


# Nhập môn An toàn thông tin

PGS. Nguyễn Linh Giang  
Bộ môn Truyền thông và  
Mạng máy tính



# Nội dung

- I. Nhập môn An toàn thông tin
- II. Đảm bảo tính mật
  - I. Các hệ mật khóa đối xứng (mã hóa đối xứng)
  - II. Các hệ mật khóa công khai ( mã hóa bất đối xứng )
- III. Bài toán xác thực
  - I. Cơ sở bài toán xác thực
  - II. Xác thực thông điệp
  - III. Chữ ký số và các giao thức xác thực
  - IV. Các cơ chế xác thực trong các hệ phân tán
- IV. An toàn an ninh hệ thống
  - I. Phát hiện và ngăn chặn xâm nhập ( IDS, IPS )
  - II. Lỗ hổng hệ thống

# Nội dung

- Tài liệu môn học:
  - W. Stallings “Networks and Internetwork security”
  - W. Stallings “Cryptography and network security”
  - Introduction to Cryptography – PGP
  - D. Stinson – Cryptography: Theory and Practice

# Các chủ đề tiểu luận

- 1. Các hệ mật khóa công khai.
  - Cơ sở xây dựng hệ mật khóa công khai
  - Các hệ mật khóa công khai.
  - Các sơ đồ ứng dụng.
- 2. Hạ tầng khóa công khai PKI
  - Cấu trúc hạ tầng khóa công khai.
  - Chứng chỉ số, các chuẩn;
  - Triển khai thực tế. Các ứng dụng trong các giao dịch.
  - Các hệ thống mã nguồn mở.

# Các chủ đề tiểu luận

- 3. Bảo mật cho mạng IP. IPSec. Mạng riêng ảo VPN. Ứng dụng.
- 4. Bài toán xác thực thông điệp.
  - Các cơ chế xác thực
  - Hàm băm và hàm mã hóa xác thực.
  - Các giao thức xác thực.
- 5. Chữ ký số.
  - Các cơ chế tạo chữ ký số. Giao thức chữ ký số.
  - Các dịch vụ chữ ký số.
  - Chữ ký mù.
  - Ứng dụng.

# Các chủ đề tiểu luận

- 6. Phát hiện xâm nhập mạng.
  - Các cơ chế phát hiện xâm nhập mạng.
  - Phát hiện theo dấu hiệu
  - Phát hiện theo bất thường
  - Phân tích các đặc trưng thống kê của mạng.
  - Ứng dụng.
- 7. Bảo mật cho mạng không dây. Phân tích các đặc trưng thống kê của các dạng tấn công từ chối dịch vụ. Xác thực và bảo mật trong mạng không dây. Phát hiện bất thường trong mạng không dây.

# Các chủ đề tiểu luận

- 8. Bảo mật hệ thống, bảo mật mạng. Các chính sách, các chuẩn. Phân tích đối với Windows và Unix-Linux. Các chính sách an ninh mạng cho mạng Cisco.
- 9. Bảo vệ dữ liệu đa phương tiện trong quá trình phân phối qua hệ thống mạng mở. Vấn đề bảo mật, bảo vệ bản quyền và kiểm soát sử dụng dữ liệu đa phương tiện.

# Các chủ đề tiểu luận

- 10. Bảo mật cho web services;
- 11. Đăng nhập 1 lần với GSS-API;
- 12. Xác thực Kerberos;
- 13. SSL và TLS;
- 14. IPSecurity;
- 15. Xác thực X509



# Các chủ đề tiểu luận

- 16. Hạ tầng khóa công khai PKI
- 17. PGP và bảo mật thư tín điện tử
- 18. S/MIME
- 19. Secure electronic transaction
- 20. Firewall, các kiến trúc;
- 21. Proxy, thiết kế và xây dựng proxy;

# Các chủ đề tiểu luận

- 22. Các hệ thống phát hiện xâm nhập dựa trên dấu hiệu;
- 23. Các hệ thống phát hiện xâm nhập dựa trên bất thường;
- 24. Bảo mật mạng LAN không dây;
- 25. Các dạng tấn công vào mạng sensor.
- 26. Các dạng tấn công từ chối dịch vụ;
- 27. Tấn công SQL Injection, phát hiện và tìm kiếm lỗi SQL Injection;
- 28. Phát hiện tấn công quét cổng;
- 29. Các phương pháp, quy trình phát hiện lỗ hổng hệ thống.
- 30. Các mô hình tiền điện tử trong giao dịch điện tử.

# Đánh giá

- Giữa kỳ và quá trình: 30%
  - Điểm danh: 1/3.
- Thi hết môn: 70%
- Liên hệ giáo viên:
- [giangnl@soict.hust.edu.vn](mailto:giangnl@soict.hust.edu.vn); số Bộ môn: 024-38682596; mobile: 0984933165

# Chương I. Nhập môn

1. Nhập môn
2. Các dịch vụ, cơ chế an toàn an ninh thông tin và các dạng tấn công vào hệ thống mạng
3. Các dạng tấn công
4. Các dịch vụ an toàn an ninh
5. Các mô hình an toàn an ninh mạng

