BỘ CÔNG THƯƠNG

TRƯỜNG CAO ĐẲNG CÔNG NGHIỆP VÀ THƯƠNG MẠI

GIÁO TRÌNH

MÔ ĐUN: AN TOÀN MẠNG

NGHỀ QUẢN TRỊ MẠNG MÁY TÍNH

TRÌNH ĐỘ: CAO ĐẲNG NGHỀ

Ban hành kèm theo Quyết định số: /QĐ-CDCN&TM ngày tháng năm 2018 của Hiệu trưởng Trường Cao đẳng Công nghiệp Phúc Yên

Vĩnh Phúc, năm 2018

MỤC LỤC

CHƯƠNG TRÌNH MÔN HỌC/ MÔ ĐUN

Tên mô đun: An toàn mạng
Mã mô đun: MĐCC13030181
Thời gian thực hiện mô đun: 90 giờ; (Lý thuyết: 30 giờ; Thực hành, thí nghiệm, thảo luận, bài tập: 57 giờ; Kiểm tra: 3 giờ)

I. Vị trí, tính chất của mô đun:

Mô đun được bố trí sau khi học sinh học xong các môn học chung, các môn học cơ sở chuyên ngành đào tạo chuyên môn nghề.

- Tính chất của môn học: Là mô đun chuyên ngành bắt buộc.

II. Mục tiêu mô đun:

+ ***Kiến thức***:

- Xác định được các thành phần cần bảo mật cho một hệ thống;
- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Liệt kê được các tình huống tấn công mạng;
- Mô tả được cách thức mã hoá thông tin;
- Mô tả kiến trúc mạng có sử dụng tường lửa;
- Mô tả cách thức xây dựng hệ thống phát hiện xâm nhập, ngăn ngừa xâm nhập;
- Phân loại được các loại virus thông dụng và phương pháp phòng chống virus.

+ ***Kỹ năng***:

- Thiết lập được các cách thức bảo mật;
- Thiết lập tường lửa bảo vệ mạng;

+ ***Thái độ***: Chủ động lĩnh hội kiến thức, hoàn thành các bài tập được giao

- Về kiến thức:

III. Nội dung mô đun:

1. Nội dung tổng quát và phân phối thời gian:

TT	Nội dung mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành	Kiểm tra
1	Bài 1. Tổng quan về an toàn và bảo mật thông tin**;**	12	6	6	
2	Bài 2: Mã hóa thông tin	12	6	6	
3	Bài 3: Các hình thức tấn công mạng phổ biến	24	6	17	1
4	Bài 4: Công nghệ bức tường lửa	18	6	11	1
5	Bài 5: Hệ thống IDS/IPS và cách phòng chống virus	24	6	17	1
	Tổng cộng	***90***	***30***	***57***	***3***

2. Nội dung chi tiết:

Bài 1: Tổng quan về an toàn và bảo mật thông tin; Thời gian: 12 giờ *(LT: 6; TH: 6)*

Mục tiêu:

+ ***Kiến thức***:

- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Xác định được các thành phần của một hệ thống bảo mật.

+ ***Kỹ năng***:

- Xác định được các thao tác bảo vệ dữ liệu quan trọng

+ ***Thái độ***: Tích cực trong việc xây dựng bài, chủ động tìm hiểu bài và thực hành bài học

Nội dung:

1.1. Các khái niệm chung

1.2. Nhu cầu bảo vệ thông tin

1.3. Các chính sách bảo mật

1.3.1. Điều khiển truy cập

1.3.2. Xác thực

1.3.3. Kiểm toán

Bài 2: Mã hóa thông tin; Thời gian: 12 giờ *(LT: 6; TH: 6)*

Mục tiêu:

+ ***Kiến thức****:*

- Liệt kê và phân biệt được các kiểu mã hóa dữ liệu ;
- Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản ;
- Mô tả về hạ tầng ứng dụng khóa công khai.

+ ***Kỹ năng***:

- Giải quyết được các bài toán liên quan đến các thuật toán mã hoá

+ ***Thái độ***: Tích cực trong việc xây dựng bài, chủ động tìm hiểu bài và thực hành bài học

Nội dung:

2.1. Cơ bản về mã hóa (Cryptography)

2.2. An toàn của thuật toán

2.3. Phân loại các thuật toán mã hóa

Bài 3: Các hình thức tấn công mạng phổ biến Thời gian: 24 giờ *(LT: 6; TH: 17; KT:1)*

Mục tiêu:

+ ***Kiến thức***:

- Liệt kê được các tình huống tấn công mạng;
- Mô tả được các mô hình tấn công mạng.

+ ***Kỹ năng***:

-Xác định được các nguy cơ có thể tấn công mạng máy tính.

+ ***Thái độ***: Tích cực trong việc xây dựng bài, chủ động tìm hiểu bài và thực hành bài học

Nội dung:

3.1. Các kiểu tấn công

3.1.1. Tấn công trực tiếp

3.1.2. Nghe trộm

3.1.3. Giả mạo địa chỉ

3.1.4. Vô hiệu hóa các chức năng của hệ thống

3.1.5. Lỗi của người quan trị hệ thống

3.1.6. Tấn công vào yếu tố con người

3.2. Cách thức tấn công

3.2.1. Minh họa khái quát một kịch bản tấn công

3.2.2. Tấn công chủ động

3.2.3. Tấn công thụ động

Bài 4: Công nghệ bức tường lửa Thời gian: 18 giờ *(LT: 6; TH: 11; KT:1)*

Mục tiêu:

+ ***Kiến thức***:

- Liệt kê chức năng, cấu trúc của tường lửa;
- Mô tả được kiến trúc mạng sử dụng tường lửa.

