BÀI MỞ ĐẦU: GIỚI THIỆU VỀ AN TOÀN BẢO MẬT THÔNG TIN

0.1 Giới thiệu chung

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên,…đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh, yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của doanh nghiệp. Vì vậy an toàn và bảo mật thông tin là nhiệm vụ rất quan trọng và khó lường trước được, nhưng tựu trung lại gồm ba hướng chính sau:

- Bảo đảm an toàn thông tin tại máy chủ
- Bảo đảm an toàn cho phía máy trạm
- Bảo mật thông tin trên đường truyền

Ở đây chúng ta sẽ tập trung xem xét các nhu cầu an ninh và đề ra các biện pháp an toàn cũng như vận hành các cơ chế để đạt được các mục tiêu đó.

Nhu cầu an toàn bảo mật thông tin:

- An toàn thông tin đã thay đổi rất nhiều trong thời gian gần đây. Trước kia hầu như chỉ có nhu cầu bảo mật thông tin, nay đòi hỏi thêm nhiều yêu cầu mới như an ninh tại máy chủ và trên mạng.
- Trước kia các phương pháp truyền thống được cung cấp bởi các cơ chế hành chính và phương tiện vật lý như nơi lưu trữ bảo vệ các tài liệu quan trọng và cung cấp giấy phép được quyền sử dụng các tài liệu mật đó.
- Ngày nay máy tính đòi hỏi các phương pháp tự động để bảo vệ các tệp và các thông tin lưu trữ. Nhu cầu bảo mật rất lớn và rất đa dạng, có mặt khắp mọi nơi, mọi lúc. Do đó không thể không đề ra các qui trình tự động hỗ trợ bảo đảm an toàn thông tin.
- Việc sử dụng mạng và truyền thông đòi hỏi phải có các phương tiện bảo vệ dữ liệu khi truyền. Trong đó có cả các phương tiện phần mềm và phần cứng, đòi hỏi có những nghiên cứu mới đáp ứng các bài toán thực tiễn đặt ra.

Các khái niệm. Chúng ta thống nhất một số thuật ngữ cơ bản:

- An ninh máy tính: tập hợp các công cụ được thiết kế để bảo vệ dữ liệu và chống hacker xâm nhập vào máy tính.
- An ninh thông tin: các phương tiện bảo vệ dữ liệu ở nơi lưu trữ và trên đường truyền.
- 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 là tập trung vào an ninh mạng gồm các phương tiện để bảo vệ, chống, phát hiện, và hiệu chỉnh các phá hoại an ninh khi truyền chúng trên các hệ thống mạng liên kết với nhau.

0.2 Nguy cơ và hiểm họa đối với hệ thống thông tin.

Ta xét một số ví dụ vi phạm an ninh sau:

1. Người sử dụng (NSD) A truyền file đến NSD B. Trong file có chứa thông tin nhạy cảm như danh sách lương mà cần bảo mật. NSD C, không được quyền đọc file đó, đã theo dõi đường truyền và lấy được bản sao của file trong quá trình truyền nó.
2. Người quản trị mạng D truyền thông điệp đến máy tính E dưới sự quản trị của mình. Thông điệp chỉ thị máy E cập nhật file phân quyền đến máy tính đó. NSD F ngắt thông điệp, sửa nội dung của nó, bổ sung hoặc xóa bớt bản nhập, và sau đó chuyển tiếp cho E, mà nhận thông điệp như đến từ D và cập nhật file phân quyền tương ứng.
3. Hơn nữa, thay vì ngắt thông điệp, NSD F xây dựng thông điệp của riêng mình với các bản nhập mong muốn và truyền thông điệp này tới E như là nó được truyền từ D. Máy tính E nhận được thông điệp như đến từ người quản trị D và cập nhật file phân quyền truy cập tương ứng.
4. Nhân viên bị đuổi việc không cảnh báo trước. Trưởng phòng nhân sự gửi thông báo đến quản trị hệ thống yêu cầu hủy tài khoản của nhân viên đó. Khi việc hủy đang thực hiện, máy chủ gửi thông điệp đến file nhân viên để khẳng định lại hành động đó. Nhân viên này ngắt thông điệp, trì hoãn nó để thực hiện việc truy cập cuối cùng lấy các thông tin nhạy cảm. Sau đó thông điệp được chuyển tiếp, hành động được thực hiện và khẳng định được truyền. Hành động của nhân viên đó không bị phát hiện trong khoảng thời gian nào đó
5. Thông điệp được gửi từ khách hàng đến người môi giới với lệnh mua một số cổ phiếu. Sau đó, giá cổ phiếu bị giảm xuống, khách hàng từ chối việc đã gửi lệnh mua.