# Nhập môn

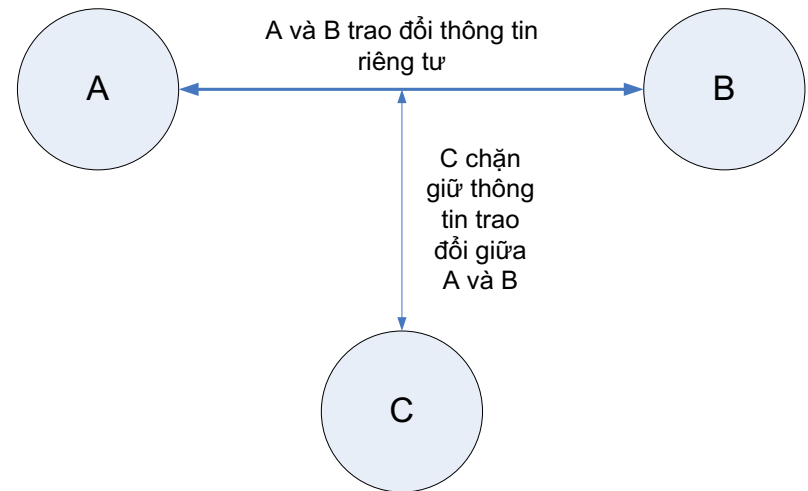
- Bối cảnh bảo mật thông tin:
  - Trước khi xuất hiện máy tính: Bảo vệ thông tin, tài liệu:
    - Các cơ chế bảo vệ;
    - Khoá kho hồ sơ lưu trữ văn bản.
  - Khi xuất hiện máy tính - bảo vệ thông tin điện tử:
    - Sao chép thông tin dễ dàng
    - Cần thiết có các công cụ tự động để bảo mật các tệp, các dạng thông tin chứa trong máy tính.
    - Đặc biệt khi hệ thống được chia sẻ tài nguyên trên mạng.  
Vấn đề **Computer Security**.

# Nhập môn

- Khi xuất hiện các hệ phân tán và sử dụng mạng để truyền dữ liệu và trao đổi thông tin: Bảo vệ thông tin, dữ liệu truyền trên mạng
  - Truyền dữ liệu giữa người sử dụng và máy tính,
  - Giữa máy tính và máy tính.
  - Nhu cầu bảo vệ các dữ liệu trong khi truyền → **Network Security**.
- Không có ranh giới rõ rệt giữa Computer Security và Network Security.
- Chương trình tập trung vào: an toàn thông tin liên mạng: internetwork security.

# Nhập môn

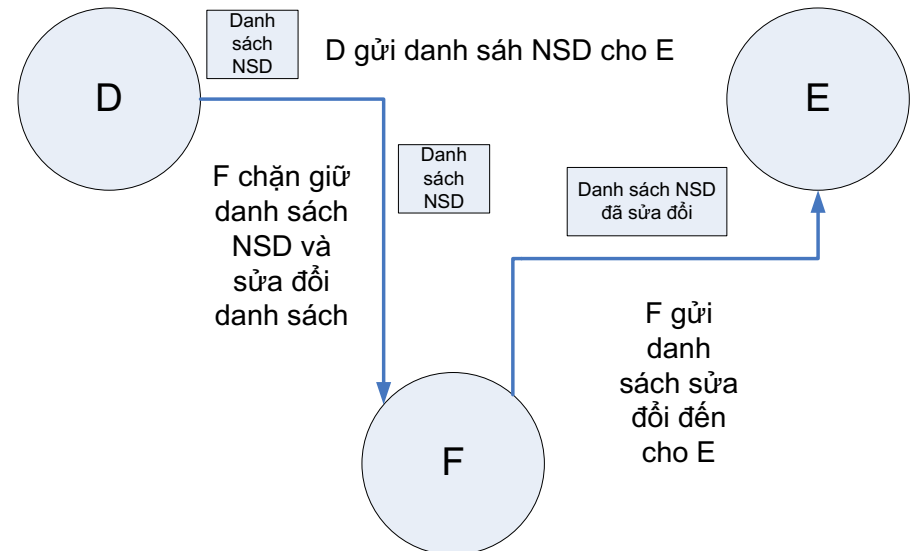
- Một số ví dụ về vấn đề bảo vệ an toàn thông tin:
  - Truyền file:
    - A truyền file cho B;
    - Trong file chứa những thông tin bí mật;
    - C không được phép đọc file nhưng có thể theo dõi được quá trình truyền file và sao chép file trong quá trình truyền.



# Nhập môn

- 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.

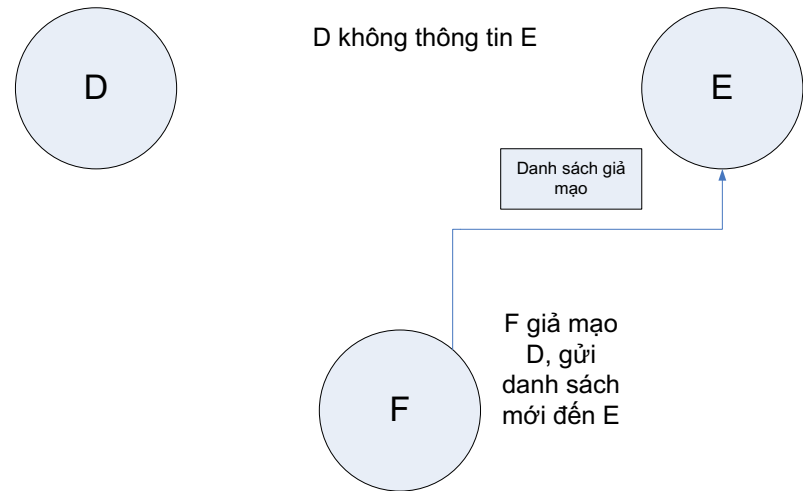




# Nhập môn

- 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



# Nhập môn

- Sự phức tạp trong bài toán Bảo mật liên mạng:
  - Không tồn tại phương pháp thích hợp cho mọi trường hợp.
  - Các cơ chế bảo mật luôn đi đôi với các biện pháp đối phó.
  - Lựa chọn những giải pháp thích hợp với từng ngữ cảnh sử dụng.