+ ***Kỹ năng***:

- Xác định được các mô hình tường lửa.

+ ***Thái độ***: Tích cực trong việc xây dựng bài, chủ động tìm hiểu bài và thực hành bài học

Nội dung:

4.1. Các mức bảo vệ an toàn.

4.2. Tổng quan về bức tường lửa.

4.3. Tường lửa lọc gói.

4.4. Tường lửa mức ứng dụng.

4.5. Các mô hình triển khai tường lửa.

Bài 5: Hệ thống IDS/IPS và cách phòng chống virus Thời gian: 24 giờ *(LT: 6; TH: 17; KT:1)*

Mục tiêu:

+ ***Kiến thức***:

- Trình bày được khái niệm về hệ thống phát hiện xâm nhập cập, ngăn ngừa xâm nhập.
- Mô tả được nguyên tắc hoạt động của hệ thống, IDS/IPS.
- Mô tả được virus máy tính.
- Trình bày được cách thức lây lan của virus máy tính.

+ ***Kỹ năng***:

- Thiết lập được hệ thống ngăn ngừa xâm nhập.
- Phân biệt được các loại virus.

+ ***Thái độ***: Tích cực trong việc xây dựng bài, chủ động tìm hiểu bài và thực hành bài học

Nội dung :

5.1. Cách thức xây dựng hệ thống IDS/IPS

5.1.1. Hệ thống phát hiện xâm nhập IDS

5.1.2. Hệ thống ngăn ngừa xâm nhập IPS

5.2. Phòng chống virus

5.2.1. Giới thiệu tổng quan về virus tin học

5.2.2. Cách thức lây lan – phân loại và cách phòng chống

IV. Điều kiện thực hiện chương trình:

1. Phòng học chuyên môn hóa, nhà xưởng.

STT	Loại phòng học	Số lượng	Diện tích (m^2)	Danh mục trang thiết bị chính hỗ trợ giảng dạy		
				Tên thiết bị	**Số lượng**	**Phục vụ mô đun**
1	Giảng đường	1	60	- Bàn ghế	40 Bộ	Các mô đun lý thuyết
				- Bảng	1 Chiếc	
				- Máy chiếu	1 Chiếc	
				- Màn chiếu	1 Chiếc	
				- Quạt	5 Chiếc	
2	Phòng thực hành, thực tập	1	100	- Bàn ghế	10 Bộ	Các mô đun thực hành, thực tập
				- Máy chiếu	1 Bộ	
				- Quạt	5 Chiếc	
				Máy tính	30 bộ	

2. Trang thiết bị máy móc.

3. Học liệu, dụng cụ, nguyên vật liệu:

- Đề cương bài giảng, giáo án;
- Slide bài giảng theo từng mô đun An toàn mạng
- Câu hỏi, bài tập thực hành, bài tập tình huống

4. Các điều kiện khác.

- Tài liệu phát tay, và các tài liệu liên quan khác đến mô đun;
- Các biểu mẫu, hình ảnh minh họa.

V. Phương pháp và nội dung đánh giá:

1. Nội dung

- Về kiến thức:

+ Trình bày được các kiến thức nền tảng về An toàn mạng

+ Trình bày được giải pháp An toàn mạng, bảo mật mạng, an toàn dữ liệu

- Về kỹ năng:

+ Xây dựng được hệ thống An toàn mạng

+ Bảo mậy được hệ thống mạng

+ Triển khai lắp đặt hệ thống mạng

- Năng lực tự chủ và trách nhiệm:

- Ý thức chấp hành tốt nội quy học tập.
- Tác phong và trách nhiệm đối với tập thể lớp.
- Đảm bảo an toàn.

2. Phương pháp đánh giá:

- Tham gia ít nhất 70% thời gian học lý thuyết, 80% giờ thực hành, thực tập theo quy định của môn đun;
- Tham gia đầy đủ các bài kiểm tra và các bài thực hành.
- Điểm trung bình chung các điểm kiểm tra đạt từ 5.0 trở lên theo thang điểm 10
- Đánh giá trong quá trình học:
  + Kiểm tra thường xuyên 01 kiểm tra viết (trắc nghiệm, thực hành);
  + Kiểm tra định kỳ 02 bài thực hành cá nhân hoặc nhóm.
- Đánh giá cuối môn học: Thi tự luận
- Thang điểm 10.

VI. Hướng dẫn sử dụng chương trình:

1. Phạm vi áp dụng chương trình:

Mô đun: An toàn mạng được sử dụng để giảng dạy cho trình độ Cao đẳng năm 2017.

2. Hướng dẫn một số điểm chính về phương pháp giảng dạy mô đun:

- Tuỳ theo nội dung của mỗi bài mà giáo viên có thể sử dụng những phương pháp mang tính chất vừa truyền thống vừa hiện đại như: thuyết trình, trực quan, hoạt động nhóm..
- Để đảm bảo và nâng cao chất lượng đào tạo của môn học rất cần có sự đầu tư cơ sở vật chất, trang thiết bị, đồ dùng dạy học như: phòng học thực hành máy tính, máy chiếu đa năng, giáo trình, các Video trực quan, Các thiết bị phần cứng và thiết bị mạng máy tính

3. Những trọng tâm chương trình cần chú ý:

- Tổng quan được công nghệ mạng không dây
- Phân biệt được vai trò, chức năng, các đặc tính kỹ thuật khi bảo mật mạng không dây
- Tổng quan được môn hình mạng máy tính, lắp đặt, và kết nối được mạng máy tính theo chuẩn kết nối cơ bản và nâng cao.