Sau đây là sơ lược các giải pháp an ninh có thể bổ sung cho các tình huống trên:

1. NSD A mã hóa file trước khi truyền cho B bằng 1 thuật toán mã hóa tốt và 1 khóa chia sẻ giữa A và B. NSD C không có khóa giải mã nên không đọc được nội dung file.
2. Người sử dụng D cần gửi bản cập nhật file phân quyền kèm một bản nén của file đó (còn gọi là bản băm), để khi E nhận được file phân quyền, sẽ tạo bản nén của file nhận được, rồi so sánh với bản nén đính kèm file. Nếu hai bản nén này giống nhau, chứng tỏ file không bị thay đổi, ngược lại nếu khác nhau, chứng tỏ file này đã bị sửa đổi.
3. Bản thông điệp cập nhật quyền truy cập mà C gửi cho D cần được C ký, để khi nhận được D sẽ kiểm tra chữ ký xem có phải C gửi không và nội dung có bị sửa không. Ngoài ra có thể xác nhận thêm địa chỉ máy chủ gửi thông điệp đó, để biết là thông điệp được gửi từ máy chủ C hay máy khác.

4. Thông điệp hủy quyền truy cập của nhân viên bị đuổi việc cần được kiểm tra về thời gian gửi, thời gian nhận để đảm bảo không bị trì hoãn trên đường truyền. Đồng thời xác nhận tính toàn vẹn của thông điệp được gửi từ máy chủ quản trị và đến nơi nhận trong thời gian cho phép.
5. Lệnh mua cổ phiếu của khách hàng cần được khách hàng ký trước khi gửi, để khách hàng không thể từ chối rằng đã đặt lệnh mua các cổ phiếu đó (sau khi biết giá cổ phiếu xuống). Đồng thời cũng có giải pháp để đảm bảo rằng người môi giới đã nhận được lệnh mua của khách hàng trong một khoảng thời gian ngay sau đó.

An ninh mạng vừa hay vừa phức tạp, vì có một số nguyên nhân sau:

1. An ninh bao gồm cả việc truyền, và trên mạng càng không đơn giản. Yêu cầu là bảo mật, xác thực, chống từ chối và toàn vẹn.
2. Trong khi phát triển cơ chế bảo mật và thuật toán, cần phải xem xét các tấn công có thể. Đôi khi kẻ tấn công nhìn nhận vấn đề dưới góc độ khác, nên chúng khai thác được các điểm yếu của hệ thống.
3. Đã có các cơ chế an ninh rồi, còn cần phải quyết định dùng chúng ở đâu trên giao thức nào, ở thiết bị nào và thông qua các dịch vụ gì.
4. Cơ chế an ninh thông thường bao gồm nhiều thuật toán và giao thức, nhiều bên tham gia, ví dụ như muốn mã hóa, thì hai bên phải chia sẻ khóa mật, các thuật toán mã hóa và giải mã. Rồi việc phân phối khóa giữa người gửi và người nhận như thế nào, khung thời gian cho việc truyền như thế nào.

Trước hết ta xem xét các hiểm họa có trên hệ thống và phân loại chúng. Các hiểm họa đối với hệ thống có thể được phân loại thành hiểm họa vô tình hay cố ý, chủ động hay bị động.

- Hiểm họa vô tình: khi người dùng khởi động lại hệ thống ở chế độ đặc quyền, họ có thể tùy ý chỉnh sửa hệ thống. Nhưng sau khi hoàn thành công việc họ không chuyển hệ thống sang chế độ thông thường, vô tình để kẻ xấu lợi dụng.
- Hiểm họa cố ý: như cố tình truy cập vào hệ thống một cách trái phép.
- Hiểm họa bị động: là hiểm họa nhưng chưa hoặc không tác động trực tiếp lên hệ thống, như nghe trộm các gói tin trên đường truyền.
- Hiểm họa chủ động: là việc sửa đổi thông tin, thay đổi tình trạng hoặc hoạt động của hệ thống.

