BỘ CÔNG THƯƠNG

TRƯỜNG CAO ĐẲNG THƯƠNG MẠI VÀ DU LỊCH

GIÁO TRÌNH

MÔN HỌC: AN TOÀN VÀ BẢO MẬT THÔNG TIN

NGÀNH: CÔNG NGHỆ THÔNG TIN (ƯDPM)

TRÌNH ĐỘ: TRUNG CẤP

(Ban hành kèm theo Quyết định số: 405/QĐ-CĐKT ngày 05 tháng 07 năm 2022 của Trường Cao đẳng Thương mại và Du lịch

Thành phố Thái Nguyên, năm 2022

(Lưu hành nội bộ)

TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Môn học "An toàn và bảo mật thông tin" là một môn học quan trọng trong lĩnh vực công nghệ thông tin. Mục tiêu chính của môn học này là giúp học sinh hiểu và áp dụng các biện pháp để bảo vệ hệ thống thông tin khỏi các mối đe dọa và tấn công.

Học sinh sẽ được giới thiệu về các khái niệm cơ bản về an toàn thông tin, bao gồm bảo mật mạng, bảo mật dữ liệu, và quản lý rủi ro. Từ đó sẽ học cách xác định và đánh giá các lỗ hổng bảo mật, áp dụng biện pháp bảo mật phù hợp và tạo ra kế hoạch ứng phó với xâm nhập.

Môn học cũng sẽ trang bị cho học sinh kiến thức về chuẩn và quy tắc bảo mật thông tin quan trọng, giúp học sinh tham gia vào việc bảo vệ thông tin trong môi trường công việc thực tế. An toàn và bảo mật thông tin là một khía cạnh quan trọng của mọi doanh nghiệp và tổ chức, và môn học này cung cấp nền tảng để hiểu và thực hiện các biện pháp an toàn cần thiết.

Tài liệu học tập được biên soạn theo đúng chương trình đào tạo và các quy định về cách trình bày của Nhà trường. Nội dung của tài liệu học tập bao gồm các chương, trong mỗi chương bao gồm các phần nội dung chủ yếu như sau:

- Mục tiêu của chương.
- Nội dung bài giảng lý thuyết.
- Bài tập vận dụng.

Nhằm tạo điều kiện cho người học có một bộ tài liệu tham khảo mang tính tổng hợp, thống nhất và mang tính thực tiễn sâu hơn. Nhóm người dạy chúng tôi đề xuất và biên soạn ***Giáo trình An toàn và bảo mật thông tin*** dành riêng cho người học trình độ Trung cấp.

Nội dung của giáo trình bao gồm các chương sau:

Chương 1: Giới thiệu chung

Chương 2: Lỗ hổng bảo mật và các phần mềm độc hại

Chương 3: Các dạng tấn công và các phần mềm độc hại

Chương 4: Đảm bảo an toàn thông tin dựa trên mã hóa

Chương 5: Các kỹ thuật và công nghệ đảm bảo an toàn thông tin

Trong quá trình biên soạn, chúng tôi đã tham khảo và trích dẫn từ nhiều tài liệu được liệt kê tại mục Danh mục tài liệu tham khảo. Chúng tôi chân thành cảm ơn các tác giả của các tài liệu mà chúng tôi đã tham khảo.

Bên cạnh đó, giáo trình cũng không thể tránh khỏi những sai sót nhất định. Nhóm tác giả rất mong nhận được những ý kiến đóng góp, phản hồi từ quý đồng nghiệp, các bạn người học và bạn đọc.

Trân trọng cảm ơn./.

Thành phố Thái Nguyên, ngày 20 tháng 08 năm 2022

MỤC LỤC

GIÁO TRÌNH MÔN HỌC

1. Tên môn học: AN TOÀN VÀ BẢO MẬT THÔNG TIN

2. Mã môn học: MH22

3. Vị trí, tính chất, ý nghĩa và vai trò của môn học:

3.1. Vị trí: Giáo trình dành cho người học trình độ Trung cấp tại trường Cao đẳng Thương mại và Du lịch.

3.2. Tính chất: Giáo trình cung cấp kiến thức, kỹ năng và năng lực tự chủ và trách nhiệm cho người học. Môn học "An toàn hệ thống thông tin" là một môn học quan trọng và đa dạng, nhấn mạnh sự kết hợp giữa kiến thức lý thuyết và thực hành, nhằm phát triển kiến thức và kỹ năng để bảo vệ hệ thống thông tin trong môi trường công nghệ thông tin ngày càng phức tạp.

3.3. Ý nghĩa và vai trò của môn học: Môn học "An toàn hệ thống thông tin" đóng vai trò quan trọng trong việc bảo vệ thông tin và hệ thống của tổ chức khỏi các mối đe dọa mạng. Nó giúp bảo vệ thông tin quan trọng, đảm bảo sự uy tín của tổ chức và đối phó với mối đe dọa liên quan đến bảo mật thông tin.

4. Mục tiêu của môn học:

4.1. Về kiến thức:

A1. Hiểu về các mối đe dọa và tấn công mạng

A2. hiểu cách bảo mật mạng và hệ thống máy tính, bao gồm việc xác định lỗ hổng bảo mật, áp dụng biện pháp bảo mật, và giám sát hệ thống

A4. Biết cách đánh giá rủi ro bảo mật thông tin và tạo ra kế hoạch ứng phó với xâm nhập.

Về kỹ năng:

B1. Kỹ năng phân tích hệ thống và mạng để xác định lỗ hổng bảo mật, đánh giá rủi ro, và tìm hiểu về các mối đe dọa mạng

B2. Cách triển khai biện pháp bảo mật, bao gồm việc cấu hình hệ thống, xác định các quy tắc tường lửa, và thiết lập các công cụ bảo mật.

B3. Kỹ năng bảo vệ dữ liệu quan trọng, bao gồm việc mã hóa thông tin, quản lý quyền truy cập, và áp dụng các biện pháp bảo mật dữ liệu cá nhân.B4. Kỹ năng tạo bài thuyết trình

4.3 Về năng lực tự chủ và trách nhiệm:

C1. Năng lực quản lý thời gian

C2. Trách nhiệm với công việc

C3. Năng lực học tập và làm việc độc lập

C4. Năng lực quản lý thông tin

C5. Tự chủ trong việc giải quyết vấn đề

5. Nội dung của môn học

5.1. Chương trình khung

Mã MH	Tên môn học	Số tín chỉ	Thời gian học tập *(giờ)*			
			Tổng số	Trong đó		
				Lý thuyết	Thực hành/ thực tập/ bài tập/ thảo luận	Thi/ Kiểm tra
I	**Các môn học chung**	**12**	**255**	**94**	**148**	**13**
MH01	Chính trị	2	30	15	13	2
MH02	Pháp luật	1	15	9	5	1
MH03	Giáo dục thể chất	1	30	4	24	2
MH04	Giáo dục quốc phòng và an ninh	2	45	21	21	3
MH05	Tin học	2	45	15	29	1
MH06	Ngoại ngữ	4	90	30	56	4
II	**Các môn học chuyên môn**	**64**	**1560**	**504**	**1013**	**43**
II.1	***Môn học cơ sở***	***16***	***240***	***224***	***-***	***13***
MH07	Tin học văn phòng	2	30	12	17	1
MH08	Bảng tính Excel	2	30	12	17	1
MH09	Cấu trúc máy tính	2	30	28	-	2
MH10	Mạng máy tính	2	30	15	14	1
MH11	Lập trình cơ bản	2	30	28	-	2
MH12	Cấu trúc dữ liệu và giải thuật	2	30	28	-	2
MH13	Cơ sở dữ liệu	2	30	28	-	2
MH14	Lắp ráp và bảo trì máy tính	2	30	28	-	2
II.2	***Môn học chuyên môn***	***46***	***1290***	***313***	***948***	***28***
MH15	Ngoại ngữ ch.ngành CNTT	4	60	57	-	3
MH16	Hệ điều hành Windows Server	2	30	28	-	2
MH17	Quản trị CSDL với Access 1	3	45	43	-	2
MH18	Quản trị CSDL với SQL Server	3	45	27	17	1
MH19	Lập trình Windows 1 (VB.NET)	3	45	43	-	2
MH20	Thiết kế và quản trị website	3	45	43	-	2
MH21	Đồ họa ứng dụng	2	30	28	-	2
MH22	An toàn và bảo mật thông tin	2	30	28	-	2
MH23	TH xây dựng phần mềm quản lý	4	120	-	114	6

MH24	TH thiết kế và quản trị website	4	120	-	114	6
MH25	Thực tập tốt nghiệp	16	720	-	720	
II.3	***Môn học tự chọn****(chọn 1 trong 2)*	***2***	***30***	***28***	***-***	***2***
MH26	Kỹ năng giao tiếp, phục vụ khách hàng	2	30	28	-	2
MH27	Lập trình mạng	2	30	28	-	2
	Tổng cộng	**76**	**1815**	**598**	**1161**	**56**

5.2. Chương trình chi tiết môn học

Số TT	Tên chương, mục	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành	Kiểm tra
1	Chương 1. Giới thiệu chung	2	2		
2	Chương 2. Lỗ hổng bảo mật và các điểm yếu hệ thống	4	4		
3	Chương 3. Các dạng tấn công và các phần mềm độc hại	6	6		
4	Chương 4. Đảm bảo an toàn thông tin dựa trên mã hóa	14	12		2
5	Chương 5. Các kỹ thuật và công nghệ đảm bảo an toàn thông tin	4	4		
	Cộng	**30**	**28**	**0**	**2**

6. Điều kiện thực hiện môn học:

6.1. Phòng học Lý thuyết/Thực hành: Đáp ứng phòng học chuẩn

6.2. Trang thiết bị dạy học: Projetor, máy vi tính, bảng, phấn

6.3. Học liệu, dụng cụ, mô hình, phương tiện: Giáo trình, mô hình học tập,…

6.4. Các điều kiện khác: Người học tìm hiểu thực tế về công tác xây dựng phương án khắc phục và phòng ngừa rủi ro tại doanh nghiệp.

7. Nội dung và phương pháp đánh giá:

7.1. Nội dung:

- Kiến thức: Đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức
- Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kỹ năng.
- Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp.

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

7.2. Phương pháp:

Người học được đánh giá tích lũy môn học như sau:

7.2.1. Cách đánh giá

- Việc đánh giá kết quả học tập của người học được thực hiện theo quy định tại Thông tư 04/2022/TT-BLĐTBXH ngày 30/3/2022 của Bộ Lao động – Thương binh và Xã hội; Quy chế Tổ chức đào tạo trình độ trung cấp, trình độ cao đẳng theo phương thức tích luỹ mô-đun, tín chỉ của Nhà trường ban hành kèm theo Quyết định số 246/QĐ-CĐTMDL ngày 01/6/2022 của Hiệu trưởng Trường cao đẳng Thương mại và Du lịch và hướng dẫn cụ thể theo từng môn học/mô-đun trong chương trình đào tạo:

Điểm đánh giá	**Trọng số**
+ Điểm kiểm tra thường xuyên (Hệ số 1)	40%
+ Điểm kiểm tra định kỳ (Hệ số 2)	
+ Điểm thi kết thúc môn học	60%

7.2.2. Phương pháp đánh giá

Phương pháp đánh giá	**Phương pháp tổ chức**	**Hình thức kiểm tra**	**Thời điểm kiểm tra**
Thường xuyên	Viết/ Thuyết trình	Tự luận/ Trắc nghiệm	Sau 15 giờ.
Định kỳ	Viết/ Thuyết trình	Tự luận/ Trắc nghiệm	Sau 20 giờ
Kết thúc môn học	Viết	Tự luận và trắc nghiệm	Sau 30 giờ

7.2.3. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc môn học được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến một chữ số thập phân.

- Điểm môn học là tổng điểm của tất cả điểm đánh giá thành phần của môn học nhân với trọng số tương ứng. Điểm môn học theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy định của Bộ Lao động Thương binh và Xã hội về đào tạo theo tín chỉ.

8. Hướng dẫn thực hiện môn học

8.1. Phạm vi, đối tượng áp dụng: Đối tượng Trung cấp Công nghệ thông tin (ƯDPM)

8.2. Phương pháp giảng dạy, học tập môn học

8.2.1. Đối với người dạy

*** Lý thuyết:** Áp dụng phương pháp dạy học tích cực bao gồm: thuyết trình ngắn, nêu vấn đề, hướng dẫn đọc tài liệu, bài tập tình huống, câu hỏi thảo luận….

*** Bài tập:** Phân chia nhóm nhỏ thực hiện bài tập theo nội dung đề ra.

*** Thảo luận:** Phân chia nhóm nhỏ thảo luận theo nội dung đề ra.

*** Hướng dẫn tự học theo nhóm:** Nhóm trưởng phân công các thành viên trong nhóm tìm hiểu, nghiên cứu theo yêu cầu nội dung trong bài học, cả nhóm thảo luận, trình bày nội dung, ghi chép và viết báo cáo nhóm.

8.2.2. Đối với người học: Người học phải thực hiện các nhiệm vụ như sau:

Nghiên cứu kỹ bài học tại nhà trước khi đến lớp. Các tài liệu tham khảo sẽ được cung cấp nguồn trước khi người học vào học môn học này (trang web, thư viện, tài liệu...)

- Tham dự tối thiểu 80% các buổi giảng lý thuyết. Nếu người học vắng >20% số tiết lý thuyết phải học lại môn học mới được tham dự kì thi lần sau.
- Tham dự đủ các bài kiểm tra thường xuyên, định kỳ.
- Tham dự thi kết thúc môn học.
- Chủ động tổ chức thực hiện giờ tự học.

9. Tài liệu tham khảo:

[1]. Bài giảng An toàn hệ thống thông tin, Bộ môn CNTT, Trường Cao đẳng Thương mại – Du lịch

[2]. Giáo trình An toàn hệ thống thông tin – ĐH Bách khoa Hà Nội

[3]. Giáo trình An toàn bảo mật hệ thống thông tin – CĐ Kinh tế kỹ thuật TP. Hồ Chí Minh

[4]. Nguyễn Thanh Hải, Giáo trình tin học văn phòng, Nhà xuất bản Văn hoá thông tin, 2003.

[5]. Giáo trình An toàn bảo mật dữ liệu – ĐH Công nghệ thông tin và truyền thông (Đại học Thái Nguyên)

Chương 1: GIỚI THIỆU CHUNG

❖ GIỚI THIỆU CHƯƠNG 1

Chương 1 của môn học "An toàn và bảo mật thông tin" là một phần quan trọng để học viên làm quen với lĩnh vực an toàn hệ thống thông tin. Chương này cung cấp một cái nhìn tổng quan về tầm quan trọng của an toàn thông tin và nhiệm vụ quan trọng của môn học

❖ MỤC TIÊU CHƯƠNG 1

Sau khi học xong chương này, người học có khả năng:

➢ ***Về kiến thức:***

- *Hiểu khái niệm cơ bản về an toàn thông tin và tại sao nó quan trọng đối với tổ chức và cá nhân.*
- *Biết cách nhận diện các mối đe dọa mạng phổ biến, như virus máy tính, tấn công mạng, và lừa đảo trực tuyến.*
- *Hiểu các chuẩn bảo mật quốc tế và ngành công nghiệp, cũng như quy định liên quan đến bảo mật thông tin.*
- *Hiểu vai trò và trách nhiệm của người quản lý an toàn thông tin trong tổ chức và biết cách đảm bảo an toàn hệ thống thông tin.*

➢ ***Về kỹ năng:***

- *Nhận các mối đe dọa mạng phổ biến, như virus máy tính, tấn công mạng, và lừa đảo trực tuyến.*
- *Nắm vững các chuẩn bảo mật quốc tế và ngành công nghiệp, cũng như quy định liên quan đến bảo mật thông tin.*
- *Hiểu vai trò và trách nhiệm của người quản lý an toàn thông tin trong tổ chức và biết cách đảm bảo an toàn hệ thống thông tin.*
- *Nắm vững tầm quan trọng của an toàn thông tin trong việc bảo vệ dữ liệu quan trọng, tránh mất lạc tài chính, và đảm bảo uy tín của tổ chức.*

➢ ***Về năng lực tự chủ và trách nhiệm:***

- *Năng lực về quản lý thời gian, trách nhiệm với công việc*
- *Năng lực học tập và làm việc độc lập*
- *Tự chủ trong việc giải quyết vấn đề*

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 1

- *Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, dạy học theo vấn đề); yêu cầu người học thực hiện câu hỏi thảo luận và bài tập chương 1 (cá nhân hoặc nhóm).*
- *Đối với người học: chủ động đọc trước giáo trình (chương 1) trước buổi học; hoàn thành đầy đủ câu hỏi thảo luận và bài tập tình huống chương 1 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.*

❖ **ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 1**

- ***Phòng học chuyên môn hóa/nhà xưởng:*** Phòng học thực hành
- ***Trang thiết bị máy móc:*** Máy chiếu, máy tính và các thiết bị dạy học khác
- ***Học liệu, dụng cụ, nguyên vật liệu:*** Chương trình môn học, giáo trình, tài liệu tham khảo, giáo án, phim ảnh, và các tài liệu liên quan.
- ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 1**

- **Nội dung:**

✓ *Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức*

✓ *Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.*

✓ *Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:*

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ ***Điểm kiểm tra thường xuyên:*** *1 điểm kiểm tra (hình thức: hỏi miệng)*

✓ ***Kiểm tra định kỳ lý thuyết:*** *không có*

❖ **NỘI DUNG CHƯƠNG 1**

1.1. Khái quát về an toàn thông tin

1.1.1. Thông tin

** Thông tin là gì?*

Có rất nhiều khái niệm thông tin nhưng khái niệm thông tin là gì chính xác nhất đó là: Thông tin là những gì con người thu nhận được từ thế giới xung quanh như sự vật, sự kiện,…Thông tin đem lại nhiều kiến thức, sự hiểu biết cho con người. Theo wikipedia,

định nghĩa thông tin là giải quyết sự không chắc chắn; đó là câu trả lời cho câu hỏi "thực thể là gì". Do đó, xác định được cả bản chất của các đặc tính đó. Thông tin được liên kết với các dữ liệu vì dữ liệu đại diện cho các giá trị sẽ được quy cho các tham số.

Về mặt truyền thông, thông tin được thể hiện dưới dạng nội dung của tin nhắn hoặc thông qua sự quan sát trực tiếp, gián tiếp. Thông tin cũng có thể được mã hóa thành nhiều dạng khác nhau để truyền và giải thích.

Tựu chung, khái niệm về thông tin là sự phản ánh sự vật, sự việc, hiện tượng của thế giới khách quan, các hoạt động của con người trong đời sống xã hội. Điều cơ bản là con người sẽ tiếp nhận thông tin để làm tăng hiểu biết cho mình và tiến hành những hoạt động có ích cho cộng đồng.

** Thông tin số là gì?*

Thông tin số được định nghĩa tại Khoản 11 Điều 3 Nghị định 71/2007/NĐ-CP Hướng dẫn Luật công nghệ thông tin về công nghiệp công nghệ thông tin đó là:

Sản phẩm nội dung thông tin số bao gồm các văn bản, dữ liệu, hình ảnh, âm thanh được thể hiện dưới dạng thông tin số, được lưu giữ, truyền đưa trên môi trường mạng.

(Bài giảng điện tử được thực hiện dưới dạng thông tin số)

Theo quy định pháp luật hiện hành thì sản phẩm nội dung thông tin số hiện nay bao gồm các loại sản phẩm sau:

a) Giáo trình, bài giảng, tài liệu học tập dưới dạng điện tử;

b) Sách, báo, tài liệu dưới dạng số;

c) Các loại trò chơi điện tử bao gồm trò chơi trên máy tính đơn, trò chơi trực tuyến, trò chơi trên điện thoại di động; trò chơi tương tác qua truyền hình;

d) Sản phẩm giải trí trên mạng viễn thông di động và cố định;

đ) Thư viện số, kho dữ liệu số, từ điển điện tử;

e) Phim số, ảnh số, nhạc số, quảng cáo số;

g) Các sản phẩm nội dung thông tin số khác.

Hiểu một cách đơn giản, thông tin số là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

** Khái niệm tổ chức thông tin trong máy tính là gì?*

Chức năng chính của máy tính hiện nay là xử lý thông tin. Trong quá trình xử lý, máy tính cần tìm đến, đọc và ghi các thông tin trên thiết bị lưu trữ. Nếu tổ chức thông minh một cách hợp lý thì việc truy cập đến sẽ rất nhanh chóng nhất là khi khối lượng thông tin lớn. Để thực hiện được, hệ điều hành tổ chức thông tin cần phải theo cấu trúc hình cây gồm các tệp và thư mục.

1.1.2. 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, theo trang Wikipedia (https://en.wikipedia.org/wiki/Information_security).

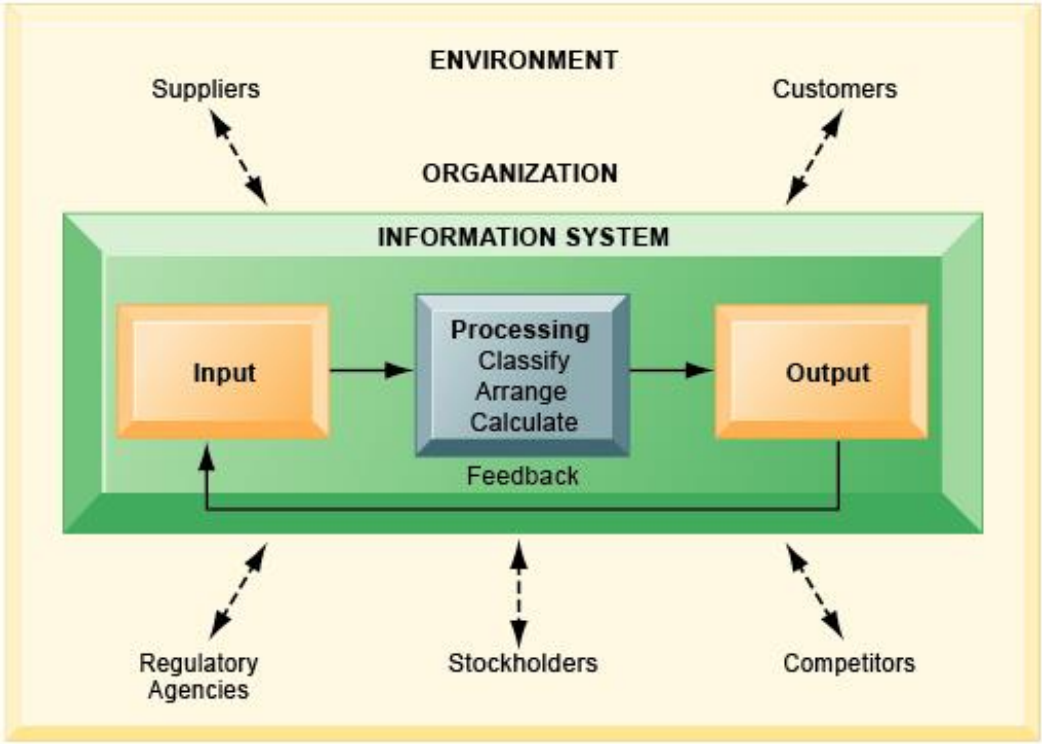
Theo cuốn Principles of Information Security [1], An toàn thông tin là việc bảo vệ các thuộc tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn dùng (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải.

(Các thuộc tính cần bảo vệ của tài sản thông tin: Bí mật - Confidentiality, Toàn vẹn - Integrity và Sẵn dùng - Availability)

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 lưu ra các thiết bị lưu trữ vật lý đặt ở một vị trí khác.

1.1.3. Hệ thống thông tin

Hệ thống thông tin (Information system), theo cuốn Fundamentals of Information Systems Security [2] là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số. Trong nền kinh tế số, hệ thống thông tin đóng vai trò rất quan trọng trong hoạt động của các tổ chức, cơ quan và doanh nghiệp (gọi chung là tổ chức). Có thể nói, hầu hết các tổ chức đều sử dụng các hệ thống thông tin với các quy mô khác nhau để quản lý các hoạt động của mình.



(Hình ảnh minh họa mô hình một hệ thống thông tin điển hình)

Trong mô hình này, mỗi hệ thống thông tin gồm ba thành phần chính:

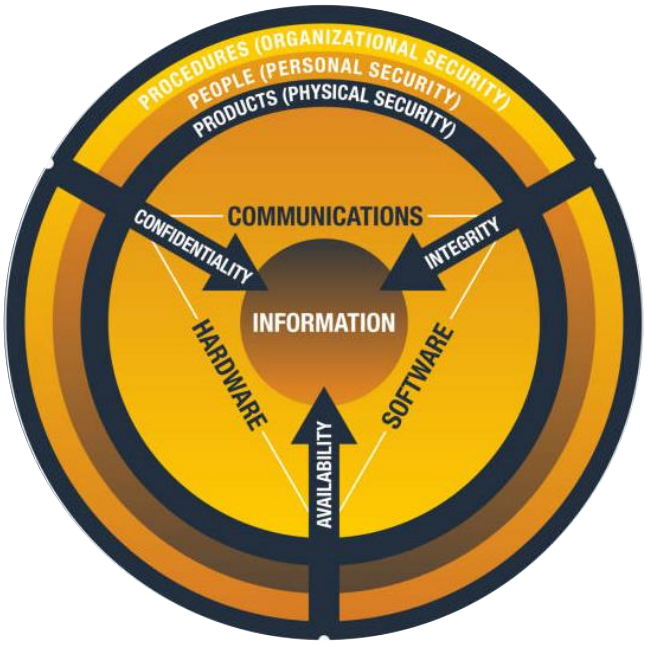
(i) thành phần thu thập thông tin (Input)

(ii) thành phần xử lý thông tin (Processing)

(iii) thành phần kết xuất thông tin (Output).

Hệ thống thông tin được sử dụng để tương tác với khách hàng (Customers), với nhà cung cấp (Suppliers), với cơ quan chính quyền (Regulatory Agencies), với cổ đông (Stockholders) và với đối thủ cạnh tranh (Competitors). Có thể nêu là một số hệ thống thông tin điển hình như các hệ lập kế hoạch nguồn lực doanh nghiệp, các máy tìm kiếm và các hệ thống thông tin địa lý.

Trong lớp các hệ thống thông tin, hệ thống thông tin dựa trên máy tính (Computer-based information system), hay sử dụng công nghệ máy tính để thực thi các nhiệm vụ là lớp hệ thống thông tin được sử dụng rộng rãi nhất. Hệ thống thông tin dựa trên máy tính thường gồm các thành phần: phần cứng (Hardware) để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu; phần mềm (Software) chạy trên phần cứng để xử lý dữ liệu; cơ sở dữ liệu (Databases) để lưu trữ dữ liệu; mạng (Networks) là hệ thống truyền dẫn thông tin/dữ liệu; và các thủ tục (Procedures) là tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.



(Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin)

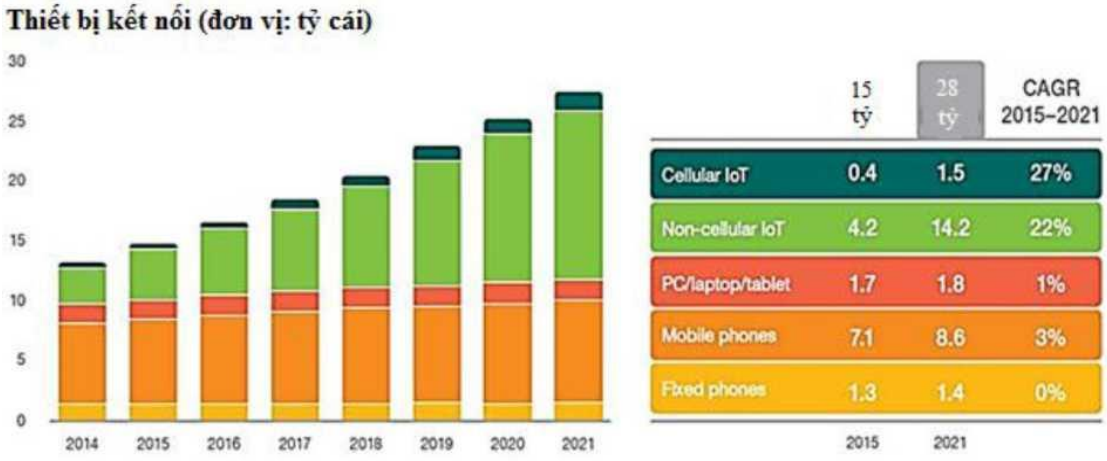
1.1.4. Một số khái niệm liên quan

* *Truy nhập (Access)* là việc một chủ thể, người 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.

