HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN

An toàn mạng thông tin

TEL1401

Giảng viên: TS. Phạm Anh Thư

Điện thoại/E-mail: 0912528188

thupa80@yahoo.com, thupaptit@gmail.com

Bộ môn: Mạng viễn thông - KhoaViễn thông 1

Học kỳ/Năm biên soạn: I/ 2022-2023

Học phần An toàn mạng thông tin

- **Tên môn học: An toàn mạng thông tin**
- **Giờ tín chỉ:**
  - **Lý thuyết:** 36 tiết
  - **Bài tập, kiểm tra:** 8 tiết.
  - **Thi cuối kỳ:** Thi trắc nghiệm trên máy
  - **Giờ tự học:** 30 tiết

Nội dung

- **Chương 1:** Tổng quan an toàn mạng thông tin: khái niệm, dịch vụ, kiến trúc an toàn mạng thông tin, …
- **Chương 2:** Mật mã hóa: mật mã hóa khóa đối xứng và mật mã hóa khóa công khai
- **Chương 3:** Các giải thuật toàn vẹn dữ liệu: hàm băm, mã xác thực bản tin MAC
- **Chương 4:** Xác thực: Quản lý và phân phối khóa, xác thực người sử dụng
- **Chương 5**: An toàn mạng Internet: an toàn lớp giao vận, an toàn ứng dụng WEB, an toàn thư điện tử, IPsec, …
- **Chương 6**: An toàn hệ thống thông tin: Phần mềm độc hại, tấn công DoS, phát hiện xâm nhập, tường lửa, …

Tài liệu tham khảo

- Bài giảng An toàn mạng thông tin, Bộ môn Mạng viễn thông – Học viện CNBCVT.
- William Stalling, Lawrie Brown, Cryptography and Network Security –Principles and Practice. Pearson, 4th Edition, 2018.
- William Stalling, Computer Security – Principles and Practice. Pearson Education Inc., 7th Edition, 2017.
- J. M. Kizza, A guide to Computer Network Security, Springer, 2009.

Đánh giá môn học

Chuyên cần	• 10% (Đánh giá dựa trên số giờ đi học, ý thức chuẩn bị bài và tinh thần tích cực thảo luận)
Bài tập, thảo luận trên lớp 20%	• 10% - đánh giá theo nhóm (BT tiểu luận)
	• 10% - đánh giá nội dung riêng từng cá nhân (BT trên lớp)
Kiểm tra giữa kỳ	• 10%
Bài thi cuối kỳ	• Sinh viên đi học đủ 70% lý thuyết, làm đủ bài kiểm tra, bài tập thảo luận nhóm sẽ có quyền dự thi cuối kỳ. • 60% , thi trắc nghiệm trên máy

Yêu cầu lớp học

Chính sách đối với môn học và các yêu cầu khác

- Các bài tập phải đúng hạn. Nếu không đúng hạn sẽ bị trừ điểm;
- Nghỉ 1 kíp trừ 2đ, đi học muộn trừ 1đ
- Thiếu 1 điểm thành phần của môn học sẽ không được thi hết môn.
- Không sử dụng điện thoại trong lớp
- Không nói chuyện riêng trong lớp
- Không gục xuống bàn ngủ

Khái niệm An toàn mạng truyền thông

- **Khi công nghệ máy tính chưa phát triển: các biện pháp bảo mật thông tin:**
  - Đóng dấu và ký niêm phong
  - Dùng mật mã mã hóa thông điệp để chỉ có người gửi và người nhận hiểu được thông điệp. Phương pháp này thường được sử dụng trong chính trị và quân sự.
  - Lưu giữ tài liệu mật trong các két sắt có khóa
- Khi mạng Internet phát triển: ngày càng có nhiều thông tin được lưu giữ trên máy vi tính và gửi đi trên mạng Internet. Và do đó **xuất hiện nhu cầu về an toàn và bảo mật thông tin trên máy tính:**
  - Bảo vệ thông tin trong quá trình truyền thông tin trên mạng (Network Security)
  - Bảo vệ hệ thống máy tính, và mạng máy tính, khỏi sự xâm nhập phá hoại từ bên ngoài (System Security)

Khái niệm An toàn mạng

- An toàn thông tin trên mạng máy tính bao gồm các phương pháp nhằm bảo vệ thông tin được lưu giữ và truyền thông trên mạng.

- An toàn mạng thông tin hay Internet bao gồm các phương pháp nhằm ngăn chặn, phát hiện, bảo vệ và khắc phục các vi phạm liên quan đến truyền thông thông tin trên mạng.

Khái niệm an toàn máy tính

- An toàn máy tính: bảo vệ hệ thống thông tin nhằm đạt được các mục tiêu đảm bảo tính toàn vẹn, tính sẵn sàng, tính bảo mật (và một số mục tiêu an toàn khác) của tài nguyên hệ thống thông tin (bao gồm phần cứng, phần mềm, firmware, thông tin/dữ liệu, và truyền thông).

