An toàn và bảo mật thông tin

Người trình bày: Lương Thái Lê

Môn học
An toàn và bảo mật thông tin

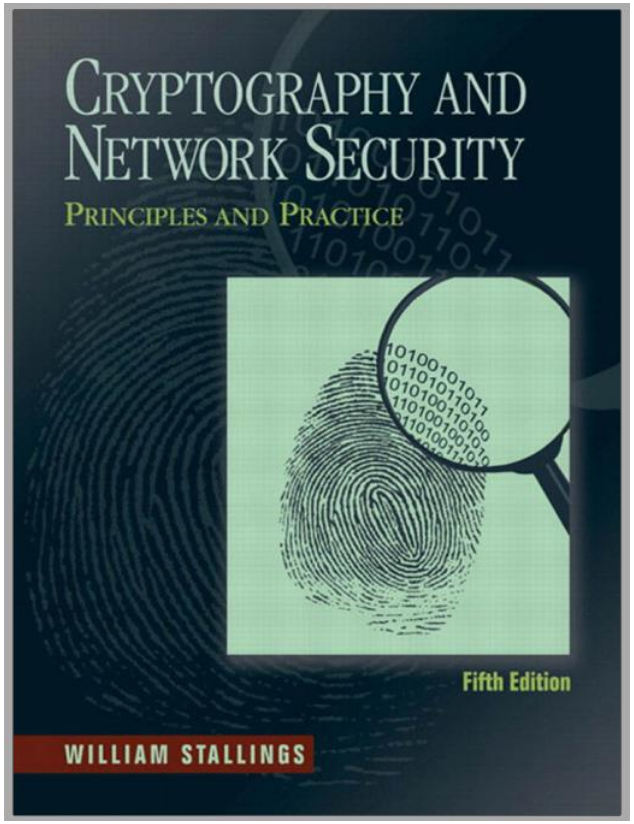
- Bài 1: Giới thiệu tổng quan
- Bài 2: Mã cổ điển
- Bài 3: Trường hữu hạn
- Bài 4: Mã khối hiện đại
- Bài 5: Mã công khai
- Bài 6: Xác thực thông điệp
- Bài 7: Một số ứng dụng
- Bài 8: An ninh hệ thống

Thông tin giảng viên

- ThS. Lương Thái Lê
- mobile: 0973.223.450
- email: luongthaile80@gmail.com
- Bộ môn: Khoa học máy tính
- Khoa: CNTT – ĐH GTVT

Tài liệu tham khảo

1. **Cryptography And Network Security Principles And Practice** - Fifth Edition - William Stallings - Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall
2. **Giáo trình An toàn và bảo mật thông tin** – TS. Trần Văn Dũng, Khoa CNTT, ĐH GTVT, 2018



Bài 1: Giới thiệu tổng quan

Thời lượng: 3 tiết

Nội dung bài 1: Giới thiệu tổng quan

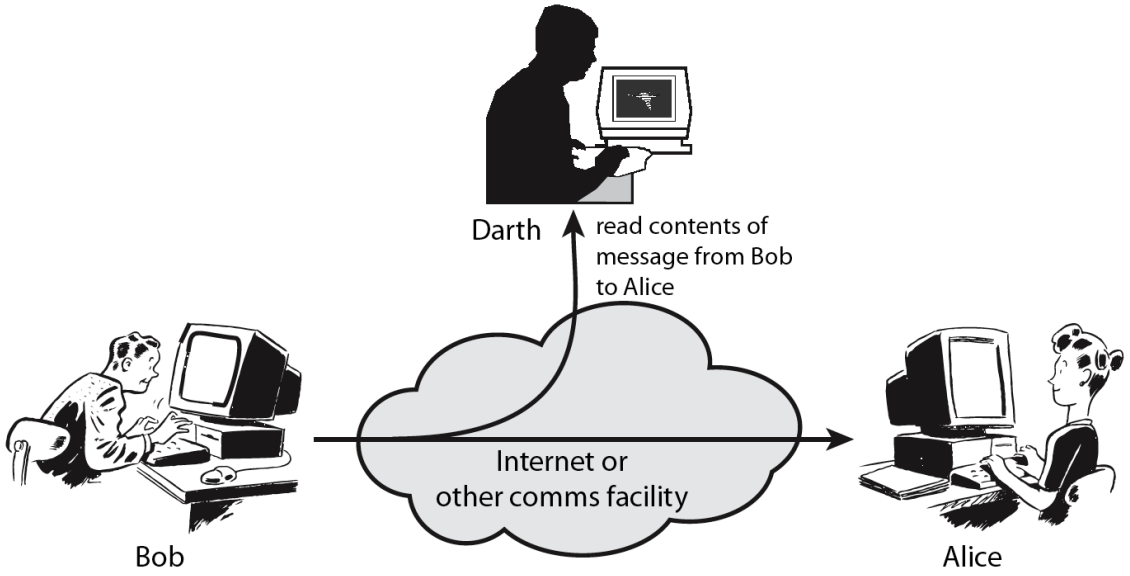
1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

1.1. Bối cảnh và ý nghĩa của môn học

- Sự bùng nổ của các hệ thống máy tính và việc kết nối chúng qua các mạng ngày càng thúc đẩy các tổ chức, cá nhân lưu trữ và trao đổi thông tin qua mạng
  - Vụ tin tặc tấn công cảng hàng không Việt Nam 2016
- Dẫn đến nhu cầu bảo mật dữ liệu và các nguồn tài nguyên, đảm bảo xác thực thông tin và bảo vệ hệ thống khỏi tấn công mạng

=>Môn học an toàn và bảo mật thông tin đã phát triển mạnh mẽ, đưa ra nhiều ứng dụng đáp ứng nhu cầu tăng cường an ninh mạng

1.2 Ví dụ về hành vi vi phạm an toàn thông tin



1.3. Một số khái niệm cơ bản

- **An ninh máy tính**: Sự bảo vệ một hệ thống thông tin tự động nhằm đạt được các mục tiêu bảo vệ tính toàn vẹn, tính sẵn có và bảo mật của tài nguyên hệ thống thông tin (bao gồm phần cứng, phần mềm, phần sụn, thông tin /dữ liệu và viễn thông).