Đối với mỗi hệ thống thông tin, mối đe dọa và hậu quả tiềm ẩn là rất lớn, nó có thể xuất phát từ những nguyên nhân sau:

- Từ phía người sử dụng: xâm nhập bất hợp pháp, ăn cắp tài sản có giá trị.
- Trong kiến trúc hệ thống thông tin: tổ chức hệ thống kỹ thuật không có cấu trúc hoặc không đủ mạnh để bảo vệ thông tin.
- Ngay trong chính sách bảo mật an toàn thông tin: không chấp hành các chuẩn an toàn, không xác định rõ các quyền trong vận hành hệ thống.
- Thông tin trong hệ thống máy tính cũng sẽ dễ bị xâm nhập nếu không có công cụ quản lý, kiểm tra và điều khiển hệ thống.

- Nguy cơ hay lỗ hổng nằm ngay trong cấu trúc phần cứng của các thiết bị tin học và trong phần mềm hệ thống và ứng dụng do hãng sản xuất cài sẵn các loại 'rệp' điện tử theo ý đồ định trước, gọi là 'bom điện tử'.
- Nguy hiểm nhất đối với mạng máy tính là tin tặc, từ phía bọn tội phạm.

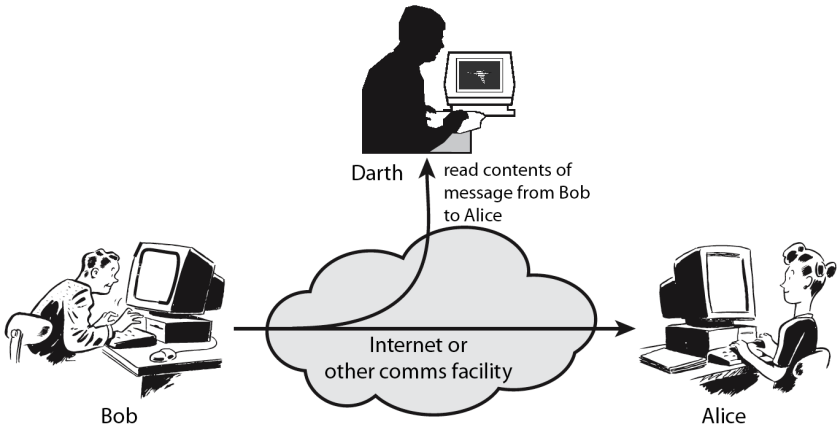
0.3 Phân loại tấn công an ninh

Các hệ thống trên mạng có thể là đối tượng của nhiều kiểu tấn công:

- Tấn công giả mạo là một thực thể tấn công trong khi giả danh một thực thể khác. Tấn công giả mạo thường được kết hợp với các dạng tấn công khác như tấn công chuyển tiếp và tấn công sửa đổi thông báo.
- 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 một thực thể không thể thực hiện chức năng của mình, gây cản trở cho các thực thể khác thực hiện chức năng của chúng.
- Tấn công từ bên trong hệ thống xảy ra khi người dùng hợp pháp cố tình hoặc vô ý can thiệp hệ thống trái phép. Còn tấn công từ bên ngoài là nghe trộm, thu chặn, giả mạo người dùng hợp pháp và vượt quyền hoặc lách qua các cơ chế kiểm soát truy cập.

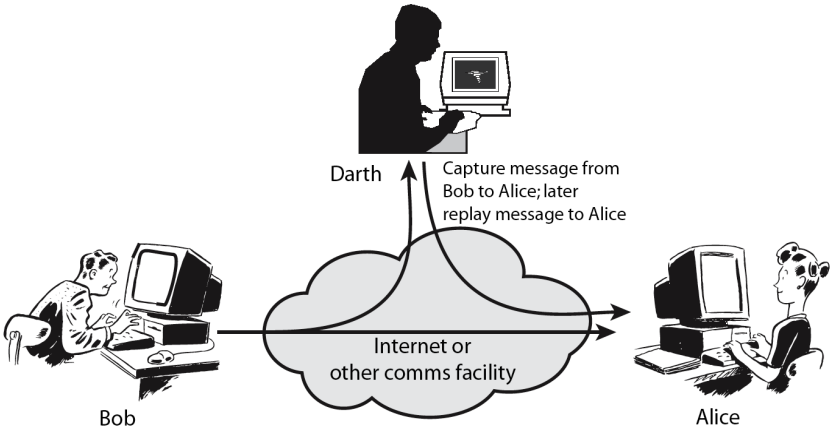
0.3.1 Tấn công bị động

Tấn công bị động là do thám, theo dõi đường truyền để: nhận được nội dung bản tin hoặc theo dõi luồng truyền tin.