Khái niệm an toàn máy tính

Tính bí mật (confidentiality):

- Bảo mật dữ liệu: bảo vệ dữ liệu khỏi bị lộ trái phép.
- Tính riêng tư: bảo đảm rằng các thông tin liên quan đến cá nhân không bị lộ, hay bị lưu giữ trái phép.

Khái niệm an toàn máy tính

Tính toàn vẹn (intergrity):

- Tính toàn vẹn dữ liệu: bảo đảm dữ liệu, chương trình chỉ được xử lý, thay đổi bởi quá trình được phân quyền hoặc hành động của các cá nhân hoặc thiết bị được quyền.
- Tính toàn vẹn hệ thống: bảo đảm rằng hệ thống thực hiện các chức năng đúng đắn, không bị can thiệp từ các cá nhân trái phép.

Khái niệm an toàn máy tính

Tính sẵn sàng (availability)

- Tính sẵn sàng: bảo đảm rằng hệ thống làm việc chính xác và dịch vụ sẵn sàng cho người sử dụng hợp pháp.

Các mục tiêu an toàn khác

- Tính xác thực (authenticity): tính đúng đắn được xác minh và tin cậy, xác nhận được bản tin, nguồn gốc.
- Tính trách nhiệm giải trình (accountability): mục tiêu an toàn thiết lập các yêu cầu cho hoạt động của thực thể phải được theo dõi đối với thực thể. Hỗ trợ chống chối bỏ, cô lập lỗi, phát hiện xâm nhập, hồi phục, …

Kiến trúc an toàn

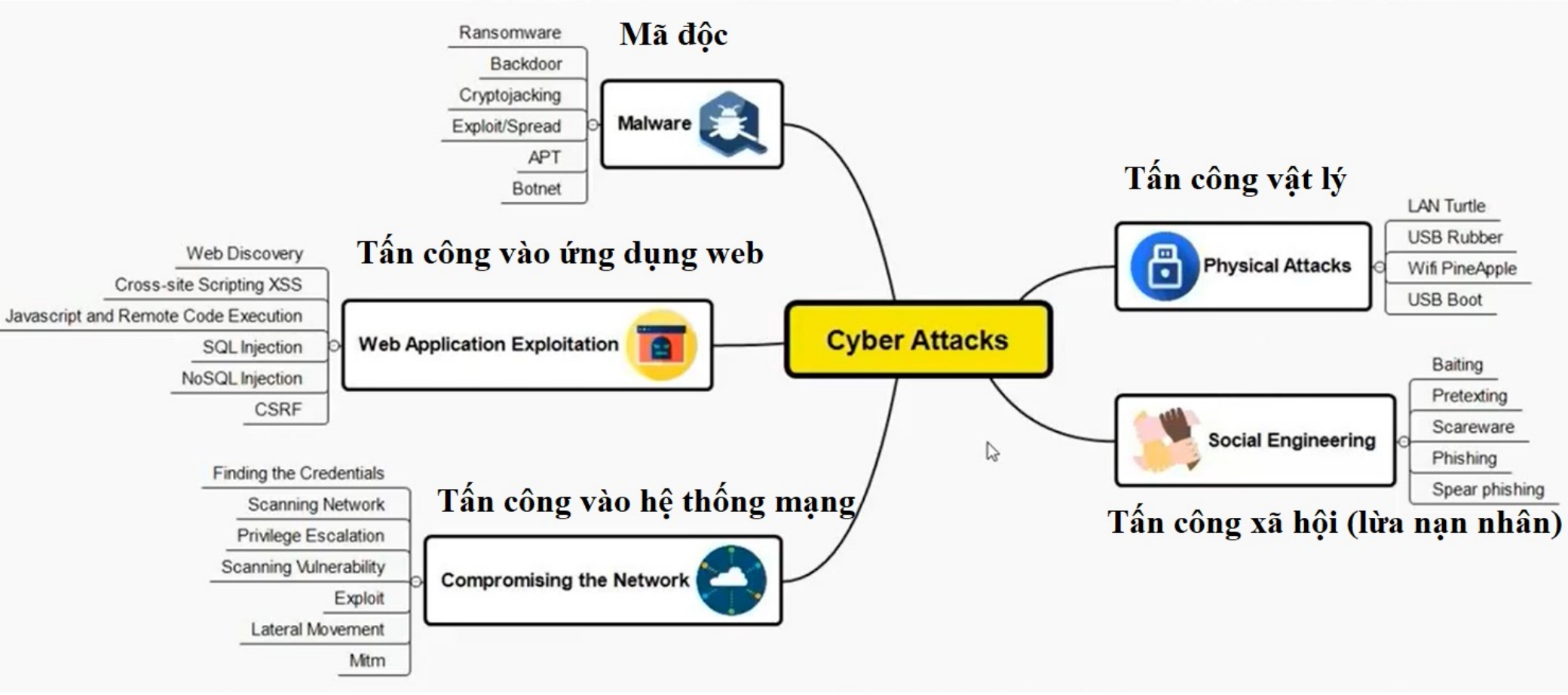
- ITU-T đã đưa ra khuyến nghị X.800 định nghĩa kiến trúc an toàn cho mô hình OSI
  - Giúp cho các nhà quản lý trong việc tổ chức cung cấp dịch vụ an toàn
  - Giúp các nhà cung cấp cơ sở hạ tầng cũng như nhà cung cấp thiết bị và dịch vụ có thể triển khai các đặc tính an toàn cho các sản phẩm và dịch vụ của họ

- Kiến trúc an toàn tập trung vào các kiểu tấn công, các cơ chế an toàn, và các dịch vụ an toàn.