BÀI 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN

Giới thiệu:

Bảo mật là một trong những lĩnh vực mà hiện nay giới công nghệ thông tin khá quan tâm. Một khi Internet ra đời và phát triển, nhu cầu trao đổi thông tin trở nên cần thiết. Mục tiêu của việc nối mạng là làm cho mọi người có thể sử dụng chung tài nguyên từ những vị trí địa lý khác nhau. Cũng chính vì vậy mà các tài nguyên cũng rất dễ dàng bị phân tán, dẫn đến một điều hiển nhiên là chúng sẽ bị xâm phạm, gây mất mát dữ liệu cũng như các thông tin có giá trị. Càng giao thiệp rộng thì càng dễ bị tấn công, đó là một quy luật. Từ đó, vấn đề bảo vệ thông tin cũng đồng thời xuất hiện, bảo mật ra đời.

Tất nhiên, mục tiêu của bảo mật không chỉ nằm gói gọn trong lĩnh vực bảo vệ thông tin mà còn nhiều phạm trù khác như kiểm duyệt web, bảo mật internet, bảo mật http, bảo mật trên các hệ thống thanh toán điện tử và giao dịch trực tuyến….

Mọi nguy cơ trên mạng đều là mối nguy hiểm tiềm tàng. Từ một lỗ hổng bảo mật nhỏ của hệ thống, nhưng nếu biết khai thác và lợi dụng với tầng suất cao và kỹ thuật hack điêu luyện thì cũng có thể trở thành tai họa.

Theo thống kê của tổ chức bảo mật nổi tiếng CERT (Computer Emegancy Response Team) thì số vụ tấn công ngày càng tăng. Cụ thể năm 1989 có khoản 200 vụ, đến năm 1991 có 400 vụ, đến năm 1994 thì con số này tăng lên đến mức 1330 vụ, và sẽ còn tăng mạnh trong thời gian tới.

Như vậy, số vụ tấn công ngày càng tăng lên với mức độ chóng mặt. Điều này cũng dễ hiểu, vì một thực thể luôn tồn tại hai mặt đối lập nhau. Sự phát triển mạnh mẽ của công nghệ thông tin và kỹ thuật sẽ làm cho nạn tấn công, ăn cắp, phá hoại trên internet bùng phát mạnh mẽ.

Internet là một nơi cực kỳ hỗn loạn. Mọi thông tin mà bạn thực hiện truyền dẫn đều có thể bị xâm phạm, thậm chí là công khai. Bạn có thể hình dung internet là một phòng họp, những gì được trao đổi trong phòng họp đều được người khác nghe thấy. Với internet thì những người này không thấy mặt nhau, và việc nghe thấy thông tin này có thể hợp pháp hoặc là không hợp pháp.

Tóm lại, internet là một nơi mất an toàn. Mà không chỉ là internet các loại mạng khác, như mạng LAN, đến một hệ thống máy tính cũng có thể bị xâm phạm. Thậm chí, mạng điện thoại, mạng di động cũng không nằm ngoài cuộc. Vì thế chúng ta nói rằng, phạm vi của bảo mật rất lớn, nói không còn gói gọn trong một máy tính một cơ quan mà là toàn cầu.

Mục tiêu:

- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Xác định được các thành phần của một hệ thống bảo mật;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1.1. Các khái niệm chung

Mục tiêu:

- Mô tả được các đối tượng tấng công hệ thống mạng ;

- Xác định được các lỗ hổng bảo mật.

1.1.1. An toàn thông tin

- *An toàn thông tin* (Information security) là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép

- *An toàn thông tin* là việc bảo vệ các thuộc tính *bí mật* (confidentiality), tính *toàn vẹn* (integrity) và tính *sẵn dùng* (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải.

- An toàn thông tin gồm hai lĩnh vực chính là *An toàn công nghệ thông tin* (Information technology security, hay IT security) và *Đảm bảo thông tin* (Information assurance). An toàn công nghệ thông tin, hay còn gọi là *An toàn máy tính* (Computer security) là việc đảm bảo an toàn cho các hệ thống công nghệ thông tin, bao gồm các hệ thống máy tính và mạng, chống lại các cuộc tấn công phá hoại. Đảm bảo thông tin là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố, như thiên tai, hỏng hóc, trộm cắp, phá hoại,… Đảm bảo thông tin thường được thực hiện sử dụng các kỹ thuật *sao lưu ngoại vi* (offsite backup), trong đó dữ liệu thông tin từ hệ thống gốc được sao lọu ra các thiết bị lưu trữ vật lý đặt ở một vị trí khác.

- *Truy nhập* (Access) là việc một chủ thể, ngọời dùng hoặc một đối tượng có khả năng sử dụng, xử lý, sửa đổi, hoặc gây ảnh hưởng đến một chủ thể, người dùng hoặc một đối tượng khác. Trong khi người dùng hợp pháp có quyền truy nhập hợp pháp đến một hệ thống thì tin tặc truy nhập bất hợp pháp đến hệ thống.

- *Tài sản* (Asset) là tài nguyên của các tổ chức, cá nhân được bảo vệ. Tài sản có thể là tài sản lô gíc, như một trang web, thông tin, hoặc dữ liệu. Tài sản có thể là tài sản vật lý, như hệ thống máy tính, thiết bị mạng, hoặc các tài sản khác.