0.3.2 Tấn công chủ động

Tấn công chủ động là thay đổi luồng dữ liệu như giả mạo một người nào đó, lặp lại bản tin trước, thay đổi bản tin khi truyền, trì hoãn và tấn công từ chối dịch vụ.



0.4 Dịch vụ, cơ chế, tấn công

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: bảo vệ tấn công, cơ chế an ninh và dịch vụ an ninh.

Sau đây chúng ta xét chúng theo trình tự ngược lại:

0.4.1 Dịch vụ

Đây là các công cụ đảm bảo an ninh của hệ thống xử lý thông tin và truyền thông tin trong tổ chức. Chúng được thiết lập để chống lại các tấn công phá hoại. Có thể dùng một hay nhiều cơ chế an toàn để cung cấp dịch vụ.

Thông thường người ta cần phải tạo ra các liên kết với các tài liệu vật lý: như có chữ ký, xác thực ngày tháng, các bảo vệ cần thiết chống khám phá, sửa sai, phá hoại, được công chứng, chứng nhận, có chủ quyền hoặc có bản quyền.

0.4.2 Cơ chế

Từ các công việc thực tế để chống lại các phá hoại an ninh, người ta đã hệ thống và sắp xếp lại tạo thành các cơ chế an ninh khác nhau. Đây 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 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. Do đó chúng ta sẽ dành một thời lượng nhất định tập trung vào lý thuyết mã.

0.4.3 Tấn công

Ta xác định rõ thế nào là các hành động tấn công phá hoại an ninh. Đó là mọi hành động chống lại sự an toàn thông tin của các tổ chức.

An ninh thông tin là bàn về bằng cách nào chống lại sự tấn công vào hệ thống thông tin hoặc phát hiện ra chúng. Trên thực tế có rất nhiều cách và nhiều kiểu tấn công khác nhau. Thường thuật ngữ đe dọa và tấn công được dùng như nhau. Cần tập trung chống một số kiểu tấn công bị động và chủ động phổ biến.

0.5 Mô hình an ninh mạng

0.5.1 Kiến trúc an ninh mở

Để giúp cho việc hoạch định chính sách và xây dựng hệ thống an ninh tốt. Bộ phận chuẩn hóa tiêu chuẩn của tổ chức truyền thông quốc tế (International Telecommunication Union) đã nghiên cứu và đề ra Kiến trúc an ninh X800 dành cho hệ thống trao đổi thông tin mở OSI. Trong đó, định nghĩa một cách hệ thống phương pháp xác định và cung cấp các yêu cầu an ninh. Nó cung cấp cho chúng ta một cách nhìn tổng quát, hữu ích về các khái niệm mà chúng ta nghiên cứu.

Trong tài liệu các thuật ngữ chuẩn trên Internet RFC 2828 đã nêu các thuật ngữ cụ thể hơn về an ninh.

0.5.2 Các dạng tấn công

- Tấn công bị động: do thám, theo dõi đường truyền để:
  - nhận được nội dung bản tin hoặc;
  - theo dõi phân tích luồng truyền tin.
- Tấn công chủ động có các dạng sau:
  - Giả mạo một người nào đó: mang danh người khác gửi cho người nhận;
  - Lặp lại bản tin: đọc trộm tin, rồi gửi cho người nhận
  - Thay đổi bản tin khi truyền: ngắt dòng tin, chỉnh sửa, rồi gửi cho người nhận
  - Từ chối dịch vụ: gửi quá nhiều yêu cầu đến máy chủ, làm trì hoãn bản tin.

0.5.3 Dịch vụ an ninh

Nói về dịch vụ an ninh, X800 định nghĩa đây là dịch vụ cung cấp cho 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 đã nêu định nghĩa dịch vụ an ninh là dịch vụ trao đổi và xử lý cung cấp việc bảo vệ cho hệ thống, đặc biệt cho các thông tin nguồn.

