An ninh mạng

Bài 1: Giới thiệu về an ninh mạng

Thời lượng học: 3 tiết

Môn học An ninh mạng

- Bài 1: Mở đầu
- Bài 2: Mã đối xứng
- Bài 3: Mã công khai
- Bài 4: Các ứng dụng xác thực
- Bài 5: Luyện tập bài tập
- Bài 6: An ninh mạng
- Bài 7: An ninh hệ thống
- Bài 8: Một số ứng dụng

Tình huống dẫn nhập

- Sự bùng nổ của các hệ thống máy tính và việc kết nối chúng qua các mạng ngày làm gia tăng sự phụ thuộc của các tổ chức, cá nhân lưu trữ và trao đổi thông tin qua mạng
- 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 mã hóa và an ninh mạng đã phát triển mạnh mẽ đưa ra nhiều ứng dụng đáp ứng nhu cầu tăng cường an ninh mạng

Nội dung bài: Giới thiệu về an ninh mạng

- Nhiệm vụ an ninh mạng
- Các nguy cơ phá hoại hệ thống
- Chuẩn kiến trúc an ninh ITU-T X800
- Thuật ngữ an ninh RFC 2828
- Các kiểu tấn công an ninh.
- Các dịch vụ an ninh.
- Các cơ chế an ninh.
- Mô hình an ninh trên mạng.
- Mô hình an ninh truy cập mạng.

Mục tiêu

- Nhận biết các mối đe dọa 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
- Xác định được mục đích môn học

1.1 Nhu cầu an ninh mạng

- an ninh thông tin đã thay đổi rất nhiều trong thời gian gần đây
- Các phương pháp truyền thống được cung cấp bởi các cơ chế hành chính và phương tiện vật lý
- Máy tính đòi hỏi các phương pháp tự động để bảo vệ các files và các thông tin lưu trữ
- Việc sử dụng mạng và truyền thông đòi hỏi phải có các phương tiện bảo vệ dữ liệu khi truyền
- *Câu hỏi: Bạn có thể nêu một số ví dụ về nhu cầu an ninh mạng trong thực tế?*
- *Trả lời: giữ bí mật tài khoản, chống virus, bảo vệ thông tin mật về tài chính, kinh doanh, quản trị trang Web, phân quyền đăng tin, chống phá hoại dữ liệu điểm,…*

1.2 Các nhiệm vụ an ninh

- an ninh máy tính: tập hợp các công cụ được thiết kế để bảo vệ dữ liệu và chống hackers
- an ninh thông tin: các phương tiện bảo vệ dữ liệu khi lưu trữ và truyền chúng
- an ninh mạng: các phương tiện bảo vệ dữ liệu khi truyền chúng trên tập các mạng liên kết với nhau

Mục đích của môn học

- Tập trung vào an ninh mạng
- An ninh mạng gồm các phương tiện để bảo vệ, chống, phát hiện, và hiệu chỉnh các phá hoại an toàn khi truyền và lưu trữ thông tin.

1.3 Các vấn đề về an ninh

- Một số người dùng mánh lới để lấy thông tin cá nhân của người khác
- Có thể phân loại:
  - Ăn cắp danh tính
  - Mạo danh người khác
- Vấn đề cốt lõi:
  - Không có xác thực
  - Người thông báo có đúng người đã tuyên bố không?
- Làm sao có thể kiểm chứng tính xác thực:
  - Kiểm tra địa chỉ URL (có ai chứng nhận không)
  - Nội dung có bị thay đổi không
  - Thông tin cá nhân có được giữ bí mật không

1.4 Kiến trúc an ninh OSI

- Tổ chức ITU (international Telecommunication Union) đề xuất kiến trúc an ninh OSI X800.
- Kiến trúc ITU X800 dành cho hệ thống trao đổi thông tin mở OSI đưa ra một cách tiếp cận hệ thống về an ninh
- 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

