CHƯƠNG I
GIỚI THIỆU

ThS. Nguyễn Cao Đạt
E-mail: dat@hcmut.edu.vn

Tham khảo

[1]. Cryptography and Network Security: chương 1

[2]. Network Security: A Beginner's Guide: module 1, 2, 3, 4

[3]. http://en.wikipedia.org/wiki/Information_security

NỘI DUNG TRÌNH BÀY

- **Giới thiệu**
- **An toàn thông tin**
- **Chính sách an toàn thông tin**
- **An ninh mạng**
- **An ninh mạng trong thực tế**
- **Thảo luận**

GIỚI THIỆU

- **Một số trích dẫn quan trọng**
  - McAfee
  - Số lượng các cuộc tấn công bằng phần mềm độc hại để thâm nhập hoặc gây hại cho một hệ thống máy tính tăng 500% trong năm 2008 – tương đương với tổng cộng của 5 năm trước đó cộng lại.
  - Trong đó 80% tất cả các cuộc tấn công bằng phần mềm độc hại có động lực là tài chính, với những kẻ tấn công cố ăn cắp thông tin dữ liệu cá nhân vì lợi nhuận; 20% các cuộc tấn công còn lại có các mục đích liên quan tới tôn giáo, gián điệp, khủng bố hoặc chính trị.
  - Dẫn chứng: Mã hóa dữ liệu đòi tiền chuộc, virus đòi tiền chuộc.

GIỚI THIỆU

- **Một số trích dẫn quan trọng**
  - Phát biểu của Barack Obama vào ngày 29/05/2009
  - "Sự thịnh vượng về kinh tế của nước Mỹ trong thế kỷ 21 sẽ phụ thuộc vào an ninh có hiệu quả của không gian mạng, việc đảm bảo an toàn cho không gian mạng là xương sống mà nó làm nền vững chắc cho một nền kinh tế thịnh vượng, một quân đội và một chính phủ mở, mạnh và hiệu quả".
  - "Trong thế giới ngày nay, các hành động khủng bố có thể tới không chỉ từ một ít những kẻ cực đoan đánh bom tự sát, mà còn từ một vài cái gõ bàn phím trên máy tính – một vũ khí huỷ diệt hàng loạt".

GIỚI THIỆU

- **Báo cáo tổng kết an ninh mạng 2020 và dự báo 2021**
- **Báo cáo an ninh mạng 2021 & 2022**
- **Những con số ấn tượng**
  - Các nỗ lực lừa đảo (chiếm 55%), gia tăng phần mềm độc hại
  - malware (28%) và ransomware (19%).
  - Mỗi ngày có hơn 100.000 trang web, 10.000 tập tin độc hại.
  - 87% tổ chức đã bị khai thác một lỗ hổng bảo mật hiện có.
  - 96% các tổ chức quan tâm đến bảo mật đám mây.
  - Việt Nam đã được Liên minh Viễn thông Quốc tế (International Telecommunication Union) xếp hạng thứ 25 trong số 182 quốc gia trong Chỉ số An ninh mạng Toàn cầu (GCI) 2020.

GIỚI THIỆU

- **Dự đoán xu hướng an ninh mạng**
  - 5G được triển khai thương mại hóa từ đầu năm 2021 Điều này dẫn đến nhiều mối nguy cơ mới về bảo mật với các thiết bị liên lạc không dây qua 5G.
  - Các công ty tổ chức bắt đầu chuyển sang sử dụng cloud ngày một nhiều hơn do tiện lợi và an toàn, nhưng việc cấu hình sai và lơ là trong thiết kế có thể gây ra các ảnh hưởng sâu sắc tới an ninh mạng dùng cloud.
  - Gia tăng phòng chống sử dụng các phần mềm lậu bằng cách rà soát, xử phạt các hình vi sử dụng phần mềm không có giấy phép.
  - Lừa đảo thông qua các trang mạng xã hội và đánh cắp các thông tin cá nhân gia tăng nhanh chóng.

NỘI DUNG TRÌNH BÀY

- Giới thiệu
- An toàn thông tin
- Chính sách an toàn thông tin
- An ninh mạng
- An ninh mạng trong thực tế
- Thảo luận

LÀM THẾ NÀO ĐỂ AN TOÀN THÔNG TIN

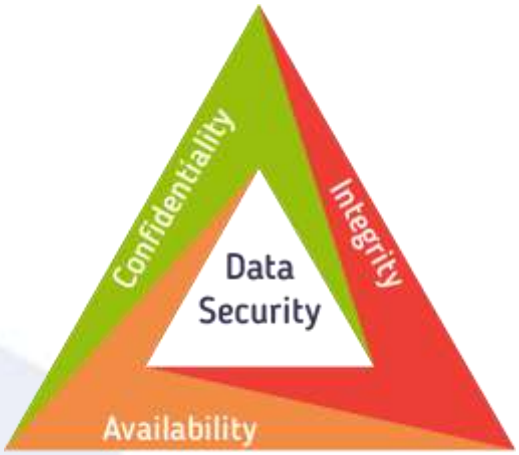
- **Giải pháp an toàn thông tin đơn lẻ**
  - Thường nghĩ đến là xây dựng tường lửa (firewall)
  - Hoặc một cái gì đó tương tự để ngăn chặn các cuộc tấn công và xâm nhập bất hợp pháp.
- **Cách tiếp cận này không hoàn toàn đúng**
  - Những giải pháp công nghệ đơn lẻ không thể cung cấp đủ sự an toàn.
  - Bản chất ATTT không đơn thuần chỉ là sử dụng một số công cụ hoặc một vài giải pháp nào đó mà để đảm bảo ATTT.
  - Cần có một cái nhìn tổng quát và khoa học hơn.

ĐỊNH NGHĨA AN TOÀN THÔNG TIN

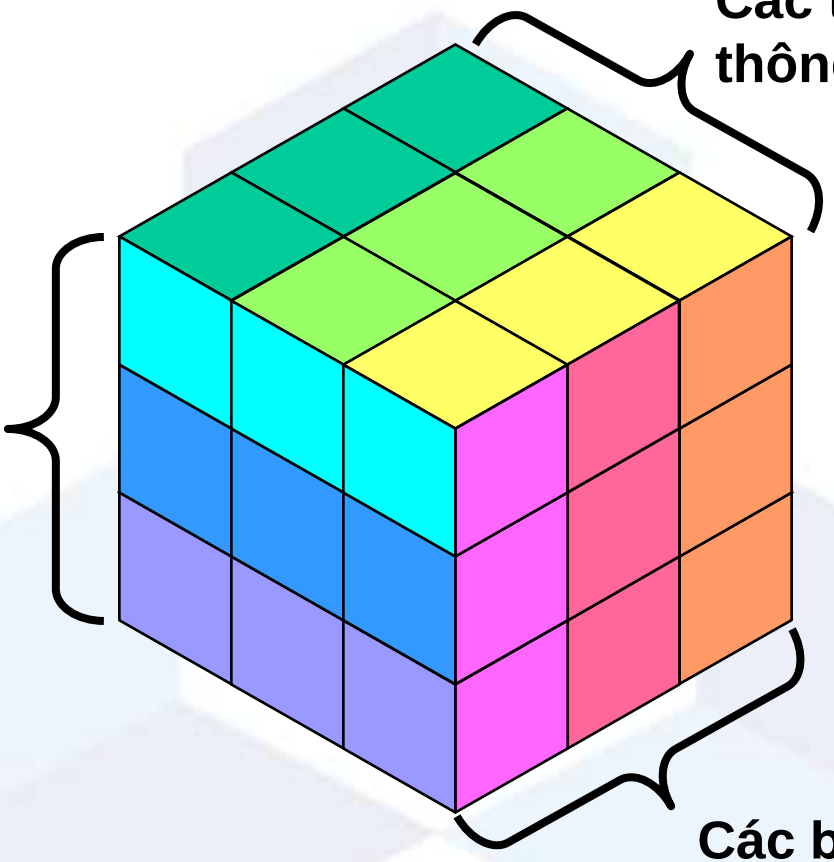
- **An toàn thông tin (*information security*)**
  - Các biện pháp được áp dụng nhằm bảo vệ thông tin và các hệ thống thông tin.
  - Ngăn chặn việc truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi, nghiên cứu, kiểm tra, ghi lại hay tiêu hủy thông tin trái phép.
- **Các thay đổi quan trọng**
  - Sử dụng máy tính để lưu trữ và xử lý thông tin.
  - Sử dụng mạng máy tính để truyền nhận thông tin.

CÁC MỤC TIÊU AN TOÀN THÔNG TIN

- ***Bí mật* (confidentiality)**
  - Ngăn chặn tiết lộ thông tin nhạy cảm từ các người dùng, tài nguyên và quy trình trái phép.
- ***Toàn vẹn* (integrity)**
  - Bảo vệ thông tin hoặc các quy trình khỏi sự sửa đổi có chủ ý hoặc vô tình.
- ***Sẵn sàng* (availability)**
  - Đảm bảo rằng các hệ thống và dữ liệu có thể được truy cập bởi người dùng có quyền khi cần.