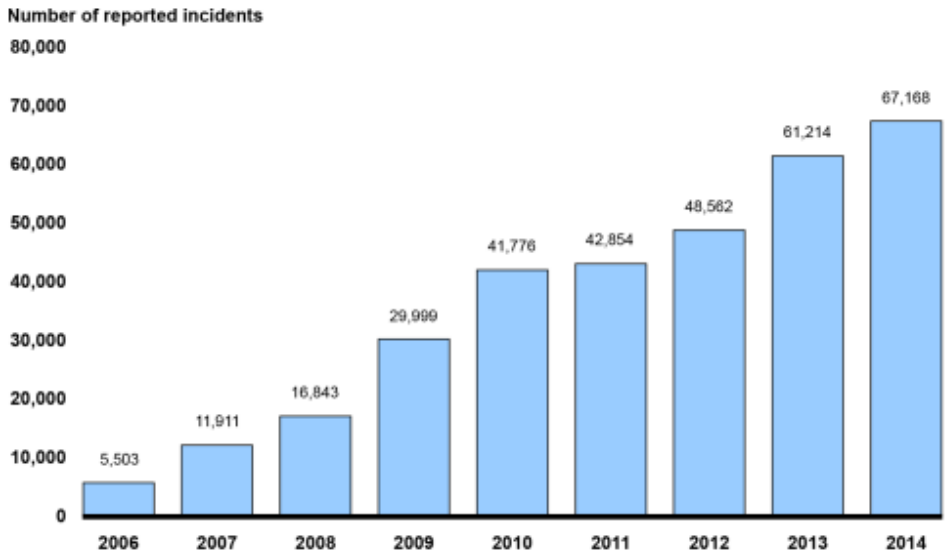
* *Tấn công (Attack)* là hành động có chủ ý hoặc không có chủ ý có khả năng gây hại, hoặc làm thỏa hiệp các thông tin, hệ thống và các tài sản được bảo vệ. Tấn công có thể chủ động hoặc thụ động, trực tiếp hoặc gián tiếp.

1.2. Một số nhìn nhận và sự cần thiết của an toàn bảo mật thông tin



(Số lượng các thiết bị kết nối vào Internet đến 2015 và dự báo đến 2021)

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của các thiết bị di động, và đặc biệt là các thiết bị loT (Internet of Things), số lượng người dùng mạng Internet và số lượng thiết bị kết nối vào mạng Internet tăng trưởng nhanh chóng. Theo thống kê và dự báo của Forbes [3] như hình ảnh trên, thì số lượng các thiết bị có kết nối Internet là khoảng 15 tỷ và dự báo sẽ tăng mạnh lên khoảng 28 tỷ thiết bị có kết nối vào năm 2021. Các thiết bị IoT kết nối thông minh là nền tảng cho phát triển nhiều ứng dụng quan trọng trong các lĩnh vực của đời sống xã hội, như thành phố thông minh, cộng đồng thông minh, ngôi nhà thông minh, ứng dụng giám sát và chăm sóc sức khỏe,...



(Số lượng các sự cố toàn hệ thống thông tin được thông báo đến Cơ quan ứng cứu khẩn cấp máy tính (US-CERT) trong giai đoạn 2006 - 2014 [4])

Cùng với những lợi ích to lớn mà các thiết bị kết nối Internet mạng lại, các sự cố mất an toàn thông tin đối với các hệ thống máy tính, điện thoại di động thông minh, các thiết bị

IoT và người dùng cũng tăng vọt. Theo số liệu ghi nhận của Cơ quan Thống kê quốc gia Hoa Kỳ cho ở hình trên, số lượng các sự cố mất an toàn hệ thống thông tin được thông báo đến Cơ quan ứng cứu khẩn cấp máy tính (US-CERT) trong giai đoạn 2006 - 2014 tăng rất mạnh, từ 5.503 vụ vào năm 2006 lên đến 67.168 vụ vào năm 2014. Ở Việt Nam, trong báo cáo "Tổng kết an ninh mạng năm 2015 và dự báo xu hướng 2016" [5], Tập đoàn Bkav cho biết 8.700 tỷ đồng là tổng thiệt hại ước tính do virus máy tính gây ra đối với người dùng Việt Nam trong năm 2015. Con số này vẫn ở mức cao và tiếp tục tăng so với 8.500 tỷ đồng của năm 2014. Dự báo trong năm 2016 và các năm tiếp theo, số lượng sự cố và thiệt hại do mất an toàn thông tin gây ra còn có thể lớn hơn nữa, do số lượng thiết bị kết nối tăng trưởng nhanh chóng và nguy cơ từ sự phát triển mạnh của các phần mềm độc hại và các kỹ thuật tấn công, phá hoại tinh vi.

Như vậy, việc đảm bảo an toàn cho thông tin, máy tính, hệ thống mạng và các thiết bị kết nối khác, chống lại các truy nhập trái phép và các cuộc tấn công phá hoại là rất cần thiết không chỉ đối với các cá nhân, cơ quan, tổ chức, doanh nghiệp mà còn cả đối với an ninh quốc gia. Hơn nữa, việc xây dựng các giải pháp an toàn thông tin chỉ thực sự hiệu quả khi được thực hiện bài bản, đồng bộ, đảm bảo cân bằng giữa tính an toàn, tính hữu dụng của hệ thống và chi phí đầu tư cho các biện pháp đảm bảo an toàn.

1.3. Các yêu cầu đảm bảo An toàn thông tin và Hệ thống thông tin

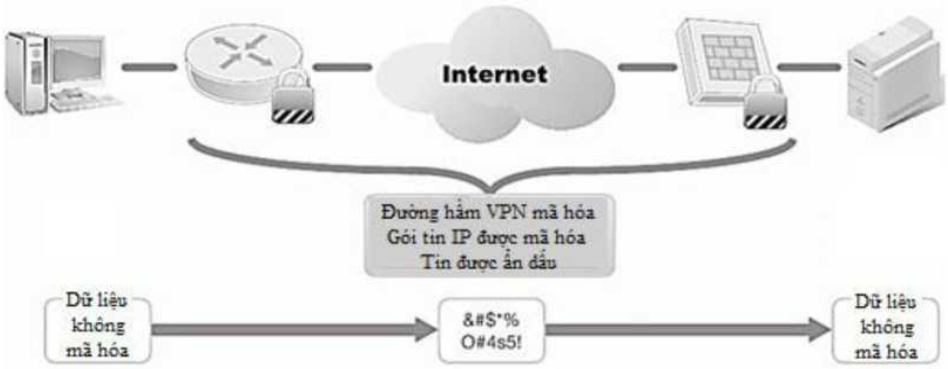
Như đã trình bày trong Mục 1, việc đảm bảo an toàn thông tin hoặc hệ thống thông tin là việc đảm bảo ba thuộc tính của thông tin hoặc hệ thống thông tin, bao gồm tính Bí mật (Confidentiality), tính Toàn vẹn (Integrity) và tính Sẵn dùng (Availability). Ngoài ra ở một số hệ thống còn bổ sung thêm yêu cầu về tính Chống thoái thác (Non-repudiation). Đây cũng là bốn yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin.

1.3.1. Bí mật (Confidentiality)

Tính bí mật đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy nhập thông tin, hệ thống. Các thông tin bí mật có thể bao gồm: (i) dữ liệu riêng của cá nhân, (ii) các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan, tổ chức và (iii) các thông tin có liên quan đến an ninh của các quốc gia và các chính phủ. Theo đó chỉ những người có thẩm quyền (có thể không gồm người soạn thảo văn bản) mới được đọc và phổ biến văn bản.

(Minh họa một văn bản được đóng dấu Confidential - Mật)

Ví dụ thực tế về tính bí mật mà chúng ta thường gặp như: Trong hệ thống ngân hàng, khách hàng chỉ được phép xem thông tin về tài khoản của mình nhưng không được phép xem thông tin tài khoản của người khác.



(Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa)

Thông tin bí mật lưu trữ hoặc trong quá trình truyền tải cần được bảo vệ bằng các biện pháp phù hợp, tránh bị lộ lọt hoặc bị đánh cắp. Các biện pháp có thể sử dụng để đảm bảo tính bí mật của thông tin như bảo vệ vật lý, hoặc sử dụng mật mã (cryptography). Hình ảnh trên minh họa việc đảm bảo tính bí mật bằng cách sử dụng đường hầm VPN, hoặc mã hóa để truyền tải thông tin.

1.3.2. Toàn vẹn (Integrity)

Tính toàn vẹn đảm bảo rằng thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu. Trong nhiều tổ chức, thông tin và dữ liệu có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế. Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin. Thông tin hoặc

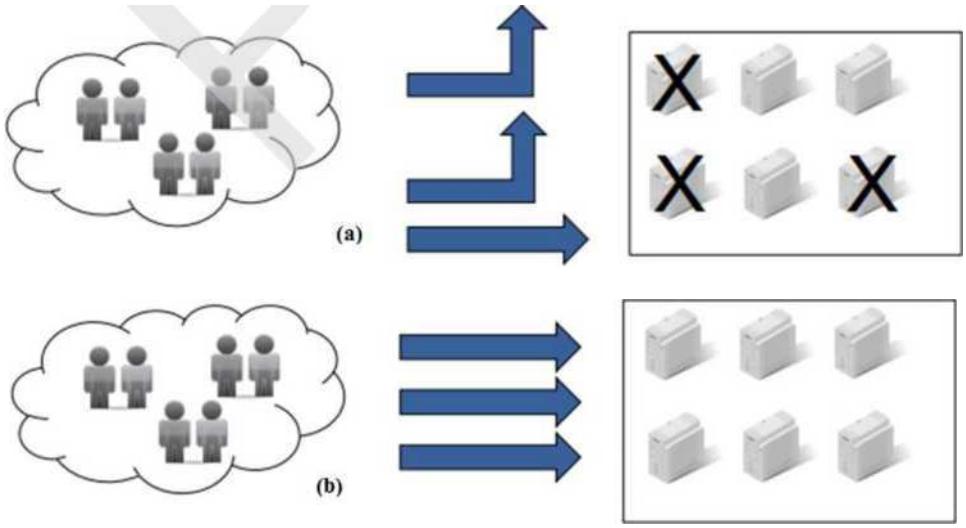
dữ liệu là toàn vẹn nếu nó thỏa mãn ba điều kiện: (i) không bị thay đổi, (ii) hợp lệ và (iii) chính xác.

Một ví dụ điển hình nhất cho tính toàn vẹn đó là: Trong hệ thống ngân hàng, một khách hàng không thể tự ý thay đổi số dư tài khoản của mình khi không có bất kỳ một hoạt động giao dịch hợp lệ nào.

1.3.3. Sẵn dùng (Availability)

Tính sẵn dùng, hoặc khả dụng đảm bảo rằng thông tin, hoặc hệ thống có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn dùng có thể được đo bằng các yếu tố:

- Thời gian cung cấp dịch vụ (Uptime);
- Thời gian ngừng cung cấp dịch vụ (Downtime);
- Tỷ lệ phục vụ: A = (Uptime) / (Uptime + Downtime);
- Thời gian trung bình giữa các sự cố;
- Thời gian trung bình ngừng để sửa chữa;
- Thời gian khôi phục sau sự cố.



(Minh họa tính sẵn dùng: (a) không đảm bảo và (b) đảm bảo tính sẵn dùng)

Trường hợp (a) hệ thống không đảm bảo tính sẵn dùng khi có một số thành phần gặp sự cố thì không có khả năng phục vụ tất cả các yêu cầu của người dùng và (b) hệ thống đảm bảo tính sẵn dùng khi các thành phần của nó hoạt động bình thường.

Ví dụ: Trong hệ thống ngân hàng, cần đảm bảo rằng khách hàng có thể truy vấn thông tin số dư tài khoản bất cứ lúc nào theo như quy định.

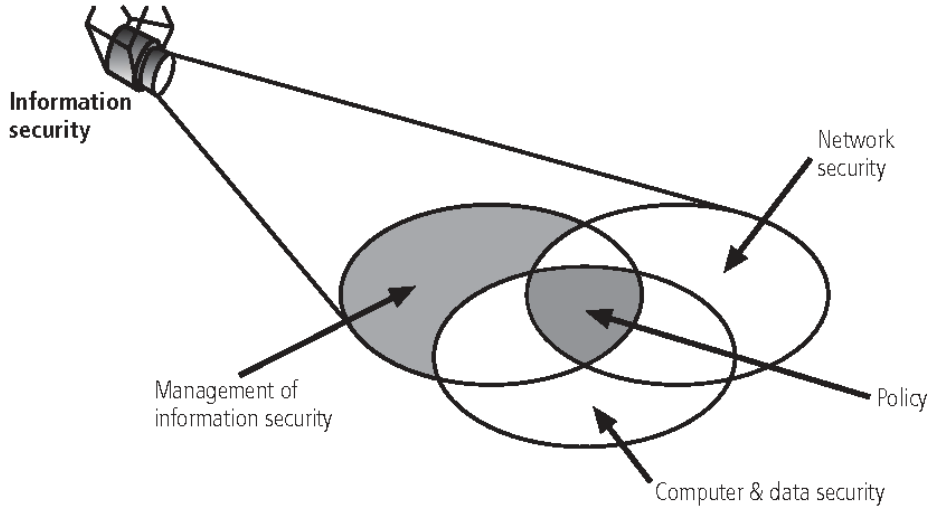
1.3.4. Chống thoái thác (Non-repudiation)

Tính chống thoái thác là khả năng ngăn chặn việc từ chối một hành vi đã làm trên hệ thống.

Ví dụ: Trong hệ thống ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi của khách hàng đã làm như rút hoặc chuyển tiền trên tài khoản của họ.

1.4. Các thành phần của an toàn thông tin

An toàn thông tin có thể được chia thành ba thành phần chính: *an toàn máy tính và dữ liệu* (Computer & data security), *an ninh mạng* (Network security) và *quản lý an toàn thông tin* (Management of information security) [1]. Ba thành phần của an toàn thông tin có quan hệ mật thiết và giao thoa với nhau, trong đó phần chung của cả ba thành phần trên là *chính sách an toàn thông tin* (Policy) như minh họa.



(Các thành phần chính của An toàn thông tin)

1.4.1. An toàn máy tính và dữ liệu (Computer & data security)

An toàn máy tính và dữ liệu là việc đảm bảo an toàn cho hệ thống phần cứng, phần mềm và dữ liệu trên máy tính; đảm bảo cho máy tính có thể vận hành an toàn, đáp ứng các yêu cầu của người sử dụng. An toàn máy tính và dữ liệu bao gồm các nội dung:

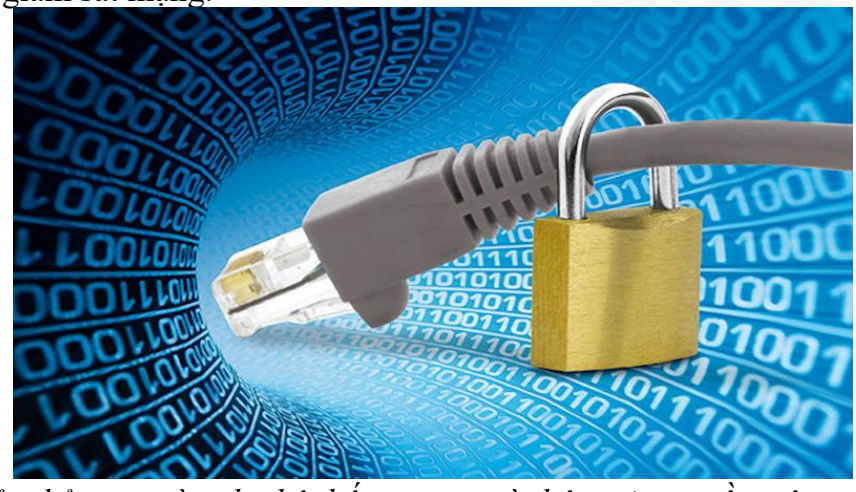
- Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ.
- Vấn đề điều khiển truy nhập;
- Vấn đề mã hóa và bảo mật dữ liệu;
- Vấn đề phòng chống phần mềm độc hại;
- Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.

(Minh họa đảm bảo an toàn máy tính và dữ liệu)

1.4.2. An ninh mạng (Network security)

An ninh mạng là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các tấn công, xâm nhập trái phép. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:

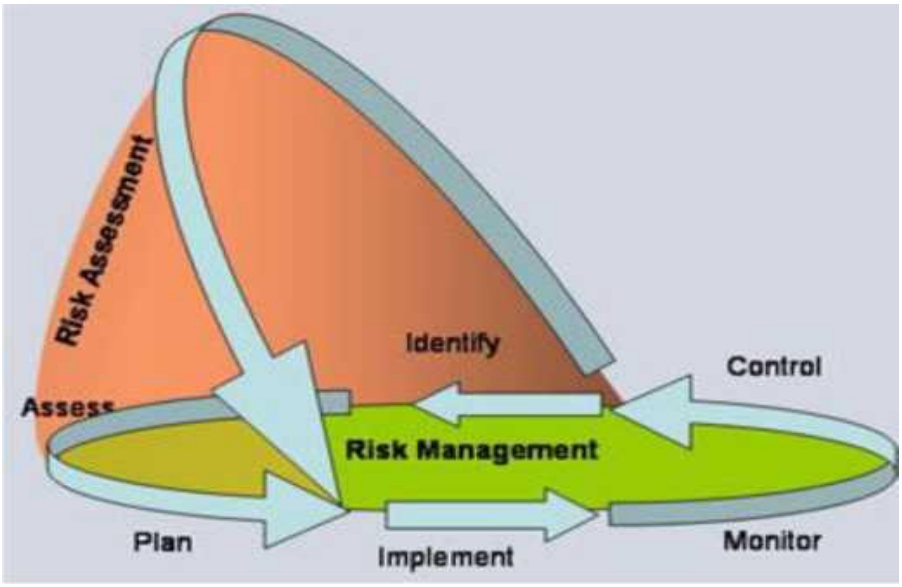
- Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập;
- Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- Vấn đề giám sát mạng.



(Đảm bảo an toàn cho hệ thống mạng và thông tin truyền trên mạng)

1.4.3. Quản lý an toàn thông tin (Management of information security)

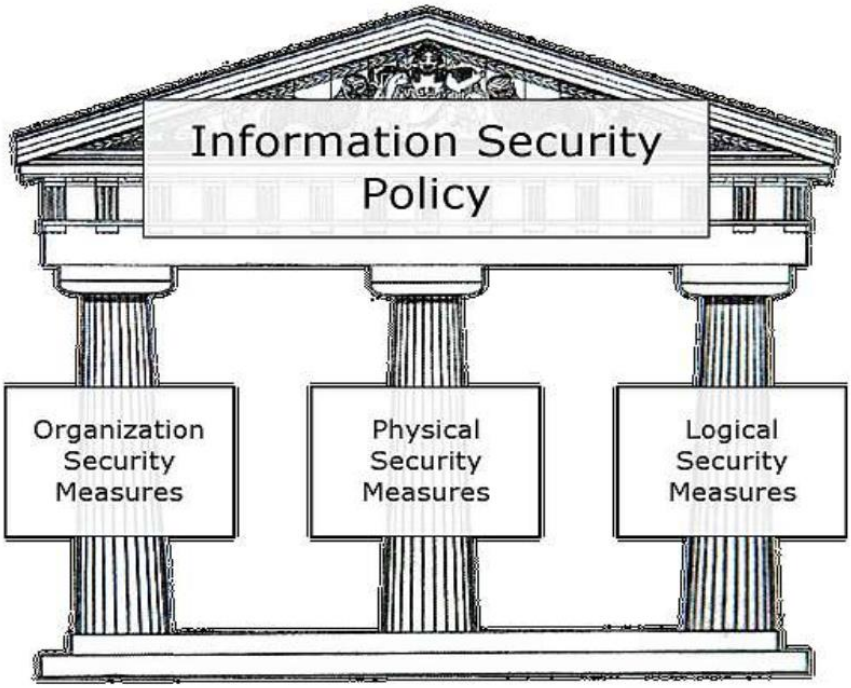
Quản lý an toàn thông tin là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Một trong các nội dung cốt lõi của quản lý an toàn thông tin là việc quản lý các rủi ro (Risk management), trong đó việc nhận dạng và đánh giá rủi ro (Risk assessment) đóng vai trò then chốt. Các nội dung khác của quản lý an toàn thông tin, bao gồm các chuẩn an toàn thông tin, chính sách an toàn thông tin và vấn đề đào tạo, nâng cao ý thức an toàn thông tin của người dùng.



(Chu trình quản lý an toàn thông tin)

Việc thực thi quản lý an toàn thông tin cần được thực hiện theo chu trình lặp lại, từ khâu lập kế hoạch (Plan), thực thi kế hoạch (Implement), giám sát kết quả thực hiện (Monitor) và thực hiện các kiểm soát (Control) như minh họa trên, do các điều kiện bên trong và bên ngoài thay đổi theo thời gian.

1.4.4. Chính sách an toàn thông tin (Policy)



(Chính sách an toàn thông tin)

Chính sách an toàn thông tin (Information security policy) là các nội quy, quy định của cơ quan, tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ. Chính sách an toàn thông tin gồm 3 thành phần:

- Chính sách an toàn ở mức vật lý (Physical security policy)
- Chính sách an toàn ở mức tổ chức (Organizational security policy)
- Chính sách an toàn ở mức logic (Logical security policy)

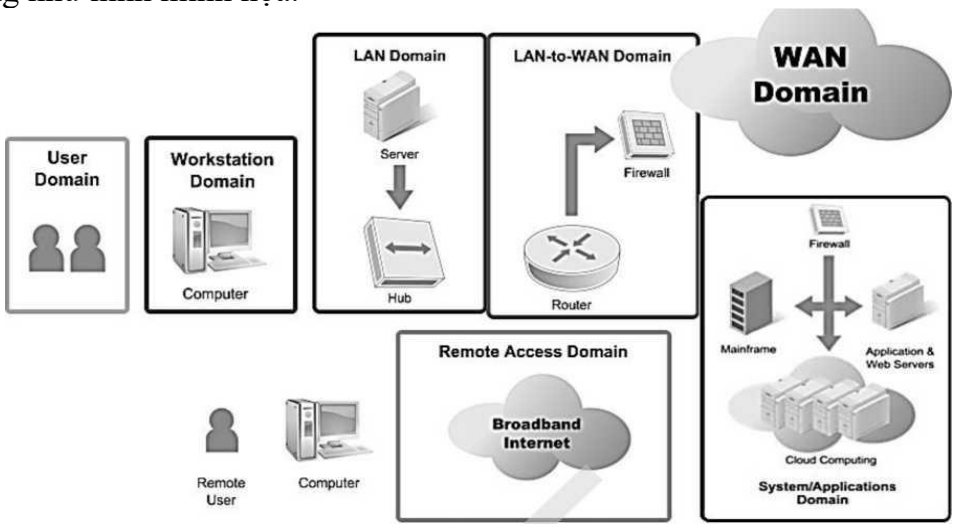
Một ví dụ về chính sách an toàn thông tin: để tăng cường an toàn cho hệ thống công nghệ thông tin, một tổ chức có thể áp dụng chính sách xác thực mạnh sử dụng các đặc

điểm sinh trắc (Biometrics), như xác thực sử dụng vân tay thay cho mật khẩu truyền thống cho hệ thống cửa ra vào trung tâm dữ liệu, hoặc đăng nhập vào hệ thống máy tính.

1.5. Các mối đe dọa và nguy cơ trong các vùng hạ tầng Công nghệ thông tin

1.5.1. Bảy vùng trong cơ sở hạ tầng CNTT

Hạ tầng công nghệ thông tin (IT Infrastructure) của các cơ quan, tổ chức, doanh nghiệp có thể có quy mô lớn hay nhỏ khác nhau, nhưng thường gồm bảy vùng theo mức kết nối mạng như hình minh họa.



(Bảy vùng trong hạ tầng CNTT theo mức kết nối mạng [2])

Các vùng cụ thể gồm: vùng người dùng (User domain), vùng máy trạm (Workstation domain), vùng mạng LAN (LAN domain), vùng LAN-to-WAN (LAN-to-WAN domain), vùng mạng WAN (WAN domain), vùng truy nhập từ xa (Remote Access domain) và vùng hệ thống/ứng dụng (Systems/Applications domain). Do mỗi vùng kể trên có đặc điểm khác nhau nên chúng có các mối đe dọa và nguy cơ mất an toàn thông tin khác nhau.

1.5.2. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT

** Vùng người dùng*

Có thể nói vùng người dùng là vùng có nhiều mối đe dọa và nguy cơ nhất do người dùng có bản chất khó đoán định và khó kiểm soát hành vi. Các vấn đề thường gặp như thiếu ý thức, coi nhẹ vấn đề an ninh an toàn, vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép; phá hoại dữ liệu, ứng dụng và hệ thống; các nhân viên bất mãn có thể tấn công hệ thống từ bên trong, hoặc nhân viên có thể tống tiền hoặc chiếm đoạt thông tin nhạy cảm, thông tin quan trọng.

** Vùng máy trạm*

Vùng máy trạm cũng có nhiều mối đe dọa và nguy cơ do vùng máy trạm tiếp xúc trực tiếp với vùng người dùng. Các nguy cơ thường gặp gồm: truy nhập trái phép vào máy trạm, hệ thống, ứng dụng và dữ liệu; các lỗ hổng an ninh trong hệ điều hành, trong các phần mềm ứng dụng máy trạm; các hiểm họa từ virus, mã độc và các phần mềm độc hại. Ngoài ra, vùng máy trạm cũng chịu các nguy cơ do hành vi bị cấm từ người dùng, như đưa CD/DVD/USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép.

** Vùng mạng LAN*

Các nguy cơ có thể có đối với vùng mạng LAN bao gồm: truy nhập trái phép vào mạng LAN vật lý, truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu; các lỗ hổng

an ninh trong hệ điều hành và các phần mềm ứng dụng máy chủ; nguy cơ từ người dùng giả mạo trong mạng WLAN; tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa do sóng mang thông tin của WLAN truyền trong không gian có thể bị nghe trộm. Ngoài ra, các hướng dẫn và cấu hình chuẩn cho máy chủ LAN nếu không được tuân thủ nghiêm ngặt sẽ dẫn đến những lỗ hổng an ninh mà tin tặc có thể khai thác.

** Vùng mạng LAN-to-WAN*

Vùng mạng LAN-to-WAN là vùng chuyển tiếp từ mạng nội bộ ra mạng diện rộng, nên nguy cơ lớn nhất là tin tặc từ mạng WAN có thể thăm dò và rà quét trái phép các cổng dịch vụ, nguy cơ truy nhập trái phép. Ngoài ra, một nguy cơ khác cần phải xem xét là lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác.

** Vùng mạng WAN*

Vùng mạng WAN, hay mạng Internet là vùng mạng mở, trong đó hầu hết dữ liệu được truyền dưới dạng rõ, nên các nguy cơ lớn nhất là dễ bị nghe trộm và dễ bị tấn công phá hoại, tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS). Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm virus, sâu và các phần mềm độc hại.