Kiến trúc an ninh cho an ninh mạng đầu cuối đến đầu cuối

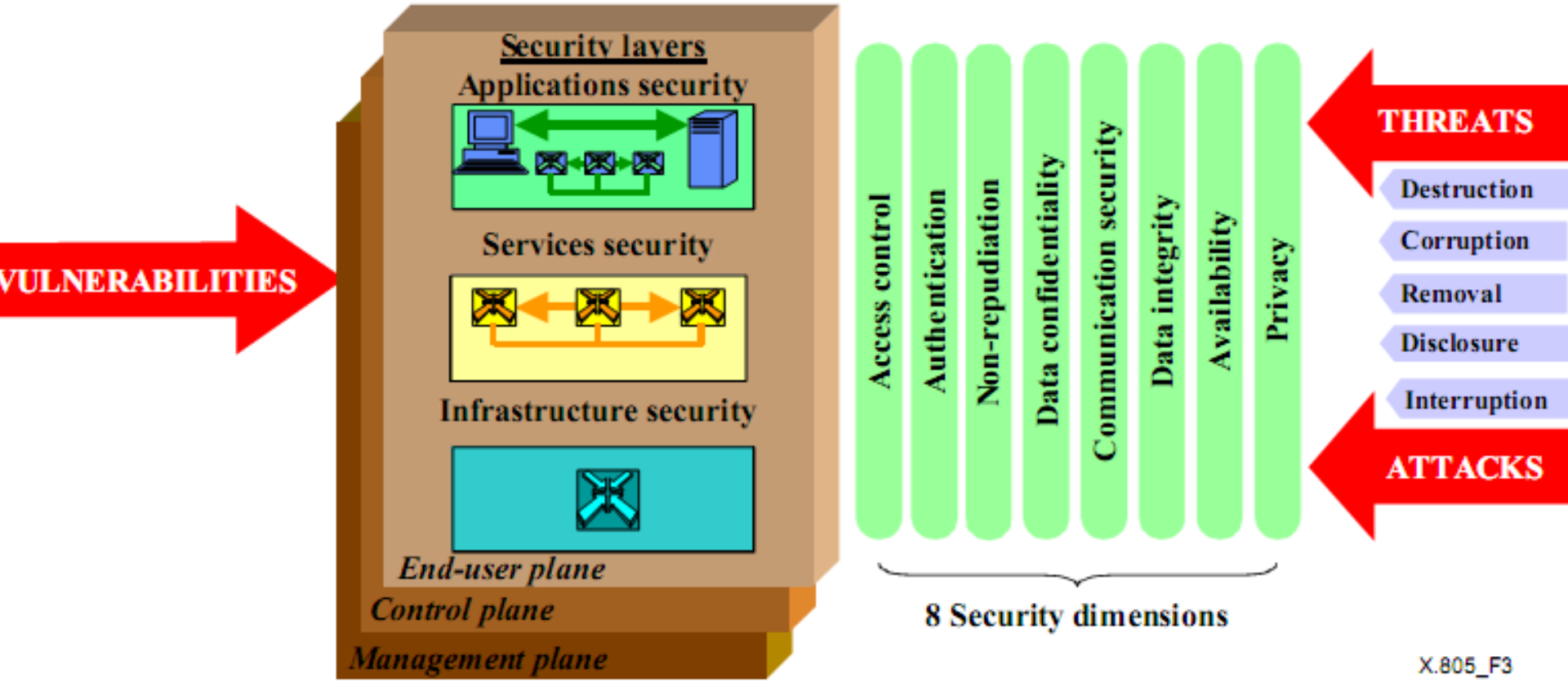


Figure 3/X.805 – Security architecture for end-to-end network security

Tấn công, cơ chế và dịch vụ

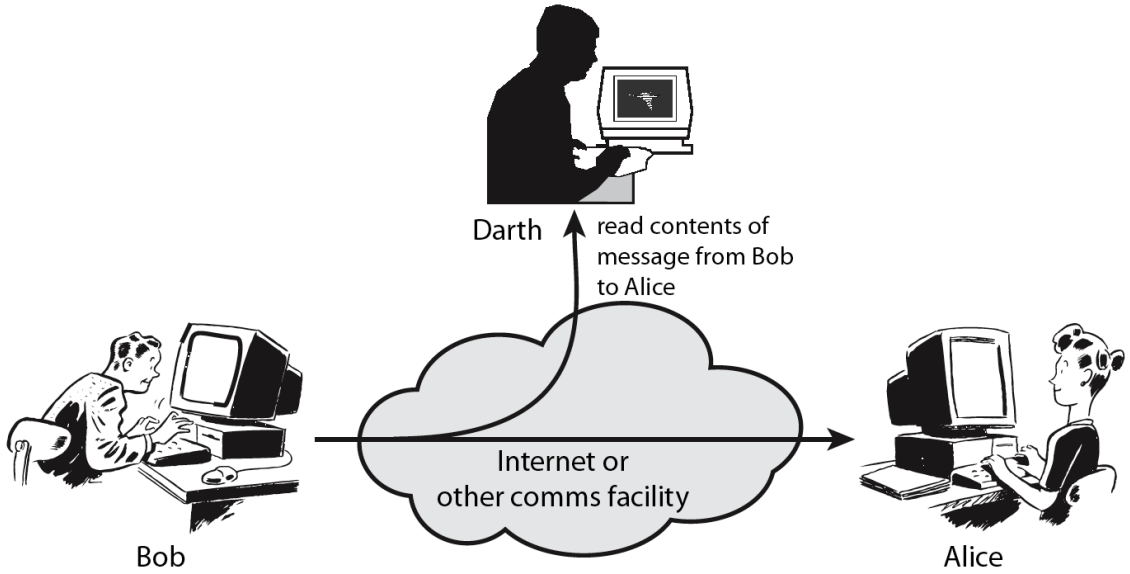
- Mọi hành động chống lại sự an toàn thông tin của các tổ chức
- Cơ chế: phát hiện, bảo vệ và khôi phục hệ thống do bị tấn công
- Dịch vụ: cung cấp biện pháp tăng cường an ninh cho các hệ thống xử lý và truyền thông tin, chống lại các tấn công