MÔ HÌNH AN TOÀN THÔNG TIN



Các trạng thái thông tin

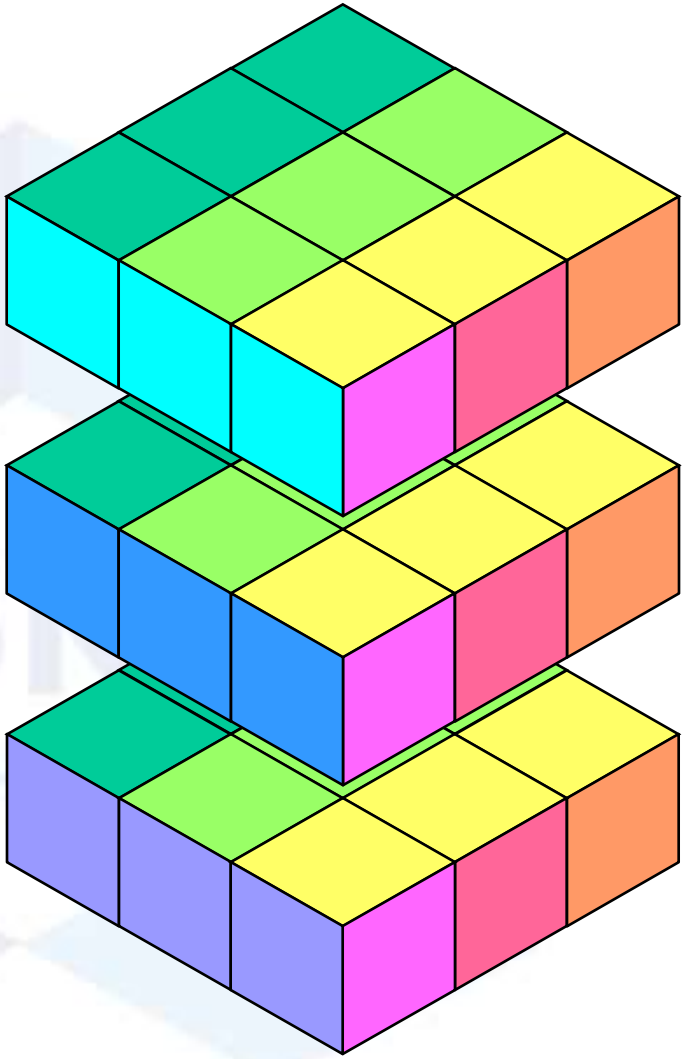
process - save -load

Các thuộc tính an toàn thông tin

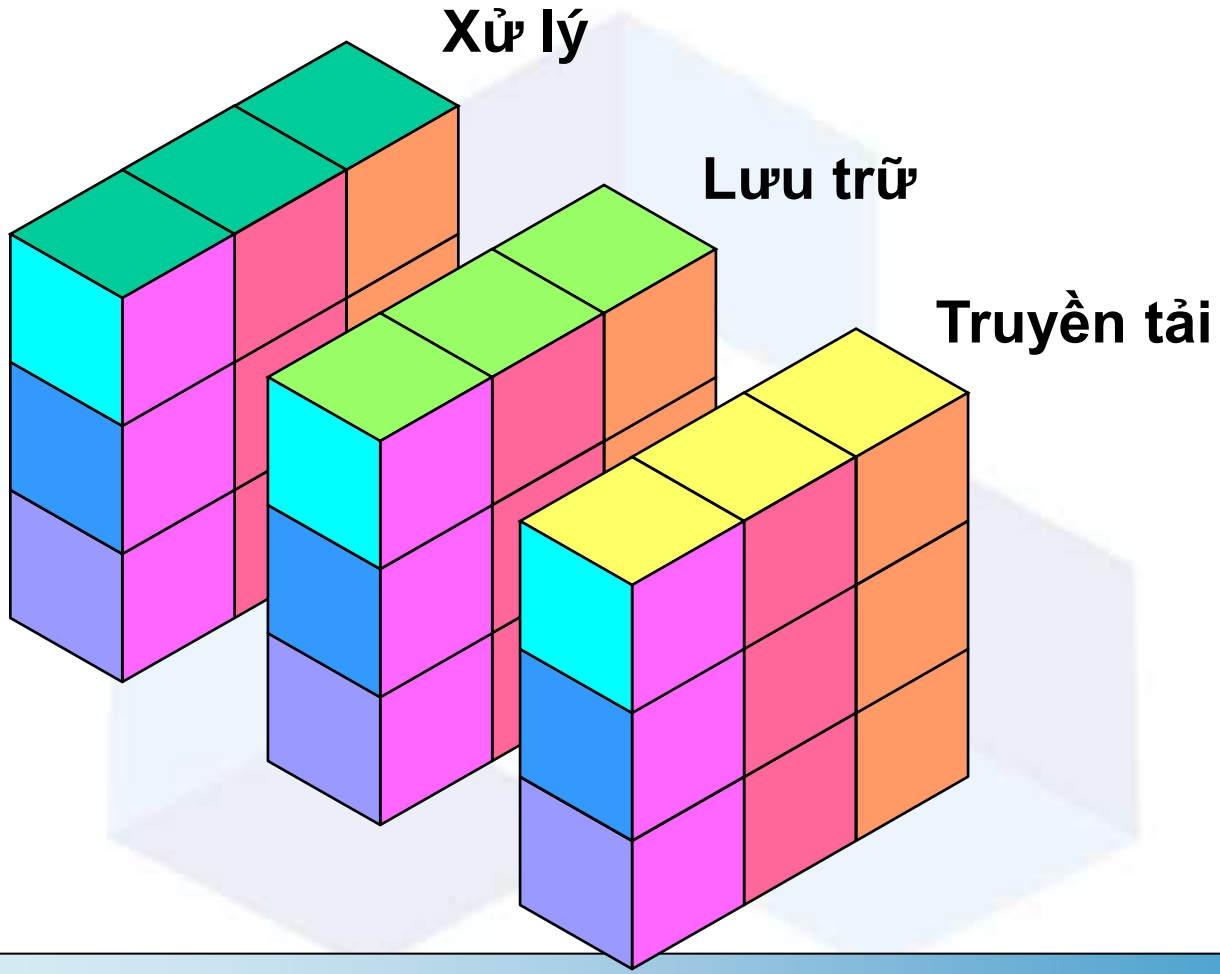
CIA

Các biện pháp đối phó

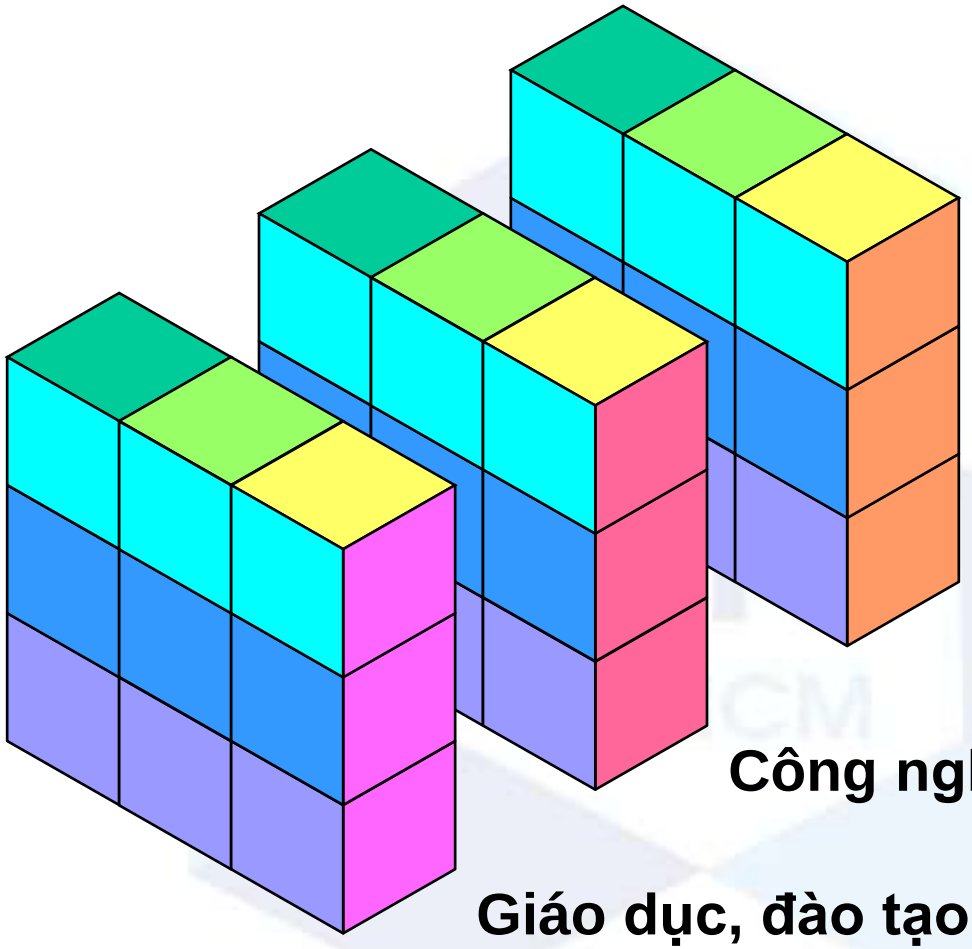
CÁC THUỘC TÍNH AN TOÀN THÔNG TIN



CÁC TRẠNG THÁI THÔNG TIN



CÁC BIỆN PHÁP ĐỐI PHÓ



Chính sách và thủ tục

Công nghệ

Giáo dục, đào tạo và nhận thức

CÁC BIỆN PHÁP ĐỐI PHÓ

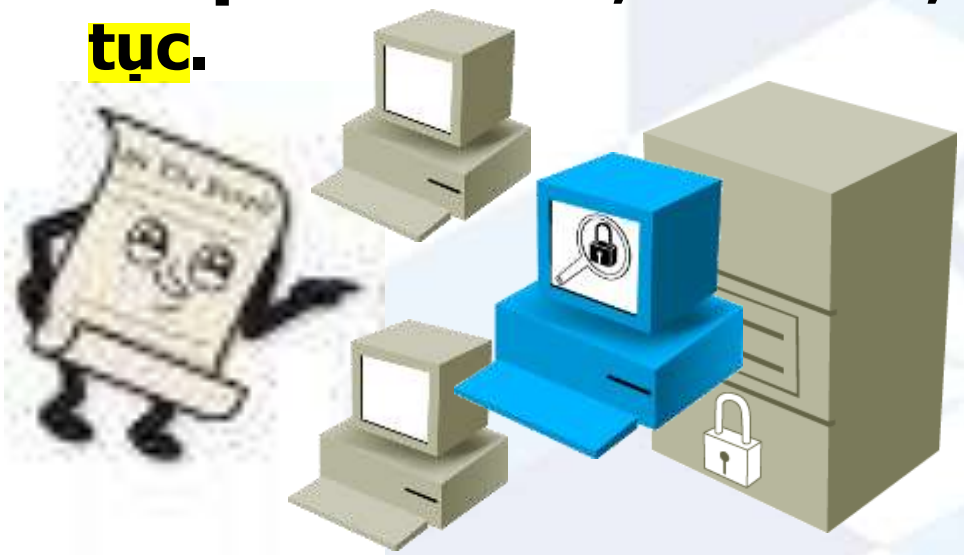
- **Phòng ngừa** - Tập trung vào việc ngăn chặn các vi phạm an ninh thông tin. Ví dụ các giải pháp tường lửa, lọc virus, email giả mạo bên cạnh việc đào tạo nâng cao nhận thức an ninh thông tin.
- **Phát hiện** - Tập trung vào việc phát hiện các vi phạm an toàn thông tin càng nhanh càng tốt. Ví dụ các hệ thống giám sát và phát hiện xâm nhập.
- **Phục hồi** - Tập trung vào việc khôi phục hệ thống sau một cuộc tấn công càng nhanh càng tốt. Ví dụ như giải pháp sao lưu, phục hồi dữ liệu sau thảm họa.

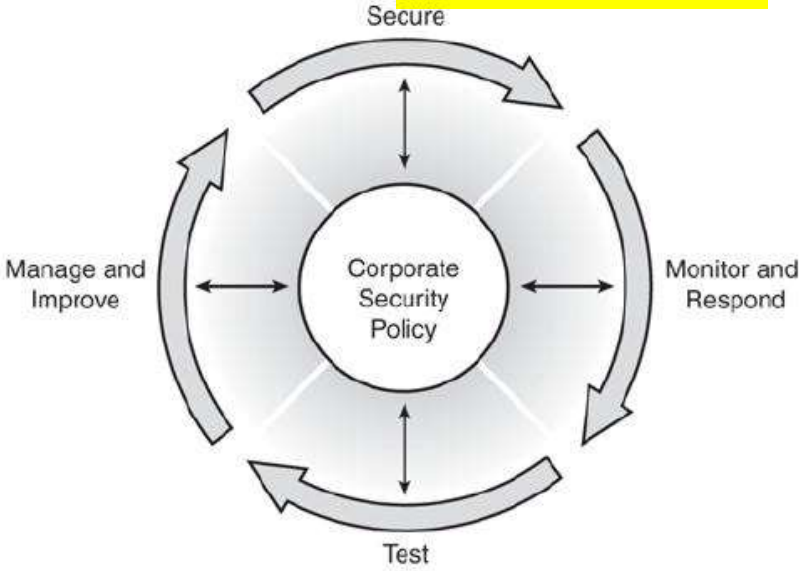
NỘI DUNG TRÌNH BÀY

- Giới thiệu
- An toàn thông tin
- Chính sách an toàn thông tin
- An ninh mạng
- An ninh mạng trong thực tế
- Thảo luận

CHÍNH SÁCH AN TOÀN THÔNG TIN

- Xác định khuôn khổ công việc nhằm bảo vệ tài sản hữu hình và vô hình của mình.
- Phải được viết một cách tổng quát, có tính thực tiễn.
- Được theo dõi, kiểm tra, quản lý và cải tiến liên tục.