** Vùng truy nhập từ xa*

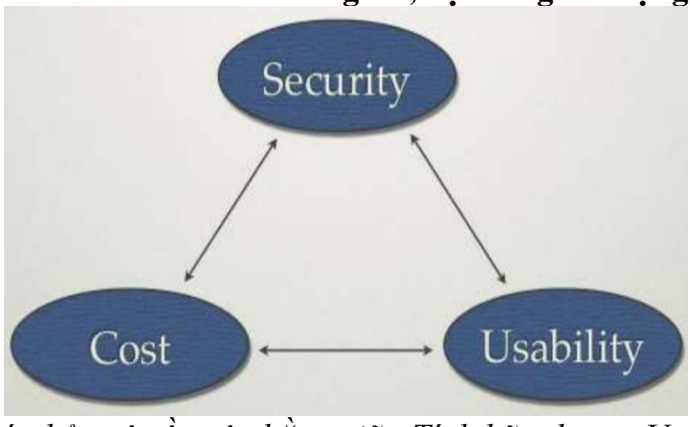
Trong vùng truy nhập từ xa, các nguy cơ điển hình bao gồm: tấn công kiểu vét cạn vào tên người dùng và mật khẩu, tấn công vào hệ thống đăng nhập và điều khiển truy nhập; truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu; các thông tin bí mật có thể bị đánh cắp từ xa; và vấn đề rò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ liệu.

** Vùng hệ thống và ứng dụng*

Trong vùng hệ thống và ứng dụng, các nguy cơ có thể bao gồm: truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp; các khó khăn trong quản lý các máy chủ với yêu cầu tính sẵn dùng cao; các lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ; các vấn đề an ninh trong các môi trường ảo của điện toán đám mây; và vấn đề hỏng hóc hoặc mất dữ liệu.

1.6. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

1.6.1. Nguyên tắc đảm bảo an toàn thông tin, hệ thống và mạng



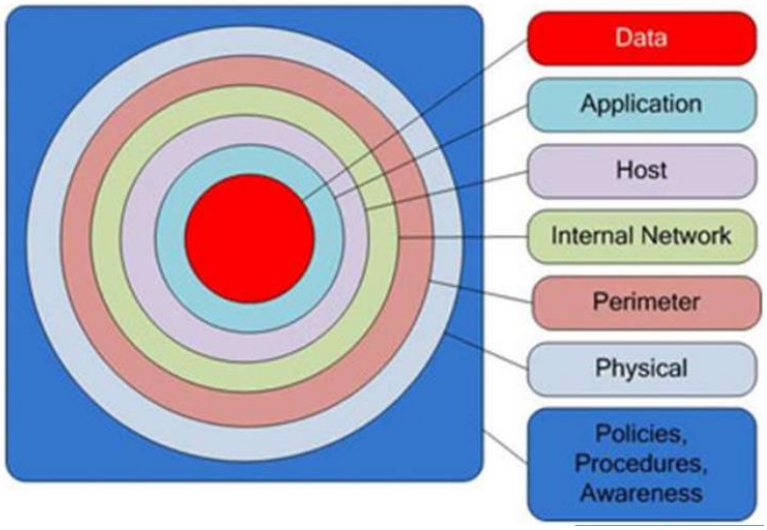
(Các lớp bảo vệ cần cân bằng giữa Tính hữu dụng - Usability, Chi phí - Cost và An toàn - Security)

Nguyên tắc chủ đạo xuyên suốt trong đảm bảo an toàn thông tin, hệ thống và mạng là Phòng vệ nhiều lớp có chiều sâu (Defence in Depth). Theo nguyên tắc này, ta cần tạo ra nhiều lớp bảo vệ, kết hợp tính năng, tác dụng của mỗi lớp để đảm bảo an toàn tối đa cho thông tin, hệ thống và mạng. Một lớp, một công cụ phòng vệ riêng rẽ dù có hiện đại, nhưng vẫn không thể đảm bảo an toàn. Do vậy, việc tạo ra nhiều lớp bảo vệ có khả năng bổ sung cho nhau là cách làm hiệu quả. Một điểm khác cần lưu ý khi thiết

kế và triển khai hệ thống đảm bảo an toàn thông tin là cần cân bằng giữa tính hữu dụng (Usability), chi phí (Cost) và an toàn (Security) như hình minh họa trên.
Hệ thống đảm bảo an toàn thông tin chỉ thực sự phù hợp và hiệu quả khi hệ thống được bảo vệ đạt mức an toàn phù hợp mà vẫn có khả năng cung cấp các tính năng hữu dụng cho người dùng, với chi phí cho đảm bảo an toàn phù hợp với tài sản được bảo vệ.

1.6.2. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin

Mô hình đảm bảo an toàn thông tin với bảy lớp bảo vệ, bao gồm lớp chính sách, thủ tục, ý thức (Policies, procedures, awareness); lớp vật lý (Physical); lớp ngoại vi (Perimeter); lớp mạng nội bộ (Internal network); lớp host (Host); lớp ứng dụng (Application) và lớp dữ liệu (Data). Trong mô hình này, để truy nhập được đến đối tượng đích là dữ liệu, tin tặc cần phải vượt qua cả 7 lớp bảo vệ.



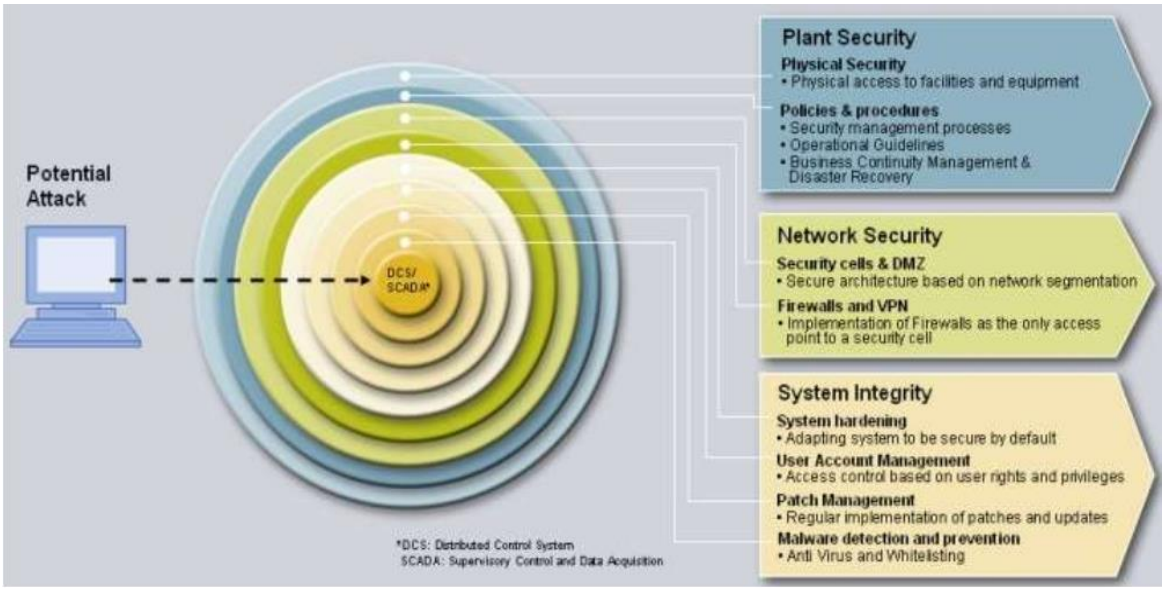
(Mô hình đảm bảo an toàn thông tin với bảy lớp)

Tương tự, mô hình phòng vệ gồm 3 lớp chính: lớp an ninh cơ quan/tổ chức, lớp an ninh mạng và lớp an ninh hệ thống. Mỗi lớp chính lại gồm một số lớp con như sau:
- Lớp an ninh cơ quan/tổ chức (Plant Security), gồm 2 lớp con:
+ Lớp bảo vệ vật lý (Physical Security) có nhiệm vụ kiểm soát các truy nhập vật lý đến các trang thiết bị hệ thống và mạng.
+ Lớp chính sách & thủ tục (Policies & procedures) bao gồm các quy trình quản lý an toàn thông tin, các hướng dẫn vận hành, quản lý hoạt động liên tục và phục hồi sau sự cố.
- Lớp an ninh mạng (Network Security), gồm 2 lớp con:
+ Lớp bảo vệ vùng hạn chế truy nhập (Security cells and DMZ) cung cấp các biện pháp bảo vệ cho từng phân đoạn mạng.
+ Lớp các tường lửa, mạng riêng ảo (Firewalls and VPN) được triển khai như điểm truy nhập duy nhất đến một phân đoạn mạng.
- Lớp an ninh hệ thống (System Integrity), gồm 4 lớp con:
+ Lớp tăng cường an ninh hệ thống (System hardening) đảm bảo việc cài đặt và cấu hình các thành phần trong hệ thống đảm bảo các yêu cầu an toàn.
+ Lớp quản trị tài khoản người dùng (User Account Management) thực hiện kiểm soát

truy nhập dựa trên quyền truy nhập và các đặc quyền của người dùng.

+ Lớp quản lý các bản vá (Patch Management) có nhiệm vụ định kỳ cài đặt các bản vá an ninh và các bản cập nhật cho hệ thống.

+ Lớp phát hiện và ngăn chặn phần mềm độc hại (Malware detection and prevention) có nhiệm vụ bảo vệ hệ thống, chống virus và các phần mềm độc hại khác.



(Mô hình đảm bảo an toàn thông tin với ba lớp chính)

❖ TÓM TẮT CHƯƠNG 1

Trong chương này, một số nội dung chính được giới thiệu:

- **Khái Niệm về An Toàn Hệ Thống Thông Tin**: Chương bắt đầu bằng việc giới thiệu khái niệm về an toàn hệ thống thông tin, tức việc đảm bảo rằng thông tin quan trọng của một tổ chức được bảo vệ khỏi mối đe dọa và xâm nhập.
- **Tầm Quan Trọng của An Toàn Thông Tin**: Chương này nhấn mạnh tầm quan trọng của an toàn thông tin trong bảo vệ dữ liệu quan trọng, tránh mất lạc tài chính, và duy trì uy tín của tổ chức.
- **Mối Đe Dọa Mạng**: Tìm hiểu về các mối đe dọa mạng phổ biến như virus máy tính, tấn công mạng, và lừa đảo trực tuyến. Chương giới thiệu các ví dụ cụ thể về những loại tấn công này.
- **Chuẩn Bảo Mật và Quy Định**: Chương này cung cấp cái nhìn về các chuẩn bảo mật và quy định quốc tế và ngành công nghiệp liên quan đến bảo mật thông tin, bao gồm việc đề cập đến ISO 27001, HIPAA, GDPR, và các quy định khác.
- **Vai Trò của Người Quản Lý An Toàn Thông Tin**: Chương này giới thiệu vai trò và trách nhiệm của người quản lý an toàn thông tin trong tổ chức, đảm bảo rằng họ chịu trách nhiệm đối với việc đảm bảo an toàn hệ thống thông tin.

❖ CÁC BÀI TẬP HỆ THỐNG KIẾN THỨC

1) An toàn thông tin (Information Security) là gì?
2) Tại sao cần phải đảm bảo an toàn cho thông tin?
3) Đảm bảo thông tin thường được thực hiện bằng cách nào?
4) An toàn hệ thống thông tin là gì?

5) Nêu các yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin.
6) An toàn thông tin gồm những thành phần cơ bản nào?
7) Nêu các rủi ro trong vùng người dùng và vùng máy trạm trong hạ tầng CNTT. Tại sao nói vùng người dùng là vùng có nhiều nguy cơ và rủi ro nhất?
8) Nêu các rủi ro trong vùng mạng LAN, LAN-to-WAN và vùng mạng WAN trong hạ tầng CNTT. Tại sao vùng mạng WAN có nguy cơ bị tấn công phá hoại cao?
9) Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là gì?
10) Mô tả một mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin.

CHƯƠNG 2. LỖ HỔNG BẢO MẬT VÀ CÁC ĐIỂM YẾU HỆ THỐNG

❖ GIỚI THIỆU CHƯƠNG 2

Chương 2 của môn học "An Toàn Hệ Thống Thông Tin" tập trung vào việc hiểu và xác định lỗ hổng bảo mật cũng như các điểm yếu trong hệ thống thông tin. Học sinh tìm hiểu về cách những lỗ hổng này có thể được tấn công và cách bảo vệ hệ thống khỏi những rủi ro này. Chương này là bước quan trọng trong việc xây dựng kiến thức và kỹ năng để đảm bảo an toàn thông tin trong môi trường công nghệ thông tin.

❖ MỤC TIÊU CHƯƠNG 2

Sau khi học xong chương này, người học có khả năng:

➢ *Về kiến thức:*

- *Hiểu các loại lỗ hổng bảo mật phổ biến, như lỗ hổng phần mềm, lỗ hổng mạng, và lỗ hổng xã hội.*
- *Nhận diện kỹ năng xác định điểm yếu trong hệ thống thông tin, bao gồm việc tìm hiểu về các lỗ hổng và thiếu sót có thể được tấn công.*
- *Hiểu về cách các phương pháp tấn công khai thác lỗ hổng bảo mật, bao gồm tấn công từ xa và tấn công bên trong tổ chức.*
- *Hiểu cách xác định và ngăn chặn các tấn công bằng cách vá các lỗ hổng, tăng cường bảo mật mạng, và thực hiện các biện pháp bảo mật.*

➢ *Về kỹ năng:*

- *Kỹ Năng phát hiện các lỗ hổng bảo mật trong hệ thống thông tin và phân biệt chúng với các điểm yếu hệ thống.*
- *Kỹ Năng đánh giá rủi ro của các lỗ hổng bảo mật và điểm yếu, đánh giá mức độ nguy cơ và ảnh hưởng.*
- *Kỹ Năng xác định các phương pháp tấn công mà tấn công lỗ hổng và điểm yếu của hệ thống thông tin.*
- *Kỹ Năng áp dụng biện pháp bảo mật để bảo vệ hệ thống khỏi tấn công, bao gồm việc vá lỗ hổng, cập nhật phần mềm, và thực hiện kiểm tra bảo mật.*

➢ *Về năng lực tự chủ và trách nhiệm:*

- *Năng lực về quản lý thời gian, trách nhiệm với công việc*
- *Năng lực học tập và làm việc độc lập*
- *Tự chủ trong việc giải quyết vấn đề*

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 2

- *Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, dạy học theo vấn đề); yêu cầu người học thực hiện câu hỏi thảo luận và bài tập chương (cá nhân hoặc nhóm).*
- *Đối với người học: chủ động đọc trước giáo trình trước buổi học; hoàn thành đầy đủ câu hỏi thảo luận và bài tập tình huống theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.*

❖ **ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 2**

- ***Phòng học chuyên môn hóa/nhà xưởng:*** Phòng học thực hành
- ***Trang thiết bị máy móc:*** Máy chiếu, máy tính và các thiết bị dạy học khác
- ***Học liệu, dụng cụ, nguyên vật liệu:*** Chương trình môn học, giáo trình, tài liệu tham khảo, giáo án, phim ảnh, và các tài liệu liên quan.
- ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 2**

- **Nội dung:**

✓ *Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức*

✓ *Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.*

✓ *Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:*

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ ***Điểm kiểm tra thường xuyên:*** *1 điểm kiểm tra (hình thức: hỏi miệng)*

✓ ***Kiểm tra định kỳ lý thuyết:*** *không có*

❖ **NỘI DUNG CHƯƠNG 2**

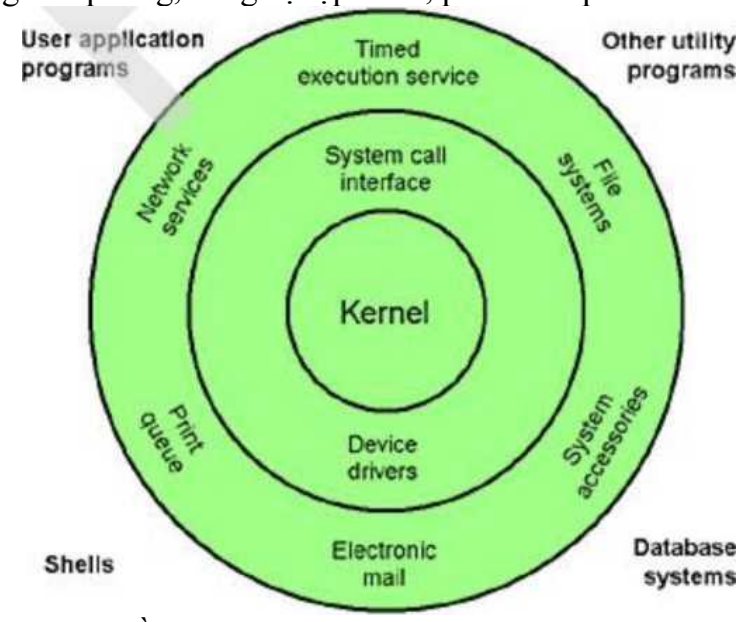
2.1. Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống

2.1.1. Khái quát về điểm yếu hệ thống và lỗ hổng bảo mật

Các thành phần của hệ thống

Một hệ thống máy tính gồm 2 thành phần cơ bản là hệ thống phần cứng và hệ thống phần mềm. Hệ thống phần cứng bao gồm các mô đun phần cứng tạo nên máy tính vật lý, bao gồm CPU, ROM, RAM, Bus,...; các giao diện ghép nối và các thiết bị ngoại vi, như bàn phím, màn hình, ổ đĩa,... và các giao diện ghép nối mạng LAN, WLAN, 3G,...

Hệ thống phần mềm bao gồm hệ điều hành và các phần mềm ứng dụng. Hệ điều hành cung cấp môi trường làm việc cho các ứng dụng và giao diện người dùng, được cấu thành từ nhân hệ điều hành, các trình điều khiển thiết bị, hệ thống quản lý tiến trình, hệ thống quản lý file, các trình cung cấp dịch vụ, tiện ích,… Các phần mềm ứng dụng là các chương trình cung cấp các tính năng hữu ích cho người dùng, bao gồm các dịch vụ (máy chủ web, cơ sở dữ liệu, DNS,...), các trình duyệt web, các ứng dụng giao tiếp, các bộ ứng dụng văn phòng, công cụ lập trình, phát triển phần mềm.



(Mô hình hệ điều hành Unix/Linux, các dịch vụ và các ứng dụng)

2.1.2. Điểm yếu hệ thống và lỗ hổng bảo mật

Trên thực tế, không có hệ thống nào là hoàn hảo, không có điểm yếu, hoặc khiếm khuyết. Các hệ thống máy tính, hoặc hệ thống thông tin là các hệ thống rất phức tạp, được cấu thành từ nhiều thành phần phần cứng, phần mềm, luôn tồn tại các lỗi, các khiếm khuyết, hay các điểm yếu. Các điểm yếu có thể tồn tại trong các mô đun phần cứng, phần mềm. Nguyên nhân có thể do lỗi thiết kế, lỗi cài đặt, hoặc lập trình, hoặc do cấu hình hoạt động không chuẩn,... Nhìn chung, các hệ thống càng phức tạp và nhiều tính năng thì khả năng xuất hiện các lỗi và điểm yếu càng tăng.

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 được 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).

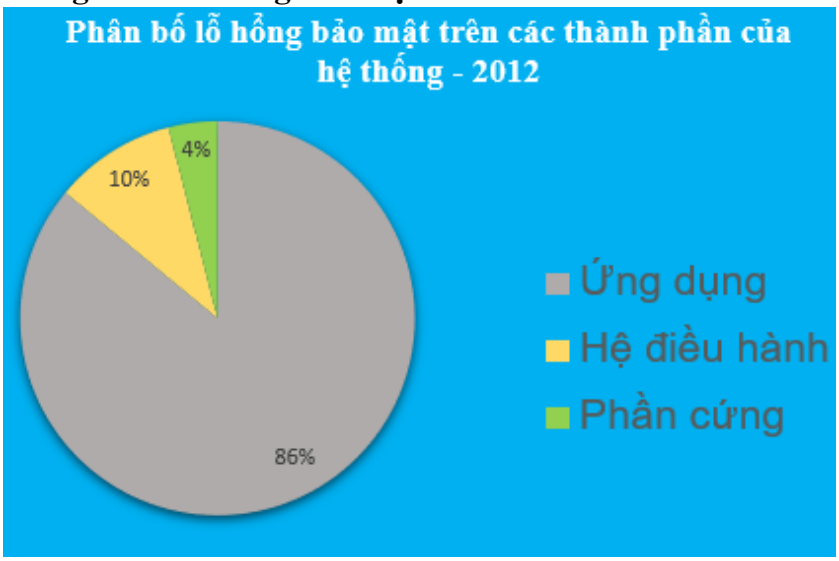
Lỗ hổng bảo mật thuộc cấp độ nguy hiểm là lỗ hổng cho phép tin tặc thực hiện mã khai thác mà không cần tương tác người dùng. Các thông tin khai thác lỗ hổng, như mã mẫu khai thác tồn tại phổ biến trên mạng. Ngoài ra, việc khai thác lỗ hổng có thể được thực hiện dễ dàng mà không yêu cầu có tài khoản hệ 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 virus, 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 virus hoặc các phần mềm độc hại cần tương tác người dùng để lây lan, như 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.

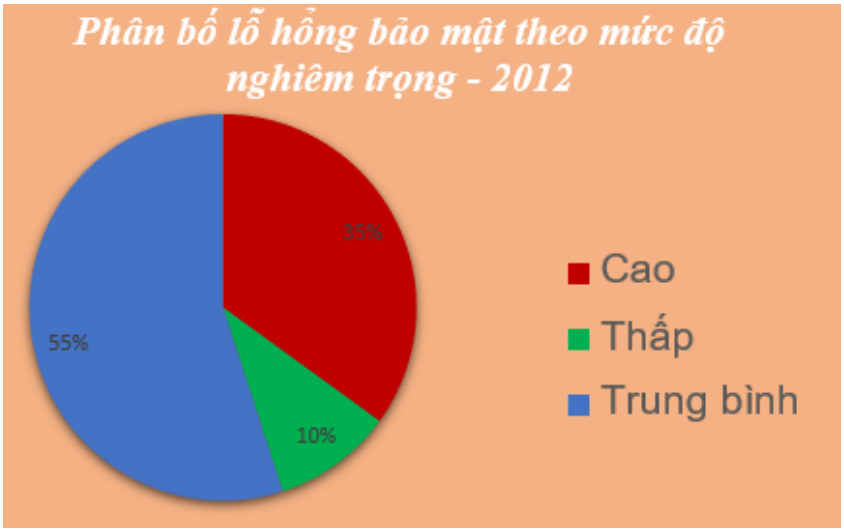
Loại cuối cùng là các lỗ hổng bảo mật thuộc cấp độ thấp. Các lỗ hổng loại này ít có ảnh hưởng đến hoạt động của tổ chức và chúng chỉ có thể bị khai thác khi tin tặc có truy nhập cục bộ hoặc truy nhập vật lý trực tiếp vào hệ thống. Mặc dù vậy, vẫn cần xem xét khắc phục định kỳ để hạn chế ảnh hưởng.

2.1.3. Một số thống kê về lỗ hổng bảo mật



(Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống)

Theo số liệu thống kê từ Cơ sở dữ liệu lỗ hổng quốc gia Hoa Kỳ [6], trong năm 2012, phân bố lỗ hổng bảo mật được phát hiện trên các thành phần của hệ thống lần lượt là phần cứng - 4%, hệ điều hành - 10% và phần mềm ứng dụng - 86%, như minh họa. Như vậy, có thể thấy các lỗ hổng bảo mật chủ yếu xuất hiện trong hệ thống phần mềm và phần lớn tồn tại trong các phần mềm ứng dụng.



(Phân bố lỗ hổng bảo mật theo mức độ nghiêm trọng)

Theo mức độ nghiêm trọng của các lỗ hổng bảo mật hệ thống minh họa như hình trên, trong năm 2012 các lỗ hổng có mức độ nghiêm trọng cao (High) chiếm 35%, các lỗ hổng có mức độ nghiêm trọng trung bình (Medium) chiếm 55% và các lỗ hổng có mức độ nghiêm trọng thấp (Low) chỉ chiếm 10%. Như vậy, ta có thể thấy, đa số các lỗ hổng bảo mật có mức độ nghiêm trọng từ trung bình trở lên và cần được xem xét khắc phục càng sớm càng tốt.

Dưới đây là hai bảng cung cấp số liệu thống kê về các loại lỗ hổng bảo mật trên các hệ điều hành phổ biến trong hai năm 2011 – 2012 và số liệu thống kê về các loại lỗ hổng bảo mật trên một số ứng dụng phổ biến trong hai năm 2011 - 2012.

Theo đó, hệ điều hành iOS cho điện thoại di động iPhone và máy tính bảng iPad có số lỗ hổng được phát hiện cao nhất và tăng cao trong những năm gần đây do sự phổ biến của iPhone và iPad. Xếp sau iOS về số lượng lỗ hổng được phát hiện là các hệ điều hành họ Microsoft Windows, bao gồm Windows 2003, 2008 servers, Windows XP, Windows 7 và Windows 8.

Operating system	# of vulnerabiliti		# of HIGH vulnerabiliti		# of MEDIUM		# of LOW vulnerabilitie	
	201	201	2012	201	2012	201	201	2011 1
Apple iOS	*t>	35	f 46	9	f 28	19	f 12	7
Microsoft	**4-45**	105	**4-40**	98	4*5	7	• 0	0
Microsoft XP	4- 42	96	4*37	91	f 5	4	4*0	1
Microsoft	**4*48**	101	4*35	89	f 12	11	• 1	1
Microsoft	**4*41**	91	**4*34**	86	f 6	4	fl	0
Microsoft	**4*42**	98	4*33	88	4* 8	9	• 1	1
Cisco IOS	*t 36	31	4*23	26	t 10	5	f 3	0
Linux Kernel	**4*45**	56	f 12	10	4*28	34	4*5	12
Oracle Solaris	t 47	39	f 7	6	f 29	19	4-11	14
VMware ESXi	t 12	7	f 11	2	• 1	1	^0	4
VMware ESX	-fr 11	7	f 9	2	f 2	1	4*0	4
Cisco IOS XE	4*9	13	4*9	12	4*0	1	• 0	0
Citrix Xen	*b 33	3	f 2	1	f 21	1	*b 10	1
Apple Mac OS X	4*21	69	4* 3	9	4* 16	50	4* 2	10
Apple Mac OS X	4* 17	66	4*3	7	4* 12	50	f 2	9

(Lỗ hổng bảo mật phát hiện trong các năm 2011 và 2012 trên các hệ điều hành)

Về các loại lỗ hổng bảo mật thì số lượng lỗ hổng được phát hiện nhiều nhất thuộc về các ứng dụng trình duyệt và email của Mozilla, trình duyệt Google Chrome, Apple Safari,... Có thể thấy các trình duyệt web tồn tại nhiều lỗ hổng bảo mật và bị tấn công khai thác nhiều nhất là do chúng là các ứng dụng được sử dụng thường xuyên nhất trên mạng Internet. Tin tặc thường khai thác các lỗ hổng trên các trang web và trình duyệt để đánh cắp các dữ liệu cá nhân của người dùng.