Tấn công sự an toàn

- Mọi hành động chống lại sự an toàn thông tin của các tổ chức
- An toàn thông tin là bàn về bằng cách nào chống lại tấn công vào hệ thống thông tin hoặc phát hiện
- Thường đe doạ và tấn công được dùng như nhau
- Có nhiều cách và nhiều kiểu tấn công
- Cần tập trung chống một số kiểu tấn công chính
  - Thụ động và
  - Chủ động

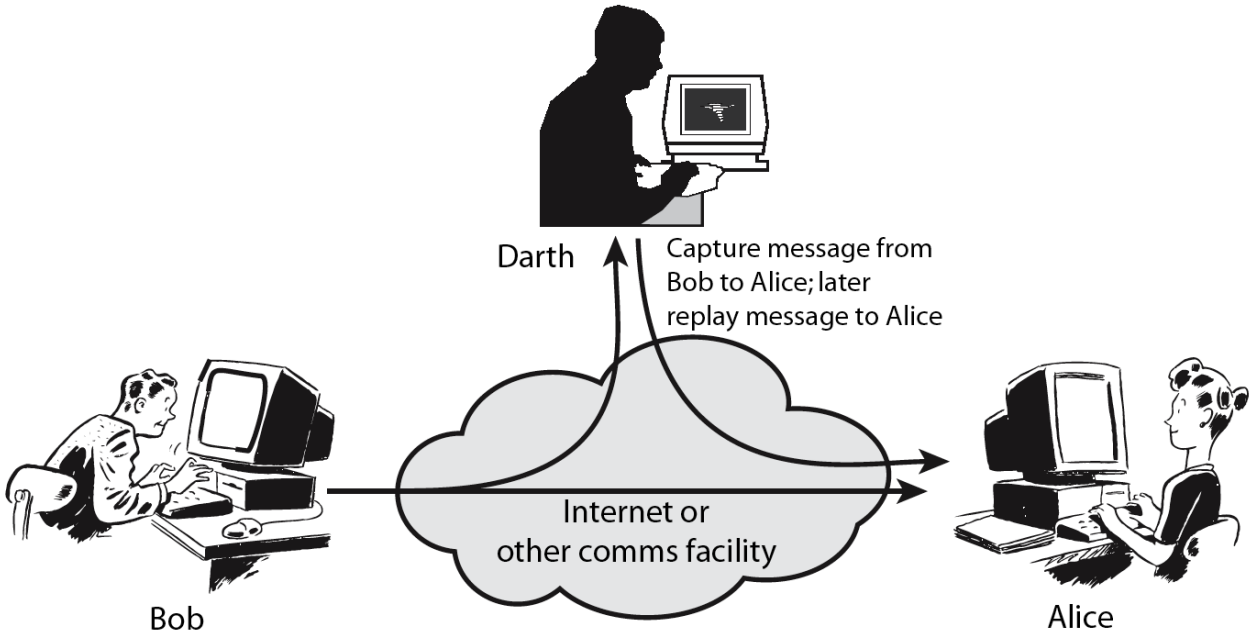
Tấn công phá hoại an ninh

- Tấn công bị động: do thám, theo dõi đường truyền để
  - nhận được nội dung bản tin hoặc
  - theo dõi luồng truyền tin
  - Khó bị phát hiện