# Computer security

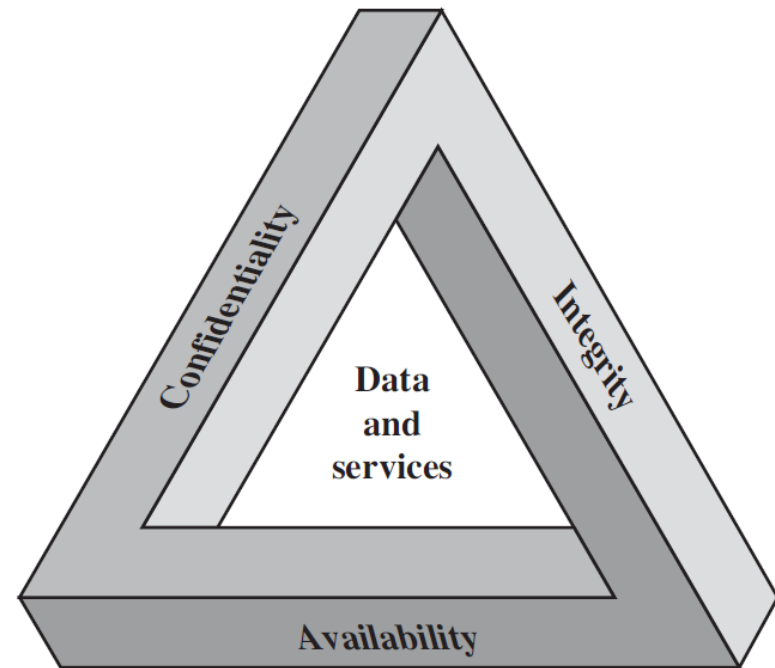
- An toàn hệ thống tính toán:
  - Mục tiêu: bảo vệ hệ thống và đạt các mục tiêu: đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của các tài nguyên hệ thống thông tin (phần cứng, phần mềm, các firmware, thông tin/dữ liệu, hạ tầng truyền thông)

# Introduction to Computer security

- 3 mục tiêu cơ bản của ATTT:
  - **Confidentiality:** Preserving authorized restrictions on information access and disclosure;
  - **Integrity:** Guarding against improper information modification or destruction;
  - **Availability:** Assures that systems work promptly and service is not denied to authorized users

# Introduction to Computer security

- The security requirement triad:
  - These three concepts form what is often referred to as the **CIA triad**
  - The three concepts embody the fundamental security objectives for both data and for information and computing services.



# Dịch vụ và cơ chế an toàn an ninh

- Mục tiêu An toàn thông tin:
  - Đánh giá được những nhu cầu về an toàn của tổ chức một cách hiệu quả;
  - Xác định và lựa chọn những sản phẩm và chính sách an ninh, cần có:
    - Những phương pháp có tính hệ thống làm cơ sở để xác định những yêu cầu an toàn an ninh mạng;
    - Đặc tả được những cách tiếp cận thỏa mãn những yêu cầu đó.
    - Một trong những phương hướng là khảo sát ba khía cạnh của an toàn an ninh thông tin.

# Kiến trúc an toàn thông tin OSI

- ITU-T3 Recommendation X.800, *Security Architecture for OSI*
- Kiến trúc ATTT OSI tập trung vào các vấn đề:
  - Tấn công vào ATTT: mọi hành vi làm giảm mức độ an toàn của hệ thống thông tin, dữ liệu của tổ chức.
  - Cơ chế ATTT: Quá trình được xây dựng để phát hiện, ngăn chặn và phục hồi hệ thống sau khi chịu tấn công;
  - Dịch vụ ATTT: tiến trình hoặc dịch vụ truyền thông làm tăng cường mức độ an toàn của hệ thống, dữ liệu trao đổi, lưu trữ, tổ chức.
    - Các dịch vụ nhằm đối phó với tấn công và sử dụng một hoặc nhiều cơ chế ATTT.

# Kiến trúc an toàn thông tin OSI

- **Mối đe dọa (Threats)**
  - Các hành vi làm ảnh hưởng hoạt động hệ thống
- **Tấn công (Attacks)**
  - Tấn công trực tiếp, làm giảm độ an toàn của hệ thống



# Kiến trúc OSI về An toàn thông tin

- Ba khía cạnh an toàn an ninh thông tin:
  - Tấn công vào an ninh thông tin
    - Mọi tác động làm giảm mức độ an toàn an ninh thông tin của hệ thống;
  - Các cơ chế an toàn an ninh
    - Các cơ chế cho phép:
      - Phát hiện,
      - Ngăn chặn hoặc
      - Khôi phục hệ thống sau khi bị tấn công;

# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Các dịch vụ an toàn an ninh thông tin:
  - Các dịch vụ làm tăng cường mức độ an toàn của hệ thống xử lý thông tin và những thông tin được truyền đi.
  - Các dịch vụ có nhiệm vụ
    - Chống lại những tấn công thông tin và
    - Sử dụng một hoặc nhiều cơ chế an toàn an ninh để cung cấp dịch vụ.

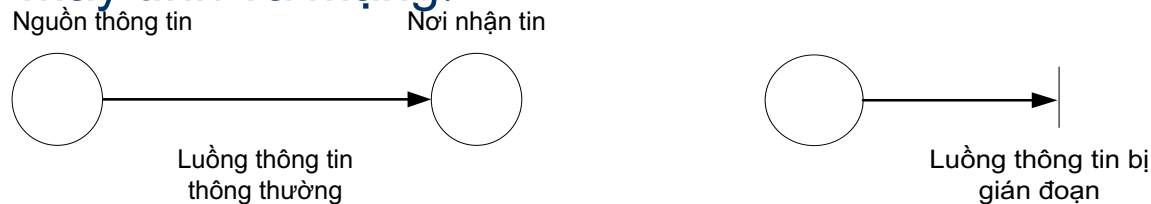
# Dịch vụ và cơ chế an toàn an ninh

## Các dạng tấn công

- Các dạng tấn công.
  - Truy nhập thông tin bất hợp pháp;
  - Sửa đổi thông tin bất hợp pháp;
  - v.v và v.v ...