- *Tấn công* (Attack) là hành động có chủ ý hoặc không có chủ ý có khả năng gây hại, hoặc làm thỏa hiệp các thông tin, hệ thống và các tài sản được bảo vệ. Tấn công có thể chủ động hoặc thụ động, trực tiếp hoặc gián tiếp.

1.1.2. Đối tượng tấn công mạng (Intruder)

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- **Hacker:** Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.
- **Masquerader:** Là những kẻ giả mạo thông tin trên mạng. Một số hình thức giả mạo như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- **Eavesdropping:** Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị. Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau: như ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

1.1.3. Các lỗ hổng bảo mật

Các lỗ hổng bảo mật là những điểm yếu kém trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Các điểm yếu hệ thống (System weaknesses) là các lỗi hay các khiếm khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, cấu hình hoạt động. Các điểm yếu có thể tồn tại trong cả các mô đun phần cứng và các mô đun phần mềm. Một số điểm yếu được phát hiện và đã được khắc phục. Tuy nhiên, có một số điểm yếu đợợc phát hiện nhưng chưa được khắc phục, hoặc các điểm yếu chưa được phát hiện, hoặc chỉ tồn tại trong một điều kiện đặc biệt nào đó. *Lỗ hổng bảo mật* (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó, bao gồm tính toàn vẹn, tính bí mật, tính sẵn dùng. Phụ thuộc vào khả năng bị khai thác, các lỗ hổng bảo mật có mức độ nghiêm trọng (severity) khác nhau. Theo Microsoft, có 4 mức độ nghiêm trọng của các lỗ hổng bảo mật: *nguy hiểm* (Critical), *quan trọng* (Important), *trung bình* (Moderate) và *thấp* (Low). Tuy nhiên, một số tổ chức khác chỉ phân loại các lỗ hổng bảo mật theo 3 mức độ nghiêm trọng: *cao* (High), *trung bình* (Medium) và *thấp* (Low).

- Lỗ hổng bảo mật thuộc *cấp độ nguy hiểm* là lỗ hổng cho phép tin tặc thực hiện mã khai thác mà không cần tương tác ngợời dùng. Các thông tin khai thác lỗ hổng, như mã mẫu khai thác tồn tại phổ biến trên mạng. Ngoài ra, việc khai thác lỗ hổng có thể đợợc thực hiện dễ dàng mà không yêu cầu có tài khoản hệ thống hoặc các điệu kiện phức tạp. Ví dụ như một số lỗ hổng tràn bộ đệm nghiêm trọng bị khai thác bởi sâu mạng hoặc email chứa vi rút, mã độc. Các lỗ hổng loại nguy hiểm cần được khắc phục ngay hoặc càng sớm càng tốt.

- Lỗ hổng bảo mật thuộc *cấp độ quan trọng* là lỗ hổng khi bị khai thác có thể dẫn đến vị phạm các yêu cầu an toàn thông tin như bí mật, toàn vẹn và sẵn dùng của dữ liệu, tài nguyên tính toán, hoặc cả hệ thống. Khác với lỗ hổng loại nguy hiểm, lỗ hổng loại quan trọng cho phép tin tặc thực hiện mã khai thác, nhưng cần có tương tác người dùng. Ví dụ vi rút hoặc các phần mềm độc hại cần tợơng tác người dùng để lây lan, nhợ sao chép các file qua thẻ nhớ USB, mở email đính kèm, thực thi mã độc,... Các lỗ hổng loại quan trọng cũng cần được khắc phục càng sớm càng tốt.

- Lỗ hổng bảo mật thuộc *cấp độ trung bình* là các lỗ hổng mà khi khai thác, tin tặc phải ở trong cùng mạng cục bộ với hệ thống nạn nhân. Một ngữ cảnh khai thác lỗ hổng loại này là tin tặc thực hiện việc bẫy nạn nhân sử dụng các kỹ thuật xã hội, như khai thác sự cả tin, tò mò và lòng tham của người dùng. Ngoài ra, việc khai thác lỗ hổng loại trung bình cũng chỉ cho phép tin tặc có quyền truy nhập rất hạn chế vào hệ thống. Với lỗ hổng loại trung bình, cần xem xét khắc phục sớm nhất hoặc định kỳ để hạn chế ảnh hưởng.

- Loại cuối cùng là các lỗ hổng bảo mật thuộc *cấp độ thấp*. Các lỗ hổng loại này ít có ảnh hưởng đến hoạt động của tổ chức và chúng chỉ có thể bị khai thác khi tin tặc có truy nhập cục bộ hoặc truy nhập vật lý trực tiếp vào hệ thống. Mặc dù vậy, vẫn cần xem xét khắc phục định kỳ để hạn chế ảnh hợởng.

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

1.2. Nhu cầu bảo vệ thông tin

Mục tiêu:

- Trình bày được các nhu cầu cần bảo vệ trên hệ thống mạng

1.2.1. Nguyên nhân

Tài nguyên đầu tiên mà chúng ta nói đến chính là dữ liệu. Đối với dữ liệu, chúng ta cần quan tâm những yếu tố sau:

1.2.2 Bảo vệ dữ liệu

Những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu sau:

- Bảo mật: những thông tin có giá trị về kinh tế, quân sự, chính sách vv... cần được bảo vệ và không lộ thông tin ra bên ngoài.

- Tính toàn vẹn: Thông tin không bị mất mát hoặc sửa đổi, đánh tráo.

- Tính kịp thời: Yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết.