Tấn công chủ động

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



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
- 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, …

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
- *Câu hỏi: Bạn có thể nêu một số dạng tấn công an ninh trong thực tế?*
- *Trả lời: hacker Web, đăng tin không có thẩm quyền, lấy mật khẩu tài khoản, làm tê liệt hệ thống, phát tán virus,…*

Dich 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
- Nhằm chống lại các tấn công an ninh
- Sử dụng một trong những cơ chế an ninh
- Thường dùng các hàm liên kết với các tài liệu vật lý
  - Chẳng hạn có chữ ký, ngày tháng, chống do thám, giả mạo hoặc phá hoại, được công chứng hoặc có người làm chứng, được ghi nhận hoặc có bản quyền

1.5 Mô hình an ninh mạng

- ITU X.800 định nghĩa dịch vụ an ninh:

  là dịch vụ cung cấp cho các tầng giao thức của các hệ thống mở trao đổi thông tin, mà đảm bảo an ninh thông tin cần thiết cho hệ thống và việc truyền dữ liệu

- RFC 2828 - Thuật ngữ an ninh Internet (chú giải của cộng đồng nghiên cứu phát triển Internet) định nghĩa dịch vụ an ninh:

  là dịch vụ trao đổi và xử lý cung cấp bởi hệ thống cho việc bảo vệ đặc biệt các thông tin nguồn

Dich vụ an ninh (X.800)

- **Xác thực**: tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố (Authentication)
- **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
- *Câu hỏi: Bạn hãy lấy ví dụ về khả năng ứng dụng của các dịch vụ trên trong thực tế?*
- *Trả lời trên trang sau*

Quan hệ giữa dịch vụ và tấn công

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

Mối đe doa và các dich vu an ninh

Table 1/X.805 – Mapping of security dimensions to security threats

Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Các dịch vụ hỗ trợ chống các tấn công

- Chống giả mạo:
  - Xác thực thực thể đầu cuối
  - Xác thực dữ liệu gốc
  - Kiểm soát quyền truy cập
- Dò rỉ thông tin
  - Bảo mật
- Sửa thông điệp
  - Toàn vẹn dữ liệu
- Phân tích đường truyền
  - Bảo mật luồng truyền
- Tấn công từ chối dịch vụ
  - Dịch vụ tính sẵn sàng

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.

Cơ chế an ninh của X800

- 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.
- *Câu hỏi: nếu cần thiết lập cơ chế mã hóa bảo mật thông tin ta cần dùng các dịch vụ nào?*
- *Trả lời trang sau*