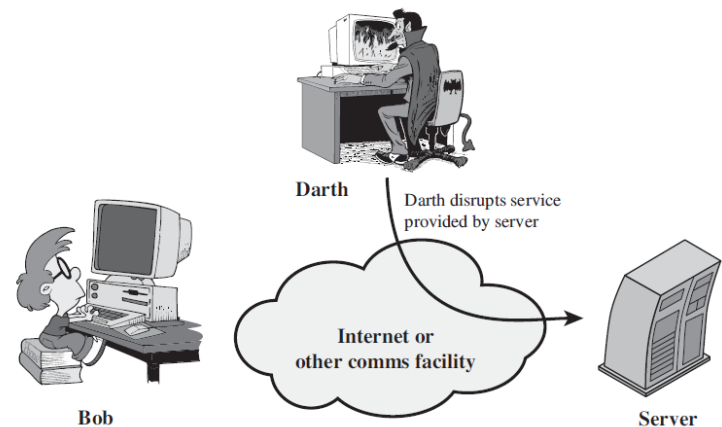
# Các dạng tấn công vào hệ thống

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



- Gián đoạn truyền tin ( interruption ):

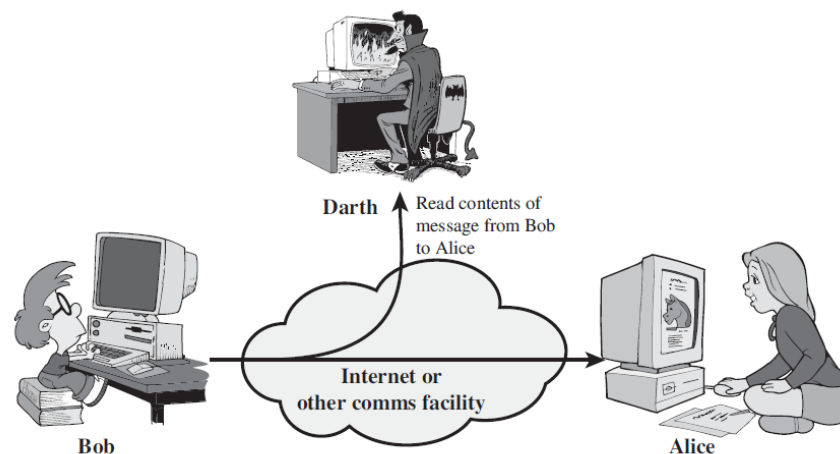
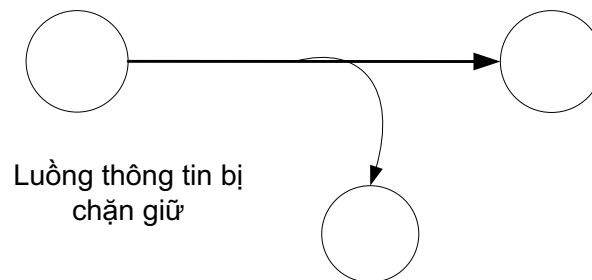
- Các thông tin quý báu có thể bị phá hủy, không sử dụng được.
    - Dạng tấn công vào tính sẵn sàng của thông tin ( availability ).
    - Ví dụ: phá hủy đĩa cứng, cắt đường dây truyền tải, phá hỏng hệ thống quản lý file.



(d) Denial of service

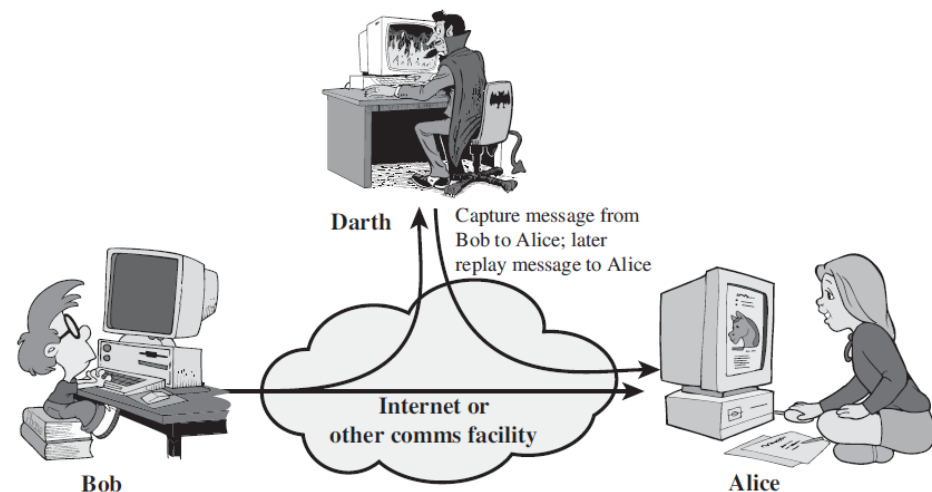
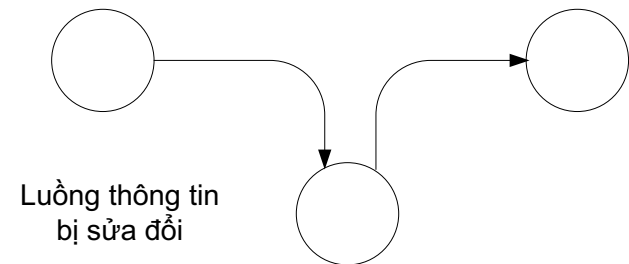
# Các dạng tấn công vào hệ thống

- Chặn giữ thông tin ( interception ):
  - Người không được uỷ quyền cố gắng truy cập tới thông tin.
  - Dạng tấn công vào tính riêng tư của thông tin ( confidentiality ).
  - Ví dụ: sao chép trái phép thông tin.