CHÍNH SÁCH AN TOÀN THÔNG TIN

- **Ba mục tiêu phải đạt được**
  - Làm rõ cái gì đang được bảo vệ và vì sao phải bảo vệ chúng.
  - Tuyên bố rõ ràng ai là người có trách nhiệm để tạo ra các bảo vệ này.
  - Cung cấp các căn cứ mà theo đó để giải thích và giải quyết mọi tranh chấp sau này khi chúng phát sinh.

VÍ DỤ VỀ CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tất cả người dùng phải có một tài khoản duy nhất bao gồm định danh và mật khẩu phù hợp với tiêu chuẩn của công ty.
- Người dùng không được chia sẻ tài khoản của mình với bất kỳ ai, bất kể chức danh hay chức vụ.
- Mật khẩu không được lưu trữ bằng văn bản hoặc bất kỳ hình thức nào có thể đọc được.
- Nếu nghi ngờ tài khoản bị thỏa hiệp, nó phải được báo cáo cho bộ phận trợ giúp và mật khẩu mới phải được yêu cầu.

CÁC TÀI LIỆU HỖ TRỢ CHÍNH SÁCH

- Tiêu chuẩn: đưa ra các yêu cầu tối thiểu cụ thể trong chính sách.
- Quy tắc: đề xuất cách tốt nhất để hoàn thành một số công việc nhất định
- Thủ tục(hướng dẫn): cung cấp phương thức hoàn thành chính sách

VÍ DỤ VỀ TIÊU CHUẨN MẬT KHẨU

- Chiều dài tối thiểu chiều dài là 8 ký tự
- Phải bao gồm cả ký tự thường và ký tự hoa.
- Phải có ít nhất một ký tự đặc biệt.
- Phải được thay đổi sau 90 ngày.
- Lịch sử mật khẩu của 4 lần sử dụng trước đó phải được lưu lại để tránh tái sử dụng các mật khẩu này.

VÍ DỤ VỀ QUY TẮC, THỦ TỤC

- **Quy tắc tạo mật khẩu**
  - Lấy một cụm từ “”**Up and At em at 7!**”
  - Chuyển thành mật khẩu mạnh **Up&atm@7!**
  - Để tạo mật khẩu khẩu khác từ cụm từ này thì thay đổi số, di chuyển vị trí biểu tượng (@, &), thay đổi dấu chấm câu.
- **Thủ tục(hướng dẫn) thay đổi mật khẩu**
  - Nhấn Ctrl + Alt + Delete để mở hộp thoại login
  - Chọn ”Change Password”
  - Nhập mật khẩu hiện tại vào ô “Old Password”
  - Nhập mật khẩu mới vào ô “New Password”
  - Nhập mật khẩu mới lần nữa vào ô “Confirm Password”
  - Chọn OK để hoàn thành quy trình.

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH

- Tuyên bố của cơ quan thẩm quyền - Giới thiệu về chính sách an toàn thông tin.
- Tiêu đề – Thông tin về miền bảo mật, tên của tổ chức, số tài liệu, ngày hiệu lực, tác giả, ..
- Các mục tiêu – Nêu những gì cố gắng đạt được bằng cách thực hiện chính sách.
- Mục đích - Tại sao chính sách được thông qua và cách thức thực thi chính sách.

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH

- Đối tượng - nêu rõ chính sách dành cho ai
- Tuyên bố chính sách - cách thực hiện chính sách
- Ngoại lệ - tình huống đặc biệt, ngoại lệ với các quy tắc thông thường.
- Điều khoản thi hành chính sách - hậu quả đối với vi phạm
- Các định nghĩa – Diễn giải các thuật ngữ để đảm bảo rằng đối tượng hiểu chính sách

NỘI DUNG TRÌNH BÀY

- Giới thiệu
- An toàn thông tin
- Chính sách an toàn thông tin
- An ninh mạng
- An ninh mạng trong thực tế
- Thảo luận

AN NINH MẠNG

- **Các biện pháp được áp dụng nhằm bảo vệ cơ sở hạ tầng mạng và dữ liệu trong quá trình truyền tải.**
- **Các nguyên tắc cốt lõi**
  - **Bí mật**(Confidentiality): Chỉ bên gửi và bên nhận mới hiểu được nội dung thông điệp.
  - **Toàn vẹn**(Integrity): Đảm bảo thông tin hệ thống, dữ liệu truyền nhận trên mạng không bị thay đổi mà không bị phát hiện.
  - **Sẵn sàng**(Availability): Đảm bảo các dịch vụ trên mạng phải có thể truy cập và có sẵn cho người dùng hợp lệ.

AN NINH MẠNG

- **Các nguyên tắc bổ sung**
  - **Xác thực**(Authentication): Xác nhận rằng các bên liên quan trong một giao dịch trên mạng đúng là những thực thể mà họ đã tuyên bố.
  - **Cấp quyền**(Authorization): Các quyền được cấp cho một cá nhân (hoặc tiến trình) mà chúng cho phép truy cập vào một tài nguyên nào đó trên mạng.
  - **Chống thoái thác**(Non-repudiation): Các bên trong một giao dịch trên mạng không thể phủ nhận các giao tác đã thực hiện.

KIẾN TRÚC AN NINH OSI

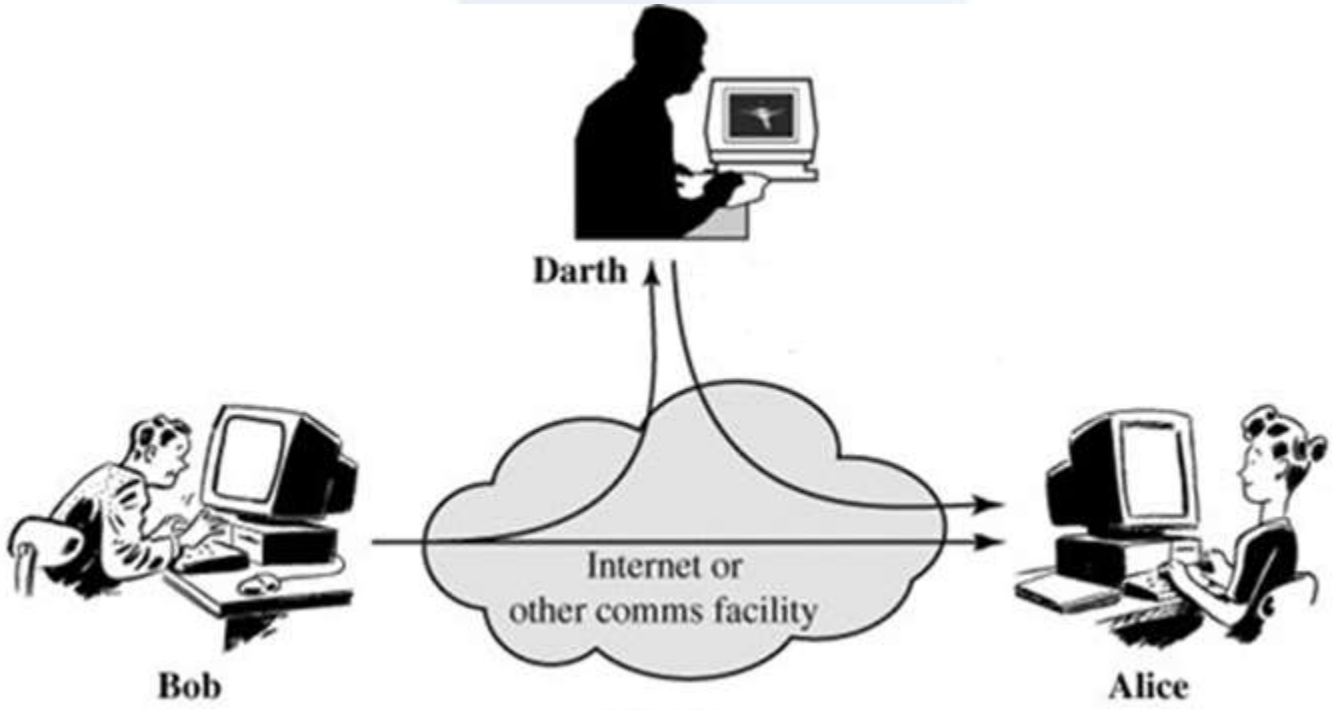
- **Khuyến nghị ITU-TX.800**
  - http://www.itu.int/rec/T-REC-X.800-199103-I/e
  - Định nghĩa một cách có hệ thống về các khía cạnh và các yêu cầu an ninh cần thiết.
  - Hữu ích cho các nhà quản lý trong việc tổ chức thực hiện nhiệm vụ an ninh thông tin.

CÁCH KHÍA CẠNH AN NINH

- **Các khía cạnh được đưa ra trong X.800**
  - Tấn công an ninh.
  - Cơ chế an ninh.
  - Dịch vụ an ninh.

CÁC HÌNH THỨC TẤN CÔNG

- **Tấn công**
  - Bất kỳ hành động vi phạm các nguyên tắc an ninh mạng thuộc sở hữu của một tổ chức.



CÁC HÌNH THỨC TẤN CÔNG

- **Ai có thể mà Bob, Alice**
  - Người dùng (trên Messenger, ..)
  - Máy chủ Web và trình duyệt Web trên các giao dịch trực tuyến
  - Ngân hàng trực tuyến, ATM
  - Máy chủ phân giải tên miền
  - Trao đổi thông tin giữa các bộ định tuyến
  - …

CÁC HÌNH THỨC TẤN CÔNG

- **Ai có thể là Darth(kẻ xâm nhập)**
  - **Phần mềm độc hại** trên thiết bị như botnet, backdoor, viruses, worms.
  - **Nghe lén trên mạng** lấy nội dung thông điệp.
  - Chủ động **chèn, thay đổi, xóa** thông điệp trên kết nối.
  - **Mạo danh:** Giả mạo địa chỉ nguồn(hay các trường khác) trong gói tin ví dụ **IP Spoofing, ..**
  - **Không tặc(hijacking):** Tiếp quản kết nối liên tục bằng cách loại bỏ bên gửi hoặc bên nhận, tự đặt mình vào vị trí đã loại bỏ.
  - **Từ chối dịch vụ:** Ngăn không cho người dùng hợp lệ sử dụng dịch vụ
  - …

CÁC HÌNH THỨC TẤN CÔNG

- ***Phân loại theo cấu trúc***
  - ***Tấn công có cấu trúc***
    - Đến từ các tin tặc có động lực và có năng lực kỹ thuật.
    - Họ hiểu, phát triển và sử dụng các kỹ thuật tấn công tinh vi để thâm nhập vào mạng các tổ chức mà không bị nghi ngờ.
    - Các nhóm này thường liên quan đến các vụ lừa đảo và trộm cắp lớn.
  - ***Tấn công phi cấu trúc***
    - Hầu hết là các cá nhân thiếu kinh nghiệm sử dụng các công cụ tấn công dễ dàng có sẵn.
    - Ngay cả các tấn công phi cấu trúc chỉ được thực hiện với mục đích thử nghiệm và thách thức các kỹ năng của tin tặc, chúng vẫn có thể gây thiệt hại nghiêm trọng cho một tổ chức.