Trong các yêu cầu này, thông thường yêu cầu về bảo mật được coi là yêu cầu số 1 đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin này không được giữ bí mật, thì những yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

1.2.3. Bảo vệ tài nguyên sử dụng trên mạng

Trên thực tế, trong các cuộc tấn công trên Internet, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như chạy các chương trình dò mật khẩu người sử dụng, sử dụng các liên kết mạng sẵn có để tiếp tục tấn công các hệ thống khác.

1.2.4. Bảo vệ danh tiếng của cơ quan

Một phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là các công ty lớn và các cơ quan quan trọng trong bộ máy nhà nước. Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.

1.3. Các chính sách bảo mật

1.3.1. Điều khiển truy nhập

- Điều khiển truy nhập: là quá trình mà trong đó người dùng được nhận dạng và trao quyền truy nhập đến các thông tin, các hệ thống và tài nguyên. Một hệ thống điều khiển truy nhập có thể được cấu thành từ 3 dịch vụ: Xác thực, Trao quyền, hoặc cấp quyền và Quản trị.

** Điều khiển truy nhập tuỳ chọn*

- Là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên thông tin nhận dạng của các chủ thể, hoặc nhóm của các chủ thể.

- Các thông tin nhận dạng chủ thể có thể gồm:

+ Bạn là ai? (CMND, bằng lái xe, vân tay,...)

+ Những cái bạn biết (tên truy nhập, mật khẩu, số PIN...)

+ Bạn có gì? (Thẻ ATM, thẻ tín dụng, ...)

** Điều khiển truy nhập bắt buộc*

- Là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên hai yếu tố chính:

+ Tính nhạy cảm của thông tin chứa trong các đối tượng;

+ Sự trao quyền chính thức cho các chủ thể truy nhập các thông tin nhạy cảm này.

** Điều khiển truy nhập dựa trên luật*

- Là cơ chế cho phép người dùng truy nhập vào hệ thống và thông tin dựa trên các luật đã được định nghĩa trước. Các luật có thể được thiết lập để hệ thống cho phép truy nhập đến các tài nguyên của mình cho người dùng thuộc một tên miền, một mạng hay một dải địa chỉ IP.

- Các luật thực hiện kiểm soát truy nhập sử dụng các thông tin trích xuất từ các gói tin, thông tin về nội dung truy nhập, có thể bao gồm:

+ Địa chỉ IP nguồn và đích của các gói tin;

+ Phần mở rộng các file để lọc các mã độc hại;

+ Địa chỉ IP hoặc các tên miền để lọc, hoặc chặn các website bị cấm;

+ Tập các từ khoá để lọc các nội dung bị cấm

1.3.2. Xác thực

+ *Xác thực* là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dung cung cấp. Đây là khâu đầu tiên cần thực hiện trong một hệ thống điều khiển truy nhập.

1.3.3. Kiểm toán

+ Sau khi người dùng đã được xác thực, *trao quyền* xác định các tài nguyên mà người dung được phép truy nhập dựa trên chính sách quản trị tài nguyên của cơ quan, tổ chức.

+ Quản trị là dịch vụ cung cấp khả năng thêm, bớt và sửa đổi các thông tin tài khoản người dùng, cũng như quyền truy nhập của người dùng trong hệ thống.

Bài tập thực hành của học viên

Câu 1: Trình bày các đối tượng tấng công hệ thống mạng

Câu 2: Đối với dữ liệu, chúng ta cần quan tâm những yếu tố nào?

BÀI 2: MÃ HÓA THÔNG TIN

Mục tiêu:

- Liệt kê và phân biệt được các kiểu mã hóa dữ liệu;
- Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản;
- Mô tả về hạ tầng ứng dụng khóa công khai;
- Thực hiện các thao tác an toàn với máy tính.

2.1. Cơ bản về mã hoá (Cryptography)

Mục tiêu:

- Trình bày được nhu cầu sử dụng mã hóa;

- Mô tả được quá trình mã hóa và giải mã.

Những điều căn bản về mã hoá

Khi bắt đầu tìm hiểu về mã hoá, chúng ta thường đặt ra những câu hỏi chẳng hạn như là: Tại sao cần phải sử dụng mã hoá ? Tại sao lại có quá nhiều thuật toán mã hoá ?...

- Bản rõ: hay thông tin chưa mã hóa là thông tin ở dạng có thể hiểu được.
- Bản mã: hay thông tin đã được mã hóa là thông tin ở dạng đã bị xáo trộn.
- Mã hóa: là hành động xáo trộn bản rõ để chuyển thành bản mã.
- Giải mã: là hành động giải xáo trộn bản mã để chuyển thành bản rõ.
- Giải thuật mã hóa là giải thuật dùng để mã hóa thông tin và giải thuật giải mã dùng để giải mã thông tin.
- Một bộ mã hóa gồm một giải thuật để mã hóa và một giải thuật để giải mã thông tin.
- Khóa/Chìa: là một chuỗi được sử dụng trong giải thuật mã hóa và giải mã.
- Không gian khóa (Keyspace) là tổng số khóa có thể có của một hệ mã hóa. Ví dụ, nếu sử dụng khóa kích thước 64 bit thì không gian khóa là 2^{64}.

2.1.1. Tại sao cần phải sử dụng mã hoá

Thuật toán Cryptography đề cập tới nghành khoa học nghiên cứu về mã hoá và giải mã thông tin. Cụ thể hơn là nghiên cứu các cách thức chuyển đổi thông tin từ dạng rõ (clear text) sang dạng mờ (cipher text) và ngược lại. Đây là một phương pháp hỗ trợ rất tốt cho trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi trên mạng, áp dụng mã hoá sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.