"Z	vulnerabilities		vulnerabilitie		vulnerabilities		# of LOW vulnerabilitie	
	201	201	2012	201	2012	201	201	2011
Mozilla Firefox	**f** 159	97	**f** 99	66	**f 55**	30	**f** 5	2
Mozilla	**f** 144	63	**f** 95	46	**f** 47	15	• 2	2
Mozilla	**f** 143	63	**f** 94	45	**f** 46	17	**f** 3	1
Mozilla Firefox	115	--	75	-	39	--	1	-

Mozilla	109	-	74	-	34	-	1	
Google Chrome	4*	275	**4*68**	162	**4-55**	113	**f** 2	0
AppleSafari	**f** 85	45	**f** 65	28	**f** 20	16	**4*0**	1
Adobe Flash	**f** 66	63	**f** 61	57	**4*5**	6	• 0	0
Apple iTunes	**f** 102	78	**4*51**	78	**f 51**	0	• 0	0
Adobe Air	**f** 54	27	**f** 51	26	**f** 3	1	• 0	0
Adobe Flash	53	-	49	-	4	-	0	-
Oracle Java	**f** 58	37	**f** 32	23	**f** 20	10	**f** 6	4
Microsoft Internet Explorer	**4*41**	45	**f** 34	31	**4*7**	14	• 0	0
FFmpeg	**f** 42	10	**f** 28	3	**f 13**	7	fl	0
Adobe Shockwave	4* 27	38	**4*** 27	38	• 0	0	• 0	0
Adobe Reader	4*25	65	**4*25**	54	**4*0**	11	• 0	0

(Lỗ hổng bảo mật phát hiện trong các năm 2011 và 2012 trên một số ứng dụng)

2.2. Các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng

Như đã đề cập trong Mục 2.1, thực tế các lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng chiếm hơn 95% số lượng lỗ hổng bảo mật được phát hiện cho thấy mức độ phổ biến của các lỗ hổng bảo mật trong hệ thống phần mềm. Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng bao gồm: lỗi tràn bộ đệm (Buffer overflows); lỗi không kiểm tra đầu vào (Unvalidated input); các vấn đề với điều khiển truy nhập (Access-control problems); các điểm yếu trong xác thực, trao quyền hoặc các hệ mật mã (Weaknesses in authentication, authorization, or cryptographic practices); và các lỗ hổng bảo mật khác.

2.2.1. Lỗi tràn bộ đệm

** Giới thiệu và nguyên nhân*

Lỗi tràn bộ đệm (Buffer overflow) là một trong các lỗi thường gặp trong các hệ điều hành và đặc biệt nhiều ở các phần mềm ứng dụng, như đã nêu ở mục 2.1 [6]. Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi của bộ nhớ đệm, là giới hạn cuối hoặc cả giới hạn đầu của bộ đệm. Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công chèn, thực hiện mã độc để kiểm soát hệ thống. Lỗi tràn bộ đệm chiếm một tỷ lệ lớn trong số các lỗi gây lỗ hổng bảo mật [6]. Tuy nhiên, trên thực tế không phải tất cả các lỗi tràn bộ đệm đều có thể bị khai thác bởi kẻ tấn công.

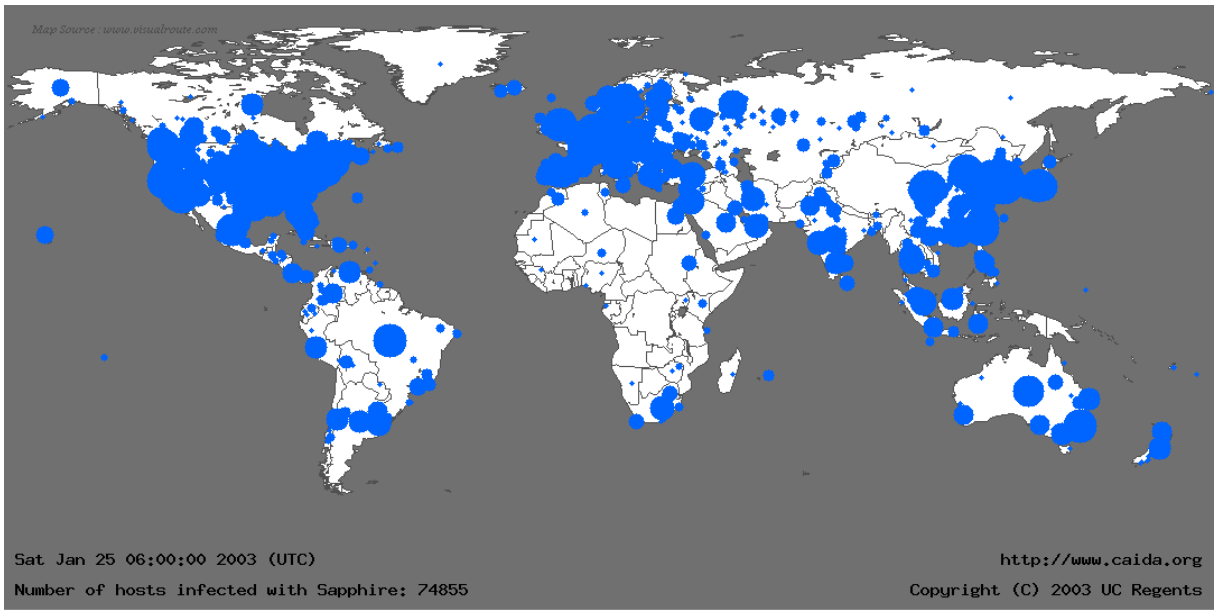
Lỗi tràn bộ đệm xuất hiện trong khâu lập trình phần mềm (coding) trong quy trình phát triển phần mềm. Nguyên nhân của lỗi tràn bộ đệm là người lập trình không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào nạp vào bộ nhớ đệm. Khi dữ liệu có kích thước quá lớn hoặc có định dạng sai được ghi vào bộ nhớ đệm, nó sẽ gây tràn và có thể ghi đè lên các tham số thực hiện chương trình, có thể khiến chương trình bị lỗi và ngừng hoạt động. Một nguyên nhân bổ sung khác là việc sử dụng các ngôn ngữ

với các thư viện không an toàn, như hợp ngữ, C và C++.

** Khai thác lỗi tràn bộ nhớ đệm*

Khi một ứng dụng chứa lỗ hổng tràn bộ đệm, tin tặc có thể khai thác bằng cách gửi mã độc dưới dạng dữ liệu đến ứng dụng nhằm ghi đè, thay thế địa chỉ trở về với mục đích tái định hướng chương trình đến thực hiện đoạn mã độc mà tin tặc gửi đến. Đoạn mã độc tin tặc xây dựng là mã máy có thể thực hiện được và thường được gọi là shellcode. Như vậy, để có thể khai thác lỗi tràn bộ đệm, tin tặc thường phải thực hiện việc gỡ rối (debug) chương trình (hoặc có thông tin từ nguồn khác) và nắm chắc cơ chế gây lỗi và phương pháp quản lý, cấp phát vùng nhớ ngăn xếp của ứng dụng.

Ví dụ điển hình nhất cho việc khai thác lỗi tràn bộ nhớ đệm là Sâu SQL Slammer (một số tài liệu gọi là sâu Sapphire) được phát hiện ngày 25/1/2003 lúc 5h30 (UTC) là sâu có tốc độ lây lan nhanh nhất lúc bấy giờ: nó lây nhiễm ra khoảng 75.000 máy chủ chỉ trong khoảng 30 phút, như minh họa bên dưới. Sâu Slammer khai thác lỗi tràn bộ đệm trong thành phần Microsoft SQL Server Resolution Service của hệ quản trị cơ sở dữ liệu Microsoft SQL Server 2000.



(Bản đồ lây nhiễm sâu Slammer (mầu xanh) theo trang www.caida.org vào ngày 25/1/2003 lúc 6h00 (giờ UTC) với 74.855 máy chủ bị nhiễm)

Sâu sử dụng giao thức UDP với kích thước gói tin 376 byte và vòng lặp chính của sâu chỉ gồm 22 lệnh hợp ngữ. Chu trình hoạt động của sâu SQL Slammer gồm:

- Sinh tự động địa chỉ IP;
- Quét tìm các máy có lỗi với IP tự sinh trên cổng dịch vụ 1434;

- Nếu tìm được, gửi một bản sao của sâu đến máy có lỗi;

- Mã của sâu gây tràn bộ đệm, thực thi mã của sâu và quá trình lặp lại.

SQL Slammer là sâu "lành tính" vì nó không can thiệp vào hệ thống file, không thực hiện việc phá hoại hay đánh cắp thông tin ở hệ thống bị lây nhiễm. Tuy nhiên, sâu tạo ra lưu lượng mạng khổng lồ trong quá trình lây nhiễm, gây tê liệt đường truyền mạng Internet trên nhiều vùng của thế giới. Do mã của SQL Slammer chỉ được lưu trong bộ nhớ nó gây tràn mà không được lưu vào hệ thống file, nên chỉ cần khởi động lại máy là có thể tạm thời xóa được sâu khỏi hệ thống. Tuy nhiên, hệ thống chứa lỗ hổng có thể bị lây nhiễm lại nếu nó ở gần một máy khác bị nhiễm sâu. Các biện pháp phòng chống triệt để khác là cập nhật bản vá cho bộ phần mềm Microsoft SQL Server 2000.

** Biện pháp phòng chống lỗi tràn bộ nhớ đệm*

Để phòng chống lỗi tràn bộ đệm một cách hiệu quả, cần kết hợp nhiều biện pháp. Các biện pháp có thể thực hiện bao gồm:

- Kiểm tra thủ công mã nguồn hay sử dụng các công cụ phân tích mã tự động để tìm và khắc phục các điểm có khả năng xảy ra lỗi tràn bộ đệm, đặc biệt lưu ý đến các hàm xử lý xâu ký tự.

- Sử dụng cơ chế không cho phép thực hiện mã trong dữ liệu DEP (Data Excution Prevention). Cơ chế DEP được hỗ trợ bởi hầu hết các hệ điều hành (từ Windows XP và các hệ điều hành họ Linux, Unix,...) không cho phép thực hiện mã chương trình chứa trong vùng nhớ dành cho dữ liệu. Như vậy, nếu kẻ tấn công khai thác lỗi tràn bộ đệm, chèn được mã độc vào bộ đệm trong ngăn xếp, mã độc cũng không thể thực hiện.

- Ngẫu nhiên hóa sơ đồ địa chỉ cấp phát các ô nhớ trong ngăn xếp khi thực hiện chương trình, nhằm gây khó khăn cho việc gỡ rối và phát hiện vị trí các ô nhớ quan trọng như ô nhớ chứa địa chỉ trở về.

- Sử dụng các cơ chế bảo vệ ngăn xếp, theo đó thêm một số ngẫu nhiên phía trước địa chỉ trở về và kiểm tra số ngẫu nhiên này trước khi trở về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trở về.

- Sử dụng các ngôn ngữ, thư viện và công cụ lập trình an toàn. Trong các trường hợp có thể, sử dụng các ngôn ngữ không gây tràn, như Java, các ngôn ngữ lập trình trên nền Microsoft .Net. Với các ngôn ngữ có thể gây tràn như C, C++, nên sử dụng các thư viện an toàn (Safe C/C++ Libraries) để thay thế các thư viện chuẩn có thể gây tràn.

2.2.2. Lỗi không kiểm tra đầu vào

** Giới thiệu*

Lỗi không kiểm tra đầu vào (Unvalidated input) là một trong các dạng lỗ hổng bảo mật phổ biến, trong đó ứng dụng không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào, nhờ đó tin tặc có thể khai thác lỗi để tấn công ứng dụng và hệ thống. Dữ liệu đầu vào (Input data) cho ứng dụng rất đa dạng, có thể đến từ nhiều nguồn với nhiều định dạng khác nhau. Các dạng dữ liệu đầu vào điển hình cho ứng dụng:

- Các trường dữ liệu văn bản (text);
- Các lệnh được truyền qua địa chỉ URL để kích hoạt chương trình;
- Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng, hoặc các tiến trình khác cung cấp;
- Các đối số đầu vào trong dòng lệnh;
- Các dữ liệu từ mạng hoặc từ các nguồn không tin cậy.

Trên thực tế, tin tặc có thể sử dụng phương pháp thủ công, hoặc tự động để kiểm tra các dữ liệu đầu vào và thử tất cả các khả năng có thể để khai thác lỗi không kiểm tra đầu vào. Theo thống kê của trang web OWASP (http://www.owasp.org), một trang web chuyên về thông kê các lỗi bảo mật ứng dụng web, lỗi không kiểm tra đầu vào luôn chiếm vị trí nhóm dẫn đầu các lỗi bảo mật các trang web trong khoảng 5 năm trở lại đây.

** Tấn công khai thác*

Có hai dạng chính tấn công khai thác lỗi không kiểm tra đầu vào: (1) cung cấp dữ liệu quá lớn hoặc sai định dạng để gây lỗi cho ứng dụng, và (2) chèn mã khai thác vào dữ liệu đầu vào để thực hiện trên hệ thống của nạn nhân, nhằm đánh cắp dữ liệu nhạy cảm hoặc thực hiện các hành vi phá hoại.

(Hình minh họa tấn công khai thác lỗi không kiểm tra đầu vào dạng (1) thông qua việc nhập dữ liệu quá lớn, gây lỗi thực hiện cho trang web)

Chúng ta minh họa tấn công khai thác lỗi không kiểm tra đầu vào dạng (2) bằng việc chèn mã tấn công SQL vào dữ liệu đầu vào, được thực hiện trên hệ quản trị cơ sở dữ liệu nhằm đánh cắp, hoặc phá hủy dữ liệu trong cơ sở dữ liệu. Giả thiết một trang web tìm kiếm sản phẩm sử dụng câu lệnh SQL sau để tìm kiếm các sản phẩm:

"*SELECT * FROM tbl_products WHERE product_name like '%" + keyword + "%'*"

trong đó tbl_products là bảng lưu thông tin các sản phẩm, product_name là trường tên sản phẩm và keyword là từ khóa cung cấp từ người dùng form tìm kiếm. Nếu người dùng nhập từ khóa là "iPhone 7", khi đó câu lệnh SQL trở thành:

"*SELECT * FROM tbl_products WHERE product_name like '%iPhone 7%'*"

Nếu trong bảng có sản phẩm thỏa mãn điều kiện tìm kiếm, câu lệnh SQL sẽ trả về tập bản ghi. Nếu không có sản phẩm nào thỏa mãn điều kiện tìm kiếm, câu lệnh SQL sẽ trả về tập bản ghi rỗng. Nếu người dùng nhập từ khóa "iPhone 7';*DELETE FROM tbl_products;*--", khi đó câu lệnh SQL trở thành:

"SELECT * FROM tbl_products WHERE product_name like '%iPhone 7';*DELETE FROM tbl_products;--%*"

Như vậy, câu lệnh SQL được thực hiện trên cơ sở dữ liệu gồm 2 câu lệnh: câu lệnh chọn SELECT ban đầu và câu lệnh xóa DELETE do tin tặc chèn thêm. Câu lệnh "*DELETE FROM tbl_products*" sẽ xóa tất cả các bản ghi trong bảng tbl_products. Sở dĩ tin tặc có thể thực hiện điều này là do hầu hết các hệ quản trị cơ sở dữ liệu cho phép thực hiện nhiều câu lệnh SQL theo mẻ (batch), trong đó các câu lệnh được ngăn cách bởi dấu (;). Ngoài ra, dấu "--" ở cuối dữ liệu nhập để loại bỏ hiệu lực của phần lệnh còn lại do "--" là ký hiệu bắt đầu phần chú thích của dòng lệnh. Ngoài DELETE, tin tặc có thể chèn thêm các lệnh SQL khác, như INSERT, UPDATE để thực hiện việc chèn thêm bản ghi hoặc sửa đổi dữ liệu theo ý đồ tấn công của mình.

** Phòng chống*

Biện pháp chủ yếu phòng chống tấn công khai thác lỗi không kiểm tra đầu vào là lọc dữ liệu đầu vào. Tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy cần được kiểm tra kỹ lưỡng. Các biện pháp cụ thể bao gồm:

- Kiểm tra kích thước và định dạng dữ liệu đầu vào;

- Kiểm tra sự hợp lý của nội dung dữ liệu;

- Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng:

+ Các ký tự đặc biệt: *, ', =, -¬

+ Các từ khóa ngôn ngữ: SELECT, INSERT, UPDATE, DELETE, DROP, (với dạng tấn công chèn mã SQL).

2.2.3. Các vấn đề với điều khiển truy nhập

Điều khiển truy nhập (Access control) là một lớp bảo vệ đặc biệt quan trọng trong hệ thống các lớp bảo vệ hệ thống và dữ liệu. Điều khiển truy nhập liên quan đến việc điều khiển ai (chủ thể) được truy cập đến cái gì (đối tượng). Điều khiển truy nhập có thể được thiết lập bởi hệ điều hành, hoặc mỗi ứng dụng, và thường gồm 2 khâu: xác thực (Authentication) và trao quyền (Authorization). Xác thực là việc xác minh tính chân thực của thông tin nhận dạng của chủ thể, còn trao quyền là việc cấp quyền truy nhập cho chủ thể sau khi thông tin nhận dạng đã được xác thực. Các chủ thể được cấp quyền truy nhập vào hệ thống theo cấp độ khác nhau dựa trên chính sách an ninh của tổ chức.

Các vấn đề thường gặp với điều khiển truy nhập là hệ thống xác thực, hoặc trao quyền yếu hoặc có lỗi. Nếu điều khiển truy nhập bị lỗi, một người dùng bình thường có thể chiếm đoạt quyền của người quản trị và toàn quyền truy nhập vào hệ thống. Hoặc, tin tặc có thể lợi dụng lỗ hổng bảo mật của hệ thống điều khiển truy nhập để truy nhập vào các file trong hệ thống. Một dạng khai thác hệ thống điều khiển truy cập điển hình là một ứng dụng chạy trên người dùng quản trị có toàn quyền truy nhập vào hệ thống, và nếu một tin tặc chiếm được quyền điều khiển ứng dụng đó sẽ có toàn quyền truy nhập vào hệ thống. Để đảm bảo an toàn cho hệ thống điều khiển truy nhập, các biện pháp sau cần được xem xét áp dụng:

- Không dùng tài khoản quản trị (root hoặc admin) để chạy các chương trình ứng dụng.

- Luôn chạy các chương trình ứng dụng với quyền tối thiểu, vừa đủ để chúng thực thi các tác vụ.

- Kiểm soát chặt chẽ người dùng, xóa bỏ hoặc cấm truy nhập với những người dùng ngầm định kiểu everyone.

- Thực thi chính sách mật khẩu an toàn.

- Chỉ cấp quyền vừa đủ cho người dùng thực thi nhiệm vụ.

2.2.4. Các điểm yếu trong xác thực, trao quyền

Do các khâu xác thực và trao quyền là hai thành phần cốt lõi của một hệ thống điều khiển truy nhập, nên các điểm yếu trong xác thực và trao quyền ảnh hưởng trực tiếp đến độ an toàn của hệ thống điều khiển truy nhập. Một điểm yếu điển hình trong khâu xác thực là mật khẩu được luu dưới dạng rõ (plaintext), dẫn đến nguy cơ bị lộ mật khẩu rất cao trong

quá truyền thông tin xác thực. Ngoài ra, việc sử dụng mật khẩu đơn giản, dễ đoán, hoặc dùng mật khẩu trong thời gian dài cũng là điểm yếu dễ bị khai thác. Việc sử dụng cơ chế xác thực không đủ mạnh, nhu các cơ chế xác thực đơn giản của giao thức HTTP cũng tiềm ẩn các nguy cơ bị tấn công khai thác.

Trong khâu trao quyền cũng tồn tại một số điểm yếu, nhu sử dụng cơ chế thực hiện trao quyền không đủ mạnh, dễ bị vượt qua. Chẳng hạn, một trang web chỉ thực hiện ẩn các links đến các trang web mà người dùng không được truy nhập mà không thực sự kiểm tra quyền truy nhập trên từng trang, nếu người dùng tự gõ URL của trang thì vẫn có thể truy nhập.

2.2.5. Các điểm yếu trong các hệ mật mã

Các vấn đề với các hệ mật mã bao gồm việc sử dụng giải thuật mã hóa, giải mã, hàm băm yếu, lạc hậu, hoặc có lỗ hổng đã biết không thể khắc phục (DES, MD4, MD5,...); Việc sử dụng khóa (key) mã hóa, giải mã yếu, nhu các khóa có chiều dài ngắn, hoặc dễ đoán. Các hệ mã hóa khóa bí mật có độ an toàn cao, tốc độ cao, nhung gặp phải khó khăn trong vấn đề trao đổi, chia sẻ các khóa bí mật. Các khóa bí mật trao đổi trong môi trường không an toàn nhu mạng Internet có thể bị lộ, bị đánh cắp. Một số vấn đề khác có thể gặp phải với các hệ mã hóa, gồm các vấn đề xác thực người gửi, người nhận, vấn đề sử dụng các khóa, các chứng chỉ hết hạn hoặc bị thu hồi, hoặc chi phí tính toán lớn, đặc biệt đối với các hệ mã hóa khóa công khai.

2.2.6. Các lỗ hổng bảo mật khác

Các thao tác không an toàn với các file cũng có thể là một lỗ hổng bảo mật nghiêm trọng. Chẳng hạn, một người dùng thực hiện đọc/ghi file luu ở những nơi mà những người dùng khác cũng có thể ghi file đó. Các lỗi điển hình khác có thể gồm:

- Không kiểm tra chính xác loại file, định danh thiết bị, các links hoặc các thuộc tính khác của file truớc khi sử dụng;

- Cho phép tải file tài liệu, hình ảnh lên máy chủ nhung không kiểm tra định dạng file và không cấm quyền thực hiện, và do vậy tin tặc có thể tải lên và thực hiện các file chứa mã độc;

- Không kiểm tra mã trả về sau mỗi thao tác với file;

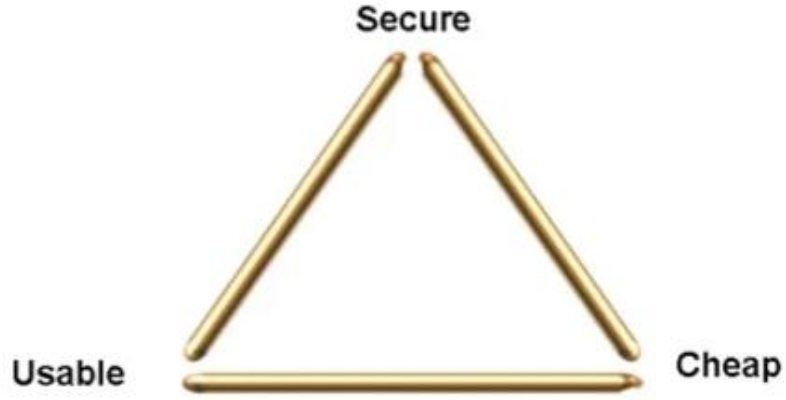
- Giả thiết một file có đuờng dẫn cục bộ là file cục bộ và bỏ qua các thủ tục kiểm tra. Tin tặc có thể khai thác lỗi này bằng cách ánh xạ file ở xa vào hệ thống file cục bộ, tức là có đuờng dẫn cục bộ và có thể đuợc thực thi trên hệ thống cục bộ.

Một dạng điểm yếu bảo mật khác xảy ra khi xuất hiện các điều kiện đua tranh (Race conditions). Một điều kiện đua tranh tồn tại khi có sự thay đổi trật tự của 2 hay một số sự kiện gây ra sự thay đổi hành vi của hệ thống. Đây là một dạng lỗi nếu chương trình chỉ có thể thực hiện đúng chức năng nếu các sự kiện phải xảy ra theo đúng trật tự. Tin tặc có thể lợi dụng khoảng thời gian giữa 2 sự kiện để chèn mã độc, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống.

2.3. Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống

2.3.1. Nguyên tắc chung

Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần được thực hiện theo nguyên tắc chung là cân bằng giữa an toàn (Secure), hữu dụng (Usable) và rẻ tiền (Cheap). Ý nghĩa cụ thể của nguyên tắc này là đảm bảo an toàn cho hệ thống ở mức phù hợp, với chi phí hợp lý và hệ thống vẫn phải hữu dụng, hay có khả năng cung cấp các tính năng hữu ích cho người dùng.



(Cân bằng giữa An toàn (Secure), Hữu dụng (Usable) và Rẻ tiền (Cheap))

2.3.2. Các biện pháp cụ thể

Trên cơ sở nguyên tắc chung của việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống, các biện pháp cụ thể cần được xem xét áp dụng với từng trường hợp cụ thể, đảm bảo hiệu quả cao. Biện pháp thiết yếu đầu tiên cần được thực hiện thường xuyên cho mọi trường hợp là thường xuyên cập nhật thông tin về các điểm yếu, lỗ hổng bảo mật từ các trang web chính thức:

- CVE - Common Vulnerabilities and Exposures: http://cve.mitre.org
- CVE Details: http://www.cvedetails.com
- US National Vulnerability Database: http://web.nvd.nist.gov
- OWASP: https://www.owasp.org/index.php/Category: Vulnerability

Biện pháp hiệu quả tiếp theo là định kỳ cập nhật các bản vá, nâng cấp hệ điều hành và các phần mềm ứng dụng, nhằm vá các lỗ hổng đã biết, cũng như tăng cường khả năng đề kháng cho hệ thống bằng các phiên bản mới an toàn hơn. Để thực hiện công việc này có

thể sử dụng các hệ thống quản lý các bản vá và tự động cập nhật định kỳ, như Microsoft Windows Updates, các tiện ích cập nhật tự động trên Linux/Unix, và tính năng tự động cập nhật của các ứng dụng, như Google Update Service. Căn cứ vào mức độ nghiêm trọng của các lỗ hổng bảo mật, tần suất cập nhật các bản vá cần được tuân thủ. Với các lỗ hổng nghiêm trọng, cần cập nhật tức thời các bản vá, còn với các lỗ hổng ít nghiêm trọng hơn, cần có kế hoạch cập nhật, hoặc khắc phục định kỳ.

Một biện pháp hiệu quả khác là sử dụng các phần mềm, hoặc công cụ rà quét các điểm yếu, lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng, để chủ động rà quét để tìm và khắc phục các điểm yếu và lỗ hổng bảo mật của hệ thống. Nhờ vậy có thể giảm thiểu nguy cơ bị lợi dụng, khai thác lỗ hổng bảo mật đã biết.

Một biện pháp bổ sung là cần có chính sách quản trị người dùng, mật khẩu và quyền truy nhập chặt chẽ ở mức hệ điều hành và mức ứng dụng, trong đó người dùng chỉ được cấp quyền truy nhập vừa đủ để thực hiện công việc được giao. Nếu người dùng được cấp nhiều quyền hơn mức cần thiết, họ có khuynh hướng lạm dụng quyền truy nhập để truy nhập vào các dữ liệu nhạy cảm, hoặc có thể bị tin tặc khai thác.

Việc sử dụng các biện pháp phòng vệ ở lớp ngoài như tường lửa, proxy cũng đem lại hiệu quả, do chúng giúp làm giảm bề mặt tiếp xúc với hệ thống, qua đó giảm thiểu khả năng bị tấn công. Tưởng lửa và proxy có thể chặn các dịch vụ, hoặc cổng không sử dụng, hoặc không thực sự cần thiết, đồng thời ghi logs các hoạt động truy nhập mạng, phục vụ cho việc phân tích, điều tra khi cần thiết.

Với các nhà phát triển phần mềm thì phát triển phần mềm an toàn là một trong các biện pháp cho phép giải quyết tận gốc vấn đề lỗ hổng bảo mật. Cần bổ sung việc đảm bảo an ninh, an toàn vào quy trình phát triển phần mềm. Ngoài ra, cần kiểm tra, kiểm thử tất cả các khâu, như thiết kế, cài đặt để tìm các điểm yếu, lỗ hổng bảo mật, và có biện pháp khắc phục phù hợp với các điểm yếu, lỗ hổng được phát hiện.