- **An ninh mạng**: các phương tiện bảo vệ dữ liệu khi truyền chúng trên tập các mạng liên kết với nhau.

1.5. Mục tiêu môn học

- Nhận biết các mối đe dọa và các hình thức tấn công an ninh mạng
- Sử dụng các dịch vụ an ninh để chống lại các kiểu tấn công
- Thiết kế các cơ chế để phát hiện, bảo vệ, khôi phục hệ thống do bị tấn công.
- Đưa ra mô hình an ninh mạng

1.6. Các phương pháp bảo vệ an toàn thông tin

1. Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
2. Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
3. Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

=>Phương pháp 3 thích hợp nhất với môi trường mạng

Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

3.1. Một số loại tấn công an ninh mạng

- *Tấn công giả mạo*: là một thực thể tấn công trong khi giả danh một thực thể khác.
- *Tấn công chuyển tiếp*: xảy ra khi một thông báo, hoặc một phần thông báo được gửi nhiều lần, gây ra các tác động tiêu cực.
- *Tấn công sửa đổi thông báo*: xảy ra khi nội dung của một thông báo bị sửa đổi, trì hoãn, nhưng không bị phát hiện.
- *Tấn công từ chối dịch vụ:* xảy ra khi kẻ tấn công có hành động ngăn cản người dùng hợp pháp truy cập hệ thống máy tính, thiết bị hoặc các tài nguyên mạng khác.

3.2. Các xu thế tấn công chính

- Các phần mềm có hại: virus, sâu - worm, ngựa thành Tơroa, bom logic, tràn bộ nhớ…
- Đánh hơi, dò tìm mật khẩu
- Tấn công làm từ chối dịch vụ phân tán (DDoS)
- Các công cụ và kỹ thuật xâm nhập vào các hệ thống máy tính phá hoại
- Thám mã, tìm khóa, đọc nội dung trái phép
- Giả mạo, tiếm quyền, khai thác trái phép
- Phân tích, dò tìm lỗ hổng, tấn công

Nội dung bài 1: Giới thiệu tổng quan

1. Ý nghĩa và mục tiêu môn học
2. Tổng quan về an toàn thông tin
3. Một số loại tấn công an ninh mạng
4. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
5. Tấn công bảo mật theo chuẩn X800
6. Các dịch vụ an ninh theo chuẩn X800.
7. Các cơ chế an ninh theo chuẩn X800.
8. Mô hình an ninh trên mạng.
9. Mô hình an ninh truy cập mạng.

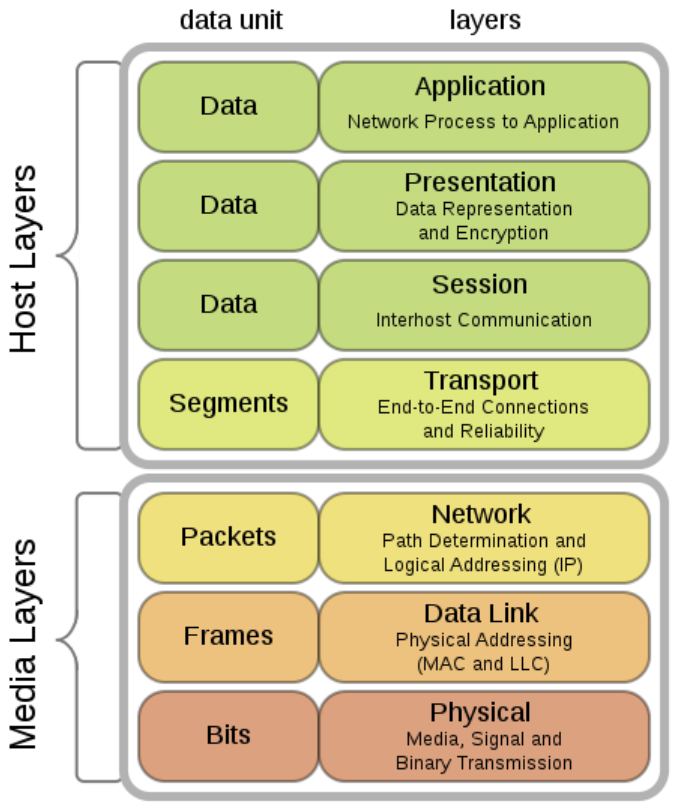
4.1. Phương pháp hệ thống bảo đảm an ninh

- Nhu cầu thực tiễn dẫn đến sự cần thiết có một phương pháp hệ thống xác định các yêu cầu an ninh của tổ chức.
- Trong đó cần có tiếp cận tổng thể xét cả ba khía cạnh của an ninh thông tin: tấn công bảo mật, cơ chế an ninh và dịch vụ an ninh.
- Cuối thập niên 1980, ISO dùng chuẩn OSI (Open System Interconnection)