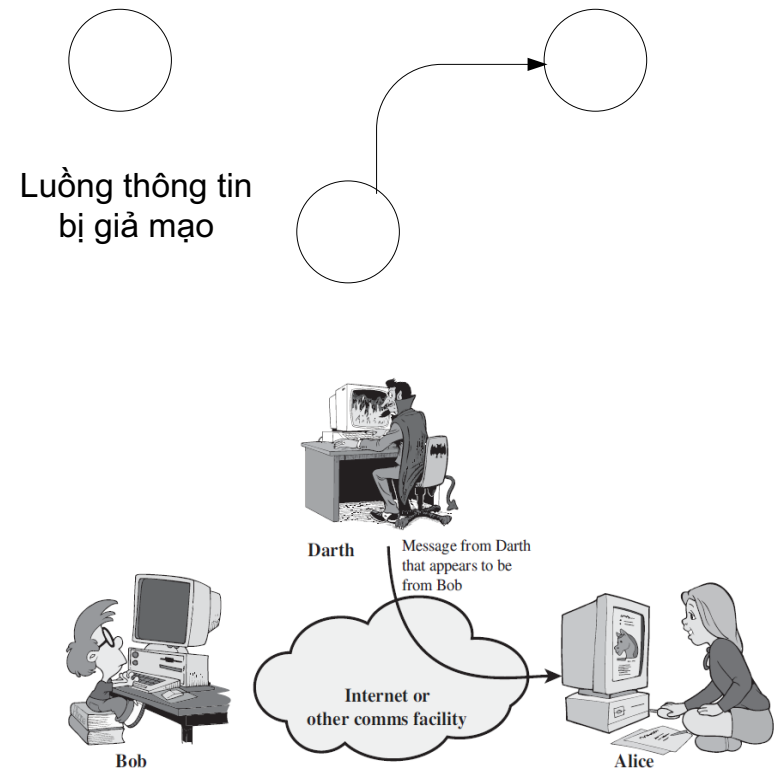
# Các dạng tấn công vào hệ thống

- Sửa đổi thông tin (modification):
  - Không những truy cập trái phép thông tin mà còn sửa đổi thông tin gốc.
  - Dạng tấn công vào tính toàn vẹn thông tin.
  - Ví dụ: truy cập trái phép vào hệ thống, sửa đổi thông tin, thay đổi nội dung thông điệp được truyền tải.



# Các dạng tấn công vào hệ thống

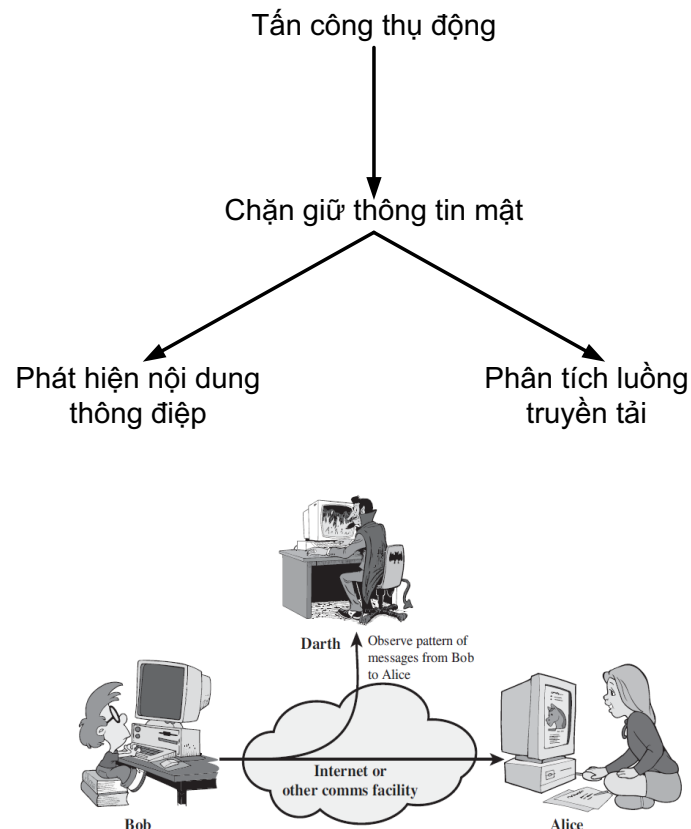
- Làm giả thông tin ( fabrication ).
  - Người không được uỷ quyền đưa những thông tin giả mạo vào hệ thống.
  - Dạng tấn công vào tính xác thực thông tin ( authenticity ).
  - Ví dụ: đưa những thông điệp giả mạo vào hệ thống, thêm những bản ghi mới vào file.



# Các dạng tấn công vào hệ thống

## Tấn công thụ động

- Dạng tấn công thụ động.
  - Tấn công thụ động tương tự hình thức nghe trộm, theo dõi quá trình truyền tin.
  - Mục đích của đối phương là thu được những thông tin được truyền tải.





# Các dạng tấn công vào hệ thống

## Tấn công thụ động

- Các dạng tấn công thụ động:
  - Phát hiện nội dung thông điệp ( release of message contents ).
    - Phương pháp chống: Ngăn chặn đối phương thu và tìm hiểu được nội dung của thông tin truyền tải.
  - Phân tích lưu lượng ( traffic analysis ).
    - Mục đích của bên truyền tải thông tin: che dấu nội dung của tin khỏi đối tượng thứ ba  $\Rightarrow$  cơ chế mật mã nội dung được sử dụng rộng rãi.
    - Vấn đề đặt ra: bên thứ ba có thể xác định được vị trí của các máy tham gia vào quá trình truyền tin, xác định được tần suất và kích thước bản tin, từ đó đoán được nội dung của bản tin.