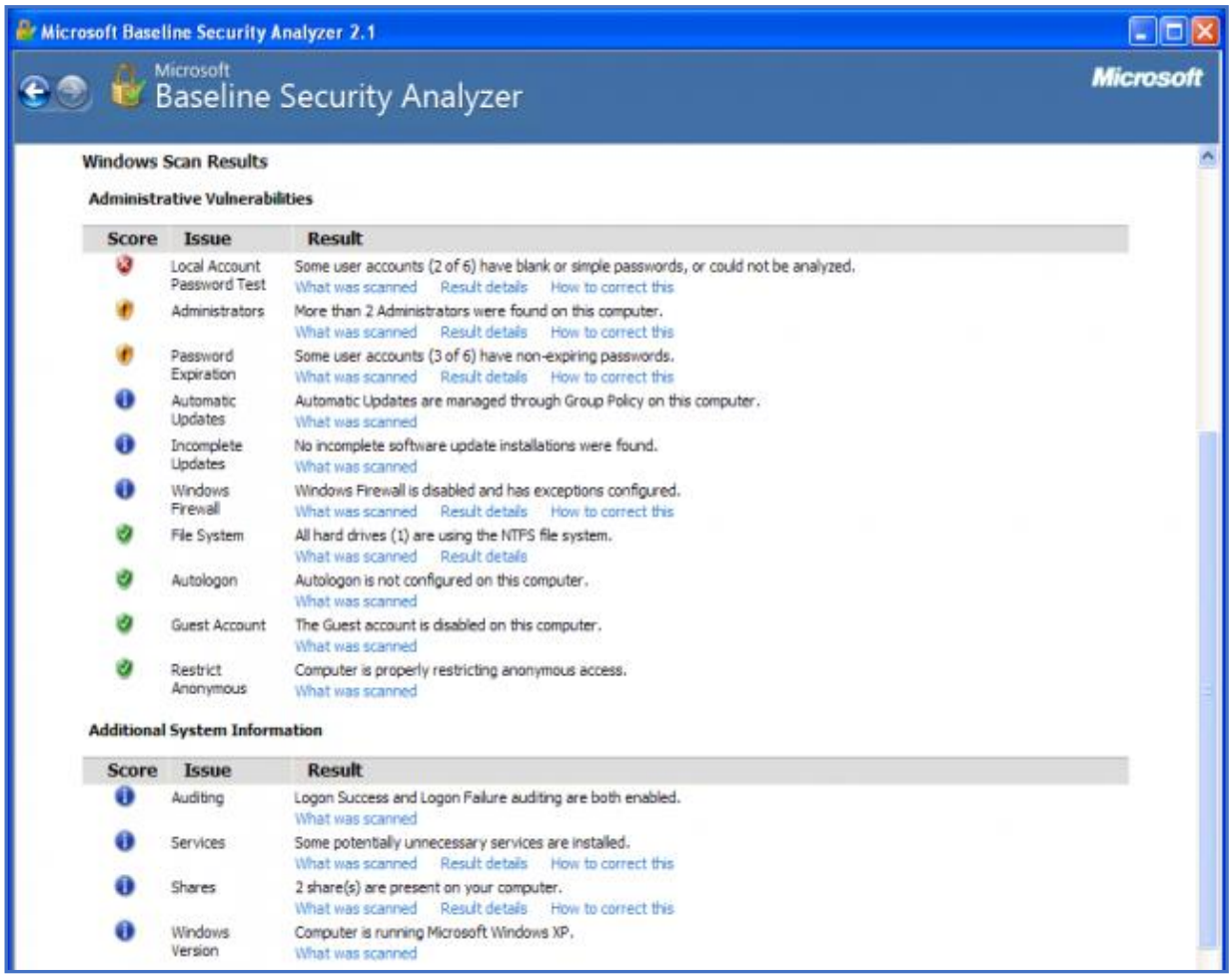
2.4. Một số công cụ rà quét điểm yếu và lỗ hổng bảo mật

Các công cụ rà quét các điểm yếu hệ thống và lỗ hổng bảo mật có thể được người quản trị sử dụng để chủ động rà quét các hệ thống, nhằm tìm ra các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống. Trên cơ sở kết quả rà quét, phân tích và đề xuất áp dụng các biện pháp khắc phục phù hợp. Các công cụ bao gồm, công cụ rà quét cổng dịch vụ, các công cụ rà quét lỗ hổng bảo mật hệ thống, và các công cụ rà quét lỗ hổng ứng dụng web, hay các trang web.

2.4.1. Công cụ rà quét lỗ hổng bảo mật hệ thống

Các công cụ rà quét lỗ hổng bảo mật hệ thống cho phép rà quét hệ thống, tìm các điểm yếu và các lỗ hổng bảo mật. Đồng thời, chúng cũng cung cấp phần phân tích chi tiết từng điểm yếu, lỗ hổng, kèm theo là hướng dẫn khắc phục, sửa chữa. Các công cụ được sử dụng rộng rãi là Microsoft Baseline Security Analyzer bookmark145cho rà quét các hệ

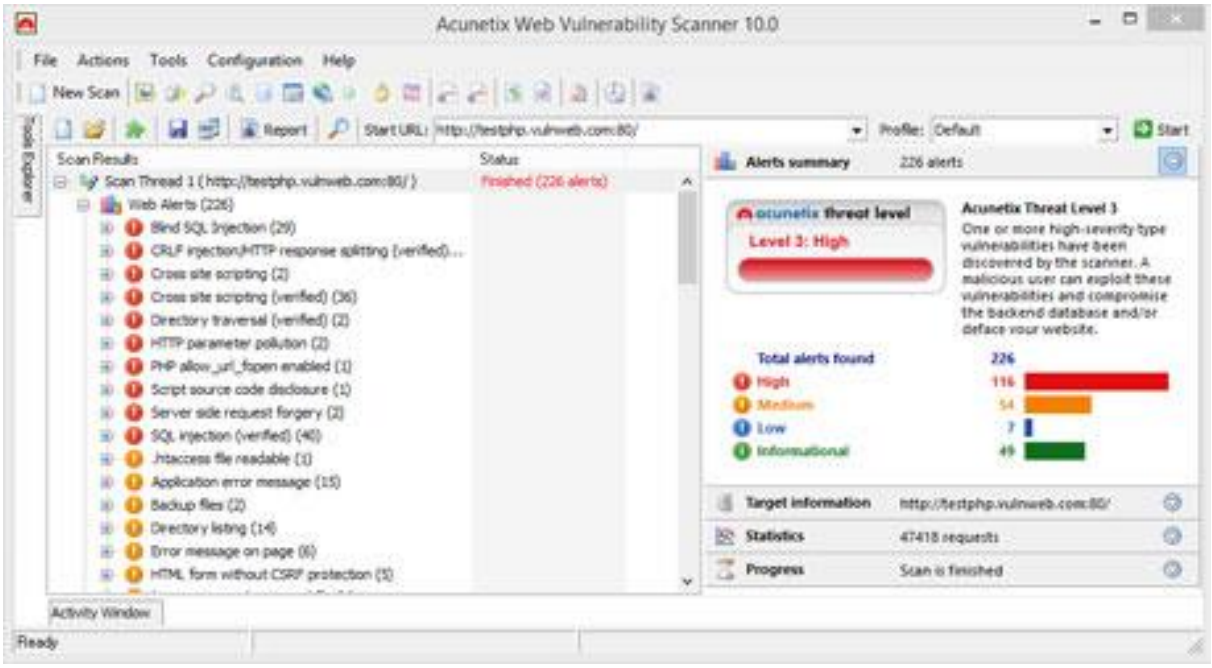
thống chạy hệ điều hành Microsoft Windows và Nessus Vulnerability Scanner cho rà quét các hệ thống chạy nhiều loại hệ điều hành khác nhau.



(Báo cáo kết quả quét của Microsoft Baseline Security Analyzer)

2.4.2. Công cụ rà quét lỗ hổng ứng dụng web

Các công cụ rà quét lỗ hổng ứng dụng web cho phép rà quét, phân tích các trang web, tìm các lỗi và lỗ hổng bảo mật. Chúng cũng hỗ trợ phân tích tình trạng các lỗi tìm được, như các lỗi XSS, lỗi chèn mã SQL, lỗi CSRF, lỗi bảo mật phiên,... Các công cụ được sử dụng phổ biến bao gồm Acunetix Web Vulnerability Scanner, IBM AppScan, Beyond Security AVDS và SQLmap.



(Kết quả quét website sử dụng Acunetix Web Vulnerability Scanner)

❖ TÓM TẮT CHƯƠNG 2

Trong chương này, một số nội dung chính được giới thiệu:

- **Lỗ Hổng Bảo Mật**: Chương bắt đầu bằng việc giới thiệu về lỗ hổng bảo mật, đó là những điểm yếu hoặc thiếu sót trong hệ thống thông tin có thể bị tấn công hoặc lợi dụng.
- **Các Loại Lỗ Hổng Bảo Mật**: Chương này trình bày các loại lỗ hổng bảo mật phổ biến, bao gồm lỗ hổng phần mềm, lỗ hổng mạng, và lỗ hổng xã hội. Một số ví dụ cụ thể về mỗi loại lỗ hổng cũng được đề cập.
- **Xác Định Điểm Yếu Hệ Thống**: Học sinh sẽ tìm hiểu cách xác định điểm yếu trong hệ thống thông tin, bao gồm việc đánh giá cấu trúc hệ thống, quá trình làm việc, và các phần mềm cụ thể.
- **Phương Pháp Tấn Công**: Các phương pháp này bao gồm tấn công từ xa, tấn công bên trong, và tấn công xã hội.
- **Bảo Vệ Hệ Thống**: Cung cấp kiến thức về cách bảo vệ hệ thống thông tin khỏi tấn công, bao gồm việc vá lỗ hổng, tăng cường bảo mật mạng, và thực hiện các biện pháp bảo mật hiệu quả.

❖ CÁC BÀI TẬP HỆ THỐNG KIẾN THỨC

1) Điểm yếu hệ thống là gì?
2) Liệt kê các nguyên nhân của sự tồn tại các điểm yếu trong hệ thống.
3) Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống?
4) Dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng là gì?
5) Lỗi tràn bộ đệm là lỗi trong khâu nào của quá trình phát triển phần mềm?
6) Các vùng bộ nhớ nào thường bị gây tràn trong tấn công khai thác lỗi tràn bộ đệm?

7) Dạng tấn công nào thường được tin tặc thực hiện trên các trang web nhắm đến các cơ sở dữ liệu?
8) Liệt kê các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm.
9) Liệt kê các biện pháp phòng chống tấn công chèn mã SQL.
10) Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần được thực hiện theo nguyên tắc chung nào?

CHƯƠNG 3. CÁC DẠNG TẤN CÔNG VÀ PHẦN MỀM ĐỘC HẠI

❖ GIỚI THIỆU CHƯƠNG 3

Chương 3 của môn học "An Toàn Hệ Thống Thông Tin" tập trung vào việc tìm hiểu về các dạng tấn công thông tin và các phần mềm độc hại mà người tấn công có thể sử dụng để xâm nhập vào hệ thống thông tin. Chương này giúp học viên hiểu cách nhận diện, đối phó và ngăn chặn các loại tấn công và phần mềm độc hại này.

❖ MỤC TIÊU CHƯƠNG 3

Sau khi học xong chương này, người học có khả năng:

➢ ***Về kiến thức:***

- *Hiểu Biết về các dạng tấn công thông tin, bao gồm tấn công từ xa, tấn công bên trong, tấn công xã hội, và tấn công theo kiểu tương tác với phần mềm độc hại.*
- *Phân biệt và định danh các loại phần mềm độc hại như virus, malware, trojan, ransomware, và spyware.*
- *Biết cách đánh giá nguy cơ và tiềm ẩn rủi ro mà các tấn công và phần mềm độc hại có thể mang lại cho hệ thống thông tin.*
- *Biết cách bảo vệ hệ thống thông tin khỏi các tấn công và phần mềm độc hại bằng cách thực hiện biện pháp bảo mật, cập nhật phần mềm, và sử dụng phần mềm chống virus và malware.*

➢ ***Về kỹ năng:***

- *Kỹ năng nhận diện các dạng tấn công thông tin và phần mềm độc hại, bao gồm việc phát hiện các dấu hiệu và hành vi bất thường.*
- *Kỹ năng đối phó với các tấn công thông tin, bao gồm việc ngăn chặn tấn công, khắc phục hậu quả, và bảo vệ hệ thống khỏi tấn công tiềm ẩn.*
- *Kỹ năng sử dụng phần mềm bảo mật để quét và loại bỏ phần mềm độc hại, và thực hiện các biện pháp bảo vệ chống lại các tấn công.*
- *Kỹ năng đánh giá rủi ro của các tấn công và phần mềm độc hại và xác định mức độ nguy cơ và ảnh hưởng.*

➢ ***Về năng lực tự chủ và trách nhiệm:***

- *Năng lực về quản lý thời gian, trách nhiệm với công việc*
- *Năng lực học tập và làm việc độc lập*
- *Tự chủ trong việc giải quyết vấn đề*

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 3

- *Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, dạy học theo vấn đề); yêu cầu người học thực hiện câu hỏi thảo luận và bài tập chương (cá nhân hoặc nhóm).*
- *Đối với người học: chủ động đọc trước giáo trình trước buổi học; hoàn thành đầy đủ câu hỏi thảo luận và bài tập tình huống theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.*

❖ **ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 3**

- ***Phòng học chuyên môn hóa/nhà xưởng:*** Phòng học thực hành
- ***Trang thiết bị máy móc:*** Máy chiếu, máy tính và các thiết bị dạy học khác
- ***Học liệu, dụng cụ, nguyên vật liệu:*** Chương trình môn học, giáo trình, tài liệu tham khảo, giáo án, phim ảnh, và các tài liệu liên quan.
- ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 3**

- **Nội dung:**

✓ *Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức*

✓ *Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.*

✓ *Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:*

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ ***Điểm kiểm tra thường xuyên:*** *1 điểm kiểm tra (hình thức: hỏi miệng)*

✓ ***Kiểm tra định kỳ lý thuyết:*** *không có*

❖ **NỘI DUNG CHƯƠNG 3**

3.1. Khái niệm về mối đe dọa và tấn công

3.1.1. Mối đe dọa

Mối đe dọa (Threat) là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống. Các tài nguyên hệ thống bao gồm phần cứng, phần mềm, cơ sở dữ liệu, các file, dữ liệu, hoặc hạ tầng mạng vật lý,... Mối đe dọa và lỗ hổng bảo mật có quan hệ hữu cơ với nhau: Các mối đe dọa thường khai thác một hoặc một số lỗ hổng bảo mật đã biết để thực hiện các cuộc tấn công phá hoại. Điều này có nghĩa là nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực. Nói chung, không

thể triệt tiêu được hết các mối đe dọa do đó là yếu tố khách quan, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị khai thác để thực hiện tấn công.
Trên thực tế, không phải tất cả các mối đe dọa đều là ác tính hay độc hại (malicious). Một số mối đe dọa là chủ động, cố ý, nhưng một số khác chỉ là ngẫu nhiên, hoặc vô tình. Các mối đe dọa thường gặp đối với thông tin, hệ thống và mạng:
- Phần mềm độc hại
- Kẻ tấn công ở bên trong
- Kẻ tấn công ở bên ngoài
- Hư hỏng phần cứng hoặc phần mềm
- Mất trộm các thiết bị
- Tai họa thiên nhiên
- Gián điệp công nghiệp
- Khủng bố phá hoại.

3.1.2. Tấn công

** Giới thiệu*

Tấn công (Attack) là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh an toàn của cơ quan, tổ chức, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và mạng. Một cuộc tấn công vào hệ thống máy tính hoặc các tài nguyên mạng thường được thực hiện bằng cách khai thác các lỗ hổng tồn tại trong hệ thống. Như vậy, tấn công chỉ có thể trở thành hiện thực nếu có sự tồn tại đồng thời của mối đe dọa và lỗ hổng, hay có thể nói: *Tấn công = Mối đe dọa + Lỗ hổng*

** Phân loại*

Có thể chia tấn công theo mục đích thực hiện thành 4 loại chính như sau:
- Giả mạo (Fabrications): Tấn công giả mạo thông tin thường được sử dụng để đánh lừa người dùng thông thường;
- Chặn bắt (Interceptions): Tấn công chặn bắt thường liên quan đến việc nghe lén trên đường truyền và chuyển hướng thông tin để sử dụng trái phép;
- Gây ngắt quãng (Interruptions): Tấn công gây ngắt quãng làm ngắt, hoặc chậm kênh truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy nhập dịch vụ của người dùng hợp pháp;
- Sửa đổi (Modifications): Tấn công sửa đổi liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.

Theo hình thức thực hiện, có thể chia các loại tấn công thành 2 kiểu chính như sau:
- Tấn công chủ động (Active attacks): Tấn công chủ động là một đột nhập, xâm nhập (intrusion) về mặt vật lý vào hệ thống, hoặc mạng. Các tấn công chủ động thực hiện sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong file, hoặc giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng.

- Tấn công thụ động (Passive attacks): Tấn công thụ động thường không gây ra thay đổi trên hệ thống. Các tấn công thụ động điển hình là nghe trộm và giám sát lưu lượng trên đường truyền.

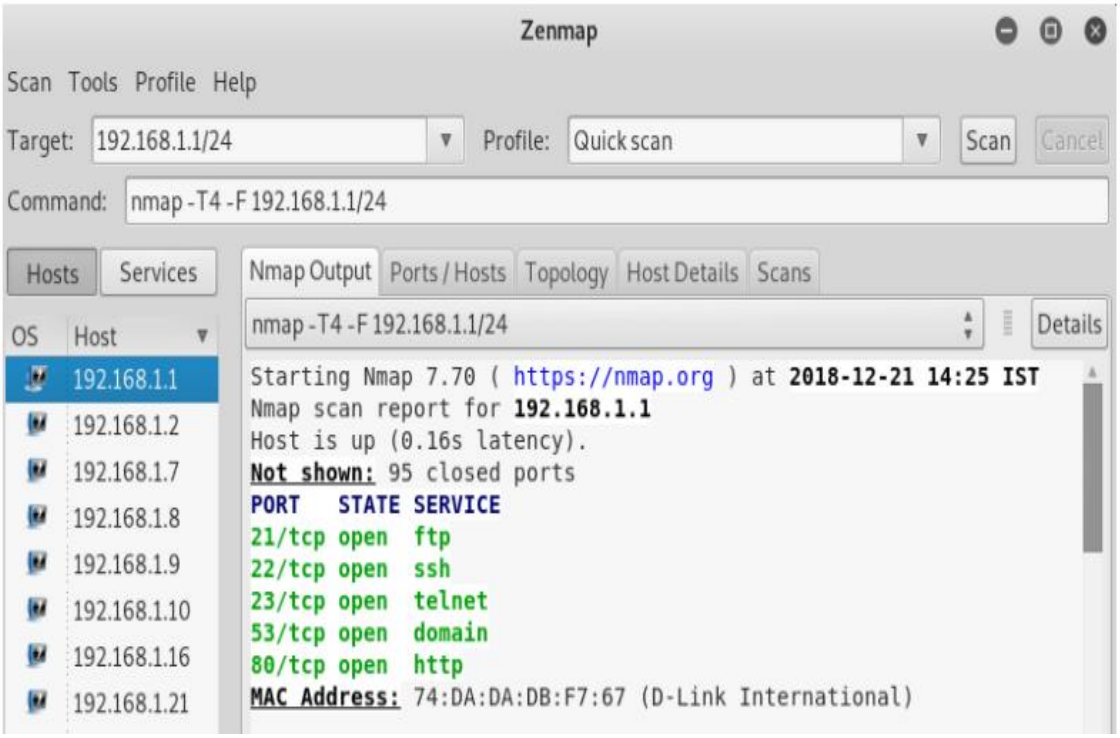
Trên thực tế, tấn công thụ động thường là giai đoạn đầu của tấn công chủ động, trong đó tin tặc sử dụng các kỹ thuật tấn công thụ động để thu thập các thông tin về hệ thống, mạng, và trên cơ sở thông tin có được sẽ lựa chọn kỹ thuật tấn công chủ động có xác suất thành công cao nhất.

3.2. Các công cụ hỗ trợ tấn công

Các công cụ hỗ trợ tấn công (Attacking assistant tools) là các công cụ phần cứng, phần mềm, hoặc các kỹ thuật hỗ trợ kẻ tấn công, tin tặc (attacker) thu thập các thông tin về các hệ thống máy tính, hoặc mạng. Trên cơ sở các thông tin thu được, tin tặc sẽ lựa chọn công cụ, kỹ thuật tấn công có xác suất thành công cao nhất. Các công cụ hỗ trợ tấn công bao gồm 4 nhóm chính: Công cụ quét điểm yếu, lỗ hổng bảo mật, công cụ quét cổng dịch vụ, công cụ nghe lén và công cụ ghi phím gõ. Các công cụ quét điểm yếu, lỗ hổng bảo mật đã được trình bày ở mục 2.4. Mục này giới thiệu 3 nhóm công cụ còn lại.

3.2.1. Công cụ quét cổng dịch vụ

Các công cụ quét cổng dịch vụ (Port scanners) cho phép quét các cổng, tìm các cổng đang mở, đang hoạt động, đồng thời tìm các thông tin về ứng dụng, dịch vụ và hệ điều hành đang hoạt động trên hệ thống.



(Giao diện của công cụ Zenmap)

Dựa trên thông tin quét cổng dịch vụ, có thể xác định được dịch vụ, ứng dụng nào đang chạy trên hệ thống:

- Cổng 80/443 mở có nghĩa là dịch vụ web đang hoạt động;

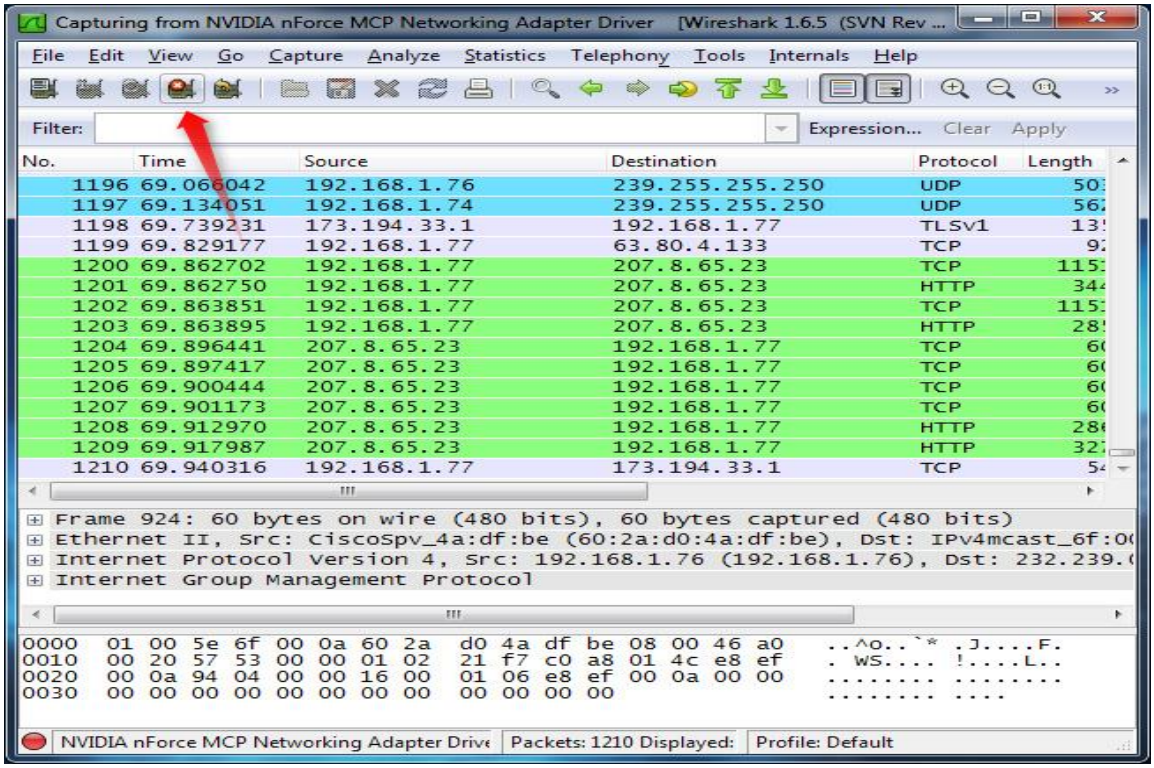
- Cổng 25 mở có nghĩa là dịch vụ gửi/nhận email SMTP đang hoạt động;
- Cổng 1433 mở có nghĩa là máy chủ Microsoft SQL Server đang hoạt động;
- Cổng 53 mở có nghĩa là dịch vụ tên miền DNS đang hoạt động,...

Các công cụ quét cổng dịch vụ được sử dụng phổ biến bao gồm: Nmap, Zenmap, Portsweep, Advanced Port Scanner, Angry IP Scanner, SuperScan và NetScanTools. Hình ảnh trên là giao diện của công cụ quét cổng dịch vụ Nmap/ Zenmap - một trong các công cụ quét cổng dịch vụ được sử dụng rộng rãi. Nmap cung cấp tập lệnh rà quét rất mạnh. Tuy nhiên, Nmap hơi khó dùng do chỉ hỗ trợ giao diện dòng lệnh.

3.2.2. Công cụ nghe lén

Công cụ nghe lén (Sniffers) cho phép bắt các gói tin khi chúng được truyền trên mạng. Công cụ nghe lén có thể là mô đun phần cứng, phần mềm hoặc kết hợp. Các thông tin nhạy cảm như thông tin tài khoản, thẻ tín dụng, hoặc mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe lén khi được truyền từ máy trạm đến máy chủ và bị lạm dụng. Một số công cụ phần mềm cho phép bắt gói tin truyền trên mạng:

- Tcpdump
- Wireshark
- Pcap / Wincap / Libcap (Packet capture)
- IP Tools (http://www.softpedia.com).



(Hình ảnh sử dụng Wireshark để bắt gói tin có chứa thông tin nhạy cảm)

3.2.3. Công cụ ghi phím gõ

Công cụ ghi phím gõ (Keyloggers) là một dạng công cụ giám sát bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào một file. File đã ghi

sau đó có thể được gửi cho kẻ tấn công theo địa chỉ chỉ định trước hoặc sao chép trực tiếp. Ngoài kẻ tấn công, người quản lý cũng có thể cài đặt Keylogger vào máy tính của nhân viên để theo dõi hoạt động của các nhân viên. Việc cài đặt Keylogger có thể được thực hiện tương đối đơn giản. Riêng với Keylogger phần mềm, kẻ tấn công có thể tích hợp Keylogger vào một phần mềm thông thường và lừa người dùng cài đặt vào máy tính của mình.

(Hình minh họa một Keylogger dưới dạng một khớp nối phần cứng kết nối cổng bàn phím với đầu nối bàn phím, hỗ trợ cả giao diện cổng bàn phím PS/2 và USB)

3.3. Các dạng tấn công thường gặp

Các dạng tấn công thường gặp là các dạng tấn công điển hình, xảy ra thường xuyên nhằm vào các hệ thống máy tính, hệ thống mạng và người dùng. Các dạng tấn công thường gặp bao gồm:

- Tấn công vào mật khẩu
- Tấn công bằng mã độc
- Tấn công từ chối dịch vụ
- Tấn công giả mạo địa chỉ
- Tấn công nghe lén
- Tấn công kiểu người đứng giữa
- Tấn công bằng bom thư và thư rác
- Tấn công sử dụng các kỹ thuật xã hội
- Tấn công pharming.

Phần dưới đây trình bày chi tiết về các dạng tấn công thường gặp kể trên và các biện pháp phòng chống.

3.3.1. Tấn công vào mật khẩu

** Giới thiệu*

Tấn công vào mật khẩu (Password attack) là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản của người dùng để lạm dụng. Tên người dùng và mật khẩu không

được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách đến máy chủ, hoặc các thông tin này có thể bị đánh cắp thông qua các dạng tấn công XSS, hoặc lừa đảo, bẫy người dùng cung cấp thông tin. Đây là một trong các dạng tấn công phổ biến nhất do hầu hết các ứng dụng sử cơ chế xác thực người dùng dựa trên tên người dùng, hoặc email và mật khẩu. Nếu kẻ tấn công có tên người dùng và mật khẩu thì hắn có thể đăng nhập vào tài khoản và thực hiện các thao tác như người dùng bình thường.