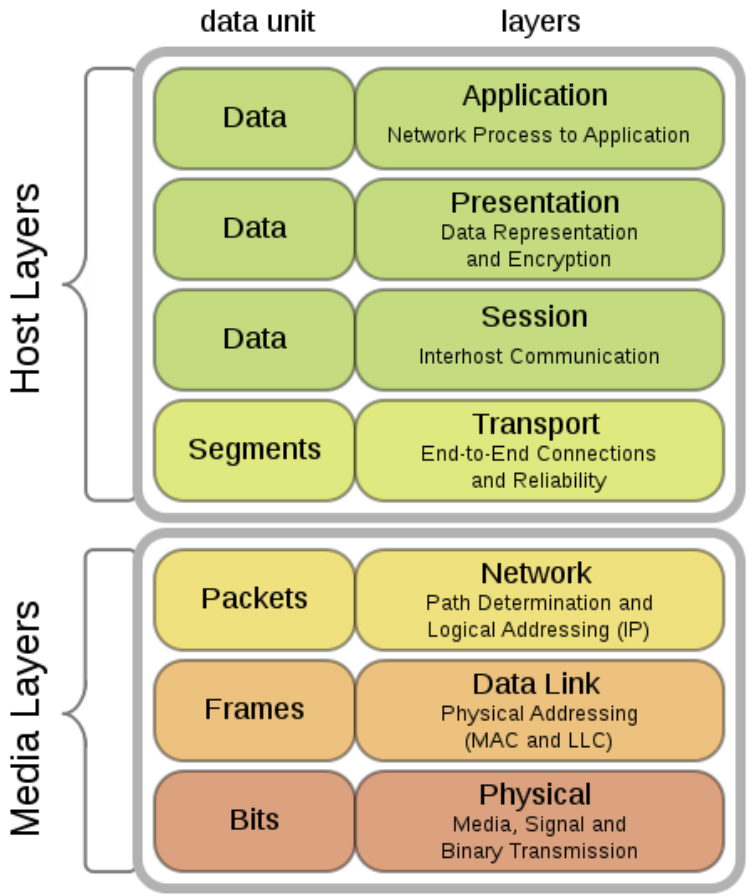
4.2. Mô hình OSI (Open Systems Interconnection)

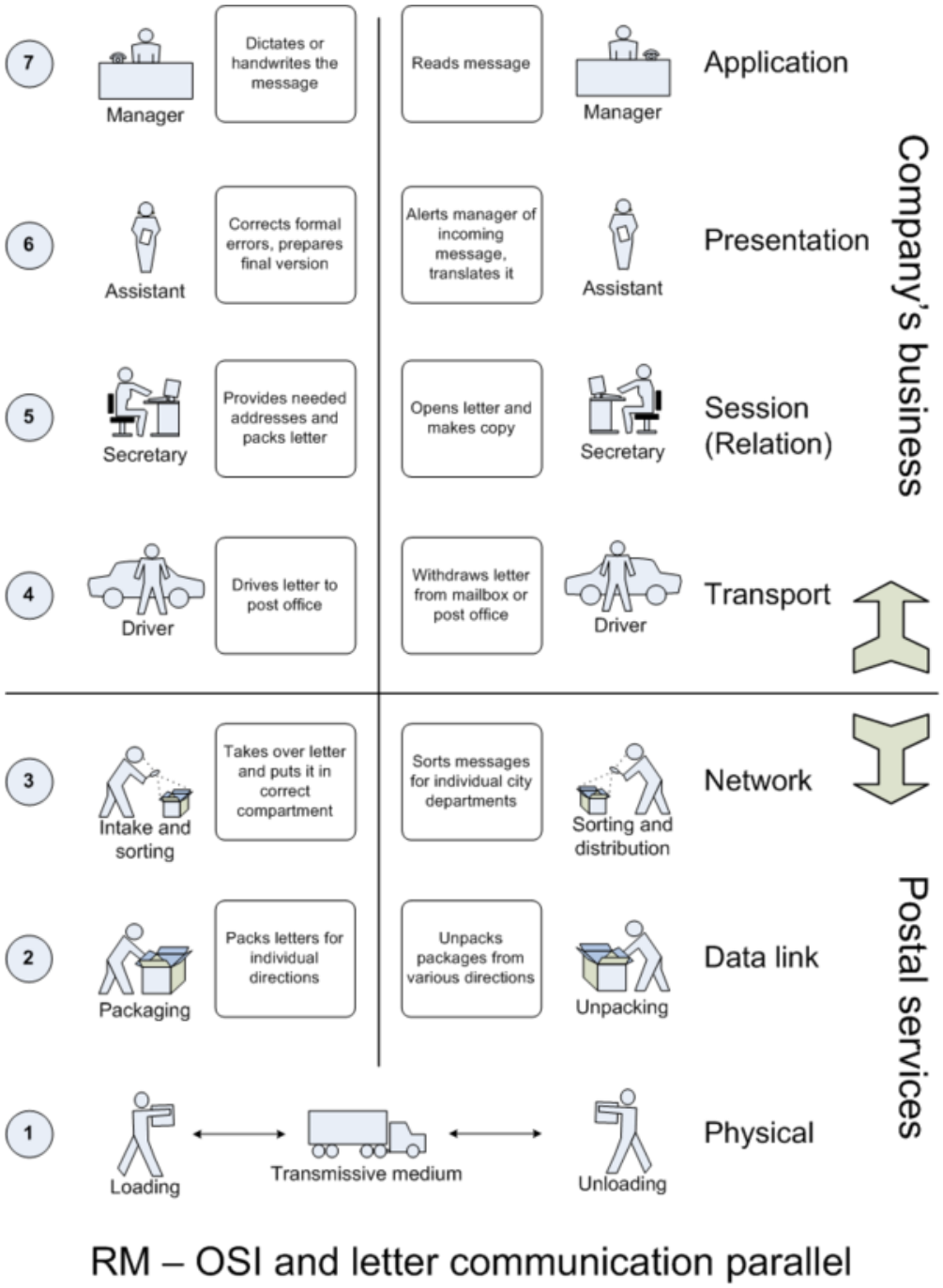
- Mục tiêu của OSI là cho phép kết nối các hệ thống máy tính không đồng nhất để việc giao tiếp giữa các ứng dụng đạt được hiệu quả.