Kiến trúc an toàn

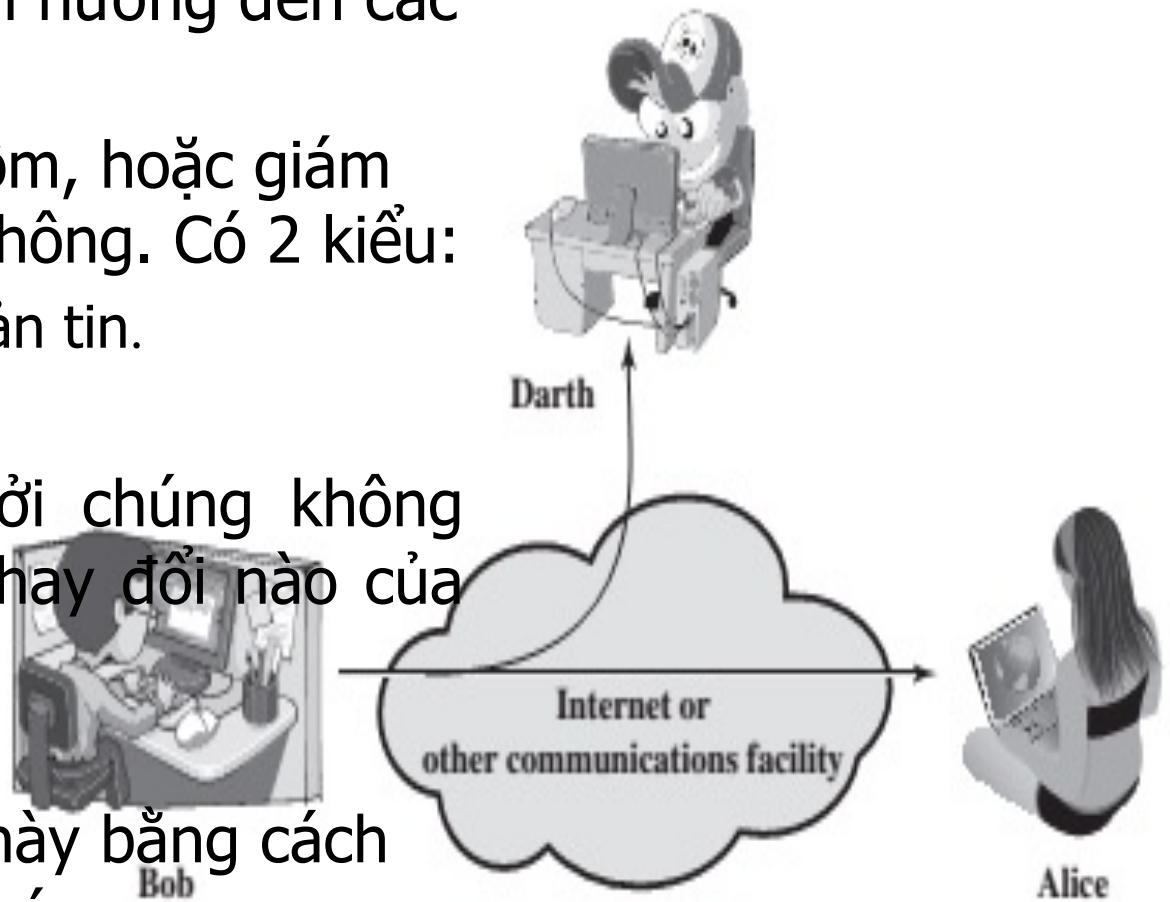
- **Tấn công an toàn**: bất kỳ hành động nào mà làm hại đến tính an toàn thông tin của một tổ chức nào đó.
- **Cơ chế an toàn:** quá trình được thiết kế để phát hiện, ngăn ngừa, hay khôi phục lại các kiểu tấn công an toàn.
- **Dịch vụ an toàn:** dịch vụ truyền thông làm tăng cường tính an toàn của hệ thống xử lý dữ liệu và thông tin của một tổ chức. Các dịch vụ này thường dùng để chống lại các tấn công an toàn, và các dịch vụ này tận dụng một hoặc nhiều cơ chế an toàn để cung cấp dịch vụ.