* *Mô tả*

Có thể chia tấn công vào mật khẩu thành 2 dạng:

- Tấn công dựa trên từ điển (Dictionary attacks): Dạng tấn công này khai thác vấn đề người dùng có xu hướng chọn mật khẩu là các từ đơn giản cho dễ nhớ. Kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển, nhờ vậy tăng khả năng thành công.
- Tấn công vét cạn (Brute force attacks): Dạng vét cạn sử dụng tổ hợp các ký tự và thử tự động. Phương pháp này thường được sử dụng với các mật khẩu đã được mã hóa. Kẻ tấn công sinh tổ hợp ký tự, sau đó mã hóa với cùng thuật toán mà hệ thống sử dụng, tiếp theo so sánh chuỗi mã hóa từ tổ hợp ký tự với chuỗi mật khẩu mã hóa thu thập được. Nếu hai bản mã trùng nhau thì tổ hợp ký tự là mật khẩu.

* *Phòng chống*

Để đảm bảo an toàn cho mật khẩu, cần thực hiện kết hợp các biện pháp sau:

- Chọn mật khẩu đủ mạnh: Mật khẩu mạnh cho người dùng thông thường cần có độ dài lớn hơn hoặc bằng 8 ký tự, gồm tổ hợp của 4 loại ký tự: chữ cái hoa, chữ cái thường, chữ số và ký tự đặc biệt (?#$...). Mật khẩu cho người quản trị hệ thống cần có độ dài lớn hơn hoặc bằng 10 ký tự cũng với các loại ký tự như mật khẩu cho người dùng thông thường.
- Định kỳ thay đổi mật khẩu. Thời hạn đổi mật khẩu tùy thuộc vào chính sách an ninh của cơ quan, tổ chức, có thể là 3 tháng, hoặc 6 tháng.
- Mật khẩu không nên lưu ở dạng rõ (plaintext). Nên lưu mật khẩu ở dạng đã mã hóa (thường dùng hàm băm).
- Hạn chế trao đổi tên người dùng và mật khẩu trên kênh truyền không được mã hóa.

3.3.2. Tấn công bằng mã độc

* *Giới thiệu*

Tấn công bằng mã độc (Malicious code attacks) là dạng tấn công sử dụng các mã độc (Malicious code) làm công cụ để tấn công hệ thống nạn nhân. Tấn công bằng mã độc có thể chia thành 2 loại:

- Khai thác các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân. Loại tấn công này lại gồm 2 dạng:

+ Tấn công khai thác lỗi tràn bộ đệm (Buffer Overflow)
+ Tấn công khai thác lỗi không kiểm tra đầu vào, gồm tấn công chèn mã SQL (SQL Injection) và tấn công sử dụng mã script, kiểu XSS, CSRF.
- Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại, như:
+ Các phần mềm quảng cáo (Adware), gián điệp (Spyware)
+ Virus
+ Zombie/Bot
+ Trojan
Tấn công khai thác lỗi tràn bộ đệm đã được đề cập ở Mục 2.2.1. Dạng tấn công lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại sẽ được đề cập ở Mục 3.4.
* *Tấn công chèn mã SQL*
Tấn công chèn mã SQL (SQL Injection) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và cuối cùng được thực hiện trên máy chủ cơ sở dữ liệu. Tùy vào mức độ tinh vi, tấn công chèn mã SQL có thể cho phép kẻ tấn công (1) vượt qua các khâu xác thực người dùng, (2) chèn, xóa hoặc sửa đổi dữ liệu, (3) đánh cắp các thông tin trong cơ sở dữ liệu và (4) chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu. Tấn công chèn mã SQL là dạng tấn công thường gặp ở các ứng dụng web, các trang web có kết nối đến cơ sở dữ liệu.
Có 2 nguyên nhân chính của lỗ hổng trong ứng dụng cho phép thực hiện tấn công chèn mã SQL là:
- Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng;
- Sử dụng các câu lệnh SQL động trong ứng dụng, trong đó có thao tác nối dữ liệu người dùng với mã lệnh SQL gốc.
* *Phòng chống*
Do tính chất nguy hiểm của tấn công chèn mã SQL, nhiều giải pháp đã được đề xuất nhằm hạn chế tác hại và ngăn chặn triệt để dạng tấn công này. Nhìn chung, cần áp dụng kết hợp các biện pháp phòng chống tấn công chèn mã SQL để đảm bảo an toàn cho hệ thống. Các biện pháp, kỹ thuật cụ thể có thể áp dụng gồm:
- Các biện pháp phòng chống dựa trên kiểm tra và lọc dữ liệu đầu vào:
+ Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy;
+ Kiểm tra kích thước và định dạng dữ liệu đầu vào;
+ Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt (như *, „„ =, --) và các từ khóa của ngôn ngữ SQL (SELECT, INSERT, UPDATE, DELETE, DROP,…) mà kẻ tấn công có thể sử dụng.

- Sử dụng thủ tục cơ sở dữ liệu (stored procedures) và cơ chế tham số hóa dữ liệu:
+ Đưa tất cả các câu truy vấn (SELECT) và cập nhật, sửa, xóa dữ liệu (INSERT, UPDATE, DELETE) vào các thủ tục. Dữ liệu truyền vào thủ tục thông qua các tham số, giúp tách dữ liệu khỏi mã lệnh SQL, nhờ đó hạn ngăn chặn hiệu quả tấn công chèn mã SQL;
+ Hạn chế thực hiện các câu lệnh SQL động trong thủ tục;
+ Sử dụng cơ chế tham số hóa dữ liệu hỗ trợ bởi nhiều ngôn ngữ lập trình web như ASP.NET, PHP và JSP.
- Các biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng cơ sở dữ liệu:
+ Không sử dụng người dùng có quyền quản trị hệ thống hoặc quản trị cơ sở dữ liệu làm người dùng truy cập dữ liệu. Ví dụ: không dùng người dùng sa (Microsoft SQL) hoặc root (MySQL) làm người dùng truy cập dữ liệu. Chỉ dùng các người dùng này cho mục đích quản trị.
+ Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục.
+ Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp trên các bảng dữ liệu. Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục.
+ Cấm hoặc vô hiệu hóa (disable) việc thực hiện các thủ tục hệ thống (các thủ tục cơ sở dữ liệu có sẵn) cho phép can thiệp vào hệ quản trị cơ sở dữ liệu và hệ điều hành nền.
- Sử dụng các công cụ rà quét lỗ hổng chèn mã SQL, như SQLMap, hoặc Acunetix Vulnerability Scanner để chủ động rà quét, tìm các lỗ hổng chèn mã SQL và có biện pháp khắc phục phù hợp.

3.3.3. Tấn công từ chối dịch vụ

* *Giới thiệu*

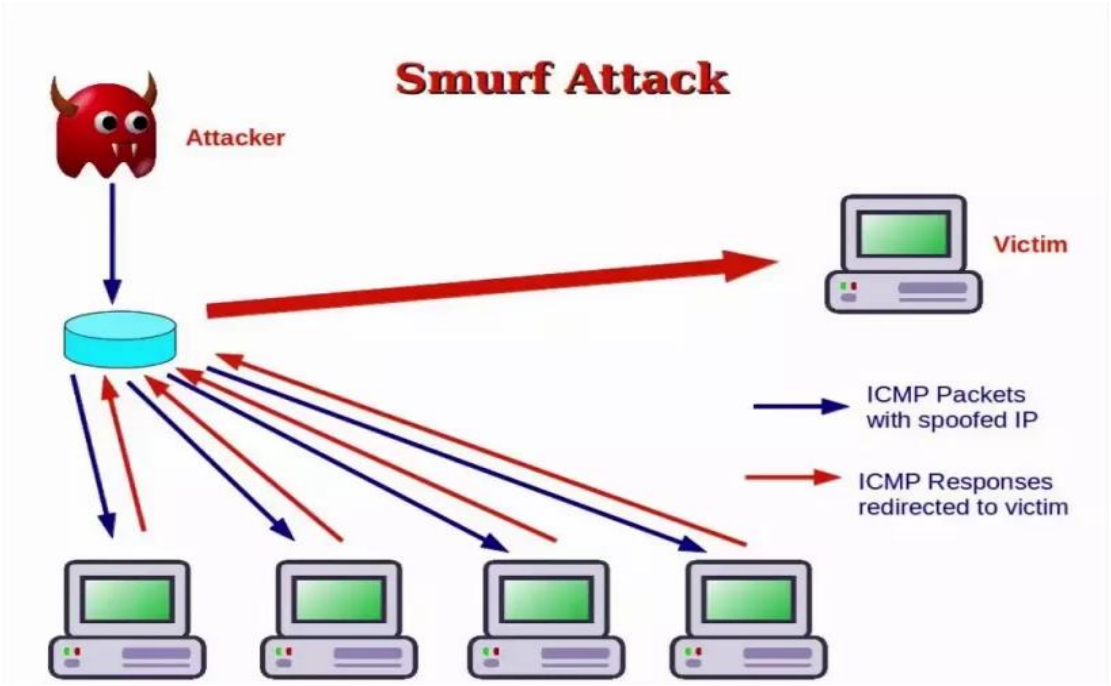
Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy nhập các tài nguyên mạng. Tấn công DoS có thể được chia thành 2 loại: (1) tấn công logic (Logic attacks) và (2) tấn công gây ngập lụt (Flooding attacks). Tấn công logic là dạng tấn công khai thác các lỗi phần mềm làm dịch vụ ngừng hoạt động, hoặc làm giảm hiệu năng hệ thống. Tấn công DoS sử dụng sâu Slammer đề cập ở Mục 2.2.1 là dạng tấn công khai thác lỗi tràn bộ đệm trong phần mềm. Ngược lại, trong tấn công gây ngập lụt, kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

Có nhiều kỹ thuật tấn công DoS đã được phát hiện trên thực tế. Các kỹ thuật tấn công DoS thường gặp bao gồm: SYN Flood, Smurf, Teardrop, Ping of Death, Land Attacks, ICMP Flood, HTTP Flood, UDP Flood,... Trong phạm vi của môn học này, chúng ta

chỉ đề cập đến 2 kỹ thuật phổ biến nhất là SYN Flood và Smurf.

** Tấn công Smurf*

Tấn công Smurf là dạng tấn công DoS sử dụng giao thức điều khiển truyền ICMP và kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân. Trên mỗi phân vùng mạng IP thường có 1 địa chỉ quảng bá, theo đó khi có một gói tin gửi tới địa chỉ này, nó sẽ được router của mạng chuyển đến tất cả các máy trong mạng đó.



(Mô hình tấn công Smurf)

- Kịch bản tấn công Smurf gồm các bước:

+ Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một địa chỉ quảng bá (IP Broadcast address) của một mạng;

+ Router của mạng nhận được yêu cầu ICMP gửi đến địa chỉ quảng bá sẽ tự động chuyển yêu cầu này đến tất cả các máy trong mạng;

+ Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời (reply) đến máy có địa chỉ IP là địa nguồn trong yêu cầu ICMP (là máy nạn nhân). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền, hoặc ngừng hoạt động.

- Phòng chống tấn công Smurf có thể sử dụng các biện pháp sau:

+ Cấu hình các máy trong mạng và router không trả lời các yêu cầu ICMP, hoặc các yêu cầu phát quảng bá;

+ Cấu hình các router không chuyển tiếp yêu cầu ICMP gửi đến các địa chỉ quảng bá;

+ Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.

Việc cấu hình các router không chuyển tiếp yêu cầu ICMP, hoặc các máy trong mạng không trả lời các yêu cầu ICMP có thể gây khó khăn cho các ứng dụng dựa trên phát

quảng bá và giao thức ICMP, như ứng dụng giám sát trạng thái hoạt động của các máy trong mạng dựa trên ICMP/Ping.

3.3.4. Tấn công từ chối dịch vụ phân tán

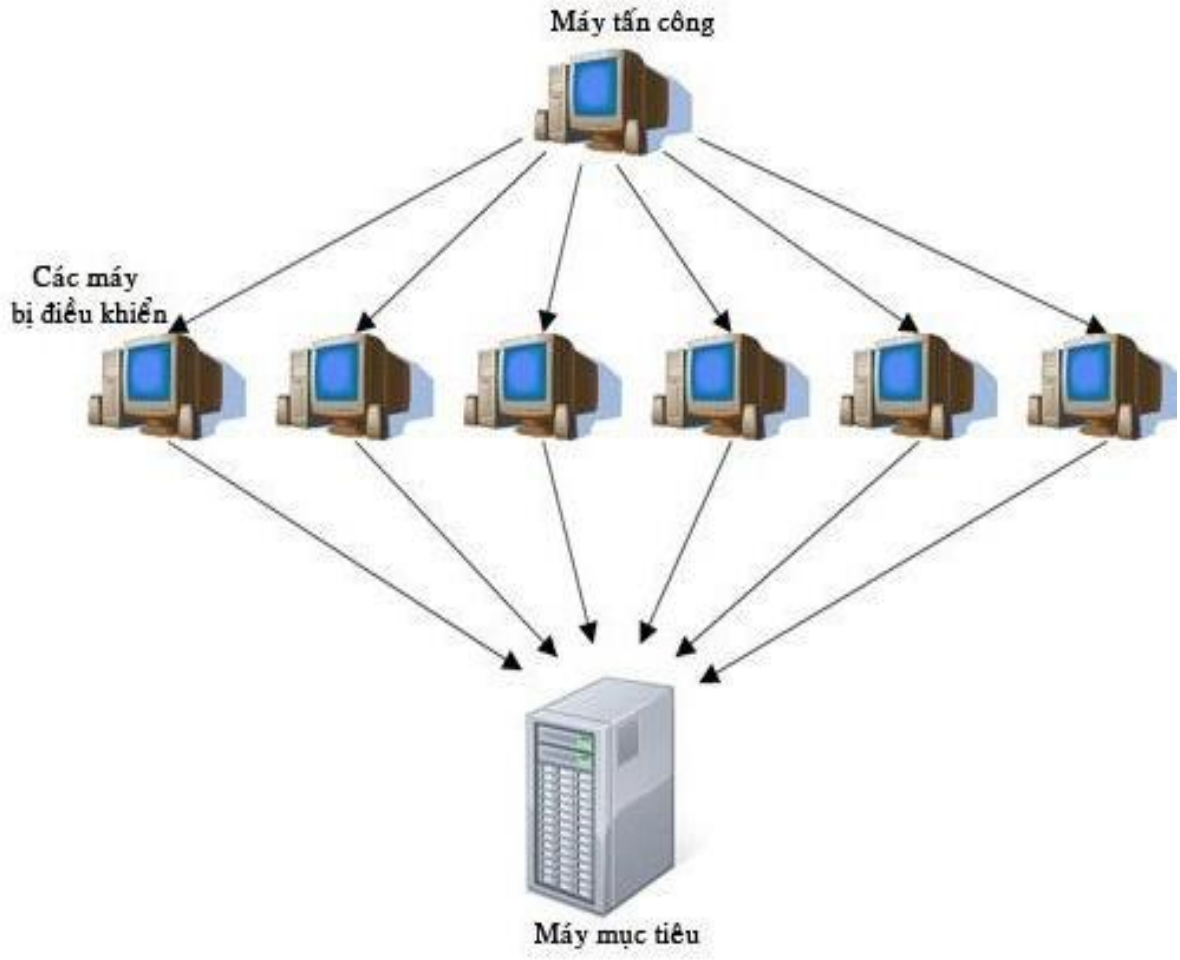
* *Giới thiệu*

Tấn công DDoS (Distributed Denial of Service) là một loại tấn công DoS đặc biệt, liên quan đến việc gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo. Điểm khác biệt chính giữa DDoS và DoS là phạm vi (scope) tấn công: trong khi số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm, thì số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc hàng trăm ngàn máy, và các máy tham gia tấn công DDoS có thể đến từ rất nhiều vị trí địa lý khác nhau trên toàn cầu. Do vậy, việc phòng chống tấn công DDoS gặp nhiều khó khăn hơn so với việc phòng chống tấn công DoS. Có thể chia tấn công DDoS thành 2 dạng chính theo mô hình kiến trúc: tấn công DDoS trực tiếp (Direct DDoS) và tấn công DDoS gián tiếp, hay phản xạ (Indirect/Reflective DDoS). Trong tấn công DDoS trực tiếp, các yêu cầu tấn công được các máy tấn công gửi trực tiếp đến máy nạn nhân. Ngược lại, trong tấn công DDoS gián tiếp, các yêu cầu tấn công được gửi đến các máy phản xạ (Reflectors) và sau đó gián tiếp chuyển đến máy nạn nhân.

* *Tấn công DDoS trực tiếp*

Tấn công DDoS trực tiếp được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- Kẻ tấn công (Attacker) chiếm quyền điều khiển hàng ngàn, thậm chí hàng chục ngàn máy tính trên mạng Internet, sau đó bí mật cài các chương trình tấn công tự động (Automated agents) lên các máy này. Các automated agents còn được gọi là các Bots hoặc Zombies (Máy tính ma)
- Các máy bị chiếm quyền điều khiển hình thành mạng máy tính ma, gọi là botnet hay zombie network. Các botnet, hay zombie network không bị giới hạn bởi chủng loại thiết bị và tô pô mạng vật lý;
- Kẻ tấn công có thể giao tiếp với các máy botnet, zombie thông qua một mạng lưới các máy trung gian (handler) gồm nhiều tầng. Phương thức giao tiếp có thể là IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP,...



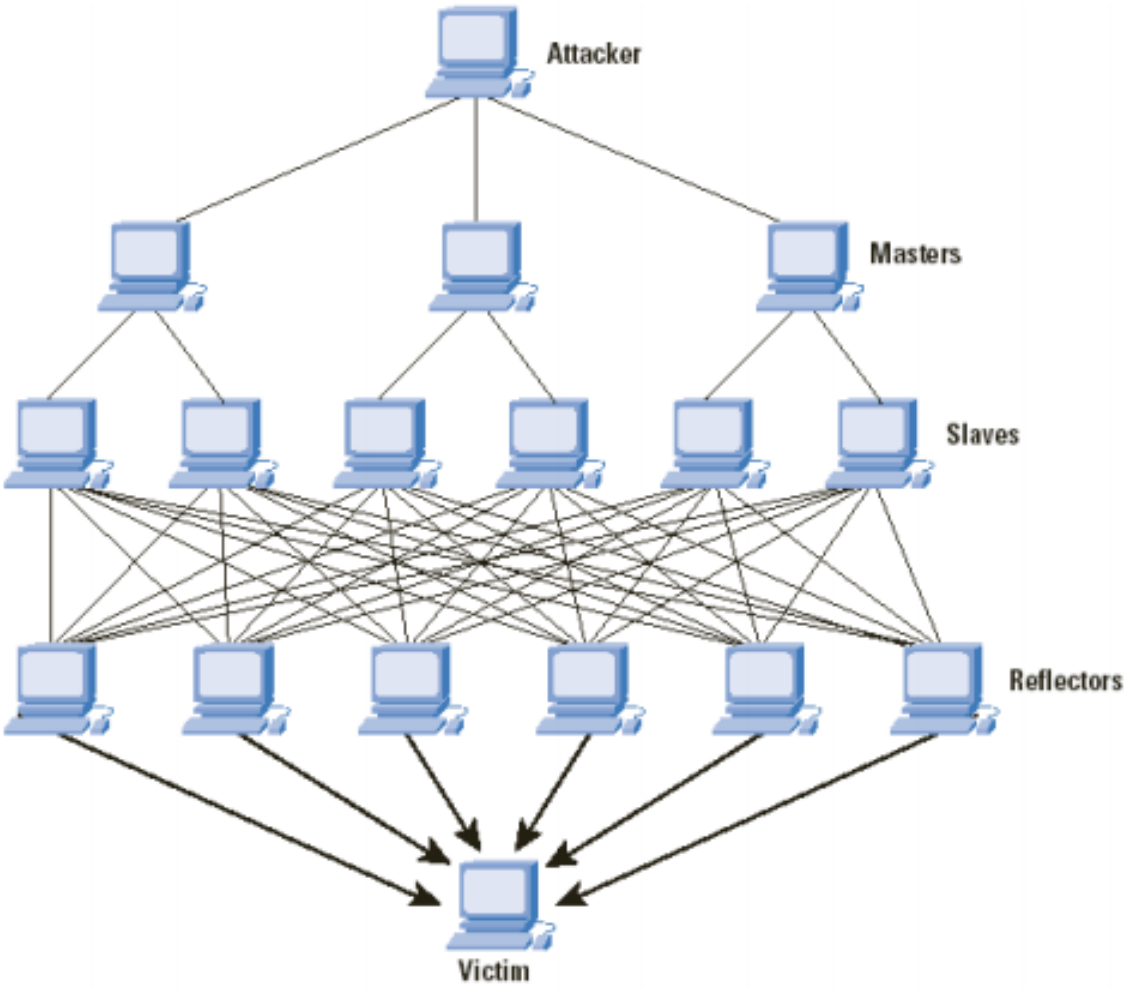
(Kiến trúc tấn công DDoS trực tiếp)

- Tiếp theo, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân tạo thành cuộc tấn công DDoS;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn, vị trí địa lý khác nhau nên rất khó đối phó và lần vết để tìm ra kẻ tấn công thực sự.

* *Tấn công DDoS gián tiếp*

Tấn công DDoS gián tiếp cũng được thực hiện theo nhiều giai đoạn theo kịch bản sau:

- Kẻ tấn công chiếm quyền điều khiển của một lượng lớn máy tính trên mạng Internet, cài đặt phần mềm tấn công tự động bot/zombie (còn gọi là slave), hình thành nên mạng botnet;
- Theo lệnh của kẻ tấn công điều khiển các Slaves/Zombies gửi một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác (Reflectors) trên mạng Internet;
- Các Reflectors gửi các phản hồi (Reply) đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;



(Kiến trúc tấn công DDoS gián tiếp hay phản xạ)

- Khi các Reflectors có số lượng lớn, số phản hồi sẽ rất lớn và gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng. Các Reflectors bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất lớn trên mạng Internet và không chịu sự điều khiển của tin tặc.

* *Phòng chống tấn công DDoS*

Nhìn chung, để phòng chống tấn công DDoS hiệu quả, cần kết hợp nhiều biện pháp và sự phối hợp của nhiều bên do tấn công DDoS có tính phân tán cao và hệ thống mạng máy tính ma (botnet) được hình thành và điều khiển theo nhiều tầng, lớp. Một số biện pháp có thể xem xét áp dụng:

- Sử dụng các phần mềm rà quét virus và các phần mềm độc hại khác nhằm loại bỏ các loại bots, zombies, slaves khỏi các hệ thống máy tính;
- Sử dụng các hệ thống lọc đặt trên các router, tường lửa của các nhà cung cấp dịch vụ Internet (ISP) để lọc các yêu cầu điều khiển (C&C - Command and Control) gửi từ kẻ tấn công đến các bots;
- Sử dụng các hệ thống giám sát, phát hiện bất thường, nhằm phát hiện sớm các dấu hiệu của tấn công DDoS.

- Sử dụng tường lửa để chặn (block) tạm thời các cổng dịch vụ bị tấn công.

3.3.5. Tấn công giả mạo địa chỉ

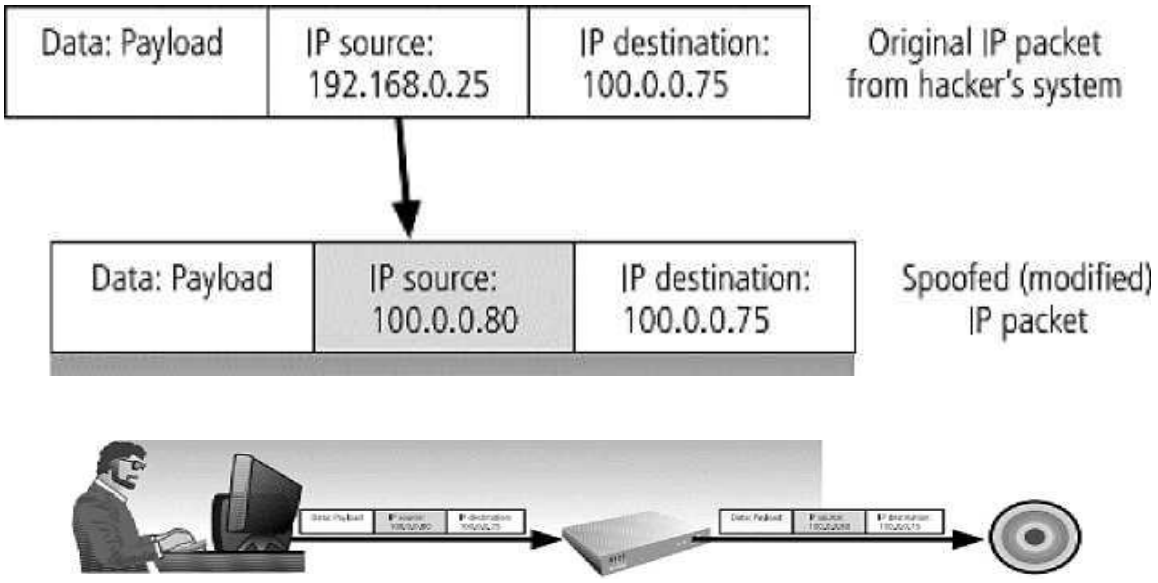
* *Giới thiệu*

Dạng tấn công giả mạo địa chỉ thường gặp nhất là tấn công giả mạo địa chỉ IP, trong đó kẻ tấn công sử dụng địa chỉ IP giả làm địa chỉ nguồn (Source IP) của các gói tin IP, thường để đánh lừa máy nạn nhân nhằm vượt qua các hàng rào kiểm soát an ninh thông thường. Chẳng hạn, nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội xâm nhập vào các máy khác trong mạng LAN đó do chính sách kiểm soát an ninh với các máy trong cùng mạng LAN thường được giảm nhẹ.

* *Kịch bản*

Cuộc tấn công giả mạo địa chỉ IP vào một máy nạn nhân trong mạng cục bộ có thể theo các bước thực hiện như sau:

- Giả sử máy của kẻ tấn công có địa chỉ IP là 192.168.0.25 và hắn muốn gửi gói tin tấn công đến máy nạn nhân có địa chỉ IP là 100.0.0.75;
- Kẻ tấn công tạo và gửi yêu cầu giả mạo với địa chỉ IP nguồn của các gói tin IP của yêu cầu là 100.0.0.80 đến máy nạn nhân. Địa chỉ 100.0.0.80 là địa chỉ cùng mạng LAN với máy nạn nhân 100.0.0.75;
- Nếu tường lửa của mạng LAN không lọc được các gói tin với địa chỉ nguồn giả mạo, yêu cầu giả mạo của kẻ tấn công có thể đến được và gây tác hại cho máy nạn nhân.