- Chuẩn OSI (Open System Interconnection – hệ thống trao đổi thông tin mở) cung cấp cho chúng ta một cách nhìn tổng quát về các khái niệm: tấn công an ninh, cơ chế an ninh và dịch vụ an ninh



4.3. Mô hình OSI





RM – OSI and letter communication parallel

4.4. Khái niệm RFC 2828, X800

- Tổ chức ITU (international Telecommunication Union) đề xuất kiến trúc an ninh X800 cho các hệ thống OSI.
- Kiến trúc ITU X800 định nghĩa dịch vụ an ninh là dịch vụ đảm bảo an ninh thông tin cần thiết cho hệ thống và việc truyền dữ liệu
- RFC 2828: cung cấp các thuật ngữ về an ninh mạng Internet (chú giải của cộng đồng nghiên cứu phát triển Internet)

4.5. Khái niệm Tấn công, cơ chế và dịch vụ

- **Tấn công bảo mật**: Mọi hành động nguy hại sự an toàn thông tin của các tổ chức
  - X800 và RFC 2828 phân loại tấn công bảo mật thành tấn công bị động và tấn công chủ động
- **Cơ chế an ninh**: gồm các công việc thực tế được hệ thống lại để chống các phá hoại an ninh, phát hiện, bảo vệ và khôi phục hệ thống do bị tấn công
  - Không có cơ chế đơn lẻ nào đáp ứng được mọi chức năng yêu cầu của công tác an ninh. Tuy nhiên có một thành phần đặc biệt nằm trong mọi cơ chế an ninh đó là: kỹ thuật mã hoá.
- **Dịch vụ an ninh**: công cụ cung cấp biện pháp tăng cường an ninh cho các hệ thống xử lý và truyền thông tin, chống lại các tấn công
  - Sử dụng một trong những cơ chế an ninh
    - Chẳng hạn có chữ ký, ngày tháng, được công chứng hoặc có người làm chứng, được ghi nhận hoặc có bản quyền; chống do thám, giả mạo hoặc phá hoại.

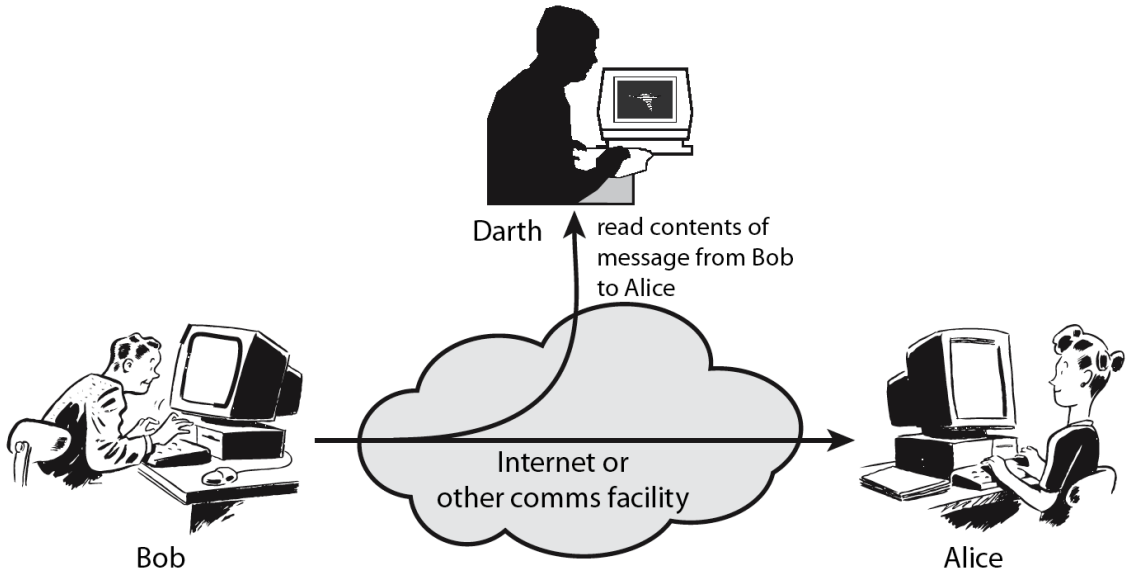
Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

5.1. Tấn công bị động (X800)

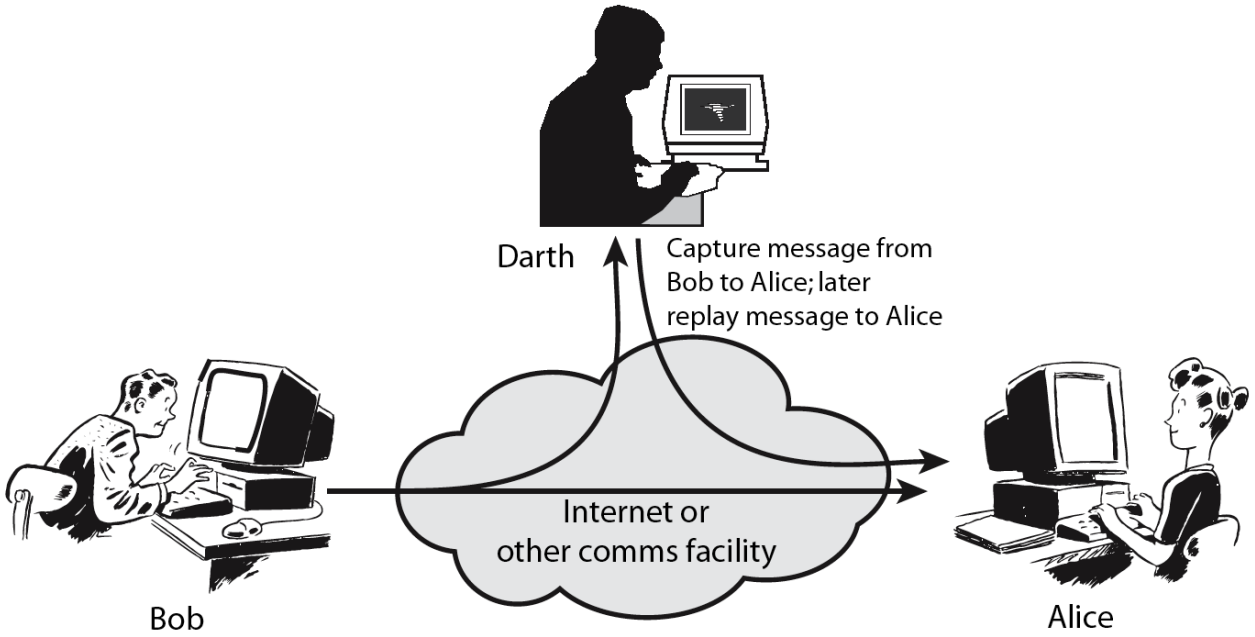
- Tấn công bị động: do thám, theo dõi đường truyền để
  - đọc được nội dung bản tin
  - theo dõi luồng truyền tin (nguồn, đích, tần suất…)