CÁC HÌNH THỨC TẤN CÔNG

- ***Phân loại theo phạm vi***
  - ***Tấn công từ ngoài***
    - Được khởi xướng bởi các cá nhân hoặc nhóm làm việc bên ngoài
    - Họ không có quyền truy cập vào các hệ thống hoặc mạng
    - Họ thu thập thông tin chủ yếu từ các điểm truy nhập mạng và sau đó xâm nhập mạng
  - ***Tấn công nội bộ***
    - Phổ biến và nguy hiểm hơn
    - Các cuộc tấn công nội bộ được bắt đầu bởi một người có quyền truy cập vào mạng
    - Theo FBI, tấn công nội bộ lạm dụng chiếm 60% đến 80% các sự cố được báo cáo
    - Những cuộc tấn công này thường đến từ những nhân viên bất mãn

CÁC HÌNH THỨC TẤN CÔNG

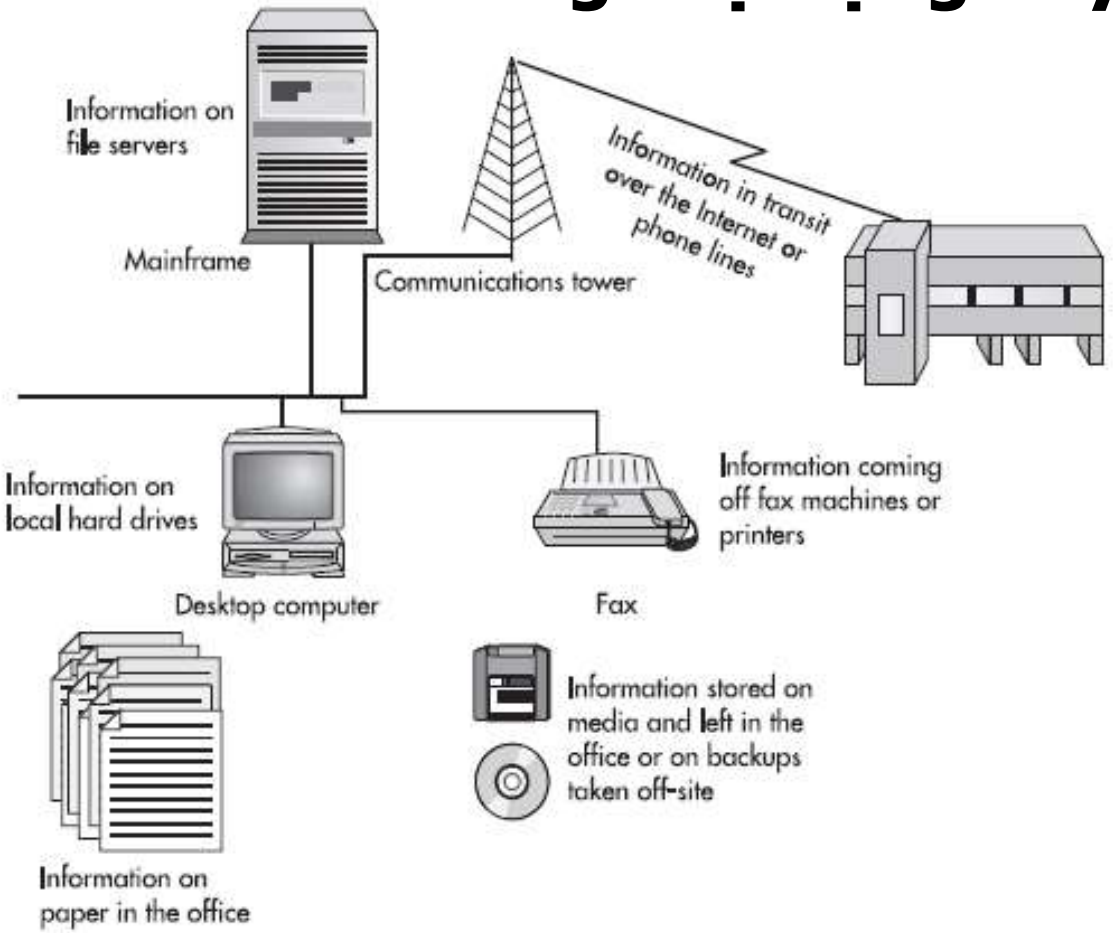
- **Phân loại theo kỹ thuật**
  - Gồm 2 loại chính là tấn công thụ động và tấn công chủ động.
  - Tấn công thụ động là các hành động lấy ra nội dung thông điệp hay phân tích lưu lượng.
  - Tấn công chủ động là các hành động thay đổi nội dung dòng dữ liệu hoặc tạo ra dòng dữ liệu sai lệch.

CÁC HÌNH THỨC TẤN CÔNG

- **Tấn công thụ động**
  - Rất khó để phát hiện.
  - Cần có biện pháp để ngăn chặn.
- **Tấn công chủ động**
  - Khá khó khăn để ngăn chặn.
  - Mục tiêu cần thiết là phát hiện và phục hồi từ bất kỳ sự gián đoạn hoặc chậm trễ do chúng gây ra.

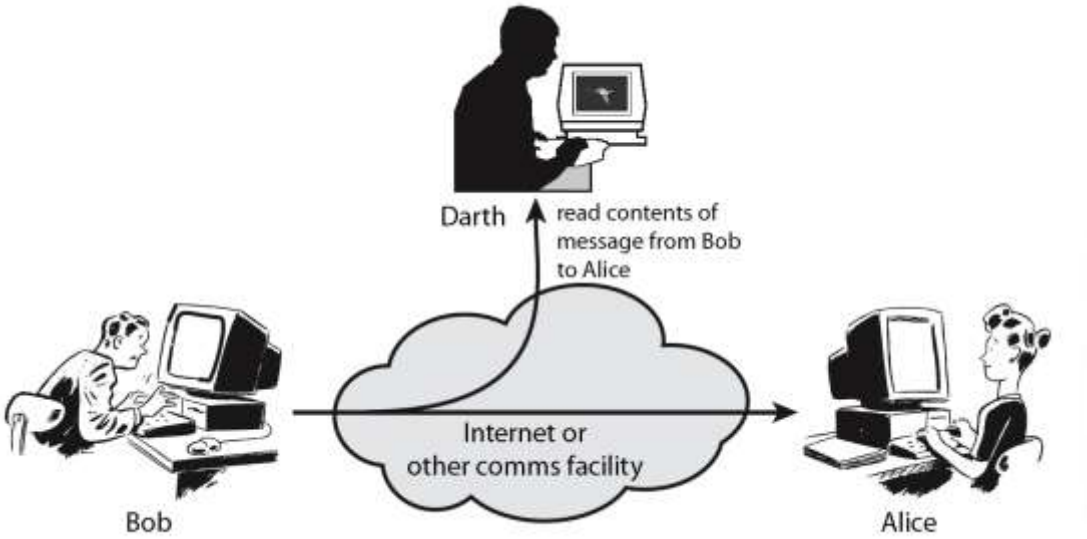
TẤN CÔNG THỤ ĐỘNG

- **Các nơi mà tấn công thụ động xảy ra**



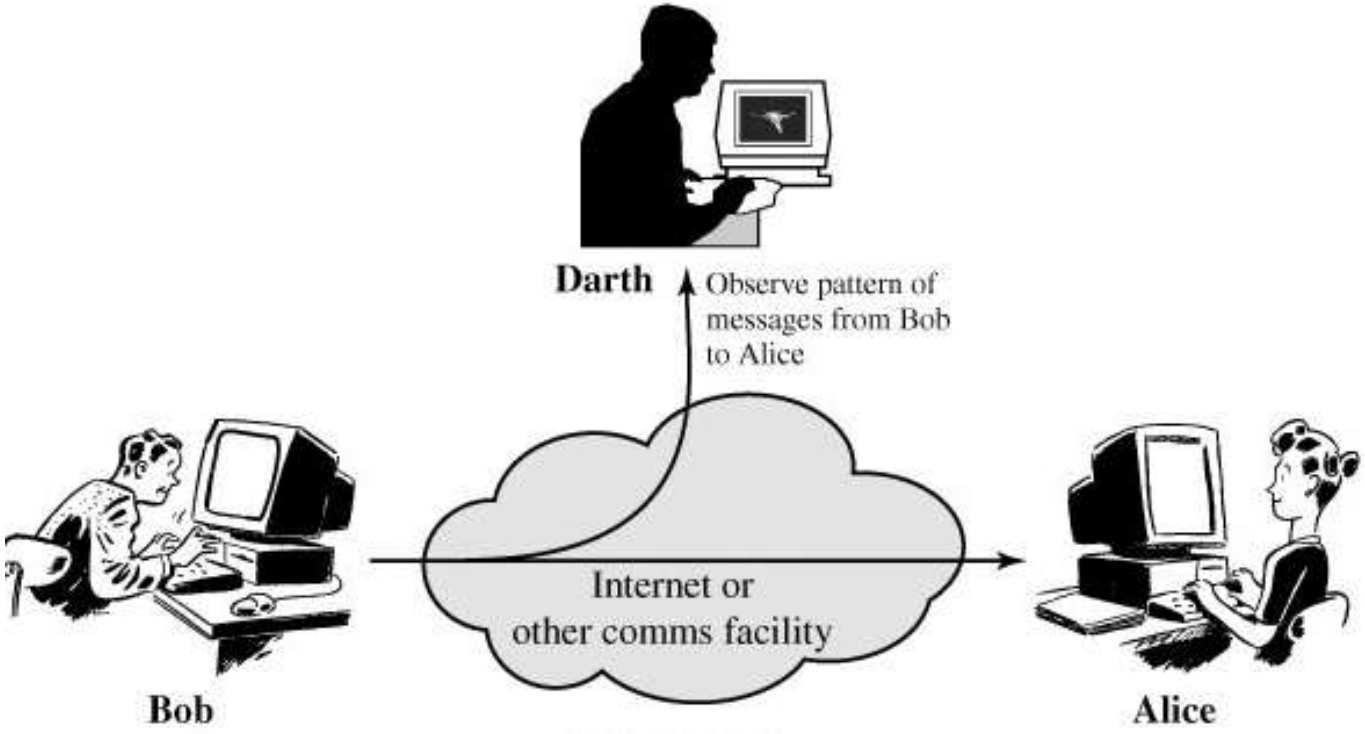
TẤN CÔNG THỤ ĐỘNG

- **Lấy ra nội dung thông điệp** confident
  - Nghe lén(eavesdropping)
  - Nghe trộm ở một vị trí nào đó mà thông điệp đi qua.
  - Mạng không dây dễ dàng bị tấn công dạng này.