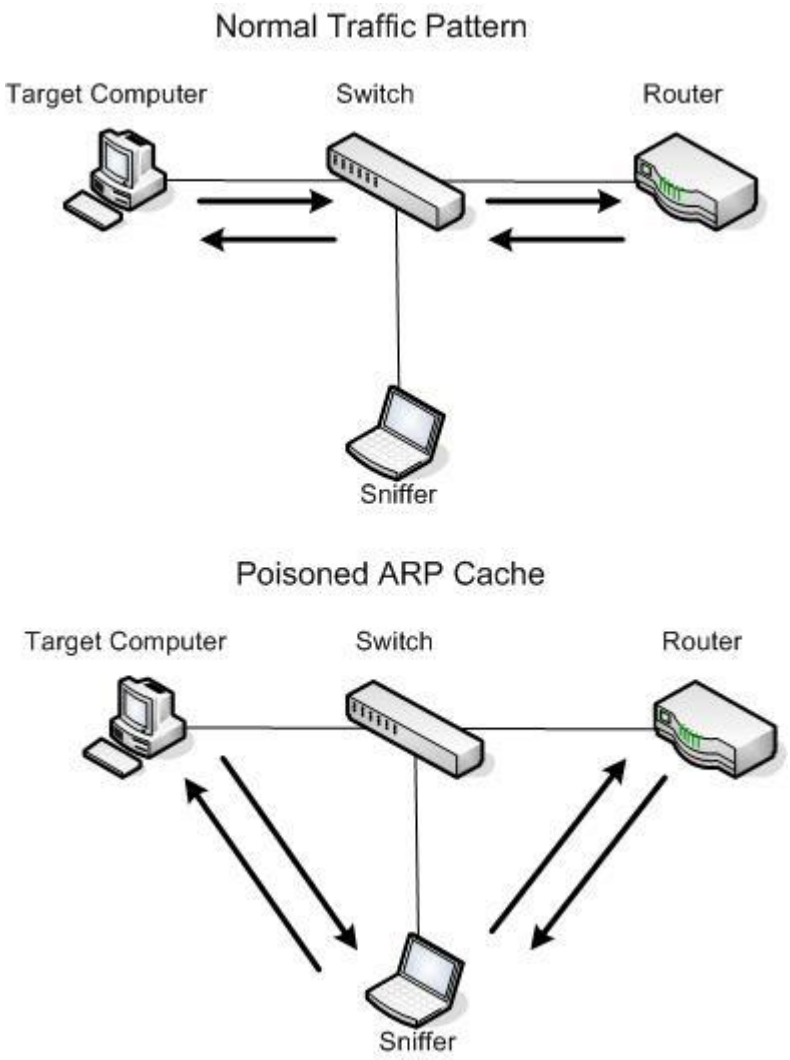


(Minh họa tấn công giả mạo địa chỉ IP)

* *Phòng chống*

Biện pháp phòng chống tấn công giả mạo địa chỉ IP hiệu quả nhất là sử dụng kỹ thuật lọc trên tường lửa, hoặc các router với nguyên tắc lọc: các gói tin từ mạng ngoài đi vào mạng LAN mà có địa chỉ nguồn là địa chỉ nội bộ của mạng LAN đó thì chúng là các gói tin giả mạo và phải bị chặn.

3.3.6. Tấn công nghe lén



(Tấn công nghe lén)

Tấn công nghe lén (Sniffing/Eavesdropping), như minh họa trên là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub, switch, router, hoặc môi trường truyền dẫn để bắt các gói tin dùng cho phân tích, hoặc lạm dụng về sau. Đây là kiểu tấn công thụ động nhằm thu thập các thông tin nhạy cảm, hoặc giám sát lưu lượng mạng. Các thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin thanh toán nếu không được mã hóa có thể bị nghe lén và lạm dụng. Các thông tin truyền trong mạng WIFI, hoặc các mạng không dây cũng có thể bị nghe lén dễ dàng do môi trường truyền dẫn vô tuyến và nếu không sử dụng các cơ chế bảo mật đủ mạnh.

Để phòng chống tấn công nghe lén, có thể áp dụng các biện pháp sau:

- Có cơ chế bảo vệ các thiết bị mạng và hệ thống truyền dẫn ở mức vật lý;
- Sử dụng các biện pháp, cơ chế xác thực người dùng đủ mạnh;
- Sử dụng các biện pháp bảo mật thông tin truyền dựa trên các kỹ thuật mã hóa.

3.3.7. Tấn công bằng bom thư và thư rác

Tấn công bằng bom thư (Mail bombing) là một dạng tấn công DoS khi kẻ tấn công gửi một lượng rất lớn email đến hộp thư của nạn nhân. Khi đó hộp thư và cả máy chủ nạn

nhân có thể bị tê liệt và không thể hoạt động bình thường. Tấn công bằng bom thư có thể được thực hiện bằng một số thủ thuật:

- Gửi bom thư bằng cách sử dụng kỹ thuật xã hội, đánh lừa người dùng phát tán email;
- Khai thác lỗi trong hệ thống gửi nhận email SMTP;
- Lợi dụng các máy chủ email không được cấu hình tốt để gửi email cho chúng.

Tấn công bằng thư rác (Spamming emails) là dạng tấn công gửi các thư không mong muốn, như thư quảng cáo, thư chứa các phần mềm độc hại. Theo một số thống kê, khoảng 70 - 80% lượng emails gửi trên mạng Internet là thư rác. Kẻ tấn công thường sử dụng các máy tính bị điều khiển (bots/zombies) để gửi email cho chúng. Spam emails gây lãng phí tài nguyên tính toán và thời gian của người dùng.

3.3.8. Tấn công sử dụng các kỹ thuật xã hội

* *Giới thiệu*

Tấn công sử dụng các kỹ thuật xã hội (Social Engineering) là dạng tấn công phi kỹ thuật nhằm vào người dùng. Dạng tấn công này khai thác các điểm yếu cố hữu của người dùng, như tính cả tin, ngây thơ, tò mò và lòng tham. Dạng thường gặp của kiểu tấn công này là thuyết phục người dùng tiết lộ thông tin truy nhập hoặc các thông tin có giá trị cho kẻ tấn công. Một số kỹ thuật mà kẻ tấn công thường áp dụng gồm:

- Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng, từ đó thuyết phục hoặc đánh lừa nạn nhân cung cấp thông tin;
- Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân/tổ chức;
- Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,...

* *Trò lừa đảo Nigeria 4-1-9*

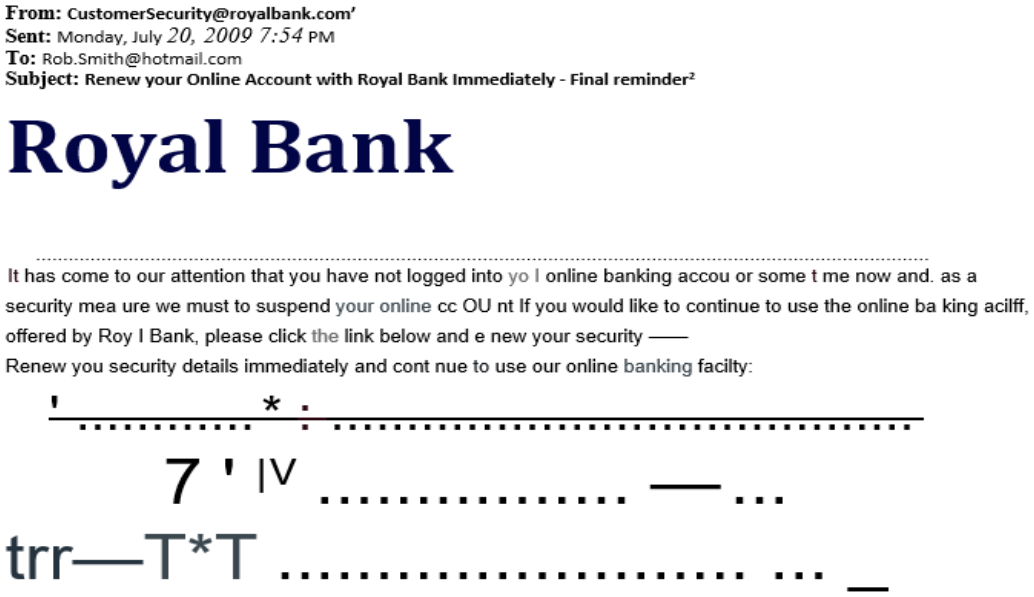
Trò lừa đảo Nigeria 4-1-9 là một trong các dạng tấn công sử dụng các kỹ thuật xã hội nổi tiếng nhất, trong đó đã có hàng chục nghìn người ở Mỹ, Canada và Châu Âu đã sập bẫy của kẻ lừa đảo. Kẻ lừa đảo lợi dụng sự ngây thơ và lòng tham của một số người với kịch bản tóm tắt như sau:

- Kẻ lừa đảo gửi thư tay, hoặc email đến nhiều người nhận, mô tả về việc có 1 khoản tiền lớn (từ thừa kế, hoặc lợi tức,..) cần chuyển ra nước ngoài, nhờ người nhận giúp đỡ để hoàn thành giao dịch. Khoản tiền có thể lên đến hàng chục, hoặc trăm triệu USD. Kẻ lừa đảo hứa sẽ trả cho người tham gia một phần số tiền (lên đến 20-30%);
- Nếu người nhận có phản hồi và đồng ý tham gia, kẻ lừa đảo sẽ gửi tiếp thư, hoặc email khác, yêu cầu chuyển cho hắn 1 khoản phí giao dịch (từ vài ngàn đến hàng chục ngàn USD);
- Nếu người nhận gửi tiền phí giao dịch theo yêu cầu thì người đó sẽ mất tiền, do giao dịch mà kẻ lừa đảo hứa hẹn là giả mạo.

Nhiều biến thể của trò lừa đảo Nigeria 4-1-9 đã xuất hiện trong những năm gần đây trên thế giới cũng như ở Việt Nam, chẳng hạn như thông báo lừa trúng thưởng các tài sản có giá trị lớn để chiếm đoạt khoản "phí trả thưởng", lừa đầu tư vào tài khoản ảo với hứa hẹn lại suất cao,…

** Phishing*

Phishing là một dạng đặc biệt phát triển rất mạnh của tấn công sử dụng các kỹ thuật xã hội, trong đó kẻ tấn công bẫy người dùng để lấy thông tin cá nhân, thông tin tài khoản, thẻ tín dụng,... Kẻ tấn công có thể giả mạo trang web của các tổ chức tài chính, ngân hàng, sau đó chúng gửi email cho người dùng (địa chỉ email thu thập trên mạng), yêu cầu xác thực thông tin. Hình minh họa phishing emails gửi cho khách hàng của mạng ngân hàng Royal Bank yêu cầu người dùng cập nhật thông tin thanh toán đã hết hạn, hoặc xác nhận thông tin tài khoản không sử dụng. Nếu người dùng làm theo hướng dẫn thì sẽ vô tình cung cấp các thông tin cá nhân, thông tin tài khoản, thẻ tín dụng cho kẻ tấn công.


From: CustomerSecurity@royalbank.com'
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately - Final reminder²

Royal Bank

It has come to our attention that you have not logged into yo l online banking accou or some t me now and. as a security mea ure we must to suspend your online cc OU nt If you would like to continue to use the online ba king acilff, offered by Roy l Bank, please click the link below and e new your security ——
Renew you security details immediately and cont nue to use our online banking facilty:

(Một phishing email gửi cho khách hàng của ngân hàng Royal Bank)

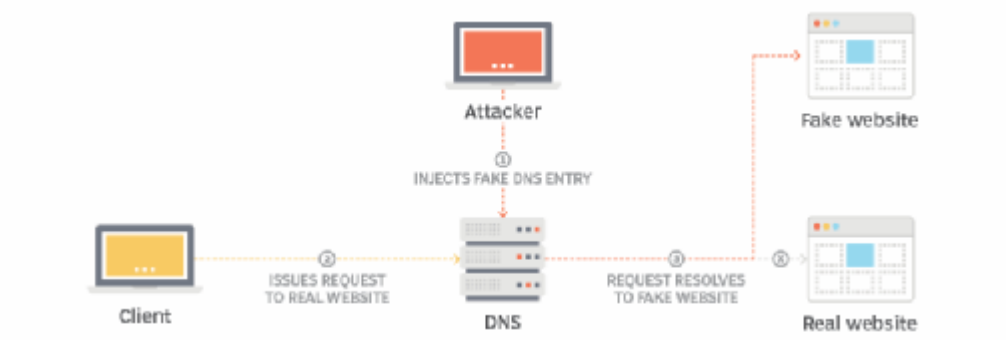
** Phòng chống*

Do tấn công sử dụng các kỹ thuật xã hội nhắm đến người dùng nên biện pháp phòng chống hiệu quả là giáo dục, đào tạo nâng cao ý thức cảnh giác cho người dùng. Một số khuyến nghị giúp người dùng phòng tránh dạng tấn công này:

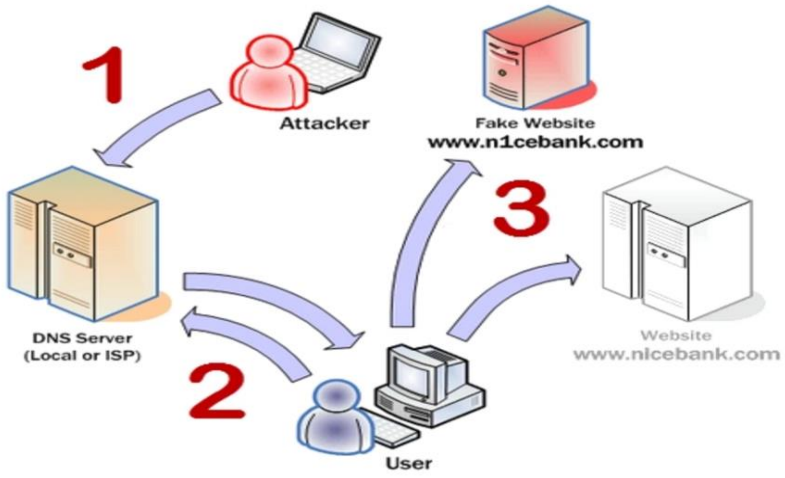
- Cảnh giác với các lời mời, hoặc thông báo trúng thưởng bằng email, tin nhắn điện thoại, hoặc quảng cáo trên các trang web, diễn đàn mà không có lý do, nguồn gốc trúng thưởng rõ ràng;
- Cảnh giác với các yêu cầu cung cấp thông tin, xác nhận tài khoản, thông tin thanh toán, thông tin thẻ tín dụng,..;
- Kiểm tra kỹ địa chỉ (URL) các trang web, đảm bảo truy nhập đúng trang web của cơ quan, tổ chức.

3.3.9. Tấn công Pharming

Pharming là kiểu tấn công vào trình duyệt của người dùng, trong đó người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu 1 website khác, thường là website độc hại. Có 2 dạng tấn công pharming: (1) kẻ tấn công thường sử dụng sâu, virus hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng và (2) kẻ tấn công cũng có thể tấn công vào hệ thống tên miền (DNS) để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.



(Tấn công pharming "cướp" trình duyệt)



(Tấn công pharming thông qua tấn công vào máy chủ DNS)

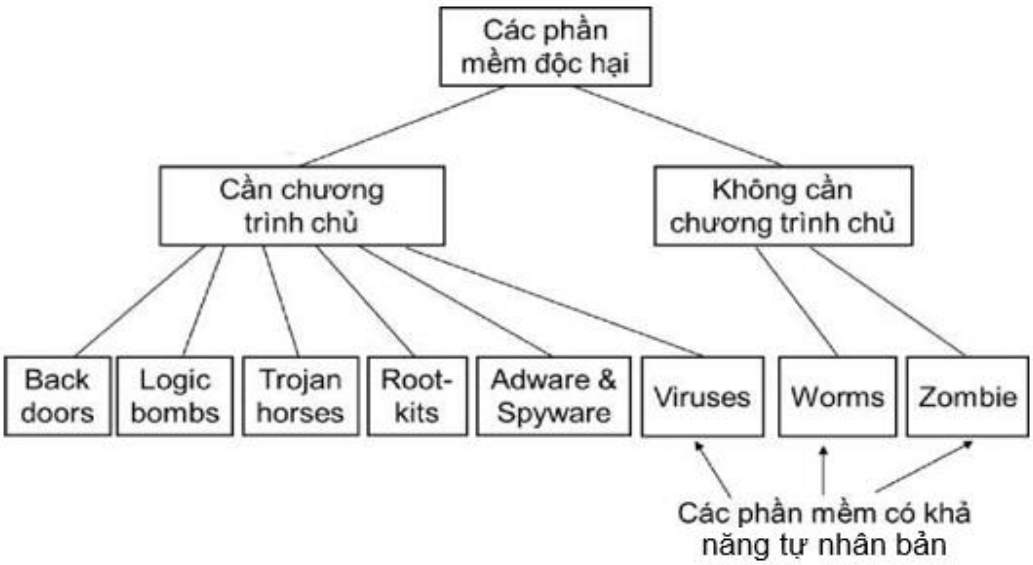
3.4. Các dạng phần mềm độc hại

3.4.1. Giới thiệu

Các phần mềm độc hại (Malware hay Malicious software) là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống. Có nhiều phương pháp phân loại các phần mềm độc hại, trong đó một phương pháp được thừa nhận rộng rãi là chia các phần mềm độc hại thành 2 nhóm chính:

- Các phần mềm độc hại cần chương trình chủ, vật chủ (host) để ký sinh và lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Logic bombs (Bom logic), Back doors (Cửa hậu), Trojan horses (Con ngựa thành Tơ roa), Virus (vi rút), Rootkits, Adware (Phần mềm quảng cáo) và Spyware (Phần mềm gián điệp).

- Các phần mềm độc hại không cần chương trình chủ, vật chủ để lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Worms (Sâu) và Zombies hay Bots (Phần mềm máy tính ma).



(Các dạng phần mềm độc hại)

Trong số các phần mềm độc hại, các phần mềm độc hại có khả năng tự lây nhiễm (self-infection), hay tự nhân bản (self-replicate) gồm Virus, Sâu và Phần mềm máy tính ma. Các dạng còn lại không có khả năng tự lây nhiễm. Việc phân loại các phần mềm độc hại kể trên mang tính chất tương đối do hiện nay, có một số phần mềm độc hại có các đặc tính của cả Virus, Sâu và Phần mềm gián điệp.

3.4.2. Logic Bombs

Logic bombs (Bom logic) là các đoạn mã độc thường được "nhúng" vào các chương trình bình thường và thường hẹn giờ để "phát nổ" trong một số điều kiện củ thể. Điều kiện để bom "phát nổ" có thể là sự xuất hiện hoặc biến mất của các file cụ thể, một thời điểm cụ thể, hoặc một ngày trong tuần. Khi "phát nổ" bom logic có thể xoá dữ liệu, file, tắt cả hệ thống...

Thực tế đã ghi nhận quả bom logic do Tim Lloyd cài lại đã "phát nổ" tại công ty Omega Engineering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom logic này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD cho công ty. Bản thân Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.

3.4.3. Trojan Horses

Trojan horses lấy tên theo tích "Con ngựa thành Tơ roa", là chương trình chứa mã độc, thường giả danh những chương trình có ích, nhằm lừa người dùng kích hoạt chúng. Trojan horses thường được sử dụng để thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập. Chẳng hạn, trong một hệ thống nhiều người dùng, một người dùng có thể tạo ra một trojan đội lốt một

chương trình hữu ích đặt ở thư mục chung. Khi trojan này được thực thi bởi một người dùng khác, nó sẽ thay đổi quyền truy nhập các file của người dùng đó, cho phép tất cả người dùng truy nhập vào các file của người dùng đó.

3.4.4. Back doors

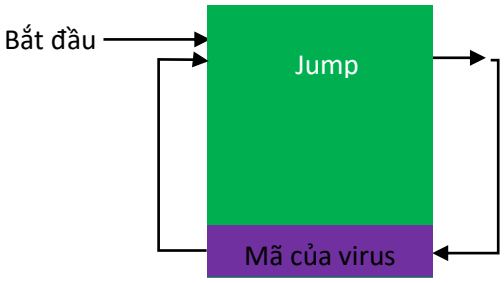
Back doors (Cửa hậu) thường được các lập trình viên tạo ra, dùng để gỡ rối và kiểm thử chương trình trong quá trình phát triển. Cửa hậu thường cho phép truy nhập trực tiếp vào hệ thống mà không qua các thủ tục kiểm tra an ninh thông thường. Khi cửa hậu được lập trình viên tạo ra để truy nhập bất hợp pháp vào hệ thống, nó trở thành một mối đe dọa đến an ninh hệ thống. Cửa hậu thường được thiết kế và cài đặt khéo léo và chỉ được kích hoạt trong một ngữ cảnh nào đó, do vậy nó rất khó bị phát hiện.

3.4.5. Virus

* *Giới thiệu*

Virus là một chương trình có thể "nhiễm" vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa virus được kích hoạt thì virus sẽ tiếp tục "lây nhiễm" sang các chương trình khác. Tương tự như virus sinh học, virus máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm virus, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...

Virus có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, virus tự động được thực hiện khi chương trình này chạy.



(Chèn và gọi thực hiện mã virus)

* *Các loại virus*

Các loại virus thường gặp bao gồm file virus, boot virus, macro virus và email virus. Boot virus là dạng virus lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record). Do boot virus lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động. Boot virus có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy nhập được.

File virus là dạng virus phổ biến nhất, đối tượng lây nhiễm của chúng là các file chương trình và các file dữ liệu. Mỗi khi chương trình được kích hoạt hoặc file dữ liệu được nạp vào bộ nhớ, virus được kích hoạt. Mọi chương trình tiếp theo được kích hoạt đều

bị lây nhiễm virus này. File virus có thể làm hỏng chương trình, hỏng hoặc phá hủy các file dữ liệu, đánh cắp các dữ liệu nhạy cam,...

Macro virus là một loại file virus đặc biệt do chúng chỉ lây nhiễm vào các tài liệu của bộ phần mềm Microsoft Office. Macro virus hoạt động được nhờ tính năng cho phép tạo và thực hiện các đoạn mã macro trong các tài liệu của bộ ứng dụng Microsoft Office, gồm ứng dụng soạn thảo Word, bảng tính Excel, trình email Outlook,.. Các đoạn mã macro thường được dùng để tự động hóa 1 số việc và được viết bằng ngôn ngữ Visual Basic for Applications (VBA). Macro virus thường lây nhiễm vào các file định dạng chuẩn (các template như normal.dot và normal.dotx) và từ đó lây nhiễm vào tất cả các file tài liệu được mở. Macro virus cũng có thể được tự động kích hoạt nhờ các auto-executed macros, như AutoExecute, Automacro và Command macro. Theo thống kê, macro virus chiếm khoảng 2/3 tổng lượng virus đã được phát hiện. Lượng tài liệu bị lây nhiễm macro virus đã giảm đáng kể từ khi Microsoft Office 2010 có thiết lập ngầm định không cho phép chạy các macro.

Email virus lây nhiễm bằng cách tự động gửi một bản copy của nó như 1 file đính kèm đến tất cả các địa chỉ email trong sổ địa chỉ của người dùng trên máy bị lây nhiễm. Nếu người dùng mở email hoặc file đính kèm, virus được kích hoạt. Email virus có thể lây nhiễm rất nhanh chóng, lan tràn trên khắp thế giới trong một thời gian ngắn.

3.4.6. Worms

Worms (Sâu) là một loại phần mềm độc hại có khả năng tự lây nhiễm từ máy này sang máy khác mà không cần chương trình chủ, vật chủ, hoặc sự trợ giúp của người dùng. Khi sâu lây nhiễm vào một máy, nó sử dụng máy này làm "bàn đạp" để tiếp tục rà quét, tấn công các máy khác. Một trong các dạng sâu phổ biến là sâu mạng (network worms) sử dụng kết nối mạng để lây lan từ máy này sang máy khác. Mặc dù sử dụng phương thức lây lan khác virus, khi sâu hoạt động, nó tương tự virus.

Sâu có thể lây lan sử dụng nhiều phương pháp khác nhau. Một số sâu chỉ sử dụng một phương pháp lây lan, nhưng một số sâu khác có khả năng lây lan theo nhiều phương pháp. Các phương pháp lây lan chính của sâu gồm:

- Lây lan qua thư điện tử: Sâu sử dụng email để gửi bản sao của mình đến các máy khác.
- Lây lan thông qua khả năng thực thi từ xa: Sâu gửi và thực thi một bản sao của nó trên một máy khác thông qua việc khai thác các lỗ hổng an ninh của hệ điều hành, các dịch vụ, hoặc phần mềm ứng dụng.
- Lây lan thông qua khả năng log-in (đăng nhập) từ xa: Sâu đăng nhập vào hệ thống ở xa như một người dùng và sử dụng lệnh để sao chép bản thân nó từ máy này sang máy khác.

Sâu Code Red được phát hiện vào tháng 7/2001 lây nhiễm thông qua việc khai thác lỗi tràn bộ đệm khi xử lý các file .ida trong máy chủ Microsoft IIS (Internet Information Service). Code Red quét các địa chỉ IP ngẫu nhiên để tìm các hệ thống có lỗi và lây

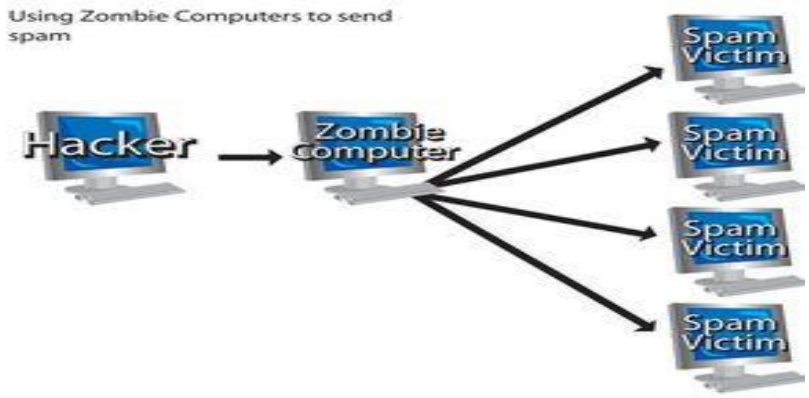
nhiễm vào 360.000 máy chủ trong vòng 14 giờ. Sau đó, sâu Nimda được phát hiện vào tháng 9/2001 là sâu có khả năng lây lan theo nhiều con đường:

- Qua email từ máy client sang client.
- Qua các thư mục chia sẻ trên mạng.
- Từ máy chủ web sang trình duyệt.
- Từ máy khách đến máy chủ nhờ khai thác các lỗi máy chủ.

Chỉ 22 phút sau khi ra đời, Nimda trở thành sâu có tốc độ lan truyền nhanh nhất trên Internet vào thời điểm đó.

3.4.7. Zombies

Zombie (còn gọi là Bot hoặc Automated agent) là một chương trình được thiết kế để giành quyền kiểm soát một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để tấn công các hệ thống khác, hoặc gửi spam emails. Tương tự như sâu, zombie có khả năng tự lây nhiễm sang các hệ thống khác mà không cần chương trình chủ, hoặc các hỗ trợ từ người dùng. Một tập hợp các máy tính zombie/bot dưới sự kiểm soát của một, hoặc một nhóm tin tặc được gọi là mạng máy tính ma, hay zombie network/botnet. Các zombies thường được điều phối và sử dụng để thực hiện các cuộc tấn công DDoS các máy chủ, các website của các công ty, hoặc các tổ chức chính phủ. Các máy tính zombies cũng có thể được sử dụng để gửi thư rác tạo ra khoản tiền không nhỏ cho các nhóm tin tặc.



3.4.8. Rootkits

Rootkit là một dạng phần mềm độc hại gồm một tập các công cụ có mục đích giành quyền truy nhập vào hệ thống máy tính mà người dùng không có thẩm quyền không thể truy nhập. Rootkit thường che giấu mình bằng cách đội lột một phần mềm khác. Rootkit có thể được cài đặt tự động, hoặc tin tặc cài đặt rootkit khi chiếm được quyền quản trị hệ thống. Do rootkit có quyền truy nhập hệ thống ở mức quản trị nên nó có toàn quyền truy nhập vào các thành phần trong hệ thống và rất khó bị phát hiện.

3.4.9. Adware và Spyware

Adware (tên đầy đủ là advertising-supported software) là các phần mềm tự động hiển thị các bảng quảng cáo trong thời gian người dùng tải hoặc sử dụng các phần mềm.