  =>Không làm thay đổi nội dung thông tin. Khó bị phát hiện nhưng dễ ngăn chặn bằng cách mã hóa dữ liệu



5.2. Tấn công chủ động (X800)

- Làm thay đổi luồng dữ liệu và tạo ra luồng dữ liệu sai lệch:



5.3. Tấn công chủ động (tiếp theo)

- Giả mạo một người nào đó: mang danh người khác gửi cho người nhận
- Lặp lại bản tin: đọc trộm tin, xong rồi gửi cho người nhận nhiều lần
- Thay đổi bản tin khi truyền: ngắt dòng tin, sửa, rồi gửi cho người nhận
- Từ chối dịch vụ: gửi quá nhiều yêu cầu đếnmáy chủ, …

=> Dễ phát hiện nhưng khó ngăn chặn

Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

6.1. Dịch vụ an ninh (X800)

- X800 định nghĩa dịch vụ an ninh gồm 5 thành phần
  1. **Xác thực**: đảm bảo tính xác thực của một hệ thống truyền thông tin =>tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố
     - *Peer entity authentication* (xác thực thực thể ngang hàng)
     - Data origin authentication (xác thực nguồn gốc dữ liệu):
  2. **Điều khiển truy cập** : ngăn chặn sử dụng trái phép tài nguyên
  3. **Bí mật dữ liệu**: bảo vệ dữ liệu không bị tiết lộ trái phép => Chống lại hình thức tấn công bị động.
  4. **Toàn vẹn dữ liệu**: đảm bảo dữ liệu không bị sửa đổi => Chống lại hình thức tấn công chủ động
  5. **Chống từ chối**: ngăn chặn hiện tượng người gửi hoặc người nhận từ chối một thông điệp đã được (họ) chuyển đi

6.2. Quan hệ giữa dịch vụ và tấn công bảo mật

	Tấn công					
Dịch vụ	Xem trộm tin	Phân tích đường truyền	Giả mạo	Trì hoãn	Sửa thông điệp	Từ chối dịch vụ
Xác thực thực thể ngang hàng			Có			
Xác thực dữ liệu gốc			Có			
Kiểm soát truy cập			Có			
Bảo mật dữ liệu	Có					
Bảo mật luồng truyền		Có				
Toàn vẹn dữ liệu				Có	Có	
Chống từ chối						
Tính sẵn sàng						Có

Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

7.1. Cơ chế an ninh

- Là cơ chế được thiết kế để phát hiện, bảo vệ hoặc khôi phục do tấn công phá hoại.
- Không có cơ chế đơn lẻ nào đáp ứng được mọi chức năng yêu cầu.
- Tuy nhiên có một thành phần đặc biệt nằm trong mọi cơ chế an ninh đó là: kỹ thuật mã hoá.
- Do đó chúng ta sẽ tập trung vào lý thuyết mã.

7.3. Mã hóa có giải ngược và Mã hóa không thể giải ngược (X800)

- **Cơ chế mã hóa có giải ngược**: là thuật toán mã hóa dùng để mã hóa dữ liệu và sau đó có thể giải mã
- **Cơ chế mã hóa không giải ngược**: gồm các thuật toán băm và các mã xác thực tin nhắn được sử dụng trong các ứng dụng xác thực tin nhắn và chữ ký số.
- *Câu hỏi: nếu cần thiết lập cơ chế mã hóa (có thể giải ngược) bảo mật thông tin ta cần dùng các dịch vụ nào?*
- *Trả lời trang sau*