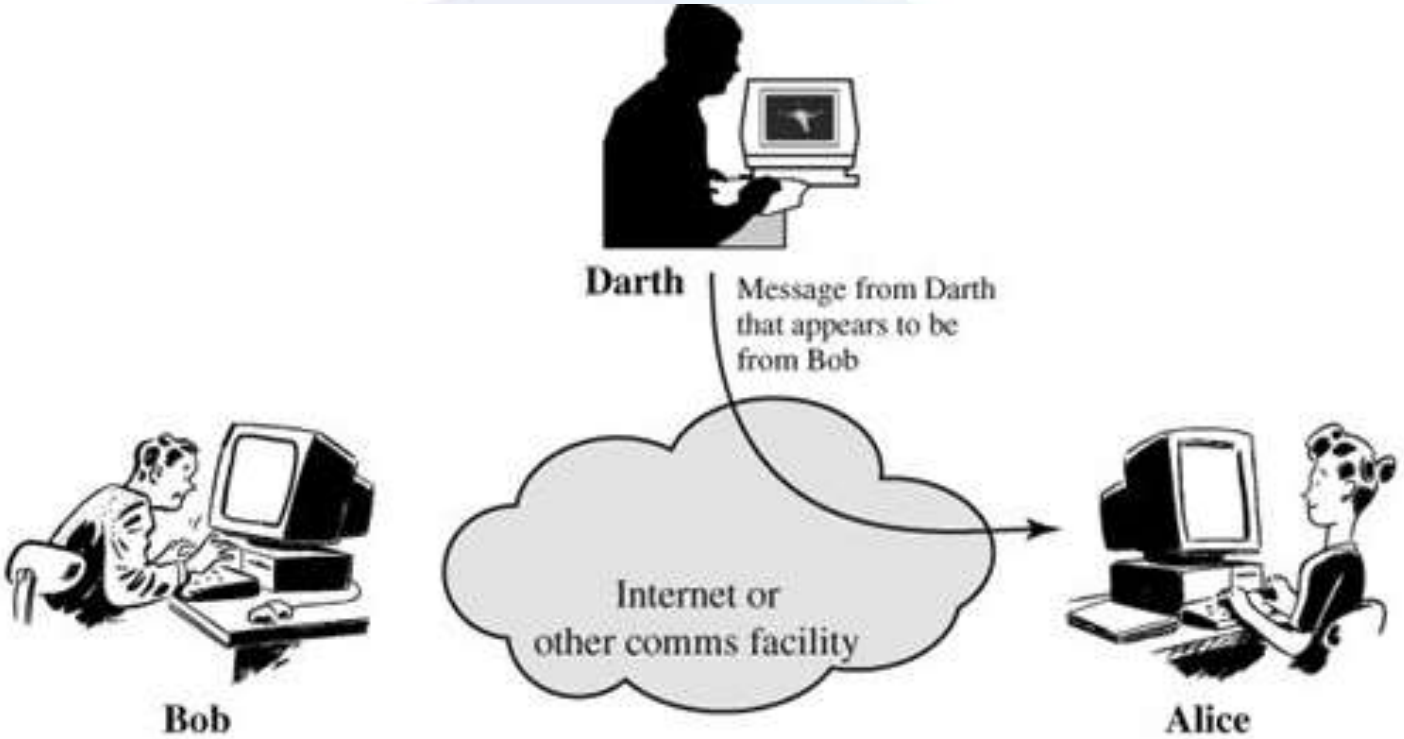
TẤN CÔNG THỤ ĐỘNG

- **Phân tích lưu lượng** confident
  - Quan sát khuôn mẫu của các thông điệp.



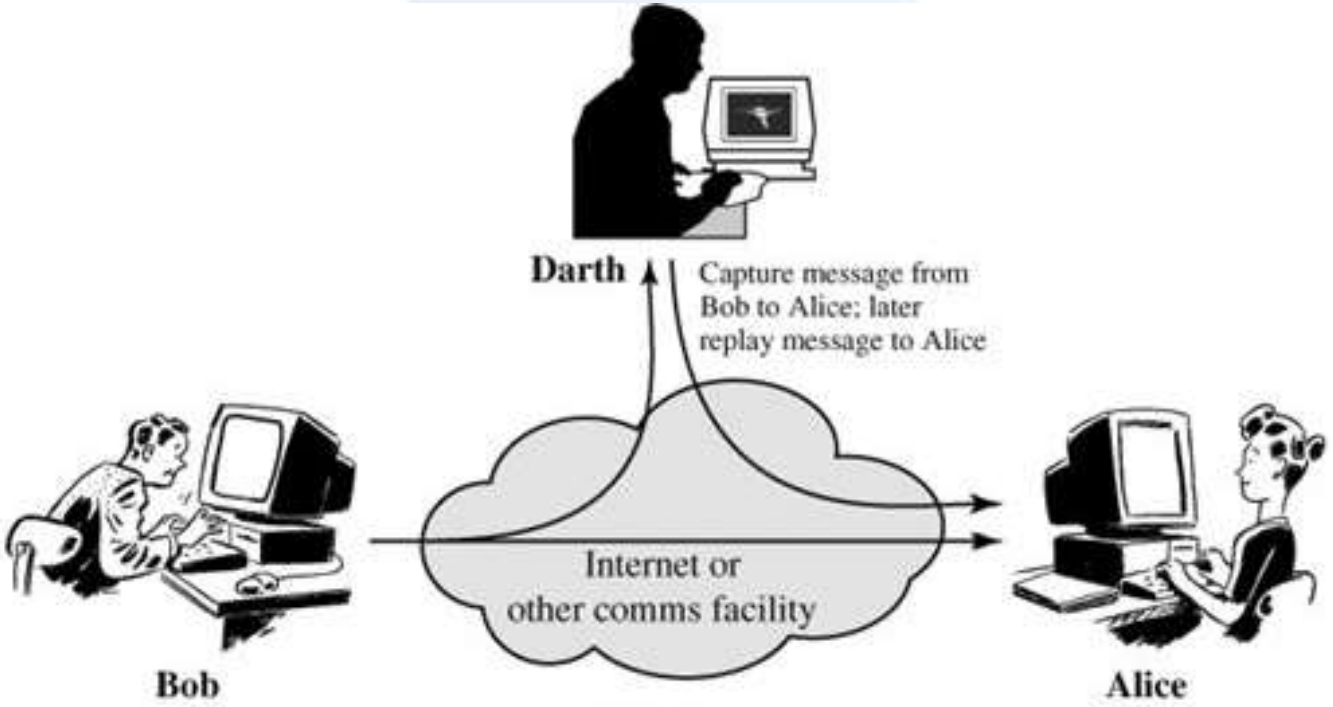
TẤN CÔNG CHỦ ĐỘNG

- **Giả mạo(masquerade)** author
  - Mạo danh một thực thể có đặc quyền.



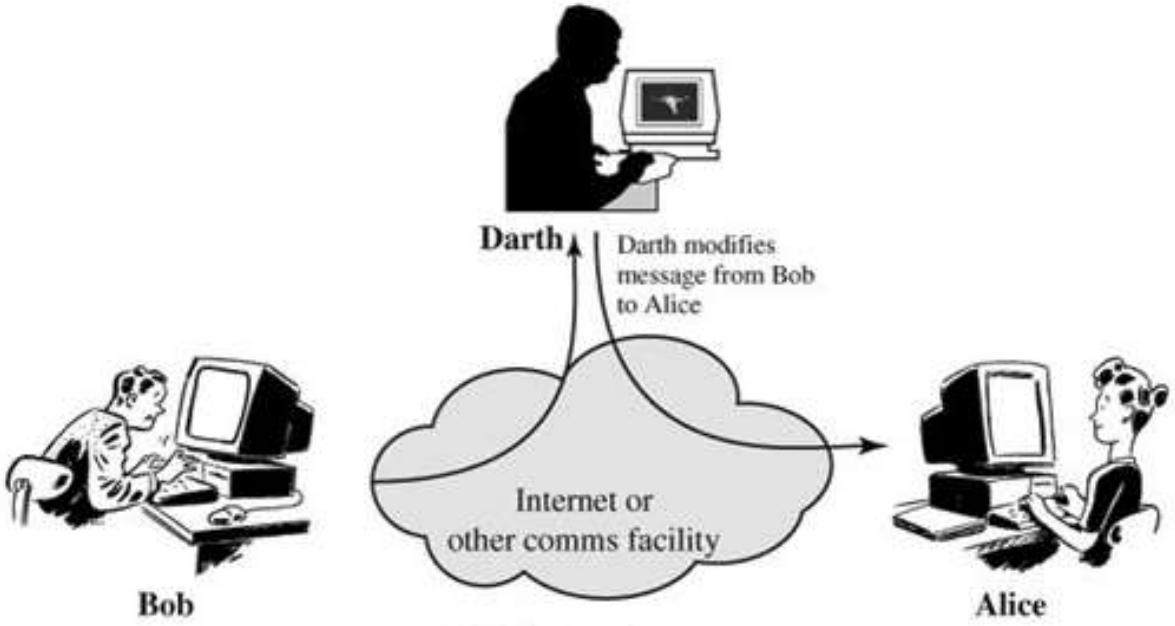
TẤN CÔNG CHỦ ĐỘNG

- **Phát lại(replay)** integrity
  - Bắt thụ động một đơn vị dữ liệu và truyền lặp lại đơn vị dữ liệu này để tạo ra một hiệu ứng trái phép.