2.1.2. Nhu cầu sử dụng kỹ thuật mã hoá

Không phải ai hay bất kỳ ứng dụng nào cũng phải sử dụng mã hoá. Nhu cầu về sử dụng mã hoá xuất hiện khi các bên tham gia trao đổi thông tin muốn bảo vệ các tài liệu quan trọng hay gửi chúng đi một cách an toàn. Các tài liệu quan trọng có thể là: tài liệu quân sự, tài chính, kinh doanh hoặc đơn giản là một thông tin nào đó mang tính riêng tư.

Như chúng ta đã biết, Internet hình thành và phát triển từ yêu cầu của chính phủ Mỹ nhằm phục vụ cho mục đích quân sự. Khi chúng ta tham gia trao đổi thông tin, thì Internet là môi trường không an toàn, đầy rủi ro và nguy hiểm,

không có gì đảm bảo rằng thông tin mà chúng ta truyền đi không bị đọc trộm trên đường truyền. Do đó, mã hoá được áp dụng như một biện pháp nhằm giúp chúng ta tự bảo vệ chính mình cũng như những thông tin mà chúng ta gửi đi. Bên cạnh đó, mã hoá còn có những ứng dụng khác như là bảo đảm tính toàn vẹn của dữ liệu.

Tại sao lại có quá nhiều thuật toán mã hoá

Theo một số tài liệu thì trước đây tính an toàn, bí mật của một thuật toán phụ thuộc vào phương thức làm việc của thuật toán đó. Nếu như tính an toàn của một thuật toán chỉ dựa vào sự bí mật của thuật toán đó thì thuật toán đó là một thuật toán hạn chế (Restricted Algrorithm). Restricted Algrorithm có tầm quan trọng trong lịch sử nhưng không còn phù hợp trong thời đại ngày nay. Giờ đây, nó không còn được mọi người sử dụng do mặt hạn chế của nó: mỗi khi một user rời khỏi một nhóm thì toàn bộ nhóm đó phải chuyển sang sử dụng thuật toán khác hoặc nếu người đó người trong nhóm đó tiết lộ thông tin về thuật toán hay có kẻ phát hiện ra tính bí mật của thuật toán thì coi như thuật toán đó đã bị phá vỡ, tất cả những user còn lại trong nhóm buộc phải thay đổi lại thuật toán dẫn đến mất thời gian và công sức.

Hệ thống mã hoá hiện nay đã giải quyết vấn đề trên thông qua khoá (Key) là một yếu tố có liên quan nhưng tách rời ra khỏi thuật toán mã hoá. Do các thuật toán hầu như được công khai cho nên tính an toàn của mã hoá giờ đây phụ thuộc vào khoá. Khoá này có thể là bất kì một giá trị chữ hoặc số nào. Phạm vi không gian các giá trị có thể có của khoá được gọi là Keyspace . Hai quá trình mã hoá và giải mã đều dùng đến khoá. Hiện nay, người ta phân loại thuật toán dựa trên số lượng và đặc tính của khoá được sử dụng.

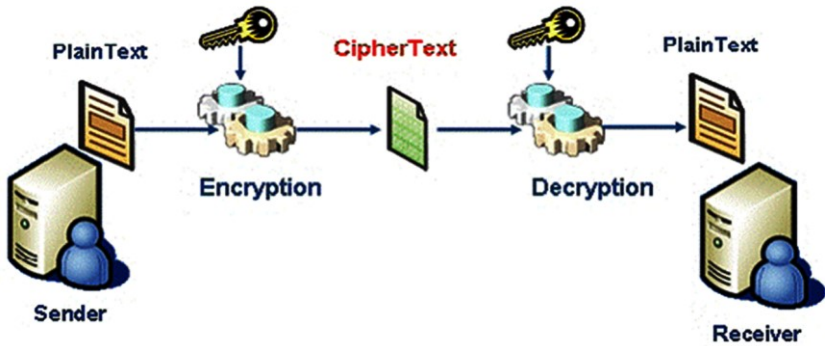
Nói đến mã hoá tức là nói đến việc che dấu thông tin bằng cách sử dụng thuật toán. Che dấu ở đây không phải là làm cho thông tin biến mất mà là cách thức chuyển từ dạng tỏ sang dạng mờ. Một thuật toán là một tập hợp của các câu lệnh mà theo đó chương trình sẽ biết phải làm thế nào để xáo trộn hay phục hồi lại dữ liệu. Chẳng hạn một thuật toán rất đơn giản mã hoá thông điệp cần gửi đi như sau:

Bước 1: Thay thế toàn bộ chữ cái “e” thành số “3”

Bước 2: Thay thế toàn bộ chữ cái “a” thành số “4”

Bước 3: Đảo ngược thông điệp

Trên đây là một ví dụ rất đơn giản mô phỏng cách làm việc của một thuật toán mã hoá. Sau đây là các thuật ngữ cơ bản nhất giúp chúng ta nắm được các khái niệm:



Hinh1: Minh hoạ quá trình mã hóa và giải mã

Sender/Receiver: Người gửi/Người nhận dữ liệu

- Plaintext (Cleartext): Thông tin trước khi được mã hoá. Đây là dữ liệu ban đầu ở dạng rõ
- Ciphertext: Thông tin, dữ liệu đã được mã hoá ở dạng mờ
- Key: Thành phần quan trọng trong việc mã hoá và giải mã
- CryptoGraphic Algorithm: Là các thuật toán được sử dụng trong việc mã hoá hoặc giải mã thông tin
- CryptoSystem: Hệ thống mã hoá bao gồm thuật toán mã hoá, khoá, Plaintext, Ciphertext

Kí hiệu chung: P là thông tin ban đầu, trước khi mã hoá. E() là thuật toán mã hoá. D() là thuật toán giải mã. C là thông tin mã hoá. K là khoá.