# Các dạng tấn công vào hệ thống

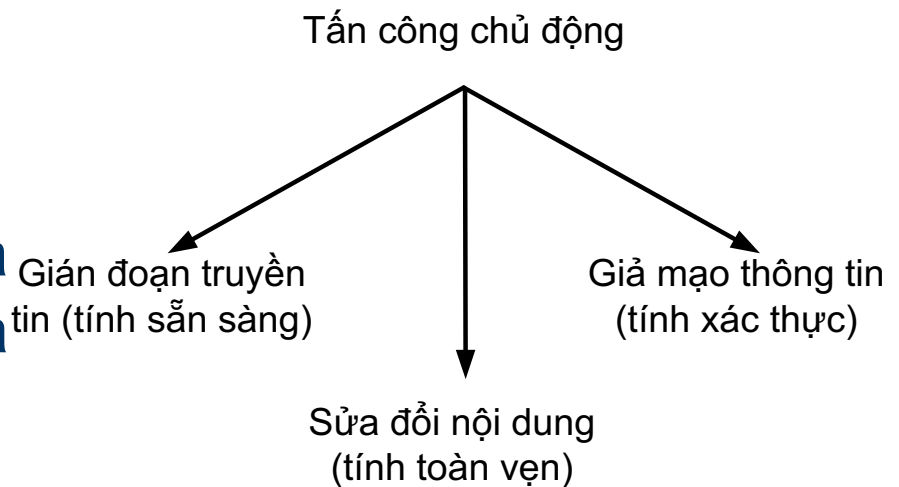
## Tấn công thụ động

- 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 vấn đề ngăn chặn hơn là vấn đề phát hiện.

# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- 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.



# Các dạng tấn công vào hệ thống

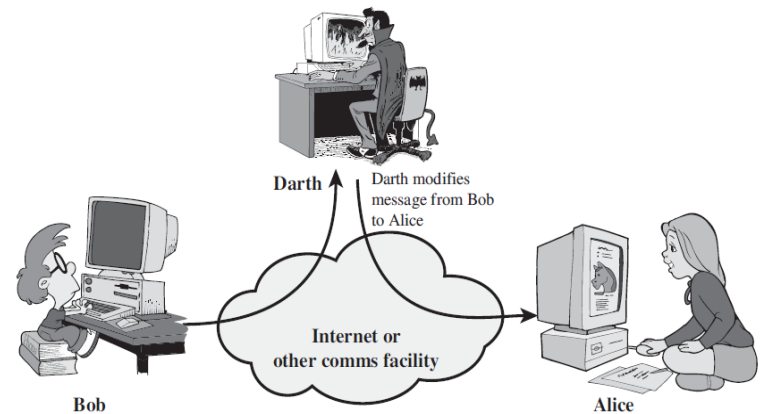
## Tấn công chủ động

- Giả danh ( masquerade ): khi đối phương giả mạo một đối tượng được uỷ quyền.
- Phát lại ( replay ): dạng tấn công khi đối phương chặn bắt các đơn vị dữ liệu và phát lại chúng tạo nên các hiệu ứng không được uỷ quyền;

# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- Thay đổi thông điệp ( modification of message ): một phần của thông điệp hợp pháp bị sửa đổi, bị làm chậm lại hoặc bị sắp xếp lại và tạo ra những hiệu ứng không được uỷ quyền.
- Phủ nhận dịch vụ ( denial of service): dạng tấn công đưa đến việc cấm hoặc ngăn chặn sử dụng các dịch vụ, các khả năng truyền thông.



(c) Modification of messages

# Các dạng tấn công vào hệ thống

## Tấn công chủ động

- Dạng tấn công chủ động:
  - Rất khó có thể ngăn chặn tuyệt đối.
  - Để ngăn chặn, yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm.
- Mục tiêu an toàn:
  - Phát hiện tấn công một cách nhanh nhất
  - Phục hồi lại thông tin trong các trường hợp dữ liệu bị phá hủy hoặc bị làm trệ.

# Dịch vụ và cơ chế an toàn an ninh

- Các cơ chế an toàn an ninh
  - Không tồn tại một cơ chế duy nhất có thể cung cấp tất cả các dịch vụ an toàn an ninh và thực hiện hết mọi chức năng đề ra.
  - Một phần tử được hầu hết mọi cơ chế bảo mật sử dụng: **các kỹ thuật mật mã**. Các phương thức truyền tải và lưu trữ thông tin dựa trên mật mã là cơ chế phổ biến để cung cấp sự an toàn thông tin.

# Các cơ chế an toàn thông tin

- Kiến trúc ATTT OSI.
- Mật mã
- Chữ ký số
- Kiểm soát truy cập
- Toàn vẹn dữ liệu
- Trao đổi xác thực
- Nhiễu luồng truyền tải



# Các cơ chế an toàn thông tin

- Kiểm soát định tuyến
- Công chứng số
- Đánh giá ATTT
- Phát hiện sự cố
- Phục hồi sự cố ATTT
- Ghi vết ATTT

# Dịch vụ và cơ chế an toàn an ninh

- Các dịch vụ an toàn an ninh.
  - Những vấn đề nảy sinh khi sử dụng dữ liệu điện tử:
    - Không có sự khác biệt giữa các bản sao chép số với những bản gốc;
    - Thay đổi nội dung của bản tin vật lý sẽ để lại dấu vết, nhưng thay đổi nội dung của bản tin điện tử không để lại dấu vết;
    - Tính xác thực:
      - Chứng thực văn bản vật lý phụ thuộc vào các thuộc tính vật lý của văn bản;
      - Chứng thực văn bản phải dựa vào nội dung của chính văn bản đó.