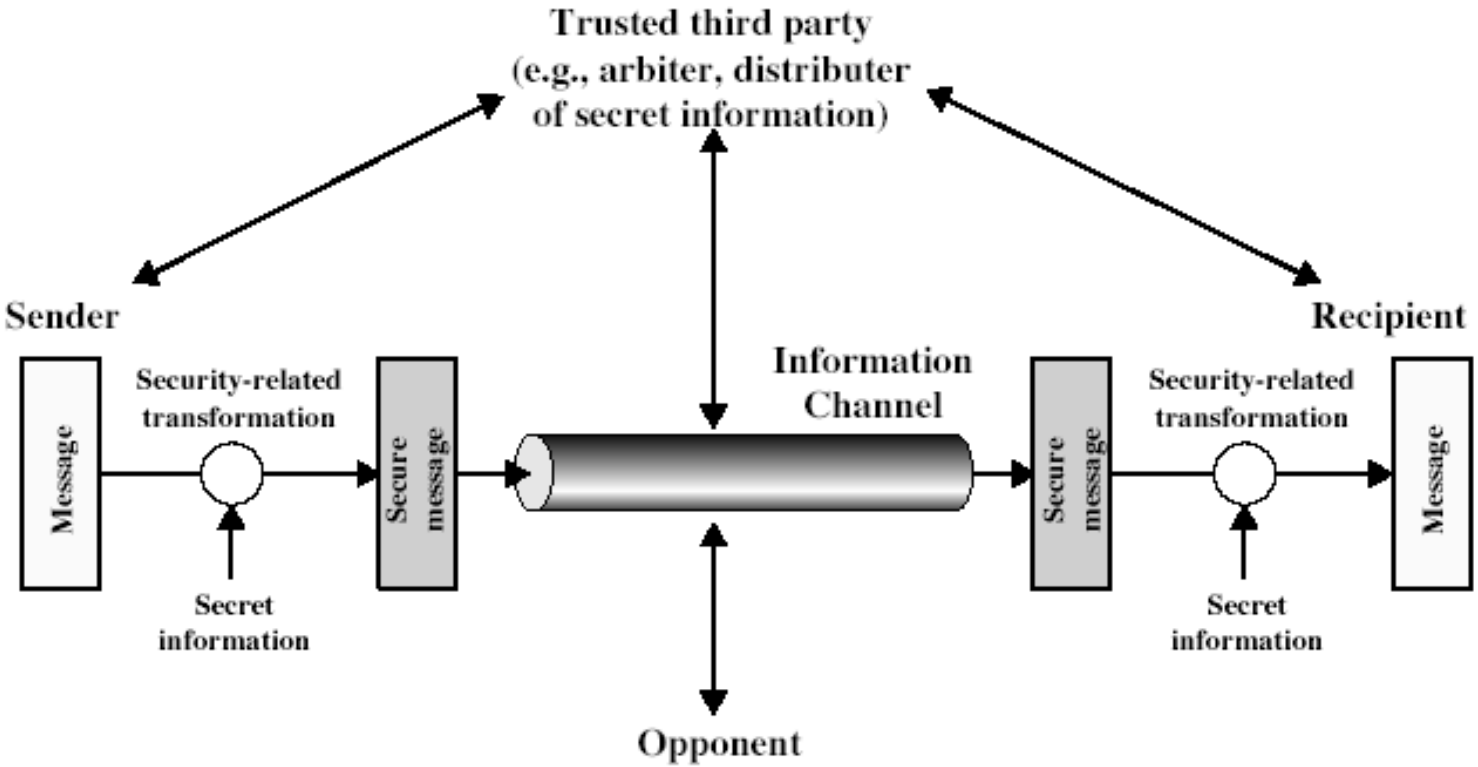
7.4. Quan hệ giữa dịch vụ và cơ chế an ninh

	Cơ chế					
Dịch vụ	Mã hóa	Chữ ký điện tử	Toàn vẹn dữ liệu	Trao đổi xác thực	Đệm đường truyền	Công chứng
Xác thực thực thể ngang hàng	Có	Có		Có		
Xác thực dữ liệu gốc	Có	Có				
Bảo mật	Có					
Bảo mật luồng truyền	Có				Có	
Toàn vẹn dữ liệu	Có	Có	Có			
Chống từ chối		Có	Có			Có
Tính sẵn sàng			Có	Có		

Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

8.1. Mô hình an ninh mạng



- Security-related transformation (sự biến đổi có tính bảo mật): thuật toán mã hóa, đoạn mã xác thực người gửi
- Secret information (thông tin bí mật): thông tin được chia sẻ giữa người gửi và người nhận mà không để đối thủ biết (khóa mã)
- Trusted third party (bên thứ 3 đáng tín cậy): trọng tài có trách nhiệm phân phối thông tin bí mật giữa 2 bên, hoặc để đảm bảo tính xác thực của 2 bên

8.2. Mô hình an ninh mạng (tiếp)

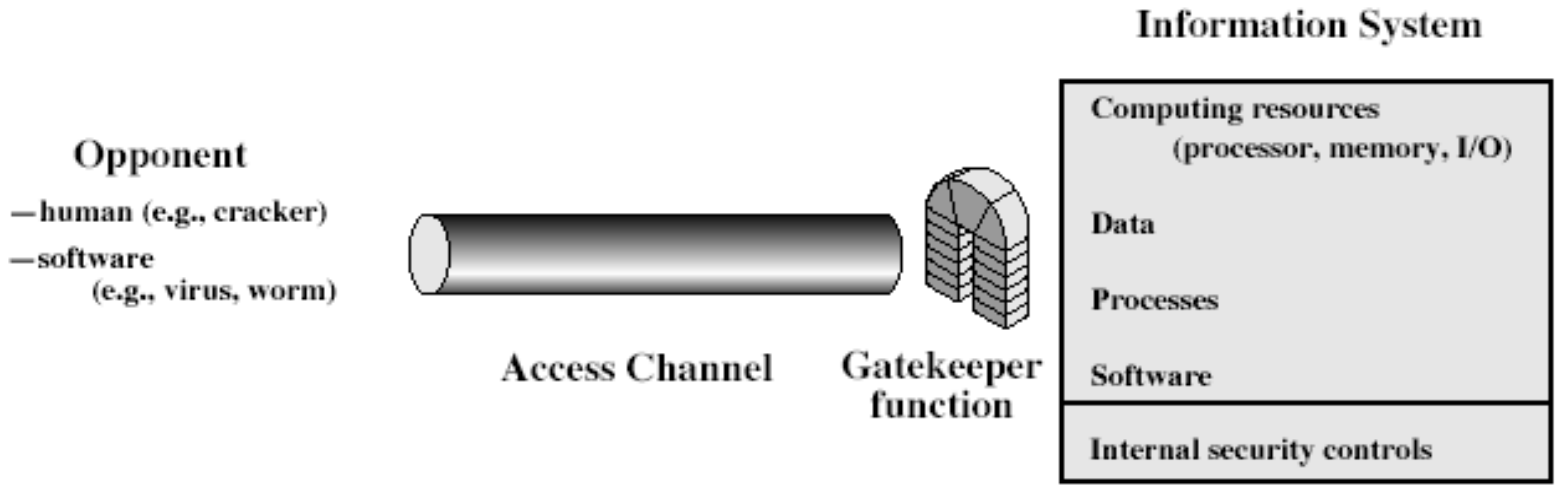
Để đảm bảo an ninh cho mô hình mạng cần thiết kế:

- thuật toán phù hợp cho việc truyền an toàn.
- sinh các thông tin mật (khoá) được sử việc truyền và thông tin mật cho các dịch vụ dụng bởi các thuật toán.
- Phát triển các phương pháp phân phối và chia sẻ các thông tin mật.
- đặc tả giao thức chung cho các bên để sử dụng để đảm bảo an ninh

Nội dung bài 1: Giới thiệu tổng quan

1. Tổng quan về an toàn thông tin
2. Một số loại tấn công an ninh mạng
3. Phương pháp hệ thống bảo đảm an ninh mạng
   - OSI, X800, RFC2828
4. Tấn công bảo mật theo chuẩn X800
5. Các dịch vụ an ninh theo chuẩn X800.
6. Các cơ chế an ninh theo chuẩn X800.
7. Mô hình an ninh trên mạng.
8. Mô hình an ninh truy cập mạng.

