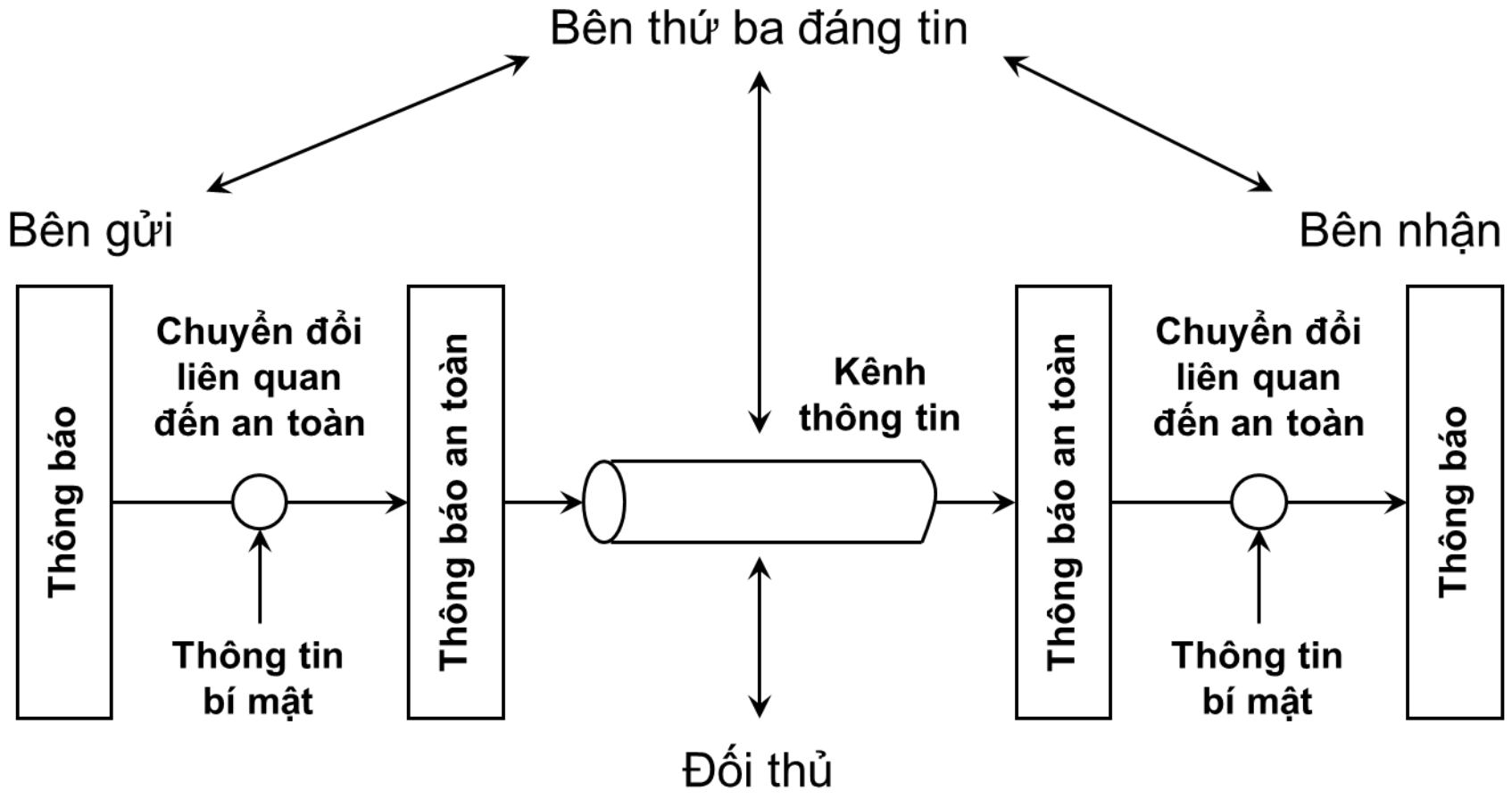
Cơ chế an ninh

- Một dịch vụ an ninh sử dụng một hoặc nhiều cơ chế an ninh
- Không có một cơ chế đơn lẻ nào hỗ trợ tất cả các dịch vụ an ninh
- Một yếu tố đặc biệt hậu thuẫn nhiều cơ chế an ninh đang được sử dụng
  - Các kỹ thuật mật mã học

Các cơ chế an ninh (X.800)

- Các cơ chế an ninh chuyên biệt
  - Được cài đặt ở một tầng giao thức chuyên biệt
  - Mã hóa, chữ ký số, điều khiển truy nhập, toàn vẹn dữ liệu, trao đổi xác thực, độn lưu lượng, điều khiển định tuyến, công chứng
- Các cơ chế an ninh phổ quát
  - Không chuyên biệt cho bất kỳ dịch vụ an ninh hay tầng giao thức đặc biệt nào
  - Tính năng đáng tin, nhãn an ninh, phát hiện sự kiện, dấu vết kiểm nghiệm an ninh, khôi phục an ninh

Mô hình an toàn mạng



Nhiệm vụ mô hình an toàn mạng

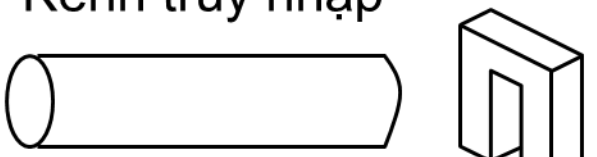
- Thiết kế giải thuật thực hiện chuyển đổi liên quan đến an toàn
- Sinh thông tin bí mật để dùng với giải thuật
- Phát triển các phương pháp phân phối và chia sẻ thông tin bí mật
- Đặc tả một giao thức cho phép các chủ thể sử dụng giải thuật an ninh và thông tin bí mật cho một dịch vụ an ninh

Mô hình an toàn 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

Nhiệm vụ an toàn truy nhập mạng

- Chức năng gác cổng
  - Các thủ tục đăng nhập dựa trên mật khẩu để từ chối truy nhập với tất cả trừ những người dùng được phép
  - Các logic kiểm tra để phát hiện và loại bỏ các bọ, virus và những tấn công tương tự khác
- Các điều khiển an ninh bên trong
  - Giám sát hoạt động và phân tích thông tin lưu giữ để phát hiện sự có mặt của các kẻ thâm nhập không mong muốn

Tổng kết

- Các động lực cho môn học
- Các định nghĩa, khái niệm và thuật ngữ về an ninh
- Các thách thức đối với an toàn máy tính
- Các mẫu kẻ tấn công
- Kiến trúc an ninh X.800
  - Tấn công an ninh, dịch vụ an ninh, cơ chế an ninh
- Các mô hình cho an toàn (truy nhập) mạng