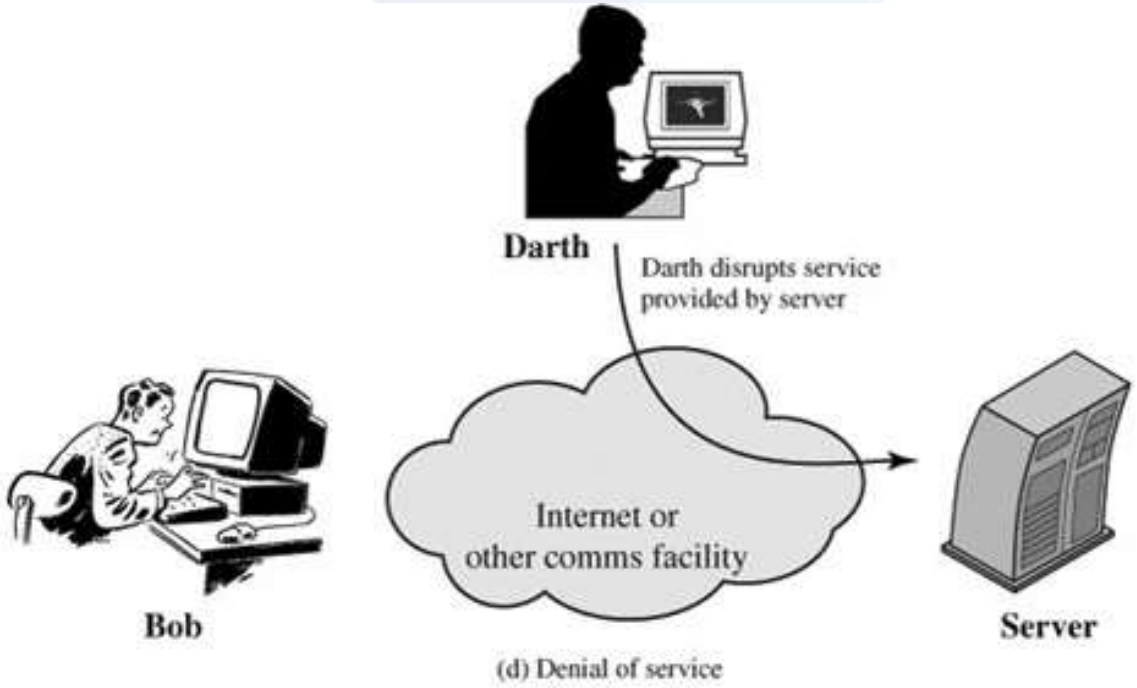
TẤN CÔNG CHỦ ĐỘNG

- **Thay đổi nội dung thông điệp** integrity
  - Một số phần của thông điệp hợp pháp được thay đổi, hoặc các thông điệp được trì hoãn hoặc sắp xếp lại, để tạo ra một hiệu ứng trái phép.



TẤN CÔNG CHỦ ĐỘNG

- **Từ chối dịch vụ** available
  - Ngăn chặn hoặc hạn chế việc sử dụng bình thường hoặc quản lý các tài nguyên trong vấn đề truyền thông.



(d) Denial of service

CÁC BIỆN PHÁP ỨNG PHÓ

- **Tấn công thụ động**
  - Ngăn chặn bằng an ninh truyền thông.
- **Tấn công chủ động**
  - Phát hiện/ngăn chặn không đầy đủ bằng an ninh truy cập mạng.
- **Khôi phục hệ thống sau tấn công chủ động**
  - Cần phân tích rủi ro xung quanh từng tình huống có thể xày ra
  - Xác định tập hợp dữ liệu nào có liên quan.
  - Tiến hành sao lưu định kỳ để đảm bảo khả năng khôi phục bất kỳ loại dữ liệu, ứng dụng và hệ thống nào bị ảnh hưởng.
  - Kế hoạch sao lưu và khôi phục hệ thống phải được viết thành văn bản và phải xác định ai là người chịu trách nhiệm cho các hành động.

CÁC CƠ CHẾ AN NINH

- **Cơ chế an ninh**
  - Một quá trình (hoặc một thiết bị) được thiết kế để phát hiện, ngăn chặn, hoặc phục hồi hệ thống khi có cuộc tấn công bảo mật.
- **Phân loại**
  - Các cơ chế an ninh cụ thể: mã hóa, chữ ký số, kiểm soát truy cập, toàn vẹn dữ liệu, xác thực giao dịch, chèn thông tin trong lưu thông, điều khiển định tuyến, công chứng.
  - Các cơ chế an ninh phổ biến khác. backup, recovery

CÁC CƠ CHẾ AN NINH CỤ THỂ

- **Mã hóa**
  - Sử dụng các thuật toán để chuyển đổi dữ liệu thành một hình thức nào đó mà không phải dễ dàng hiểu. Việc chuyển đổi và phục hồi dữ liệu phụ thuộc vào một thuật toán với không có khóa hay một hoặc nhiều khóa.
- **Chữ ký số**
  - Dữ liệu được nối thêm vào hoặc chuyển đổi mã cho phép người nhận chứng minh nguồn gốc và tính toàn vẹn của dữ liệu.
  - Chống giả mạo.

CÁC CƠ CHẾ AN NINH CỤ THỂ

- **Kiểm soát truy cập**
  - Một loạt các cơ chế kiểm soát các quyền truy cập vào các tài nguyên.
- **Toàn vẹn dữ liệu**
  - Một loạt các cơ chế được sử dụng để đảm bảo tính toàn vẹn một đơn vị dữ liệu hoặc dòng các đơn vị dữ liệu.
- **Trao đổi xác thực**
  - Cơ chế nhằm đảm bảo danh tính một thực thể bằng phương tiện trao đổi thông tin.

CÁC CƠ CHẾ AN NINH CỤ THỂ

- **Chèn thông tin trong lưu thông mạng**
  - Chèn các bit vào những khoảng trống trong một dòng dữ liệu làm thất bại những nỗ lực phân tích lưu lượng.
- **Điều khiển định tuyến**
  - Cho phép lựa chọn các tuyến đường đặc biệt an toàn cho dữ liệu nhất định và cho phép thay đổi định tuyến, đặc biệt là khi một hành vi vi phạm an ninh bị nghi ngờ.
- **Công chứng**
  - Sử dụng một bên thứ ba đáng tin cậy để đảm bảo các thuộc tính nhất định của một giao dịch trao đổi dữ liệu.

CÁC DỊCH VỤ AN NINH

- **Dịch vụ an ninh**
  - Một dịch vụ truyền thông được cung cấp bởi một hệ thống nhằm bảo vệ tài nguyên hệ thống theo một hình thức cụ thể nào đó.
  - Dịch vụ an ninh thực hiện các chính sách an ninh và được hiện thực bởi các cơ chế an ninh.

CÁC DỊCH VỤ AN NINH

- **Bao gồm**
  - Dịch vụ xác thực
  - Dịch vụ kiểm soát truy cập
  - Dịch vụ bí mật dữ liệu, dòng thông tin
  - Dịch vụ toàn vẹn dữ liệu
  - Dịch vụ chống thoái thác
  - Dịch vụ sẵn sàng = sum(n - 1)

DỊCH VỤ XÁC THỰC

- Nhằm xác thực các thực thể hoặc nguồn gốc dữ liệu.
- **Bao gồm:**
  - Xác thực thực thể ngang hàng nhằm chống các tấn công giả mạo và phát lại.
  - Xác thực nguồn gốc dữ liệu nhằm chống tấn công giả mạo.

DỊCH VỤ KIỂM SOÁT TRUY CẬP

- Trong ngữ cảnh an ninh mạng, kiểm soát truy cập là khả năng kiểm soát truy cập đến các hệ thống và các ứng dụng thông qua các liên kết thông tin liên lạc.
- Để đạt được điều này, mỗi thực thể phải được xác định hoặc chứng thực, sau đó quyền truy cập được thay đổi đối với mỗi thực thể.

DỊCH VỤ BÍ MẬT DỮ LIỆU, DÒNG THÔNG TIN

- Bảo vệ dữ liệu, dòng thông tin được truyền nhằm chống lại các tấn công thụ động.
- **Bao gồm:**
  - Dịch vụ bí mật dữ liệu nhằm chống lại tấn công lấy ra nội dung của thông điệp.
  - Dịch vụ bí mật dòng thông tin trên mạng nhằm chống lại tấn công phân tích lưu thông mạng.
  - Áp dụng trên dòng các thông điệp, thông điệp đơn hoặc một vài trường trong thông điệp.

DỊCH VỤ TOÀN VẸN DỮ LIỆU

- Đảm bảo dữ liệu nhận được là chính xác và được gởi từ một thực thể có quyền.
- **Bao gồm:**
  - Dịch vụ toàn vẹn có hướng kết nối: xem xét trên dòng các thông điệp để chắn chắn các thông điệp này là được nhân như khi gởi, không nhân bản, không thêm bớt, không thay đổi, không sắp xếp lại, không phát lại.
  - Dịch vụ toàn vẹn không hướng kết nối: xem xét trên từng thông điệp cụ thể để chắn chắn thông điệp này là được nhân như khi gởi, không thay đổi.
  - Các dịch vụ có khả năng phục hồi hoặc không.

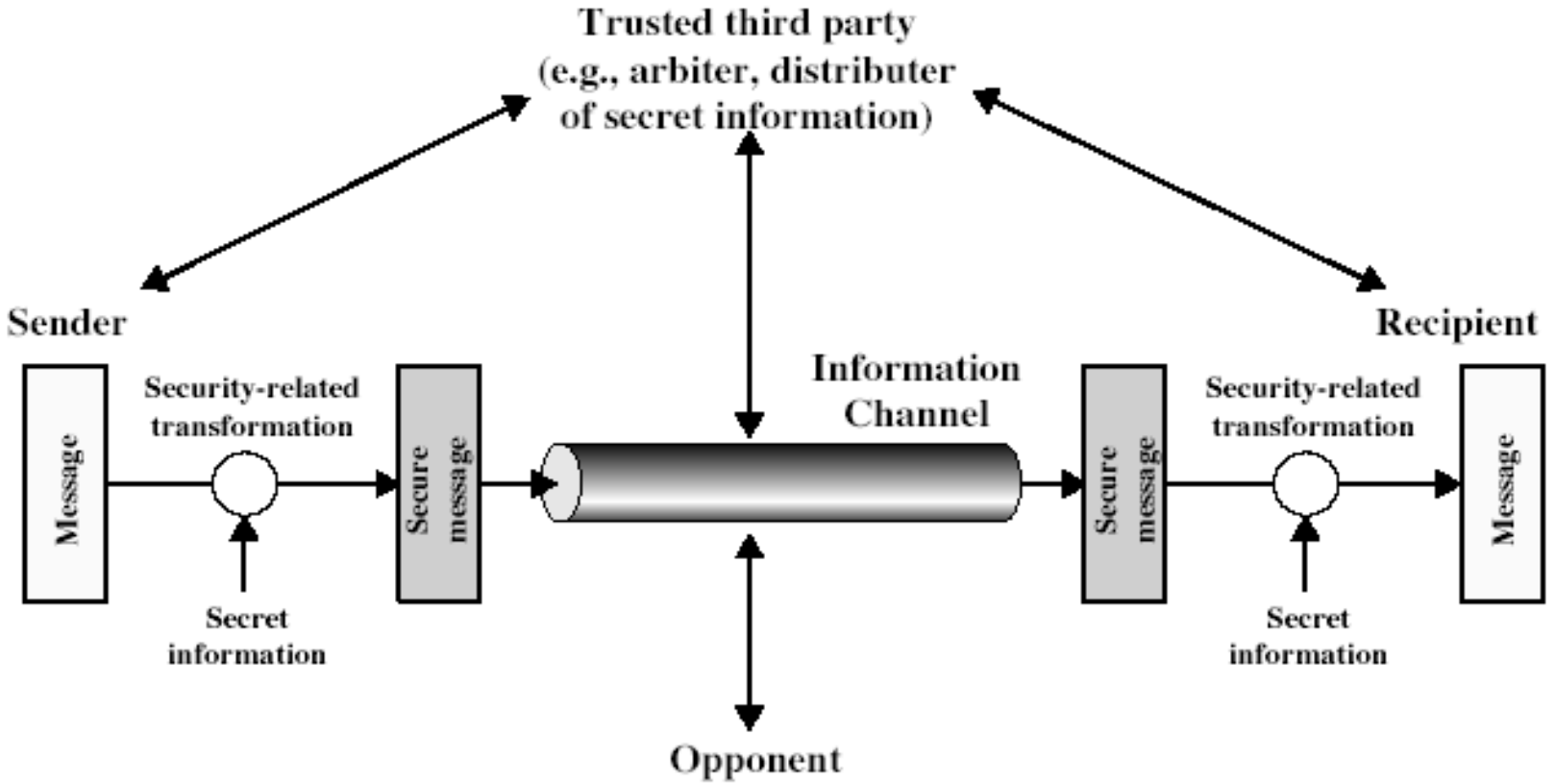
DỊCH VỤ CHỐNG THOÁI THÁC

- Chống lại sự từ chối của một trong các thực thể tham gia vào truyền thông hoặc một phần của truyền thông.
- **Bao gồm:**
  - Dịch vụ chống thoái thác về nguồn gốc: chứng minh rằng thông điệp đã được gởi từ một thực thể cụ thể.
  - Dịch vụ chống thoái thác về đích đến: chứng minh thông điệp đã được nhận từ một thực thể cụ thể