Tấn công mạng



Tấn công thụ động

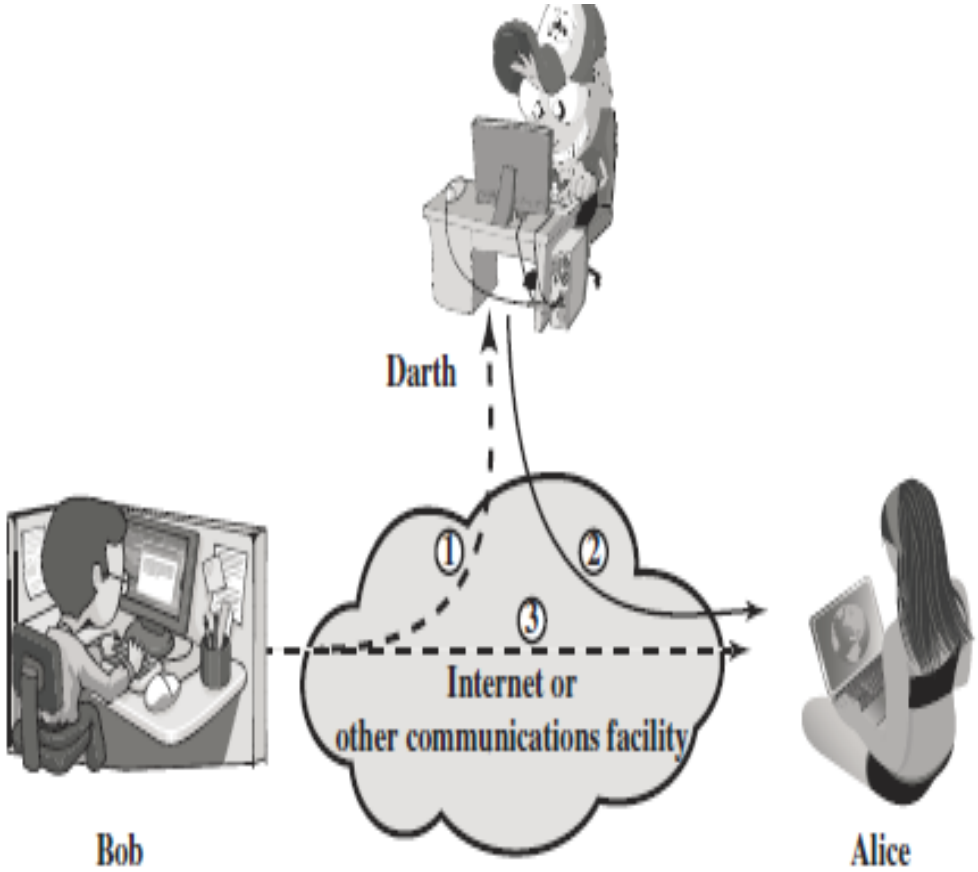
- Là việc cố gắng lấy hoặc lợi dụng thông tin hệ thống nhưng không ảnh hưởng đến các tài nguyên hệ thống
- Là các hành động nghe trộm, hoặc giám sát các hoạt động truyền thông. Có 2 kiểu:
  - Xem trộm các nội dung bản tin.
  - Phân tích luồng thông tin.
- Rất khó để phát hiện, bởi chúng không liên quan đến bất kỳ sự thay đổi nào của dữ liệu
- Ngăn ngừa kiểu tấn công này bằng cách sử dụng các kiểu mật mã hóa