2.1.3. Quá trình mã hoá và giải mã như sau:

- Quá trình mã hoá được mô tả bằng công thức: EK(P)=C
- Quá trình giải mã được mô tả bằng công thức: DK(C)=P

Bên cạnh việc làm thế nào để che dấu nội dung thông tin thì mã hoá phải đảm bảo các mục tiêu sau:

a. Confidentiality (Tính bí mật): Đảm bảo dữ liệu được truyền đi một cách an toàn và không thể bị lộ thông tin nếu như có ai đó cố tình muốn có được nội dung của dữ liệu gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung thông tin ban đầu.

b. Authentication (Tính xác thực): Giúp cho người nhận dữ liệu xác định được chắc chắn dữ liệu mà họ nhận là dữ liệu gốc ban đầu. Kẻ giả mạo không thể có khả năng để giả dạng một người khác hay nói cách khác không thể mạo danh để gửi dữ liệu. Người nhận có khả năng kiểm tra nguồn gốc thông tin mà họ nhận được.

c. Integrity (Tính toàn vẹn): Giúp cho người nhận dữ liệu kiểm tra được rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Kẻ giả mạo không thể có khả năng thay thế dữ liệu ban đầu băng dữ liệu giả mạo

d. Non-repudation (Tính không thể chối bỏ): Người gửi hay người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông tin.

2.2. An toàn của thuật toán

Mục tiêu:

- Trình bày được các thuật toán mã hóa

Nguyên tắc đầu tiên trong mã hoá là "Thuật toán nào cũng có thể bị phá vỡ". Các thuật toán khác nhau cung cấp mức độ an toàn khác nhau, phụ thuộc vào độ phức tạp để phá vỡ chúng. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:

- Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
- Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.

- Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lơn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn

Từ tạm thời ở đây có nghĩa là độ an toàn của thuật toán đó chỉ đúng trong một thời điểm nhất định nào đó, luôn luôn có khả năng cho phép những người phá mã tìm ra cách để phá vỡ thuật toán. Điều này chỉ phụ thuộc vào thời gian, công sức, lòng đam mê cũng như tính kiên trì bên bỉ. Càng ngày tốc độ xử lý của CPU càng cao, tốc độ tính toán của máy tính ngày càng nhanh, cho nên không ai dám khẳng định chắc chắn một điều rằng thuật toán mà mình xây dựng sẽ an toàn mãi mãi. Trong lĩnh vực mạng máy tính và truyền thông luôn luôn tồn tại hai phe đối lập với nhau những người chuyên đi tấn công, khai thác lỗ hổng của hệ thống và những người chuyên phòng thủ, xây dựng các qui trình bảo vệ hệ thống. Cuộc chiến giữa hai bên chẳng khác gì một cuộc chơi trên bàn cờ, từng bước đi, nước bước sẽ quyết định số phận của mối bên. Trong cuộc chiến này, ai giỏi hơn sẽ dành được phần thắng. Trong thế giới mã hoá cũng vậy, tất cả phụ thuộc vào trình độ và thời gian…sẽ không ai có thể nói trước được điều gì. Đó là điểm thú vị của trò chơi.

2.3. Phân loại các thuật toán mã hoá

Có rất nhiều các thuật toán mã hoá khác nhau. Từ những thuật toán được công khai để mọi người cùng sử dụng và áp dụng như là một chuẩn chung cho việc mã hoá dữ liệu; đến những thuật toán mã hoá không được công bố. Có thể phân loại các thuật toán mã hoá như sau:

* Phân loại theo các phương pháp:
- Mã hoá cổ điển (Classical cryptography)
- Mã hoá đối xứng (Symetric cryptography)
- Mã hoá bất đối xứng(Asymetric cryptography)
- Hàm băm (Hash function)

* Phân loại theo số lượng khoá:
- Mã hoá khoá bí mật (Private-key Cryptography)
- Mã hoá khoá công khai (Public-key Cryptography)

2.3.1. Mã hoá cổ điển:

Xuất hiện trong lịch sử, các phương pháp này không dùng khoá. Thuật toán đơn giản và dễ hiểu. Những từ chính các phương pháp mã hoá này đã giúp chúng ta tiếp cận với các thuật toán mã hoá đối xứng được sử dụng ngày nay. Trong mã hoá cổ điển có 02 phương pháp nổi bật đó là:

- Mã hoá thay thế (Substitution Cipher):

Là phương pháp mà từng kí tự (hay từng nhóm kí tự) trong bản rõ (Plaintext) được thay thế bằng một kí tự (hay một nhóm kí tự) khác để tạo ra bản mờ (Ciphertext). Bên nhận chỉ cần đảo ngược trình tự thay thế trên Ciphertext để có được Plaintext ban đầu.

Các hệ mật mã cổ điển- Hệ mã hóa thay thế(Substitution Cipher)

Chọn một hoán vị p: Z26 → Z26 làm khoá.