QUAN HỆ GIỮA CƠ CHẾ VÀ DỊCH VỤ

	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

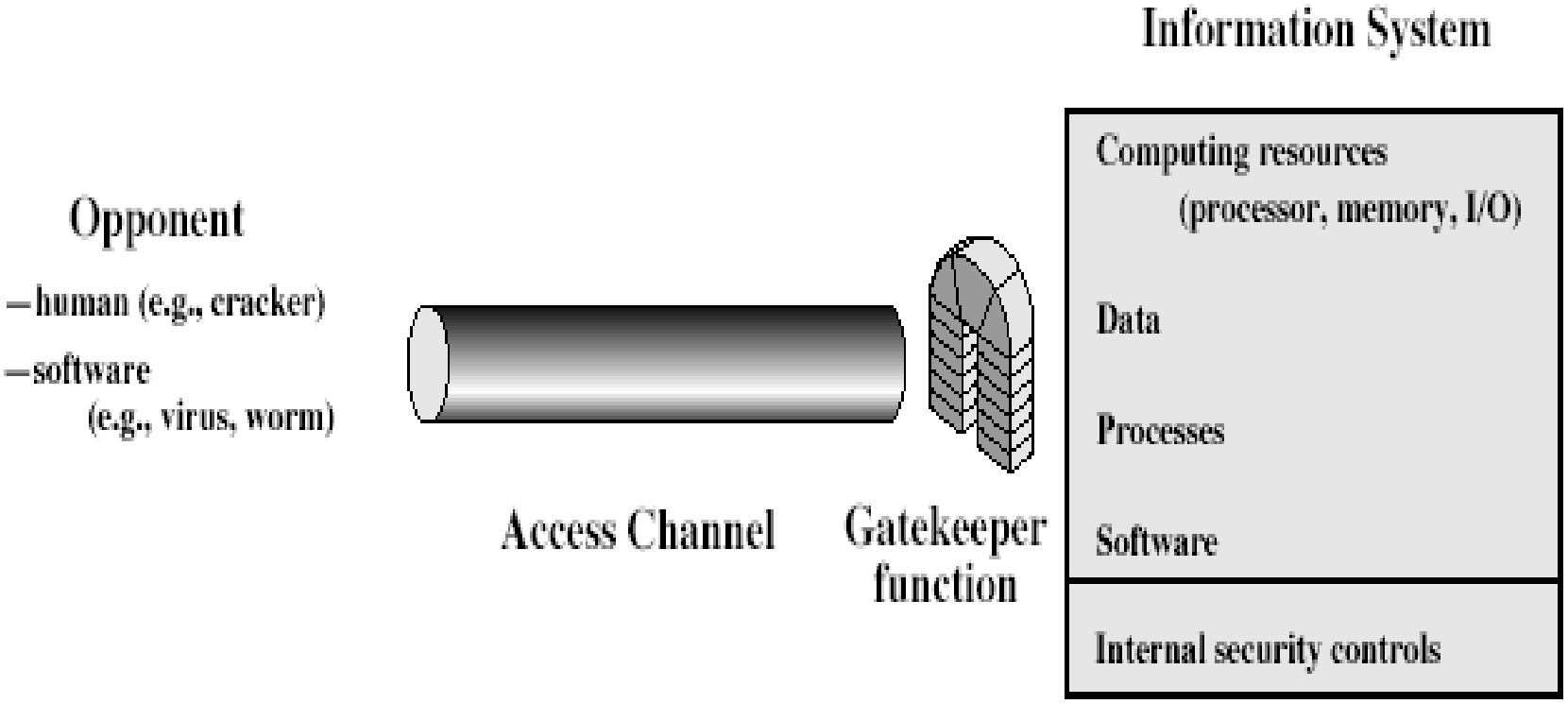
MÔ HÌNH AN NINH TRUYỀN THÔNG



MÔ HÌNH TRUYỀN THÔNG AN TOÀN

- **Các yêu cầu**
  - Lựa chọn một thuật toán thích hợp cho việc biến đổi an toàn.
  - Tạo thông tin bí mật(khóa) và chúng được sử dụng bởi thuật toán.
  - Phát triển các phương pháp để phân phối và chia sẻ thông tin bí mật.

MÔ HÌNH AN NINH TRUY CẬP MẠNG



MÔ HÌNH AN NINH TRUY CẬP MẠNG

- **Các yêu cầu**
  - Chọn các chức năng để xác định người sử dụng.
  - Hiện thực kiểm soát an ninh để đảm bảo chỉ những người sử dụng có thẩm quyền mới truy cập được các thông tin hay tài nguyên.
  - Các hệ thống tin cậy có thể hữu ích để giúp hiện thực mô hình này.

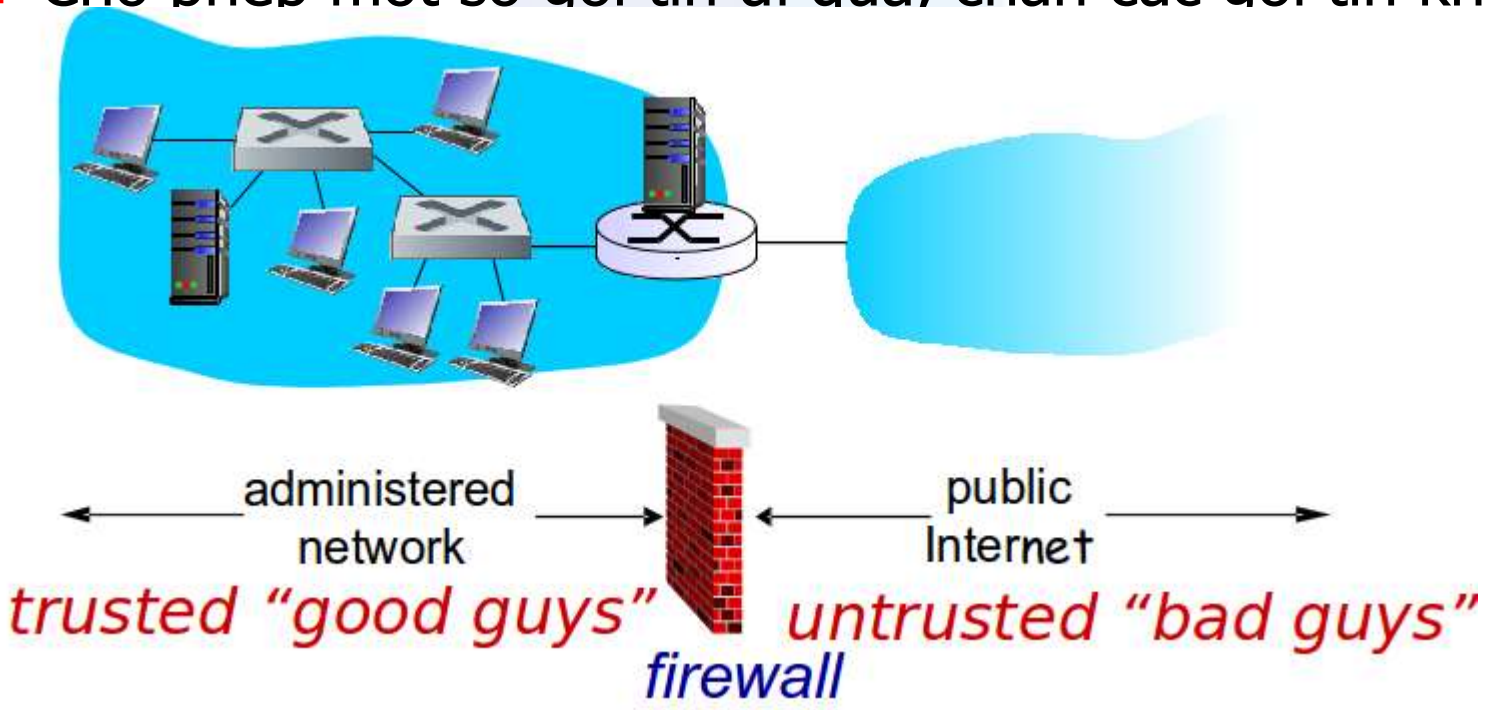
multi layer defend

NỘI DUNG TRÌNH BÀY

- Giới thiệu
- An toàn thông tin
- Chính sách an toàn thông tin
- An ninh mạng
- An ninh mạng trong thực tế
- Thảo luận

AN NINH MẠNG TRONG THỰC TẾ

- **Tường lửa** header? -> packet filter
  - Cách ly mạng nội bộ của tổ chức với mạng toàn cầu
  - Cho phép một số gói tin đi qua, chặn các gói tin khác



CHỨC NĂNG TƯỜNG LỬA

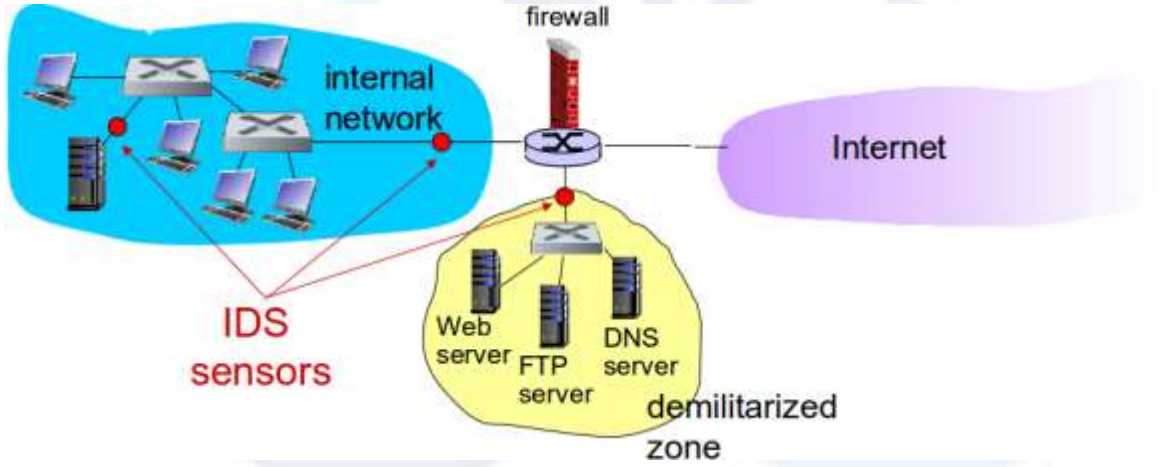
- **Tường lửa thông thường**
  - Bộ lọc gói dựa trên danh sách kiểm soát truy cập
  - Cổng mức ứng dụng
- **Tường lửa UTM(Unified Threat Management)**
  - Hợp nhất nhiều chức năng an ninh mạng
  - Tường lửa thông thường
  - Phát hiện và ngăn chặn xâm nhập
  - Lọc Web và nội dung
  - Mạng riêng ảo
  - Tích hợp mạng cục bộ không dây
  - AntiMalware / AntiVirus / AntiSpam