(a) Passive attacks

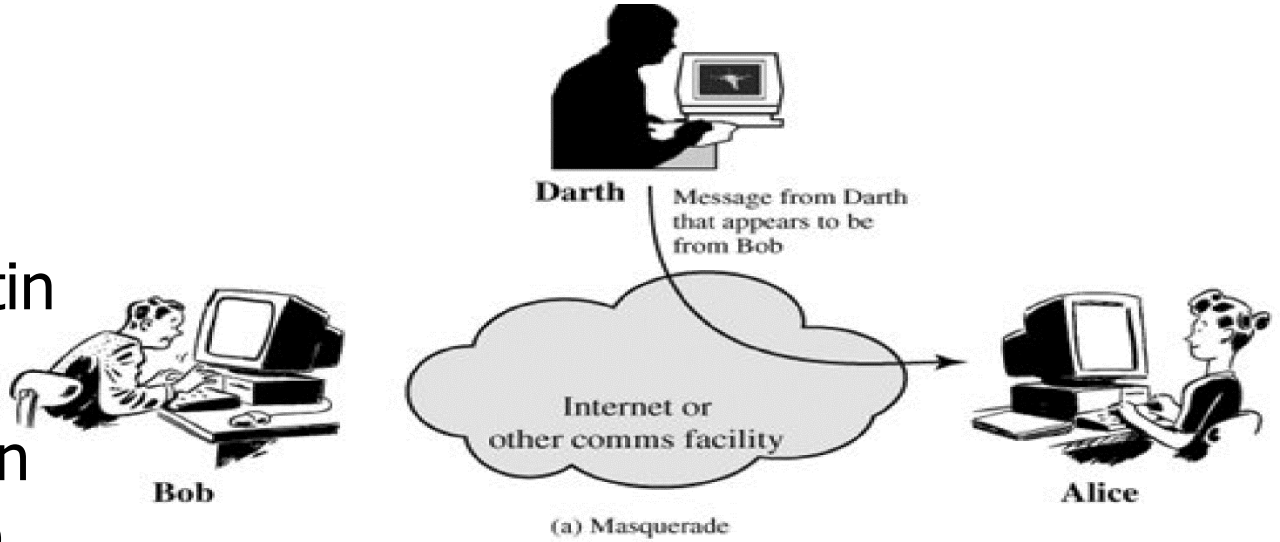
Tấn công tích cực

- Là các hành động cố gắng thay đổi các tài nguyên hệ thống hoặc gây ảnh hưởng đến hoạt động của họ.
- Liên quan đến việc sửa đổi dòng dữ liệu hoặc tạo dòng dữ liệu sai lệch
- Chia thành bốn loại sau: mạo danh (Masquerade), phát lại bản tin (replay), sửa đổi bản tin, và từ chối dịch vụ

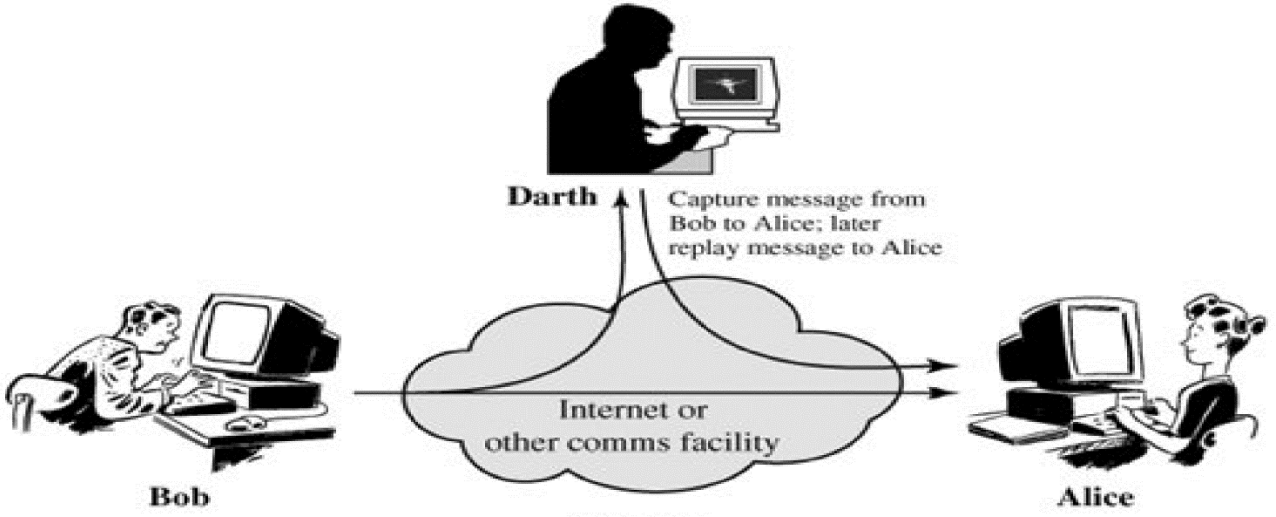


Tấn công tích cực

- **Tấn công mạo danh:** kẻ tấn công mạo danh bên gửi tin để gửi bản tin cho bên nhận.
- **Tấn công phát lại:** liên quan đến việc sao chép thụ động dữ liệu và sau đó gửi lại bản sao chép đó cho bên nhận.