VD:

Mã hoá

ep(a)=X

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

Giải mã:
dp(A)=d

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Bảng rõ "nguyenthanhnhut"
Mã hóa "SOUDHSMGXSGSGUM"

- Mã hoá hoán vị (Transposition Cipher):

Bên cạnh phương pháp mã hoá thay thế thì trong mã hoá cổ điển có một phương pháp khác nữa cũng nổi tiếng không kém, đó chính là mã hoá hoán vị. Nếu như trong phương pháp mã hoá thay thế, các kí tự trong Plaintext được thay thế hoàn toàn bằng các kí tự trong Ciphertext, thì trong phương pháp mã hoá hoán vị, các kí tự trong Plaintext vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra Ciphertext. Tức là các kí tự trong Plaintext hoàn toàn không bị thay đổi bằng kí tự khác.

Mã hoán vị - Permutation Cipher

Chuyển đổi vị trí bản thân các chữ cái trong văn bản gốc từng khối m chữ cái.

Mã hoá:

$e\pi(x1, \ldots, xm) = (x\pi(1), \ldots, x\pi m))$.

Giải mã:

$d\pi(y1, \ldots, ym) = (y\pi'(1), \ldots, y\pi'(m))$.

Trong đó, π: Z26 → Z26 là một hoán vị, $\pi' := \pi$-1 là nghịch đảo của π.

Hoán vị

x	1	2	3	4	5	6
Π(x)	3	5	1	6	4	2

x	1	2	3	4	5	6
Π^{-1}(x)	3	6	1	5	2	4

“shesellsseashellsbytheseashore”.
shesel | lsseas | hellsb | ythese | ashore
EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS
“EESLSHSALSESLSHBLEHSYEETHRAEOS”.

2.3.2. Mã hoá đối xứng:

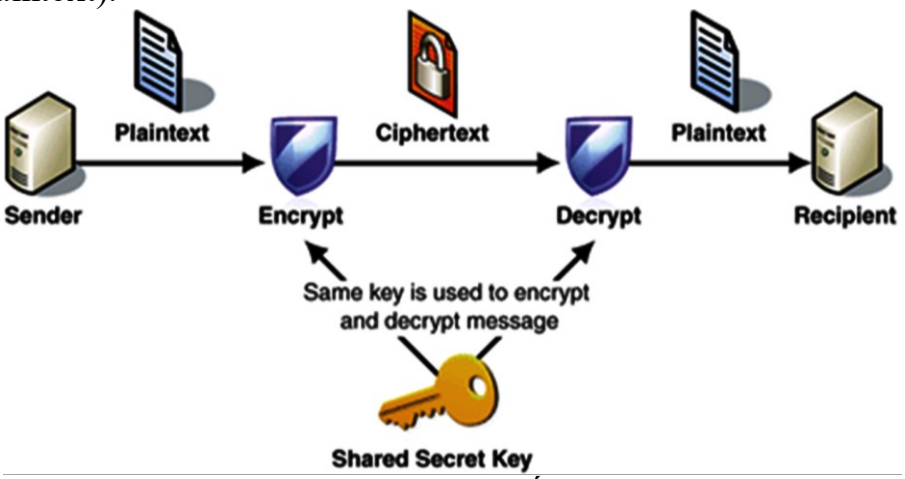
Ở phần trên, chúng ta đã tìm hiểu về mã hoá cổ điển, trong đó có nói rằng mã hoá cổ điển không dùng khoá. Nhưng trên thực nếu chúng ta phân tích một cách tổng quát, chúng ta sẽ thấy được như sau:

- Mã hoá cổ điển có sử dụng khoá. Bằng chứng là trong phương pháp Ceaser Cipher thì khoá chính là phép dịch ký tự, mà cụ thể là phép dịch 3 ký tự. Trong phương pháp mã hoá hoán vị thì khóa nằm ở số hàng hay số cột mà chúng ta qui định. Khoá này có thể được thay đổi tuỳ theo mục đích mã hoá của chúng ta, nhưng nó phải nằm trong một phạm vi cho phép nào đó.
- Để dùng được mã hoá cổ điển thì bên mã hoá và bên giải mã phải thống nhất với nhau về cơ chế mã hoá cũng như giải mã. Nếu như không có công việc này thì hai bên sẽ không thể làm việc được với nhau.

Mã hoá đối xứng còn có một số tên gọi khác như Secret Key Cryptography (hay Private Key Cryptography), sử dụng cùng một khoá cho cả hai quá trình mã hoá và giải mã.

Quá trình thực hiện như sau:

Trong hệ thống mã hoá đối xứng, trước khi truyền dữ liệu, 2 bên gửi và nhận phải thoả thuận về khoá dùng chung cho quá trình mã hoá và giải mã. Sau đó, bên gửi sẽ mã hoá bản rõ (Plaintext) bằng cách sử dụng khoá bí mật này và gửi thông điệp đã mã hoá cho bên nhận. Bên nhận sau khi nhận được thông điệp đã mã hoá sẽ sử dụng chính khoá bí mật mà hai bên thoả thuận để giải mã và lấy lại bản rõ (Plaintext).



Hình 2: Mã hóa đối xứng

Hình vẽ trên chính là quá trình tiến hành trao đổi thông tin giữa bên gửi và bên nhận thông qua việc sử dụng phương pháp mã hoá đối xứng. Trong quá trình này, thì thành phần quan trọng nhất cần phải được giữ bí mật chính là khoá. Việc trao đổi, thoả thuận về thuật toán được sử dụng trong việc mã hoá có thể tiến hành một cách công khai, nhưng bước thoả thuận về khoá trong việc mã hoá và giải mã phải tiến hành bí mật. Chúng ta có thể thấy rằng thuật toán mã hoá