# Dịch vụ và cơ chế an toàn an ninh

## Danh sách các chức năng toàn vẹn thông tin

Identification	Endorsement
Authorization	Access ( Egress )
Liscen and/or Certification	Validation
Signature	Time of Occurrence
Witnessing ( notarization )	Authenticity-software and/or file
Concurrence	Vote
Liability	Ownership
Receipt	Registration
Certification of Origination and/or receipt	Approval/Disapproval
	Privacy ( secrecy )

# Dịch vụ và cơ chế an toàn an ninh

- Phân loại các dịch vụ an toàn an ninh:
  - **Bảo mật riêng tư ( confidentiality )**: đảm bảo thông tin trong hệ thống máy tính cũng như thông tin chuyển tải trên mạng chỉ được truy cập bởi những người được uỷ quyền. Các dạng truy cập bao gồm: đọc, in, hiển thị.
  - **Xác thực ( authentication )**: đảm bảo về nguồn gốc của thông điệp hoặc văn bản điện tử.
  - **Toàn vẹn thông tin ( integrity )**: đảm bảo rằng chỉ có những người được uỷ quyền mới có thể thay đổi tài nguyên của hệ thống máy tính và truyền tải thông tin. Mọi thay đổi bao gồm ghi, xoá , sửa, tạo mới hoặc xem lại các thông điệp.

# Dịch vụ và cơ chế an toàn an ninh

- **Chống phủ định ( nonrepudiation )**: yêu cầu người gửi cũng như người nhận thông điệp không thể phủ nhận được giao dịch.
- **Kiểm soát truy cập ( access control )**: yêu cầu mọi sự truy cập tới tài nguyên thông tin đều được kiểm soát chặt chẽ từ hệ thống.
- **Tính sẵn sàng ( availability )**: yêu cầu hệ thống tính toán sẵn sàng đáp ứng dịch vụ đối với những bên được uỷ quyền mỗi khi được yêu cầu.

# Dịch vụ ATTT

- Quan hệ giữa cơ chế ATTT và dịch vụ ATTT

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 toàn thông tin

---

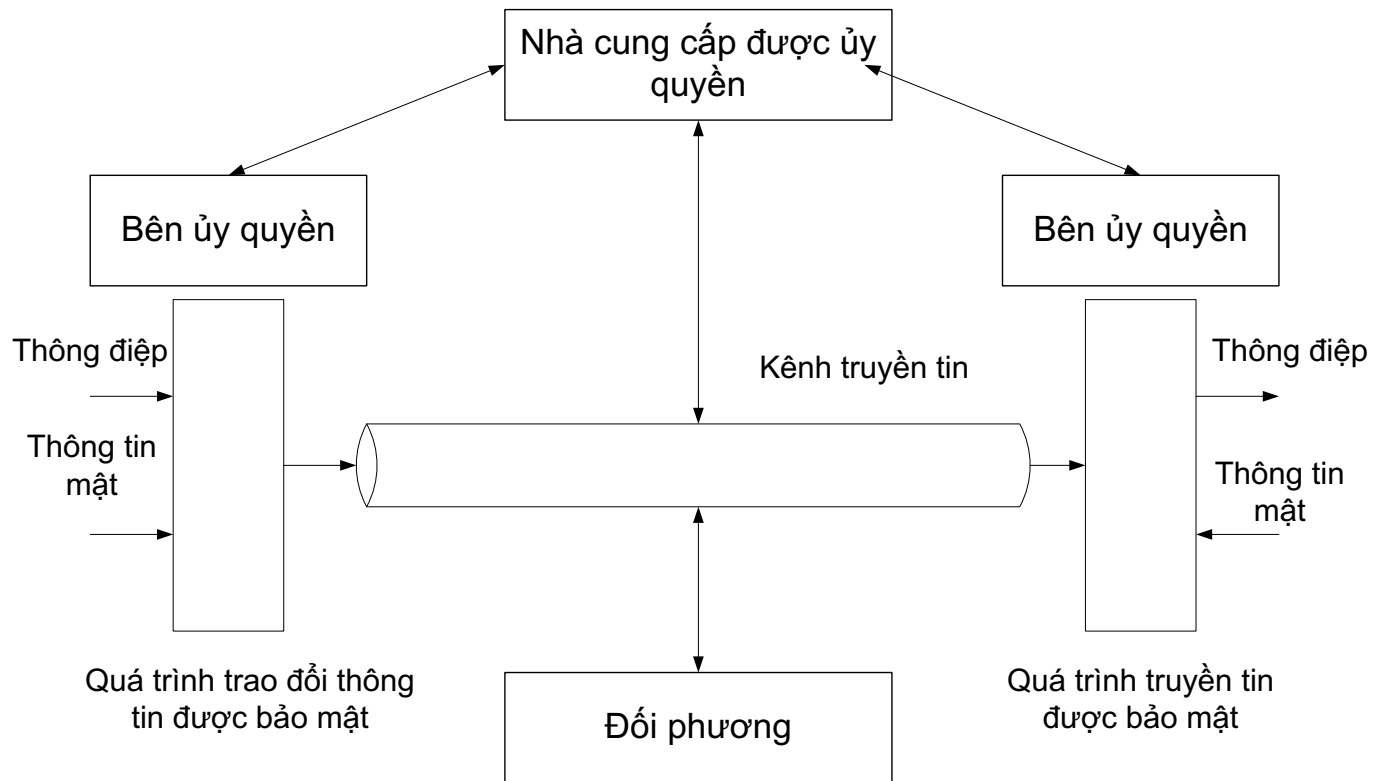
- Mô hình an toàn truyền tải và mô hình an toàn hệ thống