Tài liệu X800 đưa ra định nghĩa dịch vụ theo 6 loại chính:

- Xác thực: tin tưởng là thực thể trao đổi đúng là cái đã tuyên bố. Người đang trao đổi xưng tên với mình đúng là anh ta, không cho phép người khác mạo danh.
  - Xác thực thực thể đầu cuối: sử dụng liên kết với kết nối logic để cung cấp bằng chứng tin tưởng thực thể đã kết nối.
  - Xác thực dữ liệu gốc: trong truyền tin không kết nối, nó cung cấp bằng chứng tin tưởng rằng nguồn gốc của dữ liệu nhận được đúng là cái đã tuyên bố.
- Quyền truy cập: ngăn cấm việc sử dụng nguồn thông tin mà không có quyền. Mỗi đối tượng trong hệ thống được cung cấp các quyền hạn nhất định và chỉ được hành động trong khuôn khổ các quyền hạn đó.
- Bảo mật dữ liệu: bảo vệ dữ liệu không bị khám phá bởi người không có quyền. Chẳng hạn như dùng các ký hiệu khác để thay thế các ký hiệu trong bản tin, mà chỉ người có quyền mới có thể khôi phục nguyên bản của nó.
  - Bảo mật kết nối: bảo vệ mọi dữ liệu của người sử dụng trong kết nối.
  - Bảo mật không kết nối: bảo vệ một khối dữ liệu của người sử dụng.

  - Bảo mật trường được chọn: bảo mật trường được chọn trong dữ liệu của người sử dụng hoặc trong một khối dữ liệu.
  - Bảo mật luồng truyền: bảo vệ thông tin truyền khỏi bị theo dõi luồng truyền.
- Toàn vẹn dữ liệu: tin tưởng là dữ liệu được gửi từ người có quyền. Nếu có thay đổi như làm trì hoãn về mặt thời gian hay sửa đổi thông tin, thì bằng việc xác thực sẽ cho cách kiểm tra nhận biết là có các hiện tượng đó đã xảy ra hay không.
  - Toàn vẹn kết nối có khôi phục: cung cấp sự toàn vẹn của mọi dữ liệu của người sử dụng trong kết nối để phát hiện sửa, xóa, chèn, trì hoãn toàn bộ dãy dữ liệu với việc thử tự khôi phục.
  - Toàn vẹn kết nối không khôi phục.
  - Toàn vẹn kết nối trường được chọn: cung cấp sự toàn vẹn của trường được chọn trong dữ liệu hoặc khối dữ liệu truyền qua kết nối xem trường đó có bị sửa, chèn, xóa, trì hoãn không.
  - Toàn vẹn không kết nối: cung cấp sự toàn vẹn của khối dữ liệu không kết nối.
  - Toàn vẹn không kết nối trường được chọn.
- Chống từ chối: chống lại việc chối bỏ của một trong các bên tham gia trao đổi.
  - Từ chối gốc: người gửi cũng không chối bỏ là mình đã gửi thông tin với nội dung như vậy.
  - Từ chối đích: người nhận không thể từ chối được là tôi chưa nhận được thông tin đó. Điều này là rất cần thiết trong việc trao đổi, thỏa thuận thông tin hàng ngày.
- Tính sẵn sàng: công cụ hỗ trợ hệ thống luôn có thể được truy cập và phục vụ cho các thực thể có quyền, chống việc làm giảm hoặc mất khả năng làm việc của hệ thống.

Quan hệ giữa dịch vụ và các tấn công an ninh được thể hiện trong bảng sau:

	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

0.5.4 Cơ chế an ninh

Cơ chế an ninh được định nghĩa trong X800 như sau:

- Cơ chế an ninh chuyên dụng được cài đặt trong một giao thức của một tầng mạng nào đó:
    - Mã hoá: sử dụng thuật toán biến đổi dữ liệu thành dạng không đọc bất được, nếu không giải mã. Biến đổi và khôi phục dữ liệu phụ thuộc vào thuật toán và khóa mã hóa.
    - Chữ ký điện tử: là thông tin đính thêm vào thông điệp cho phép người nhận kiểm tra nguồn gốc và tính toàn vẹn của dữ liệu và chống giả mạo.
    - Kiểm soát quyền truy cập: nhiều cơ chế khác nhau buộc đòi hỏi quyền truy cập đến các nguồn tài nguyên.
    - Toàn vẹn dữ liệu: nhiều cơ chế khác nhau sử dụng để tin tưởng vào sự toàn vẹn của dữ liệu hoặc dòng đơn vị dữ liệu.
    - Trao đổi xác thực: cơ chế dùng cho một thực thể tin tưởng vào một thực thể khác bằng việc trao đổi thông tin.
    - Đệm truyền: chèn thêm bit vào các chỗ trống trong dòng dữ liệu truyền để chống phân tích đường truyền.
    - Kiểm soát định hướng: cho phép lựa chọn đường truyền vật lý an toàn cho dữ liệu và cho phép thay đổi đường truyền khi an ninh bị đe dọa.
    - Chứng nhận: cấp bởi bên thứ ba để tin tưởng một số tính chất của việc trao đổi thông tin.
- Cơ chế an ninh phổ dụng không chỉ rõ được dùng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào mà cung cấp:
    - Chức năng tin cậy cho một tiêu chuẩn nào đó.
    - Nhãn an ninh gắn với một nguồn tài nguyên chứng tỏ nó có tính chất nhất định.
    - Phát hiện sự kiện.
    - Theo dõi an ninh: dữ liệu thu thập được dùng để kiểm tra an ninh và là sự giám sát độc lập của vết lưu hệ thống.
    - Khôi phục an ninh: đáp ứng yêu cầu của cơ chế như kiểm soát sự kiện, các chức năng quản trị và thực hiện các hành động khôi phục.

Quan hệ giữa dịch vụ và cơ chế an ninh được thể hiện trong Bảng sau:

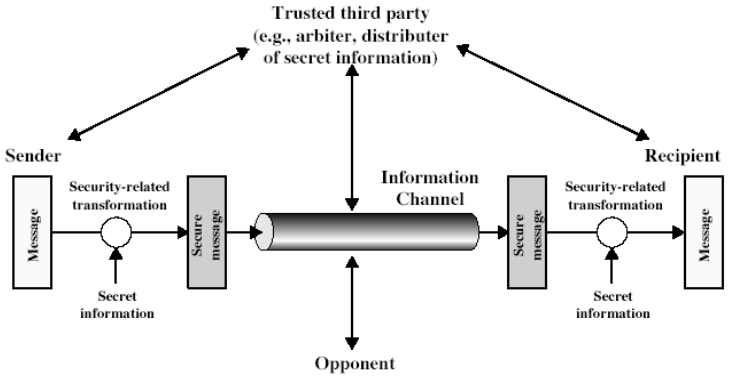
	Cơ chế					
Dịch vụ	Mã	Chữ ký điện tử	Toàn vẹn dữ liệu	Trao đổi xác thực	Đệm đường truyền	Công chứng
Xác thực đầu cuối	Có	Có		Có		
Xác thực dữ liệu gốc	Có	Có				
Bảo mật	Có					

Bảo mật luồng truyền	Có				Có	
Toàn vẹn dữ liệu	Có	Có	Có			
Chống từ chối		Có	Có			Có
Tính sẵn sàng			Có	Có		

0.5.5 Mô hình an ninh mạng tổng quát

Sử dụng mô hình an ninh mạng tổng quát đòi hỏi chúng ta phải thiết kế:

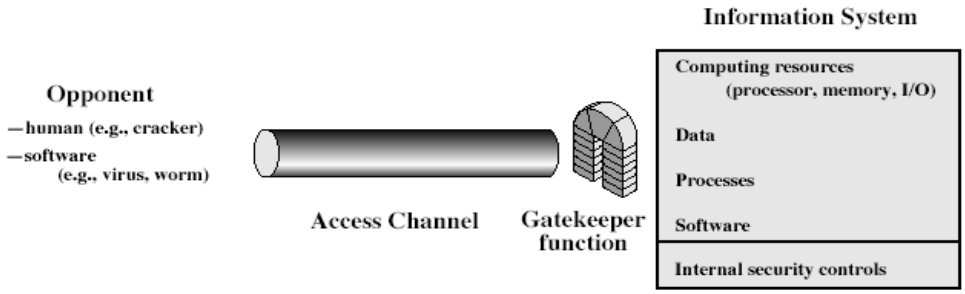
- Thuật toán phù hợp cho việc truyền an toàn.
- Phát sinh các thông tin mật (khoá) được sử dụng bởi các thuật toán.
- Phát triển các phương pháp phân phối và chia sẻ các thông tin mật.
- Đặc tả giao thức để các bên sử dụng các thuật toán và thông tin mật trong các dịch vụ an ninh.