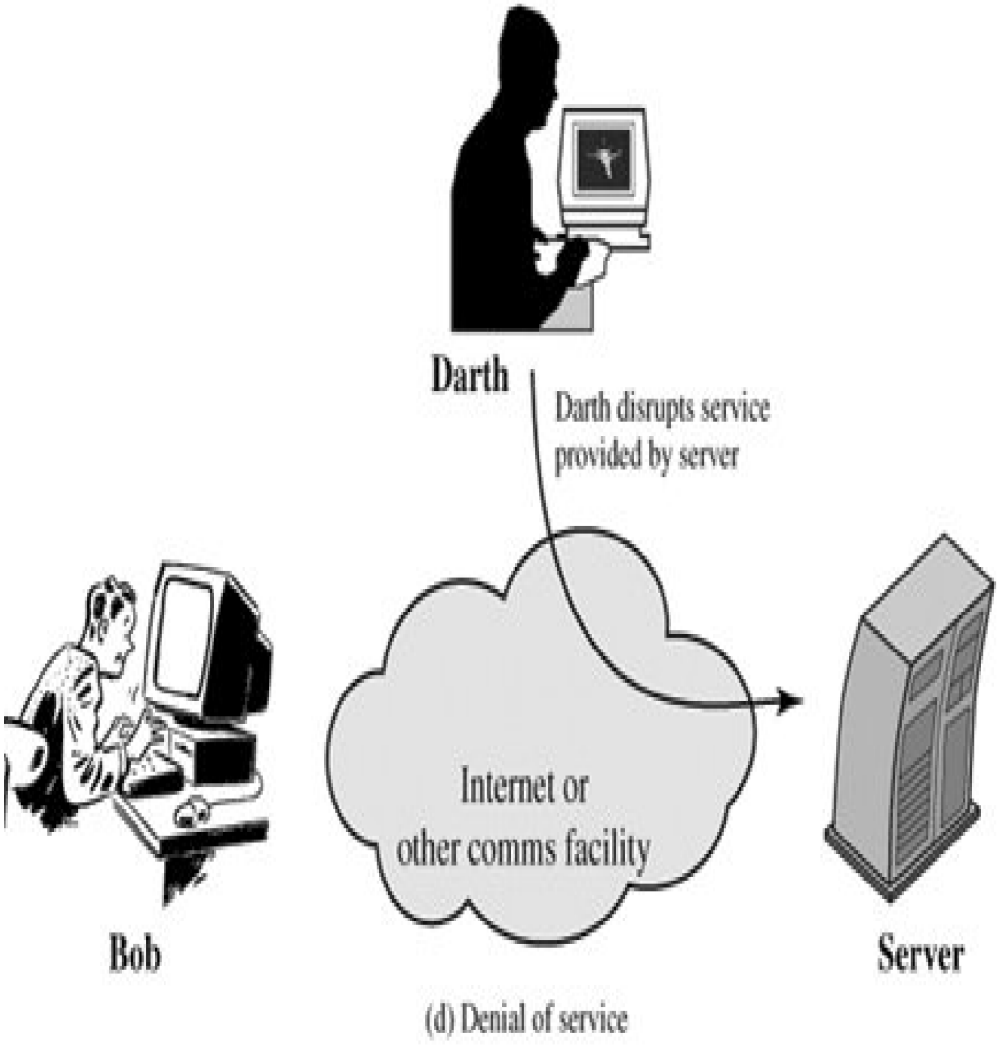
(a) Masquerade



(b) Replay

Tấn công tích cực

- **Thay đổi bản tin:** Darth chặn các bản tin Bod gửi cho Alice và ngăn không cho các bản tin này đến đích. Sau đó Darth thay đổi nội dung của bản tin và gửi tiếp cho Alice.
- **Tấn công từ chối dịch vụ:** kẻ tấn công chặn toàn bộ các bản tin được chuyển tới một đích nào đó, hay làm sập hoàn toàn mạng.



(d) Denial of service

Dịch vụ an toàn

- X.800 định nghĩa dịch vụ an toàn là một dịch vụ được cung cấp bởi lớp giao thức của các hệ thống truyền thông và đảm bảo tính an toàn của các hệ thống hoặc của việc truyền dữ liệu.
- RFC 4949 định nghĩa dịch vụ an toàn thực hiện các chính sách an toàn và được thực thi bởi các cơ chế an toàn.
- X.800 chia các dịch vụ này thành năm loại và 14 dịch vụ

Dịch vụ an toàn (1)

- Dịch vụ xác thực: đảm bảo rằng quá trình truyền thông được xác thực nghĩa là cả người gửi và người nhận không bị mạo danh.
  - *Xác thực toàn bộ các peer: cung cấp chứng thực nhận dạng thực thể peer trong một liên kết.*
  - *Xác thực dữ liệu: cung cấp chứng thực nguồn dữ liệu.*
- Kiểm soát truy cập: đưa ra việc phân quyền để sử dụng các tài nguyên mạng.

Dịch vụ an toàn (2)

- Bảo mật dữ liệu là thực hiện bảo vệ dữ liệu được truyền thông khỏi các kiểu tấn công thụ động.
- Tính toàn vẹn dữ liệu: bảo đảm tính đúng đắn hoặc mức chính xác (dữ liệu chỉ được xử lý bởi quá trình được phân quyền hoặc hành động của các cá nhân hoặc thiết bị được phân quyền) của dữ liệu. Dịch vụ toàn vẹn hướng kết nối đảm bảo rằng các bản tin được nhận mà không bị lặp, chèn, chỉnh sửa, sai thứ tự, hay truyền lại.

Dịch vụ an toàn (3)

- Dịch vụ chống chối bỏ: đưa ra các biện pháp kỹ thuật đối với việc ngăn ngừa cá nhân hoặc thực thể từ chối đã thực hiện một hành động, đặc biệt liên quan đến dữ liệu (nhận và gửi bản tin).
- Tính sẵn sàng: bảo đảm rằng không từ chối truy cập được phân quyền đối với các phân tử mạng, thông tin lưu trữ, luồng thông tin, dịch vụ và ứng dụng do các sự kiện tác động đến mạng đó. Tính sẵn sàng là đặc tính của hệ thống hoặc tài nguyên hệ thống có khả năng truy cập và sử dụng dựa trên nhu cầu bởi một thực thể hệ thống được cấp quyền, tùy thuộc vào các đặc tả hiệu năng của hệ thống đó.