# Mô hình An toàn thông tin

- Mô hình an toàn truyền tải
  - 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.
  - Mô hình truyền thống của quá trình truyền tin an toàn



# Mô hình An toàn thông tin



# Mô hình An toàn thông tin

- Tất cả các kỹ thuật đảm bảo an toàn hệ thống truyền tin đều có hai thành phần:
  - Quá trình truyền tải có bảo mật thông tin được gửi.
    - Ví dụ: mật mã thông điệp sẽ làm cho kẻ tấn công không thể đọc được thông điệp.
    - Thêm vào thông điệp những thông tin được tổng hợp từ nội dung thông điệp. Các thông tin này có tác dụng xác định người gửi.
  - Một số thông tin mật sẽ được chia sẻ giữa hai bên truyền tin.
    - Các thông tin này được coi là bí mật với đối phương.
    - Ví dụ: khóa mật mã được dùng kết hợp với quá trình truyền để mã hóa thông điệp khi gửi và giải mã thông điệp khi nhận.

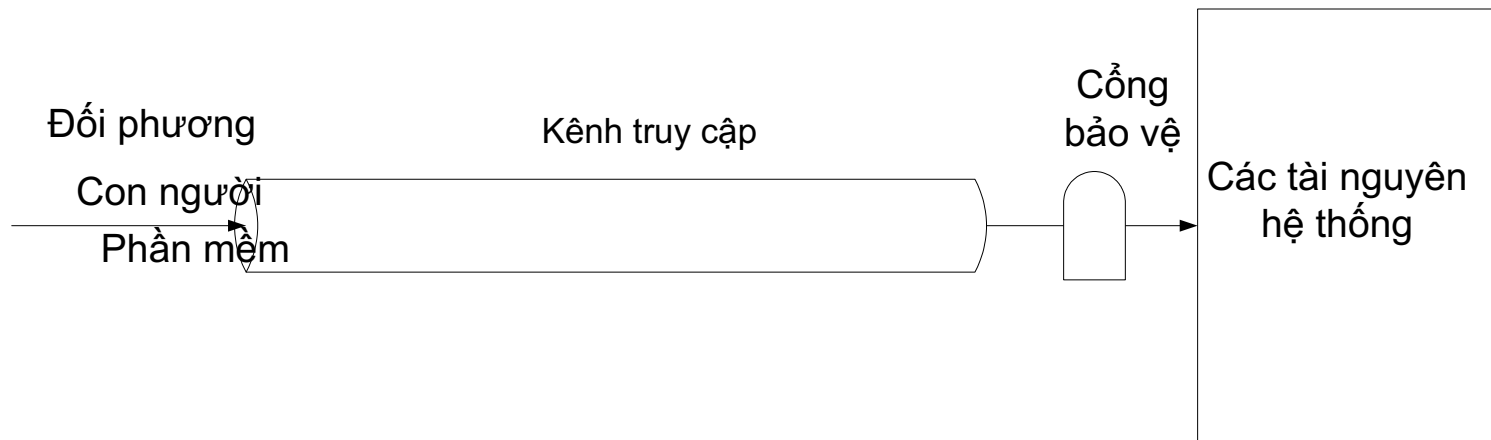
# Mô hình An toàn thông tin

- Bên thứ ba được ủy quyền: trong nhiều trường hợp, cần thiết cho quá trình truyền tin mật:
  - Có trách nhiệm phân phối những thông tin mật giữa hai bên truyền tin;
  - Giữ cho các thông tin trao đổi với các bên được bí mật đối với người tấn công.
  - Có trách nhiệm phân xử giữa hai phía truyền tin về tính xác thực của thông điệp được truyền.

# Mô hình An toàn thông tin

- Mô hình an toàn hệ thống
  - Ngăn chặn xâm nhập của các tác nhân tấn công;
  - Phát hiện xâm nhập hệ thống
  - Dò quét các lỗ hổng an ninh hệ thống;
  - Các tiến trình ngoại lai:
    - Các tiến trình truy cập tới thông tin: làm phá hủy, sửa đổi thông tin không được phép.
    - Các tiến trình dịch vụ: phát hiện các lỗi trong các dịch vụ của hệ thống để ngăn chặn việc sử dụng của những người không được ủy quyền.

# Các mô hình an toàn mạng và hệ thống



Mô hình an ninh hệ thống

# Kết chương

- Kiến trúc ATTT OSI
  - Tấn công vào hệ thống thông tin và dữ liệu
  - Các cơ chế ATTT
  - Các dịch vụ ATTT (dịch vụ bao gồm nhiều cơ chế ATTT, đáp ứng theo yêu cầu);
- Các vấn đề ATTT: mối quan hệ qua lại CIA
  - Vấn đề bảo mật: bảo mật dữ liệu và đảm bảo tính riêng tư dữ liệu
  - Vấn đề toàn vẹn: toàn vẹn dữ liệu và toàn vẹn hoạt động hệ thống

# Kết chương 1

- Tấn công: phân loại dựa trên tác động vào hệ thống
  - Tấn công thụ động
  - Tấn công chủ động
- Các cơ chế ATTT
  - Đối phó tấn công thụ động:
    - Bảo mật
    - Nhiều luồng truyền tải (chống các tấn công định vị)
  - Đối phó tấn công chủ động
    - Phát hiện sớm, chính xác, cảnh báo sớm
    - Phục hồi hệ thống nhanh nhất

# Kết chương 1

- Dịch vụ ATTT
  - Dịch vụ bảo mật
  - Dịch vụ xác thực
  - Dịch vụ toàn vẹn
  - Dịch vụ Chống phủ nhận
  - Dịch vụ kiểm soát truy cập
  - Dịch vụ Đảm bảo tính sẵn sàng
- Mô hình ATTT
  - An toàn truyền tải dữ liệu
  - An toàn hệ thống đầu cuối