0.5.6 Mô hình an ninh truy cập

Sử dụng mô hình an ninh truy cập đòi hỏi chúng ta phải:

- Lựa chọn hàm canh cổng phù hợp cho người sử dụng có danh tính. Thông thường xác thực danh tính người dùng thông qua Tài khoản và mật khẩu.
- 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. Sử dụng máy chủ kèm theo cơ sở dữ liệu phân quyền để chỉ cho phép người dùng được thực hiện các thao tác trong quyền hạn của mình.
- Các hệ thống máy tính tin cậy có thể dùng mô hình này.



TÓM LƯỢC CUỐI BÀI

Qua kiến thức bài giới thiệu an ninh mạng, anh chi nắm được:

- Các định nghĩa:
  An ninh máy tính, an ninh thông tin và an ninh mạng
- Chuẩn X.800
  - Tấn công an ninh:
    - Tấn công bị động
    - Tấn công chủ động
  - Cơ chế an ninh:
    - Cơ chế an ninh chuyên dụng
    - Cơ chế an ninh phổ dụng
  - Dịch vụ an ninh:
    - Xác thực
    - Quyền truy cập
    - Bảo mật dữ liệu
    - Toàn vẹn dữ liệu
    - Chống từ chối
    - Tính sẵn sàng của hệ thống
- Mô hình an ninh mạng
- Mô hình an ninh truy cập mạng

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

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 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 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 7: Thiết lập cơ chế bảo mật không cần 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 dịch vụ nào
A. Bảo mật
B. Tính sẵn sàng hệ thống
C. Toàn vẹn dữ liệu
D. Chống từ chối

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

TRẢ LỜI CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

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 giấu 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

CÁC THUẬT NGỮ THƯỜNG GẶP

- 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
- 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.

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
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 CÁC CÂU HỎI THƯỜNG GẶP

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

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
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

CÂU HỎI TỰ LUẬN

Câu 1. Nêu 5 ví dụ thực tế cho mỗi loại khái niệm sau đây: lỗ hổng, nguy cơ, tấn công?

Câu 2. Tại sao phải chuẩn hóa các tấn công, cơ chế và dịch vụ an ninh? Chuẩn X800 là của tổ chức nào? Thuật ngữ RFC 2828 đem lại lợi ích gì?

Câu 3. Nêu các cơ chế an ninh chuyên dụng và phổ dụng?

Câu 4. Mô tả các dịch vụ an ninh? Cho ví dụ minh họa dùng để phòng chống tấn công cụ thể nào?

Câu 5. Nêu các khía cạnh của dịch vụ xác thực?

Câu 6. Nêu các khía cạnh của dịch vụ bảo mật?

Câu 7. Nêu các khía cạnh của dịch vụ toàn vẹn dữ liệu?

Câu 8. Nêu các khía cạnh của dịch vụ chống từ chối?

Câu 9. Trên mô hình an ninh mạng tìm các vị trí có thể bị tấn công, nêu biện pháp phòng chống tương ứng?

Câu 10. Nêu các nguy cơ tấn công trên mô hình an ninh truy cập mạng và mô tả các chức năng của hàm canh cổng ngăn chặn chúng.

BÀI TẬP TRẮC NGHIỆM

1. Theo bạn dịch vụ nào không chống được tấn công mạo danh:

a) Xác thực thực thể.

b) Xác thực dữ liệu gốc.

c) Kiểm soát quyền truy cập.

d) Bảo mật luồng truyền

2. Để chống việc xem lén nội dung thông điệp bạn dùng dịch vụ nào:

a) Toàn vẹn dữ liệu

b) Chống từ chối

c) Bảo mật

d) Đảm bảo tính sẵn sàng.

3. Để chống việc sửa đổi thông điệp bạn dùng dịch vụ nào:

a) Kiểm soát quyền truy cập. b) Toàn vẹn dữ liệu.

c) Bảo mật d) Chống từ chối.