NOT FREE

AN NINH MẠNG TRONG THỰC TẾ

threshold -> fake alarm ... not detect
=> Training AI

- **Phát hiện xâm nhập**
  - Kiểm tra sâu gói tin bằng cách xem xét nội dung gói tin(ví dụ như kiểm tra các chuỗi ký tự trong gói dựa trên cơ sở dữ liệu của virus đã biết)
  - Kiểm tra mối tương quan giữa nhiều gói tin(ví dụ như quét cổng, tấn công từ chối dịch vụ)



PHÁT HIỆN XÂM NHẬP

- **Phát hiện xâm nhập dựa mẫu(signature)**
  - Xem xéti mọi gói tin đi qua nó
  - So sánh gói với mỗi mẫu trong cơ sở dữ liệu
  - Nếu trùng khớp → tạo cảnh báo
- **Hạn chế**
  - Yêu cầu kiến thức trước đây về tấn công để tạo mẫu
  - Có thể tạo ra cảnh báo giả
  - Tải xử lý lớn và có thể thất bại trong việc phát hiện các gói độc hại

PHÁT HIỆN XÂM NHẬP

- **Phát hiện xâm nhập dựa bất thường**
  - Tạo một hồ sơ lưu lượng mạng chuẩn theo quan sát trong hoạt động bình thường
  - Sau đó tìm ra sự bất thường khi lưu lượng mạng thay đổi đột ngột
- **Hạn chế**
  - Cực kỳ khó khăn để phân biệt giữa lưu lượng mạng bất thường và lưu lượng mạng bình thường

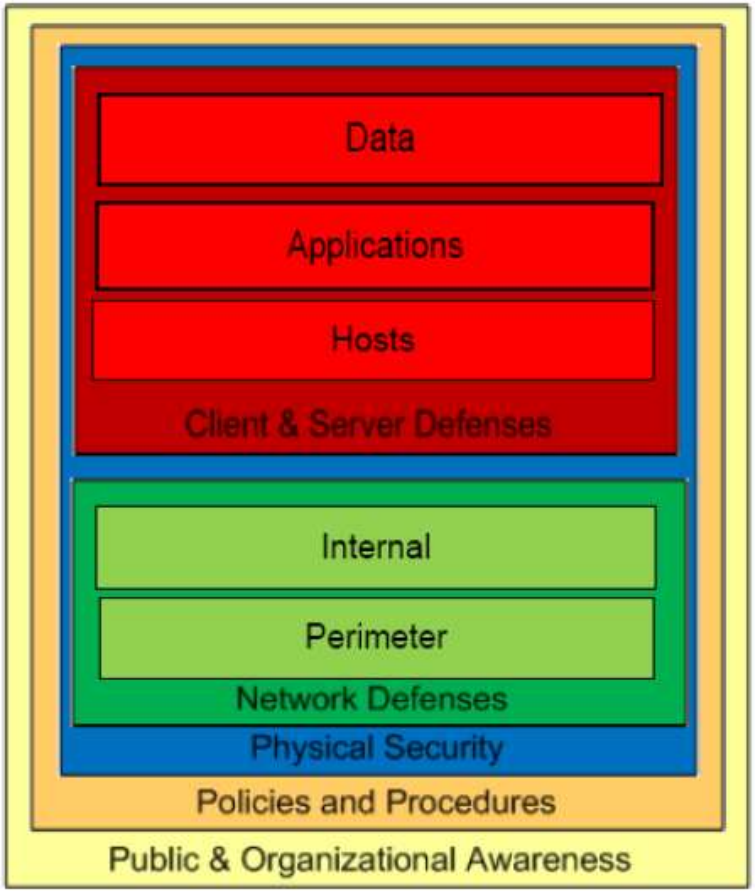
BẢO VỆ VÒNG NGOÀI

- Bảo vệ vòng ngoài giống tương tự như một pháo đài được bao quanh bởi một đường hào (Ví dụ giải pháp firewall).
- Chỉ gia cố hoặc tăng cường sức mạnh của các hệ thống vòng ngoài hoặc có thể bảo vệ được phần nào mạng nội bộ.
- **Các điểm yếu**
  - Thứ nhất, trong mô hình này không thực hiện bất kỳ biện pháp nào để bảo vệ các hệ thống bên trong đối với các tấn công nội bộ. Mà các tấn công nội bộ có thể là nguy cơ nghiêm trọng nhất của mọi tổ chức.
  - Thứ hai, mô hình bảo vệ vòng ngoài dễ thương tổn. Và một khi điều này xảy ra thì các hệ thống bên trong sẽ hoàn toàn mở trước các tấn công.

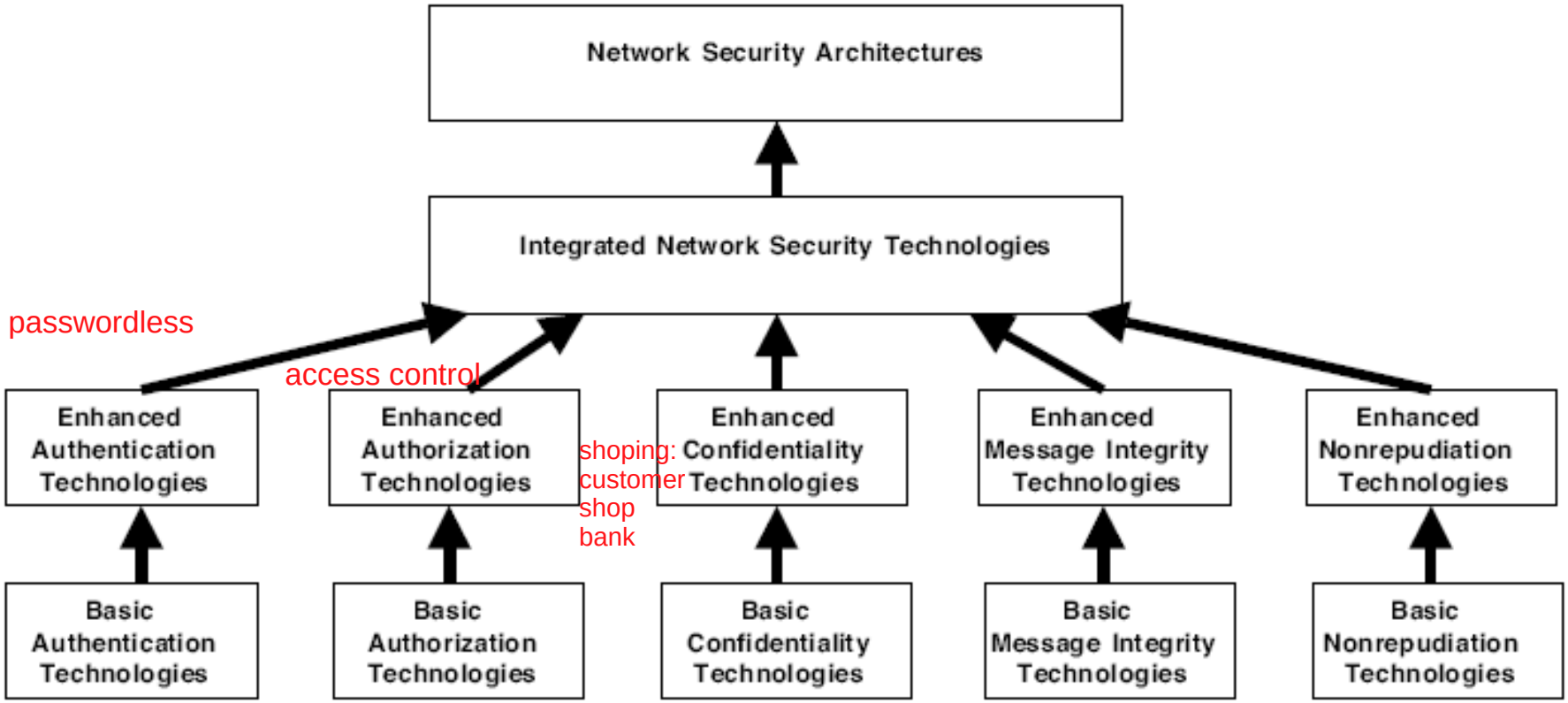
PHÒNG VỆ THEO CHIỀU SÂU

trend

- Cố gắng thực hiện bảo vệ an ninh nhờ sự gia cố và giám sát mỗi hệ thống, mỗi hệ thống sẽ là một vùng được tự bảo vệ.
- Cũng sử dụng các hệ thống bảo vệ vòng ngoài, nhưng sự an ninh của các hệ thống bên trong không chỉ dựa hoàn toàn vào vòng bảo vệ bên ngoài.



KHUNG LÀM VIỆC CỦA CÁC CÔNG NGHỆ AN NINH MẠNG



CÁC GIẢI PHÁP AN NINH

- Giải pháp mật mã.
- Giải pháp tường lửa.
- Giải pháp phân mảnh mạng. network segmentation
- Quản lý các điểm truy nhập. access point, gateway
- Giải pháp phát hiện và ngăn chặn xâm nhập.
- Giải pháp lọc nội dung. phishing mail
- Quản lý truy nhập từ xa. manage wfh: VPN
- Quản lý các sự kiện an ninh. security event
- Quản lý các tổn thương.
- ...

THẢO LUẬN

- Bạn hãy cho biết các nguyên tắc cốt lõi của an toàn thông tin
  CIA
- Bạn hãy cho biết khác biệt giữa tấn công thụ động và tấn công chủ động
  No manipulation
  detect
  prevent
  passive: gain info -> traffic
  => active
- Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin?
  confidently
- Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?
  active
- Cơ chế nào cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?
  data integrity
  authentication exchange

  access control
  routing countrol

THẢO LUẬN

- Khi ta thấy một hình ảnh trên Internet, ta có thể đảm bảo được hình ảnh đó là nguyên bản (không bị chỉnh sửa bằng các công cụ xử lý ảnh) hay không ? NO
- Khi dữ liệu máy tính bị mã hóa và bị đòi tiền chuộc, mục tiêu/nguyên tắc an toàn thông tin nào đã bị vi phạm ? availbilty + integrity
- Trong các biện pháp đối phó (phòng ngừa, phát hiện, phục hồi) theo bạn biện pháp nào khó khăn nhất ?