Cơ chế an toàn

- X.800 phân chia các cơ chế an toàn:
  - Các cơ chế được thực thi trong lớp giao thức cụ thể, như TCP hay giao thức lớp ứng dụng,
  - Các cơ chế không cụ thể với bất kỳ lớp giao thức nào hoặc dịch vụ an toàn nào.
- X.800 phân biệt các cơ chế mật mã hóa:
  - Cơ chế mật mã hóa thuật nghịch chỉ đơn giản là thuật toán mật mã cho phép dữ liệu được mật mã hóa và sau đó giải mật mã.
  - Cơ chế mật mã hóa không thuận nghịch gồm các thuật toán hàm băm và các mã xác thực bản tin được sử dụng trong các ứng dụng xác thực và chữ ký điện tử.

Cơ chế an toàn cụ thể

Thường được kết hợp vào lớp giao thức để cung cấp dịch vụ an toàn OSI

- Mật mã hóa: sử dụng các thuật toán mật mã để biến đổi dữ liệu thành một dạng dữ liệu khác
- Chữ ký số: dữ liệu được gắn thêm vào, hoặc biến đổi mật mã của, một đơn vị dữ liệu để cho phép bên nhận dữ liệu đó xác định được bên gửi và tính toàn vẹn dữ liệu, và chống lại được sự giả mạo
- Kiểm soát truy cập: Các cơ chế điều khiển truy nhập được dùng để đảm bảo rằng chỉ có một số người dùng được gán quyền mới có thể truy nhập tới các tài nguyên
- Toàn vẹn dữ liệu: các cơ chế được sử dụng để đảm bảo tính toàn vẹn của một đơn vị dữ liệu hoặc của luồng dữ liệu

Cơ chế an toàn cụ thể

Thường được kết hợp vào lớp giao thức để cung cấp dịch vụ an toàn OSI

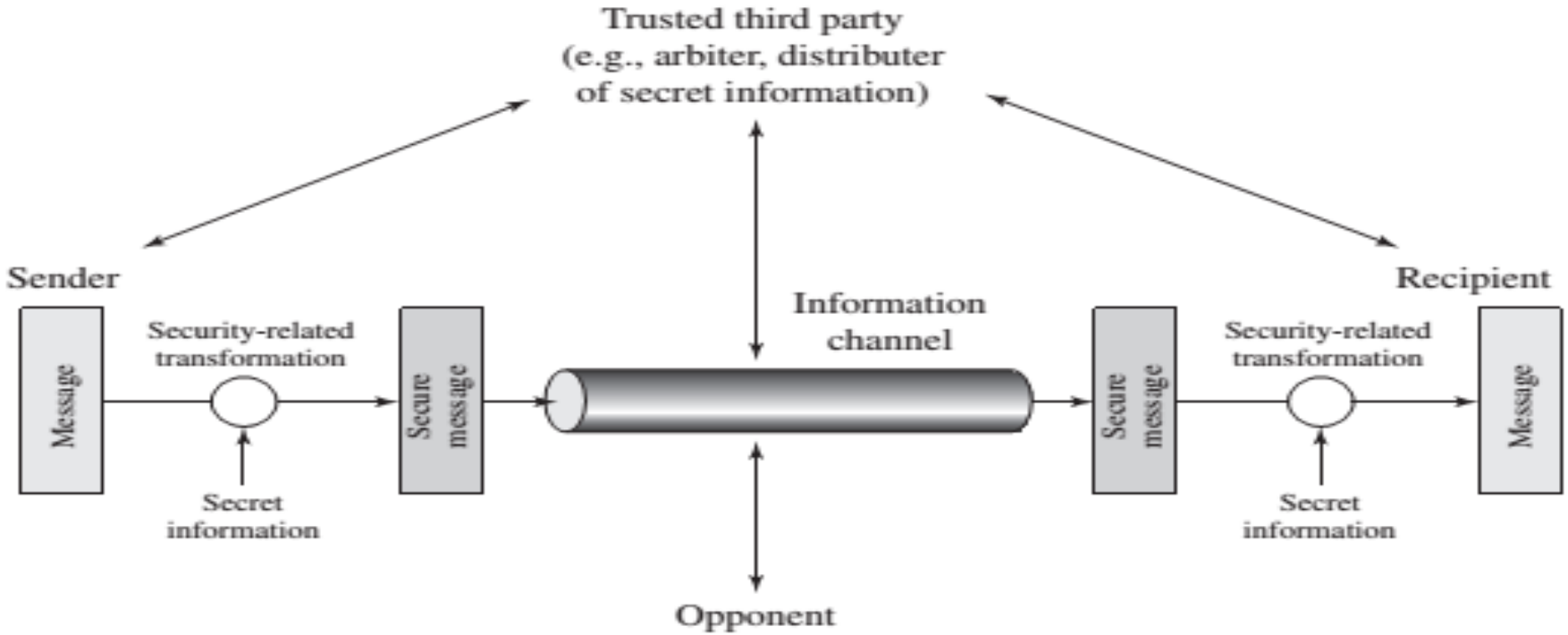
- Xác thực lẫn nhau: được sử dụng để đảm bảo định danh của người dùng bằng cách trao đổi thông tin.
- Độn lưu lượng: chèn các bit vào các khoảng trống của luồng dữ liệu để gây khó khăn cho kiểu tấn công phân tích lưu lượng
- Điều khiển định tuyến: cho phép lựa chọn các tuyến an toàn cụ thể nào đó và cho phép thay đổi định tuyến đặc biệt là khi có lỗ hổng an toàn đang xảy ra
- Chứng nhận từ bên thứ ba: sử dụng bên tin tưởng thứ 3 để đảm bảo các đặc tính xác định nào đó của việc trao đổi dữ liệu