9.1. Mô hình an ninh truy cập mạng



=>Mục tiêu: Bảo vệ một hệ thống thông tin từ một truy cập không mong muốn (hacker, virus…)

Các mối đe dọa:

- phá hủy thông tin hoặc lấy thông tin bí mật của người dùng hợp pháp (tài khoản tín dụng…)
- Chặn hoặc sửa đổi dữ liệu
- Khai thác lỗ hổng dịch vụ trong máy tính để ngăn chặn việc sử dụng bởi người dùng hợp pháp

9.2. Mô hình an ninh truy cập mạng

Sử dụng mô hình trên đòi hỏi chúng ta phải:

- Lựa chọn hàm canh cổng phù hợp cho người sử dụng hợp pháp (pass word/login, bộ sàng lọc virus – tường lửa…).
- Sử dụng các phương pháp đa dạng để phát hiện sự tồn tại của kẻ đột nhập không mong muốn
- Các hệ thống máy tính tin cậy có thể dùng mô hình này với các thuật toán phù hợp cho việc truyền an toàn.

Tóm lược cuối bài

- Đã xem xét định nghĩa:
  - an ninh máy tính và an ninh mạng
- Chuẩn X.800
  - tấn công sự an toàn
  - cơ chế an ninh và
  - dịch vụ an ninh
- Mô hình an ninh mạng
- Mô hình an ninh truy cập mạng:

Câu hỏi trắc nghiệm 1

- Câu 1: Mục đích môn học của chúng ta là
  A. An ninh máy tính
  B. An ninh thông tin
  C. An ninh mạng
  D. An ninh Internet
- Câu 2: Tấn công bị động sẽ xảy ra khi Hacker
  A. Giả mạo người khác
  B. Sửa đổi thông tin người gửi
  C. Xem trộm nôi dung thông tin
  D. Làm trễ gói tin - thay đổi thời gian gửi

Câu hỏi trắc nghiệm 2

- Câu 3: Tấn công chủ động sẽ xảy ra khi Hacker
  A. Theo dõi thông tin đường truyền
  B. Đăng thông tin phá hoại trên Web
  C. Xem trộm nôi dung thông tin
  D. Dò tìm mật khẩu
- Câu 4: Dịch vụ xác thực không bao gồm
  A. Cung cấp tài khoản - mật khẩu
  B. Kiểm chứng dấu vân tay
  C. Nhận dạng khuôn mặt người sử dụng
  D. Phân quyền truy cập

Câu hỏi trắc nghiệm 3

- Câu 5: Mục nào không là dịch vụ an ninh
  A. Toàn vẹn thông điệp
  B. Bảo mật thông tin
  C. Chống từ chối 2 phía
  D. Chữ ký điện tử
- Câu 6: Mục nào không là cơ chế an ninh
  A. Mã hóa
  B. Tính sẵn sàng hệ thống
  C. Kiểm soát truy cập
  D. Bộ đệm đường truyền

Câu hỏi trắc nghiệm 4

- Câu 7: Thiết lập cơ chế bảo mật không cần cho dịch vụ nào
  A. Xác thực thực thể đầu cuối, dữ liệu gốc
  B. Bảo mật thông điệp
  C. Chống từ chối 2 phía
  D. Toàn vẹn dữ liệu
- Câu 8: Thiết lập cơ chế toàn vẹn dữ liệu không cần cho dịch vụ nào
  A. Bảo mật
  B. Tính sẵn sàng hệ thống
  C. Toàn vẹn dữ liệu
  D. Chống từ chối

Câu hỏi trắc nghiệm 5

- Câu 9: Thành phần nào không thuộc mô hình an ninh trên mạng
  A. Mã hóa thông điệp
  B. Truyền tin an toàn
  C. Kiểm soát truy cập
  D. Xác thực các bên tham gia gửi nhận
- Câu 10: Thành phần nào không thuộc mô hình kiểm soát quyền truy cập
  A. Kẻ xâm nhập
  B. Hàm canh cổng
  C. Hệ thống thông tin - Tài nguyên tính toán
  D. Bộ công cụ mã hóa

Đáp án câu hỏi trắc nghiệm

- Câu 1
  - C, đôi khi người ta cũng chấp nhận D, vì nói đến an ninh mạng là nói đến an ninh Internet
- Câu 2
  - C, chỉ xem trộm nội dung là tấn công bị động
- Câu 3
  - B, Đăng tin trái phép là tấn công chủ động
- Câu 4
  - D, phân quyền truy cập do dịch vụ Quyền truy cập cung cấp
- Câu 5
  - D, chữ ký điện tử là cơ chế an ninh không phải dịch vụ
- Câu 6
  - B, tính sãn sàng là dịch vụ không phải cơ chế
- Câu 7
  - C, bảo mật là nhiệm vụ chính, không cần dịch vụ chống từ chối
- Câu 8
  - A, không có nhu cầu che dấu nội dung thông điệp
- Câu 9
  - C, kiểm soát truy cập không thuộc an ninh trên mạng
- Câu 10
  - D, Bộ công cụ mã hoá không thuộc Kiểm soát truy cập