Quan hệ giữa dịch vụ và cơ chế an ninh

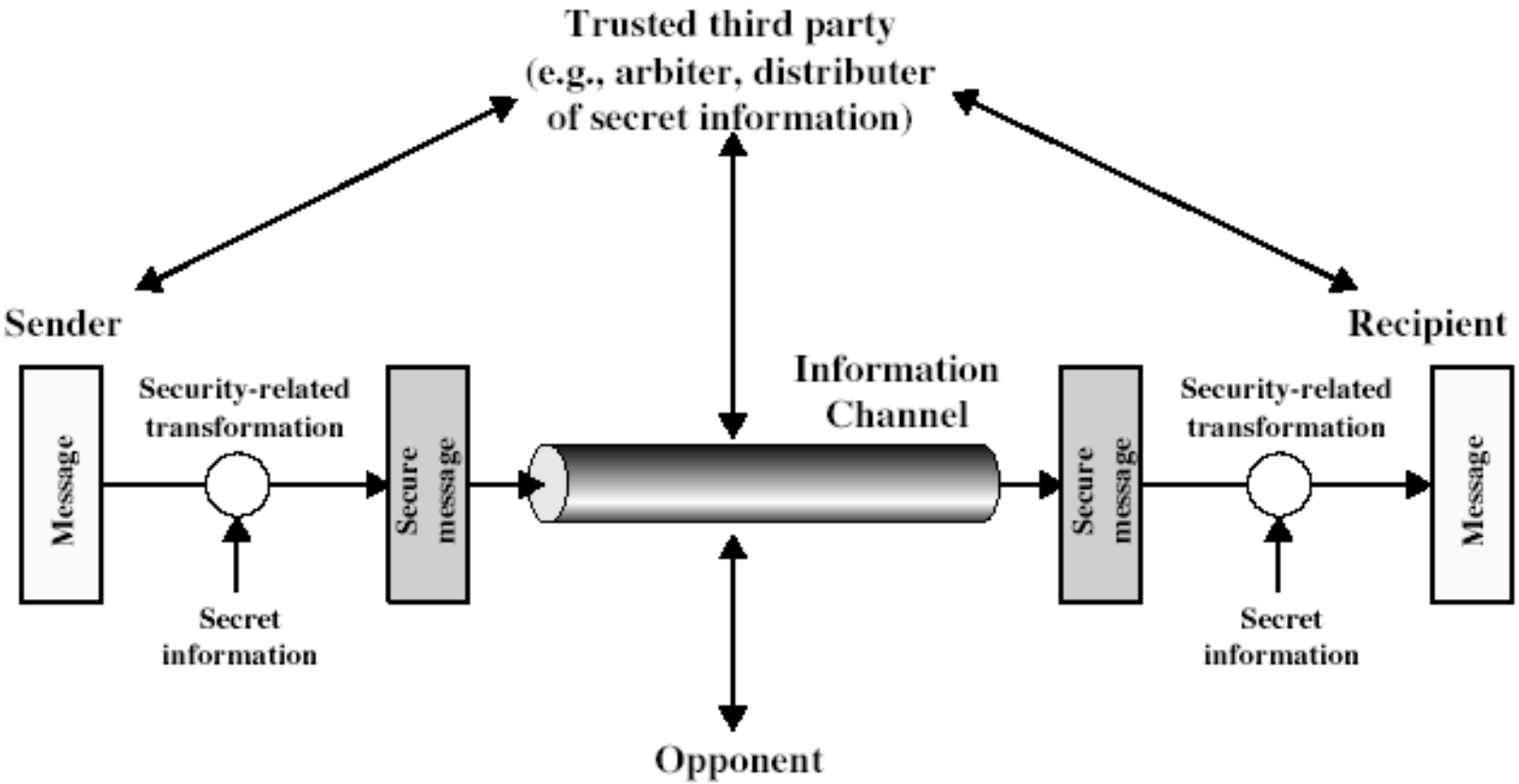
		Cơ	chế			
Dịch vụ	Mã	Chữ ký điện tử	Toàn vẹn dữ liệu	Trao đổi xác thực	Đệm đường truyền	Công chứng
Xác thực đầu cuối	có	có		có		
Xác thực dữ liệu gốc	có	có				
Bảo mật	Có					
Bảo mật luồng truyền	có				có	
Toàn vẹn dữ liệu	có	có	có			
Chống từ chối		có	có			có
Tính sẵn sàng			có	có		

Quan hệ giữa dịch vụ và cơ chế an ninh
Ví dụ: Thiết lập cơ chế mã hoá

Đây là mã hóa có giải ngược, để thiết lập được cơ chế mã hóa, X800 đề xuất sử dụng các dịch vụ sau:

- Xác thực thực thể đầu cuối
- Xác thực dữ liệu gốc
- Bảo mật thông điệp
- Bảo mật lưu lượng đường truyền
- Toàn vẹn dữ liệu