Cơ chế an toàn phổ biến

Không áp dụng cho lớp giao thức hay dịch vụ an toàn OSI cụ thể nào

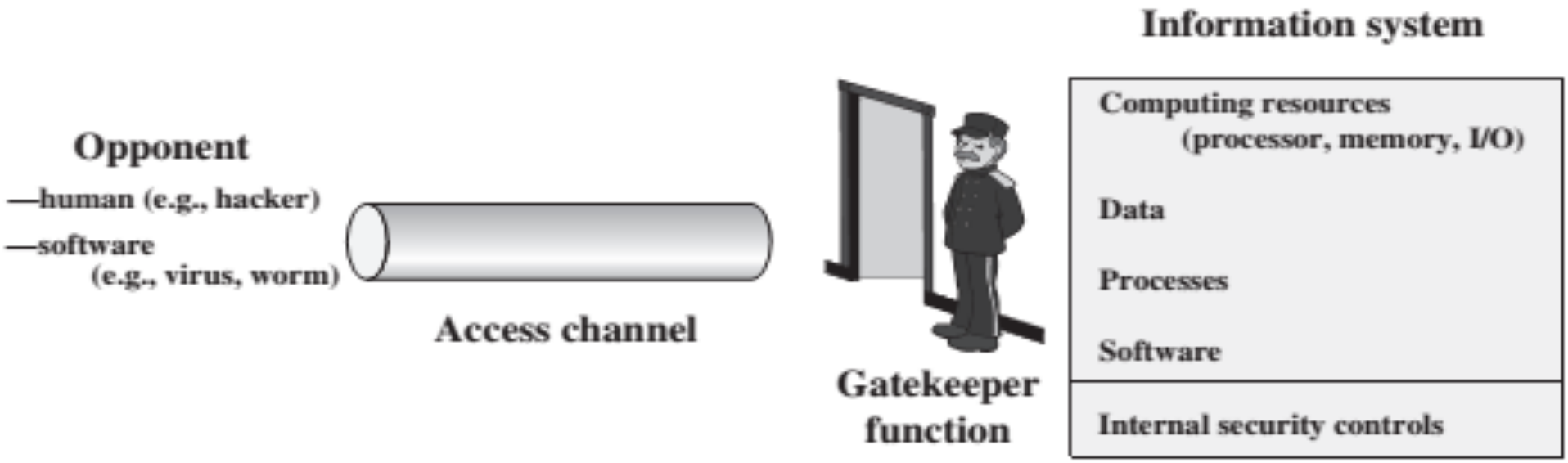
- Tính năng được tin cậy
- Nhãn an toàn
- Phát hiện sự kiện
- Kiểm toán an toàn
- Phục hồi an toàn

Mô hình an toàn mạng



- Kĩ thuật cung cấp tính an toàn:
  - Phép biến đổi an toàn lên thông tin được gửi đi, như mật mã hóa bản tin
  - Khóa bí mật được sử dụng để mật mã hóa bản tin trước khi gửi đi
- Bên thứ ba chứng thực có thể được yêu cầu để đạt được truyền dẫn an toàn: có thể chịu trách nhiệm phân phối thông tin bí mật tới bên gửi và bên nhận mà không bị phát hiện bởi bất cứ kẻ tấn công nào

Mô hình an toàn truy nhập mạng



- Cơ chế an toàn để đối phó với các truy nhập không mong muốn:
  - Chức năng gatekeeper: gồm các thủ tục đăng nhập dựa trên mật khẩu được thiết kế để bảo vệ và loại bỏ các worm, virusm và các kiểu tấn công tương tự khác
  - Các loại điều khiển trong nội bộ nhằm mục đích giám sát các hoạt động và phân tích thông tin lưu trữ để phát hiện ra sự có mặt của kẻ xâm nhập không mong muốn