4. Dịch vụ nào sau đây không phục vụ cho cơ chế chữ ký điện tử

a) Xác thực dữ liệu gốc b) Toàn vẹn dữ liệu.

c) Chống từ chối. d) Đảm bảo tính sẵn sàng của hệ thống.

5. Dịch vụ nào sau đây không phục vụ cho cơ chế toàn vẹn dữ liệu:

a) Kiểm soát quyền truy cập. b) Dịch vụ toàn vẹn dữ liệu.

c) Chống từ chối. d) Đảm bảo tính sẵn sàng của hệ thống.

6. Cơ chế nào sau đây không phải là cơ chế an ninh chuyên dụng

a) Mã hoá.

b) Chữ ký điện tử.

c) Trao đổi xác thực.

d) Khôi phục an ninh.

7. Cơ chế nào sau đây không phải là cơ chế an ninh phổ dụng

a) Nhãn an ninh.

b) Kiểm soát quyền truy cập.

c) Theo dõi an ninh.

d) Chức năng tin cậy thiết lập bởi chính sách an ninh.

8. Thiết lập cơ chế chữ ký điện tử không cần sử dụng các dịch vụ nào?

a) Xác thực.

b) Toàn vẹn dữ liệu

c) Tính sẵn sàng của hệ thống.

d) Chống từ chối.

9. Thiết lập cơ chế kiểm soát quyền truy cập cần sử dụng các dịch vụ nào?

a) Xác thực.
b) Toàn vẹn dữ liệu
c) Chống từ chối.
d) Kiểm soát truy cập

10. Thiết lập cơ chế kiểm soát định tuyến không cần sử dụng các dịch vụ nào?

a) Bảo mật
b) Bảo mật luồng truyền
c) Toàn vẹn dữ liệu.
d) Xác thực.

11. Nhận định nào sai về việc sử dụng các cơ chế an toàn

a) Các phương pháp, công cụ và thủ tục để tạo nên các tính chất an toàn.
b) Phân loại tùy theo mức độ gồm: ngăn chặn, phát hiện, khôi phục.
c) Chỉ nên dùng một trong các cơ chế, không nên dùng kết hợp nhiều cơ chế
d) Làm cho các tấn công bị thất bại

12. Nhận định nào sai về tính sẵn sàng:

a) Nhằm làm cho mọi người tin tưởng rằng mọi thông tin và nguồn gốc luôn sẵn sàng khi họ cần.
b) Bởi vì ai đó có thể tạo nên việc chối từ truy cập đến dữ liệu, nguồn gốc, dịch vụ bằng cách làm cho nó không sẵn sàng.
c) Các khía cạnh của tính sẵn sàng: hỗ trợ đạt được sự tin cậy, có thể phát hiện sự kiện bất thường.
d) Tính sẵn sàng hỗ trợ tính toàn vẹn

13. Nhận định nào sai về xác thực:

a) Xác thực là tin tưởng rằng đối tác trao đổi thông tin đúng là người xưng danh.
b) Xác thực danh tính sử dụng khi kết nối logic để tin tưởng vào danh tính người kết nối
c) Xác thực bản tin gốc dùng khi truyền bản tin để tin tưởng dữ liệu nhận được đúng là gốc.
d) Xác thực có thể dùng thay cho chữ ký điện tử.

14. Nhận định nào sai về bảo mật dữ liệu:

a) Bảo mật dữ liệu là giấu thông tin hoặc nguồn gốc để cấm khai thác không bản quyền
b) Bảo mật kết nối là bảo vệ dữ liệu của người sử dụng khi kết nối
c) Nguyên tắc "cần mới được biết", tức là mọi người sử dụng trong hệ thống chỉ được biết những gì cho phép.
d) Bảo mật sẽ đảm bảo hoàn toàn xác thực người gửi

15. Nhận định nào sai về cơ chế bảo đảm tính toàn vẹn:

a) Cơ chế cấm mọi cách thay đổi nội dung, mà không bản quyền.
b) Cơ chế phát hiện và báo cáo các vi phạm tính toàn vẹn bằng cách phân tích dữ liệu và sự kiện
c) Dùng việc mã hoá để kiểm soát sự toàn vẹn

d) Dùng hàm băm hash làm dấu vân tay của bản tin