Mô hình an ninh mạng

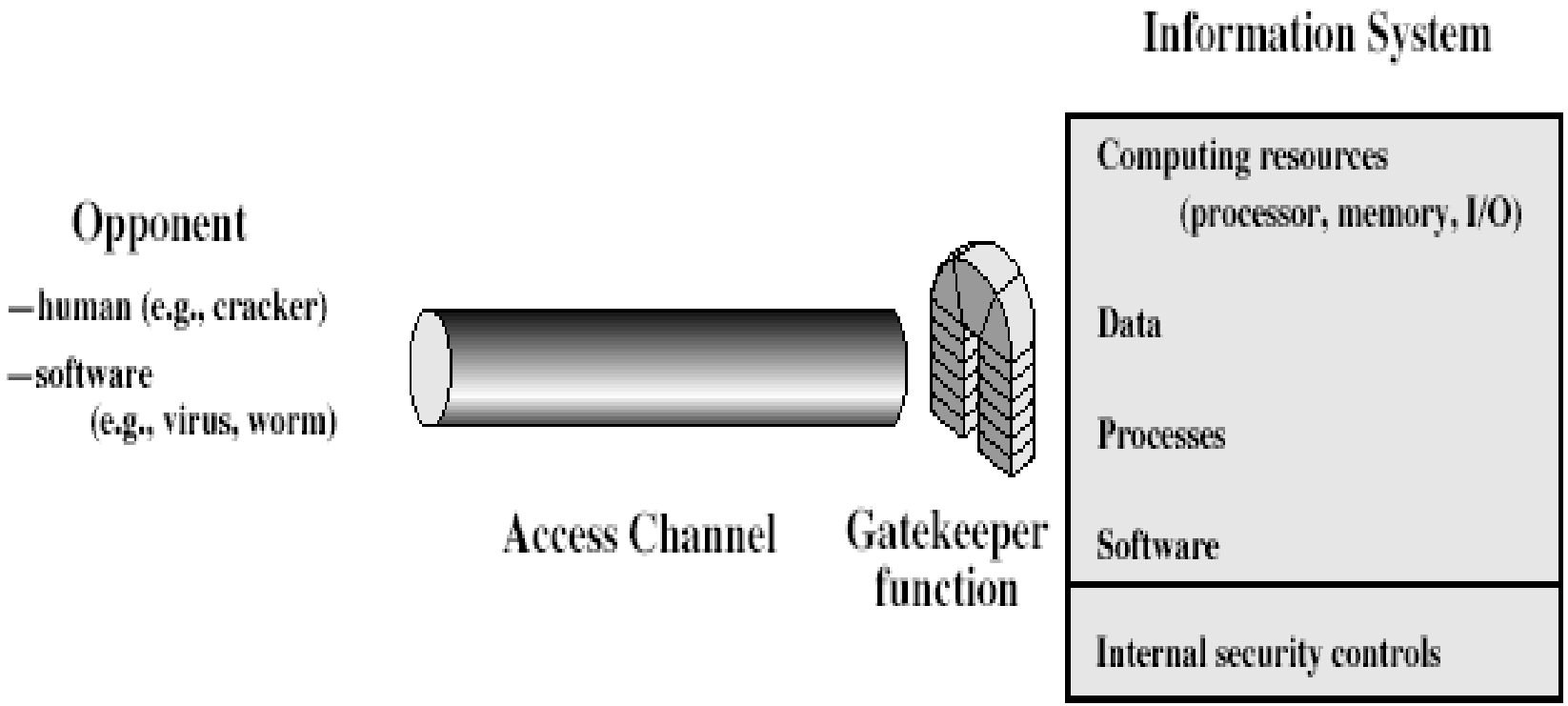


Mô hình an ninh mạng

Sử dụng mô hình trên đòi hỏi chúng ta phải thiết kế:

- thuật toán phù hợp cho việc truyền an toàn.
- Phát 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 cho các bên để sử dụng an ninh

Mô hình an ninh truy cập mạng



Mô hình an ninh truy cập mạng

Sử dụng mô hình trên đòi hỏi chúng ta phải:

- Bảo vệ thông tin trên kênh truyền
- Lựa chọn hàm canh cổng phù hợp cho người sử dụng có danh tính.
- Cài đặt kiểm soát quyền truy cập để tin tưởng rằng chỉ có người có quyền mới truy cập được thông tin đích hoặc nguồn.
- Các hệ thống máy tính tin cậy có thể dùng mô hình này.với các thuật toán phù hợp cho việc truyền an toàn.
- *Câu hỏi: Bạn có thể chỉ ra một ví dụ về mối quan hệ giữa tấn công, cơ chế và dịch vụ an ninh trên mô hình trên?*
- *Trả lời trang sau:*

Ví dụ chống tấn công Website một tổ chức

- Tấn công
  - Tiếm quyền, mạo danh, xem thông tin tài khoản
  - Sửa thông điệp, từ chối dịch vụ
- Thiết lập cơ chế
  - Hàm canh cổng kiểm soát quyền truy cập
  - Trao đổi xác thực, mã hóa, toàn vẹn dữ liệu
- Sử dụng dịch vụ:
  - Kiểm soát truy cập, toàn vẹn dữ liệu
  - Xác thực đầu cuối, xác thực dữ liệu gốc
  - Mã hóa, dịch vụ tính sẵn sàng.

Tóm lược cuối bài

- Đã xem xét định nghĩa:
  - an ninh máy tính, thông tin và mạng
- Chuẩn X.800
  - tấn công sự an toàn,
  - cơ chế an ninh và
  - dịch vụ an ninh
- Mô hình an ninh truy cập mạng:
  - Bảo vệ trên kênh truyền và kiểm soát quyền truy cập

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