Glossary - Từ điển thuật ngữ

- An ninh mạng: các phương tiện bảo vệ dữ liệu khi truyền chúng trên tập các mạng liên kết với nhau
- Lỗ hổng: là điểm yếu của hệ thống mà kẻ xâm nhập lợi dụng để khai thác tấn công.
- Mối đe dọa: khả năng tấn công từ bên ngoài hệ thống nhằm phá hoại hệ thống.
- Tấn công an ninh: mọi hành động chống lại sự an toàn thông tin của các tổ chức
- Dịch vụ an ninh: công cụ tăng cường an ninh cho các hệ thống xử lý dữ liệu và truyền thông tin của các tổ chức
- Cơ chế an ninh: Là các biện pháp được thiết kế để phát hiện, bảo vệ hoặc khôi phục do tấn công phá hoại.
- Hàm canh cổng: phát hiện và ngăn chặn các truy cập trái phép thông qua các tiêu chuẩn lọc

Glossary - Từ điển thuật ngữ - tiếp

- **Xác thực**: tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố
- **Quyền truy cập**: ngăn cấm việc sử dụng nguồn thông tin không đúng vai trò
- **Bảo mật dữ liệu**: bảo vệ dữ liệu không bị khám phá bởi người không có quyền
- **Toàn vẹn dữ liệu**: tin tưởng là dữ liệu nhận được được gửi từ người có thẩm quyền
- **Chống từ chối**: chống lại việc chối bỏ của một trong các bên tham gia trao đổi.
- **Tính sẵn sàng của hệ thống**: chống việc làm giảm hoặc mất khả năng làm việc của hệ thống
- **Cơ chế an ninh chuyên dụng**: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng, công chứng
- **Cơ chế an ninh phổ dụng**: chức năng tin cậy, nhãn an ninh, phát hiện sự kiện, vết theo dõi an ninh, khôi phục an ninh.

FAQ – Câu hỏi thường gặp

1. Nêu sự khác biệt giữa lỗ hổng và mối đe dọa
2. Lấy ví dụ về mối đe dọa liên quan đến việc phá hoại dữ liệu, phần cứng và phần mềm.
3. Cho ví dụ về mối đe dọa liên quan đến lỗi của hệ thống
4. Nêu ví dụ về lỗ hổng an ninh mạng
5. Nêu một số ví dụ tấn công an ninh
6. Nêu 6 dạng dịch vụ của an ninh mạng
7. Liệt kê một số cơ chế an ninh

FAQ – Câu hỏi thường gặp (tiếp)

8. Giải thích sự khác nhau giữa định danh và xác thực
9. Thế nào là mã hóa có giải ngược và mã hoá không có giải ngược
10. Chữ ký điện tử của 1 người với một nội dung cụ thể phụ thuộc vào những gì?
11. Nêu các khía cạnh của dịch vụ xác thực?
12. Nêu các khía cạnh của dịch vụ bảo mật?
13. Nêu các khía cạnh của dịch vụ toàn vẹn dữ liệu?
14. Nêu các khía cạnh của dịch vụ chống từ chối?
15. Theo bạn trên kênh truyền có những biện pháp an ninh nào được sử dụng
16. Nhiệm vụ của hàm canh cổng là gì?

Trả lời câu hỏi:

1. Lỗ hổng là điểm yếu của hệ thống mà kẻ xâm nhập lợi dụng để khai thác tấn công. Mối đe dọa là khả năng tấn công từ bên ngoài hệ thống nhằm phá hoại hệ thống.
2. Các mối đe dọa phá hoại
   - Virus, sâu
   - Phá hoại, ăn cắp
   - Tấn công từ chối dịch vụ
   - Xem lén
3. Các mối đe doạ do
   - Lỗi người sử dụng
   - Lỗi kỹ thuật
   - Lỗi trên đường truyền
4. Lỗ hổng an ninh:
   - Không huấn luyện người sử dụng
   - Không phòng chống virus
   - Không có thủ tục backup
   - Không kiểm soát quyền truy cập
   - Không có bức tường lửa

Trả lời câu hỏi – (tiếp 1)

5. Dò tìm mật khẩu, tiếm quyền truy cập, sửa xóa thông tin,…
6. Xem bài giảng
7. Xem bài giảng
8. Định danh: thực thể đó là ai. Xác thực: anh ta có đúng là người đã xưng tên không
9. Mã hoá có giải ngược là thay thế thông điệp bằng thông điệp khác mà người khác không đọc được, chỉ người có thông tin mật mơi có thể khôi phục lại thông điệp gốc. Mã hoá không có giải ngược là nén thông điệp về một thông tin cố định, không ai có thể khôi phục lại thông điệp gốc. Nó được dùng để giúp người nhận kiểm tra phát hiện sự thay đổi thông điệp gốc
10. Chữ ký điện tử của 1 người phụ thuộc vào thông tin mật của riêng người đó và chính nội dung ký

Trả lời câu hỏi – (tiếp 2)

11. Dịch vụ xác thực: xác thực thực thể đầu cuối, xác thực dữ liệu gốc
12. Dịch vụ bảo mật: bảo mật kết nối - bảo mật dữ liệu NSD lúc kết nối; bảo mật không kết nối - bảo mật dữ liệu của một khối dữ liệu duy nhất; bảo mật trường nào đó; bảo mật luồng truyền
13. Dịch vụ toàn vẹn dữ liệu: toàn vẹn kết nối có/không khôi phục, toàn vẹn không kết nối, và với 1 trường.
14. Dịch vụ chống từ chối: chống từ chối người gửi, nhận
15. Các biện pháp trên đường truyền: mã hóa đường truyền, bộ đệm truyền, thêm thông tin để phát hiện và khắc phục lỗi,
16. Hàm canh cổng phát hiện và ngăn chặn các truy cập trái phép thông qua các tiêu chuẩn lọc