Adware thường được đóng gói chung với các phần mềm khác có thể dưới dạng như một phần của một phần mềm hoặc một dịch vụ miễn phí. Adware trong một số trường hợp có thể được coi là một phần mềm độc hại nếu chúng được tự động cài đặt và kích hoạt mà không được sự đồng ý của người dùng.

Spyware là một dạng phần mềm độc hại được cài đặt tự động nhằm giám sát, thu thập và đánh cắp các thông tin nhạy cảm trên hệ thống nạn nhân. Có 4 loại spyware thường gặp, gồm system monitor (giám sát hệ thống), trojan, adware, and tracking cookies (các cookie theo dõi). Spyware có thể được cài đặt vào hệ thống nạn nhân thông qua nhiều phương pháp, như tích hợp, đóng gói vào các phần mềm khác, bẫy nạn nhân tự tải và cài đặt, hoặc tin tặc có thể sử dụng vi rút, sâu để tải và cài đặt. Spyware thường được trang bị khả năng ẩn mình nên rất khó có thể phát hiện bằng các phương pháp thông thường.

❖ TÓM TẮT CHƯƠNG 3

Trong chương này, một số nội dung chính được giới thiệu:

- **Các Dạng Tấn Công**: Chương này giới thiệu về các dạng tấn công thông tin như tấn công từ xa, tấn công bên trong, tấn công xã hội và tấn công tương tác với phần mềm độc hại. Học viên sẽ hiểu cách các tấn công này hoạt động và tiềm ẩn nguy cơ cho hệ thống thông tin.
- **Phần Mềm Độc Hại:** Chương này giới thiệu về các loại phần mềm độc hại như virus, malware, trojan, ransomware và spyware. Học viên sẽ hiểu cách nhận diện và đối phó với các phần mềm độc hại này.
- **Nguy Cơ và Rủi Ro**: Học cách đánh giá nguy cơ và rủi ro mà các tấn công và phần mềm độc hại có thể mang lại cho hệ thống thông tin. Điều này giúp trong việc định danh mức độ nguy cơ và ảnh hưởng của mỗi tấn công.
- **Bảo Vệ Hệ Thống**: Chương này trình bày cách bảo vệ hệ thống thông tin khỏi các tấn công và phần mềm độc hại bằng cách áp dụng biện pháp bảo mật, cập nhật phần mềm, và sử dụng phần mềm chống virus và malware.

CÁC BÀI TẬP HỆ THỐNG KIẾN THỨC

1) Mối đe dọa (threat) là gì? Nêu quan hệ giữa lỗ hổng và mối đe dọa.
2) Mô tả 4 loại tấn công chính và 2 kiểu tấn công chủ động và thụ động.
3) Nêu mục đích và các dạng tấn công vào mật khẩu.
4) Tấn công chèn mã SQL là gì? Nêu các nguyên nhân của lỗ hổng chèn mã SQL. Tấn công chèn mã SQL có khả năng cho phép tin tặc thực hiện hành động gì trên hệ thống nạn nhân?
5) Nêu các biện pháp phòng chống tấn công chèn mã SQL.
6) Tấn công pharming là gì? Mô tả các dạng tấn công pharming.
7) Phần mềm độc hại là gì? Phân loại các phần mềm độc hại.
8) Vi rút là gì? Nêu các phương pháp lây nhiễm và các loại vi rút.
9) Zombie là gì? Mô tả cơ chế hoạt động của Zombie

10. Trojan là gì? Mô tả cơ chế hoạt động của trojan

CHƯƠNG 4. ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

❖ GIỚI THIỆU CHƯƠNG 4

Chương 4 của môn học "An Toàn Hệ Thống Thông Tin" tập trung vào việc tìm hiểu về mã hóa thông tin và cách nó đóng một vai trò quan trọng trong bảo vệ thông tin. Chương này giúp học viên hiểu về cách mã hóa được sử dụng để bảo vệ dữ liệu và thông tin quan trọng trên mạng và trong hệ thống thông tin.

❖ MỤC TIÊU CHƯƠNG 4

Sau khi học xong chương này, người học có khả năng:

➢ *Về kiến thức:*

- *Hiểu về các phương pháp mã hóa thông tin, bao gồm mã hóa đối xứng và mã hóa bất đối xứng, cùng với cách chúng hoạt động.*
- *Hiểu về loại hình mã hóa thông tin như mã hóa dữ liệu trong truyền thông mạng, mã hóa ổ cứng, và mã hóa email.*
- *Hiểu vai trò của mã hóa trong bảo mật thông tin và cách nó giúp ngăn chặn truy cập trái phép vào dữ liệu quan trọng.*
-
- *Hiểu về các quy định và tiêu chuẩn liên quan đến việc sử dụng mã hóa, và tại sao tuân thủ quy định này là quan trọng trong bảo mật thông tin.*

➢ *Về kỹ năng:*

- *Kỹ năng sử dụng các công cụ và phần mềm mã hóa để bảo vệ thông tin quan trọng trên mạng và trong hệ thống thông tin.*
- *Kỹ năng cấu hình hệ thống để sử dụng mã hóa trong các ứng dụng và truyền thông mạng.*
- *Kỹ năng kiểm tra an toàn thông tin bằng cách đảm bảo rằng các dữ liệu được mã hóa một cách an toàn và đáng tin cậy.*
- *Kỹ Năng đánh giá hiệu quả của việc sử dụng mã hóa trong bảo vệ thông tin và tìm kiếm cách nâng cao cấp độ an toàn.*

➢ *Về năng lực tự chủ và trách nhiệm:*

- *Năng lực về quản lý thời gian, trách nhiệm với công việc*
- *Năng lực học tập và làm việc độc lập*
- *Tự chủ trong việc giải quyết vấn đề*

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 4

- *Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, dạy học theo vấn đề); yêu cầu người học thực hiện câu hỏi thảo luận và bài tập chương (cá nhân hoặc nhóm).*
- *Đối với người học: chủ động đọc trước giáo trình trước buổi học; hoàn thành đầy đủ câu hỏi thảo luận và bài tập tình huống theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.*

❖ **ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 4**

- ***Phòng học chuyên môn hóa/nhà xưởng:*** Phòng học thực hành
- ***Trang thiết bị máy móc:*** Máy chiếu, máy tính và các thiết bị dạy học khác
- ***Học liệu, dụng cụ, nguyên vật liệu:*** Chương trình môn học, giáo trình, tài liệu tham khảo, giáo án, phim ảnh, và các tài liệu liên quan.
- ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 4**

- **Nội dung:**

✓ *Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức*

✓ *Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.*

✓ *Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:*

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ ***Điểm kiểm tra thường xuyên:*** *1 điểm kiểm tra (hình thức: hỏi miệng)*

✓ ***Kiểm tra định kỳ lý thuyết:*** *không có*

❖ **NỘI DUNG CHƯƠNG 4**

4.1. Khái quát về mã hóa thông tin và ứng dụng

4.1.1. Các khái niệm cơ bản

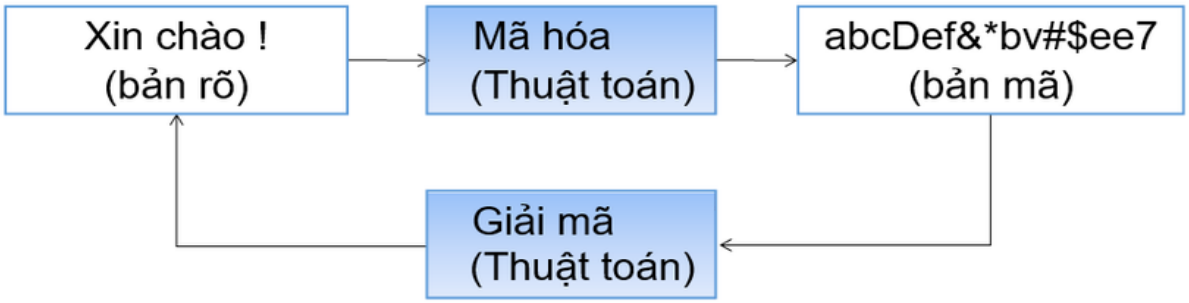
** Mật mã*

Theo từ điển Webster's Revised Unabridged Dictionary: “cryptography is the act or art of writing secret characters”, hay mật mã (cryptography) là một hành động hoặc nghệ thuật viết các ký tự bí mật. Còn theo từ điển Free Online Dictionary of Computing: “cryptography is encoding data so that it can only be decoded by specific individuals”, có nghĩa là mật mã là việc mã hóa dữ liệu mà nó chỉ có thể được giải mã bởi một số

người chỉ định.

** Bản rõ, bản mã, mã hóa và giải mã*

- Bản rõ (Plaintext), hay thông tin chưa mã hóa (Unencrypted information) là thông tin ở dạng có thể hiểu được.
- Bản mã (Ciphertext), hay thông tin đã được mã hóa (Encrypted information) là thông tin ở dạng đã bị xáo trộn.
- Mã hóa (Encryption) là hành động xáo trộn (scrambling) bản rõ để chuyển thành bản mã.
- Giải mã (Decryption) là hành động giải xáo trộn (unscrambling) bản mã để chuyển thành bản rõ.



(Các khâu Mã hóa (Encryption) và Giải mã (Decryption) của một hệ mã hóa)

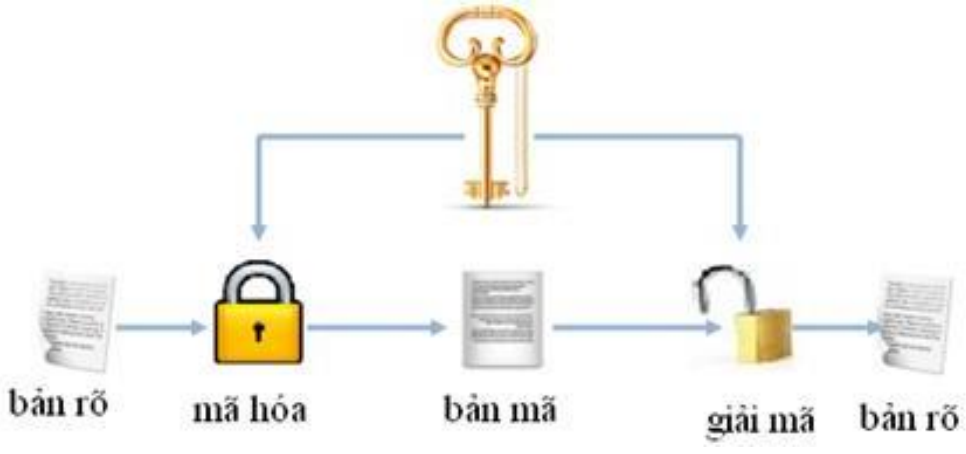
** Giải thuật mã hóa & giải mã, Bộ mã hóa, Khóa/Chìa, Không gian khóa*

Giải thuật mã hóa (Encryption algorithm) là giải thuật dùng để mã hóa thông tin và giải thuật giải mã (Decryption algorithm) dùng để giải mã thông tin.

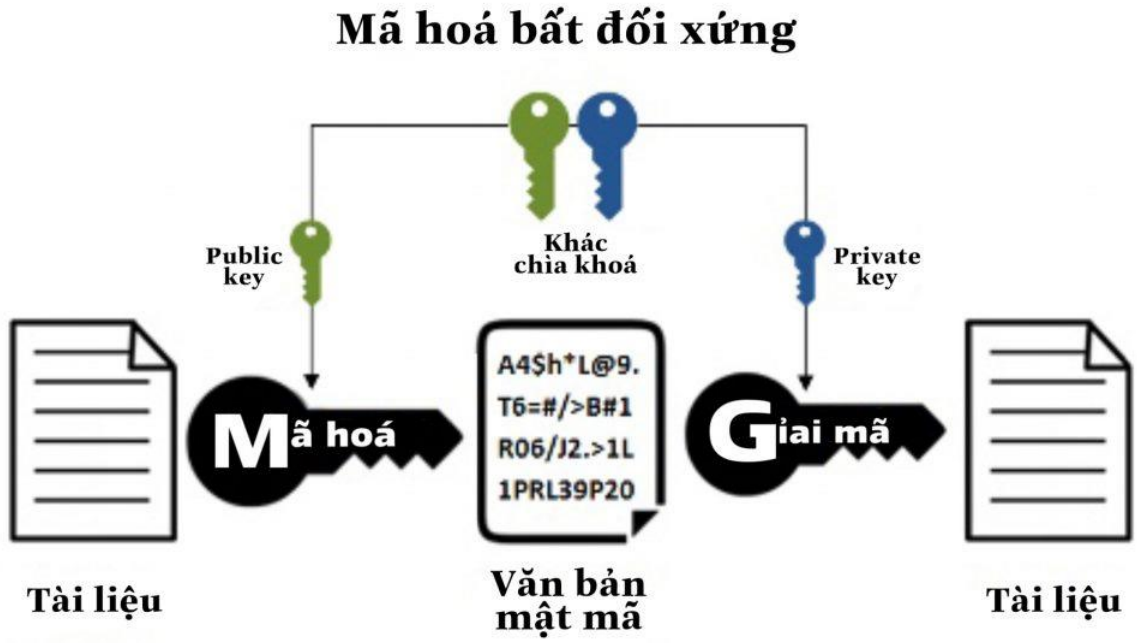
- Một bộ mã hóa (Cipher) gồm một giải thuật để mã hóa và một giải thuật để giải mã thông tin.
- Khóa/Chìa (Key) là một chuỗi được sử dụng trong giải thuật mã hóa và giải mã.
- Không gian khóa (Keyspace) là tổng số khóa có thể có của một hệ mã hóa. Ví dụ, nếu sử dụng khóa kích thước 64 bit thì không gian khóa là 2^{64}.

** Mã hóa khóa đối xứng, Mã hóa khóa bất đối xứng, Hàm băm, Thám mã*

Mã hóa khóa đối xứng (Symmetric key cryptography) là dạng mã hóa trong đó một khóa được sử dụng cho cả giải thuật mã hóa và giải mã. Do khóa sử dụng chung cần phải được giữ bí mật nên mã hóa khóa đối xứng còn được gọi là mã hóa khóa bí mật (Secret key cryptography).



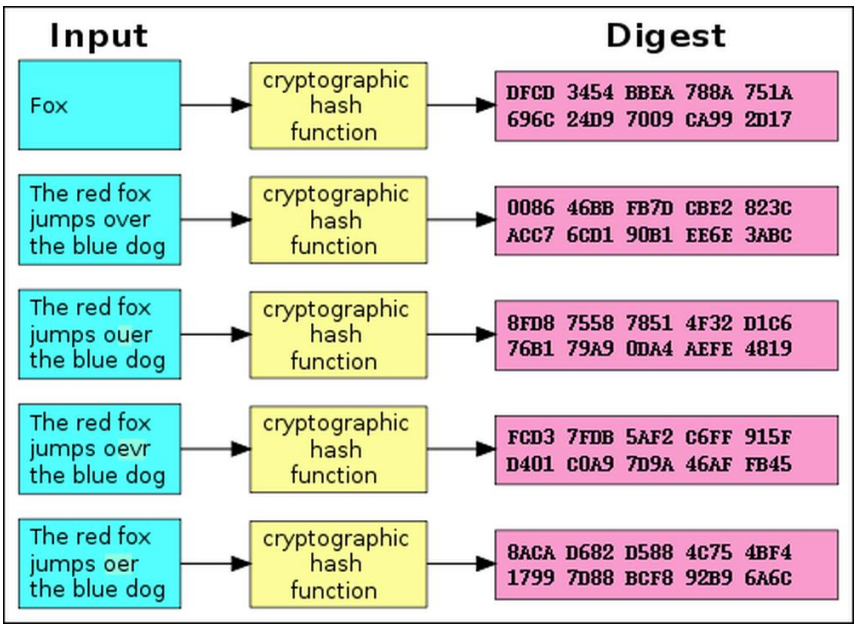
(Hình minh họa hoạt động của một hệ mã hóa khóa đối xứng, trong đó một khóa bí mật duy nhất được sử dụng cho cả hai khâu mã hóa và giải mã một thông điệp)



(Hình minh họa hoạt động của một hệ mã hóa khóa bất đối xứng, trong đó một khóa công khai (public key) được sử dụng cho khâu mã hóa và khóa riêng (private key) cho khâu giải mã thông điệp)

Mã hóa khóa bất đối xứng (Asymmetric key cryptography) là dạng mã hóa trong đó một cặp khóa được sử dụng: khóa công khai (public key) dùng để mã hóa, khóa riêng (private key) dùng để giải mã. Chỉ có khóa riêng cần phải giữ bí mật, còn khóa công khai có thể phổ biến rộng rãi. Do khóa để mã hóa có thể công khai nên đôi khi mã hóa khóa bất đối xứng còn được gọi là mã hóa khóa công khai (Public key cryptography).

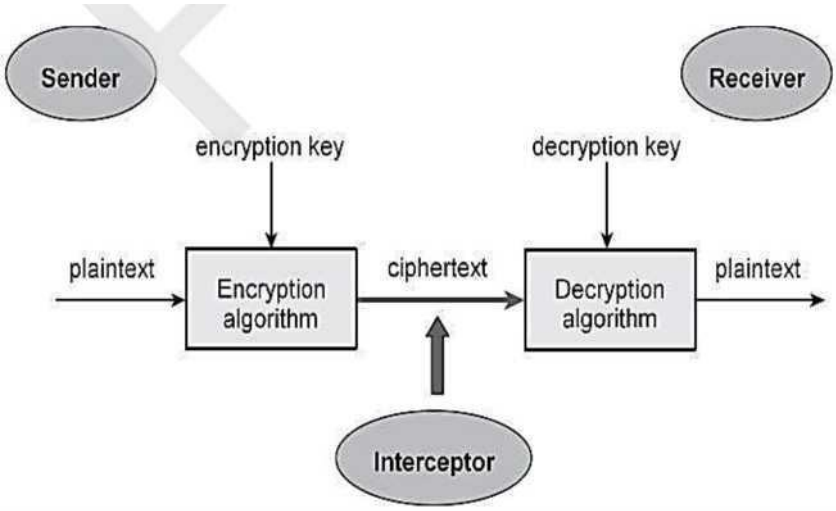
Hàm băm (Hash function) là một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định. Hình 4.4 minh họa đầu vào (Input) và đầu ra (Digest) của hàm băm. Trong các loại hàm băm, hàm băm 1 chiều (One-way hash function) là hàm băm, trong đó việc thực hiện mã hóa tương đối đơn giản, còn việc giải mã thường có độ phức tạp rất lớn, hoặc không khả thi về mặt tính toán.



(Minh họa đầu vào (Input) và đầu ra (Digest) của hàm băm)

Thám mã hay phá mã (Cryptanalysis) là quá trình giải mã thông điệp đã bị mã hóa mà không cần có trước thông tin về giải thuật mã hóa và khóa mã.

4.1.2. Các thành phần của một hệ mã hóa

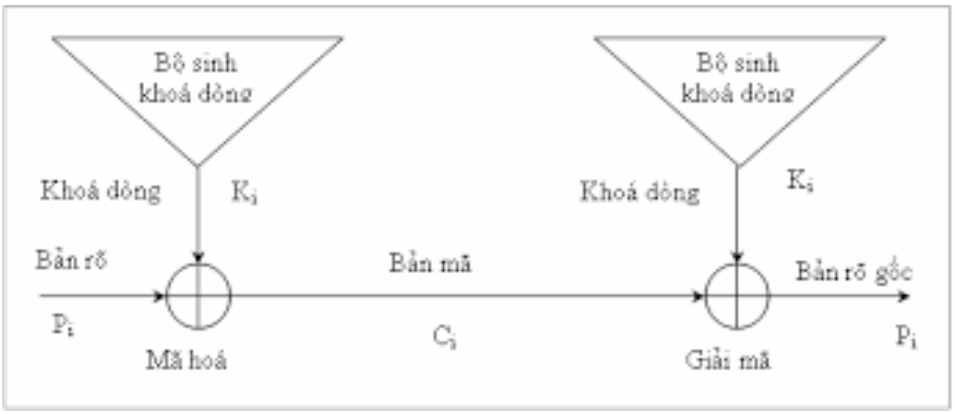


(Các thành phần của một hệ mã hóa đơn giản)

Một hệ mã hóa hay hệ mật mã (Cryptosystem) là một bản cài đặt của các kỹ thuật mật mã và các thành phần có liên quan để cung cấp dịch vụ bảo mật thông tin. Hình ảnh trên nêu các thành phần của một hệ mã hóa đơn giản dùng để đảm bảo tính bí mật của thông tin từ người gửi (Sender) truyền đến người nhận (Receiver) mà không bị một bên thứ ba nghe lén (Interceptor). Các thành phần của một hệ mã hóa đơn giản gồm bản rõ (plaintext), giải thuật mã hóa (Encryption Algorithm), bản mã (ciphertext), giải thuật giải mã (Decryption Algorithm), khóa mã hóa (encryption key) và khóa giải mã (decryption key). Một thành phần quan trọng khác của một hệ mã hóa là không gian khóa (Keyspace) - là tập hợp tất cả các khóa có thể có. Ví dụ, nếu chọn kích thước khóa là 64 bit thì không gian khóa sẽ là 2^{64}. Nhìn chung, hệ mã hóa có độ an toàn càng cao nếu không gian khóa lựa chọn càng lớn.

4.1.3. Mã hóa dòng và mã hóa khối

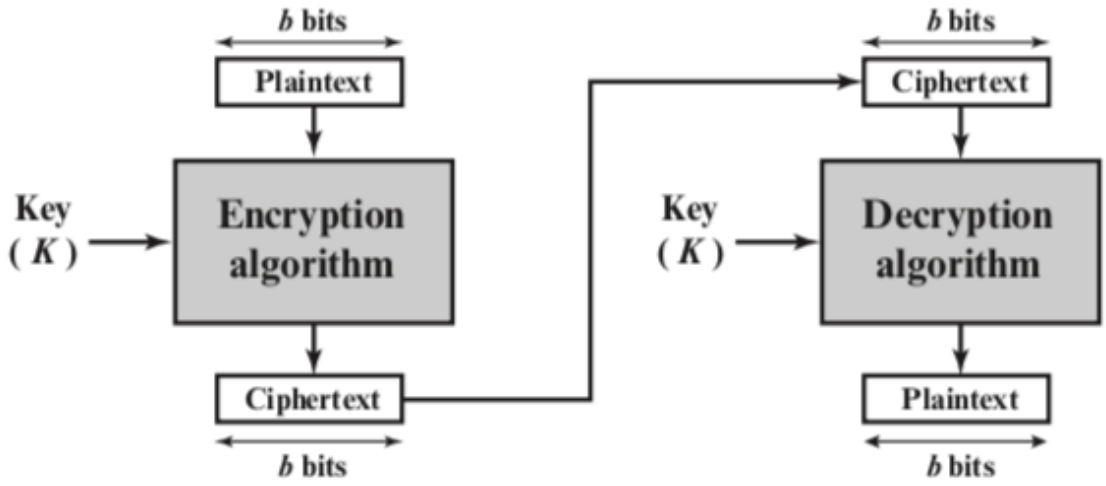
* *Mã hóa dòng*



(Mã hóa dòng - Stream cipher)

Mã hóa dòng (Stream cipher) là kiểu mã hóa mà từng bit, hoặc ký tự của bản rõ được kết hợp với từng bit, hoặc ký tự tương ứng của khóa để tạo thành bản mã. Hình ảnh trên biểu diễn quá trình mã hóa (Encrypt) và giải mã (Decrypt) trong mã hóa dòng. Theo đó, ở bên gửi các bit *Pi* của bản rõ (plaintext) được liên tục đưa vào kết hợp với bit tương ứng *Ki* của khóa để tạo thành bit mã *Ci*; Ở bên nhận, bit mã *Ci* được kết hợp với bit khóa *Ci* để khôi phục bit rõ *Pi*. Một bộ sinh dòng khóa (Keystream Generator) được sử dụng để liên tục sinh các bit khóa *Ki* từ khóa gốc *K*. Các giải thuật mã hóa dòng tiêu biểu như A5, hoặc RC4 được sử dụng rộng rãi trong viễn thông.

* *Mã hóa khối*



(Mã hóa khối (Block cipher))

Mã hóa khối (Block cipher) là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa và giải mã. Hình ảnh biểu diễn quá trình mã hóa và giải mã trong mã hóa khối. Theo đó, ở bên gửi bản rõ (Plaintext) được chia thành các khối (block) có kích thước cố định, sau đó từng khối được mã hóa để chuyển thành khối mã. Các khối mã được ghép lại thành bản mã (Ciphertext). Ở bên nhận, bản mã lại được chia thành các khối và từng lại được giải mã để chuyển thành khối rõ. Cuối cùng ghép các khối rõ để có bản rõ hoàn chỉnh. Các giải thuật mã hóa khối tiêu biểu như DES, 3-

DES, IDEA, AES được sử dụng rất rộng rãi trong mã hóa dữ liệu với kích thước khối 64, hoặc 128 bit.

4.1.4. Sơ lược lịch sử mật mã

Có thể nói mật mã là con đẻ của toán học nên sự phát triển của mật mã đi liền với sự phát triển của toán học. Tuy nhiên, do nhiều giải thuật mật mã đòi hỏi khối lượng tính toán lớn nên mật mã chỉ thực sự phát triển mạnh cùng với sự ra đời và phát triển của máy tính điện tử. Sau đây là một số mốc trong sự phát triển của mật mã và ứng dụng mật mã:

- Các kỹ thuật mã hoá thô sơ đã được người cổ Ai cập sử dụng cách đây 4000 năm.
- Người cổ Hy lạp, Ấn độ cũng đã sử dụng mã hoá cách đây hàng ngàn năm.
- Các kỹ thuật mã hoá chỉ thực sự phát triển mạnh từ thế kỷ 1800 nhờ công cụ toán học, và phát triển vượt bậc trong thế kỷ 20 nhờ sự phát triển của máy tính và ngành công nghệ thông tin.
- Trong chiến tranh thế giới thứ I và II, các kỹ thuật mã hóa được sử dụng rộng rãi trong liên lạc quân sự sử dụng sóng vô tuyến. Quân đội các nước đã sử dụng các công cụ phá mã, thám mã để giải mã các thông điệp của quân địch.
- Năm 1976 chuẩn mã hóa DES (Data Encryption Standard) được Cơ quan mật vụ Mỹ (NSA - National Security Agency) thừa nhận và sử dụng rộng rãi.
- Năm 1976, hai nhà khoa học Whitman Diffie và Martin Hellman đã đưa ra khái niệm mã hóa khóa bất đối xứng (Asymmetric key cryptography), hay mã hóa khóa công khai (Public key cryptography) đưa đến những thay đổi lớn trong kỹ thuật mật mã. Theo đó, các hệ mã hóa khóa công khai bắt đầu được sử dụng rộng rãi nhờ khả năng hỗ trợ trao đổi khóa dễ dàng hơn và do các hệ mã hóa khóa bí mật gặp khó khăn trong quản lý và trao đổi khóa, đặc biệt khi số lượng người dùng lớn.
- Năm 1977, ba nhà khoa học Ronald Rivest, Adi Shamir, và Leonard Adleman giới thiệu giải thuật mã hóa khóa công khai RSA. Từ đó, RSA trở thành giải thuật mã hóa khóa công khai được sử dụng rộng rãi nhất do RSA có thể vừa được sử dụng để mã hóa thông tin và sử dụng trong chữ ký số.
- Năm 1991, phiên bản đầu tiên của PGP (Pretty Good Privacy) ra đời.
- Năm 2000, chuẩn mã hóa AES (Advanced Encryption Standard) được thừa nhận và ứng dụng rộng rãi.

4.1.5. Ứng dụng của mã hóa

Mã hoá thông tin có thể được sử dụng để đảm bảo an toàn thông tin với các thuộc tính: bí mật (confidentiality), toàn vẹn (integrity), xác thực (authentication), không thể chối bỏ (non-repudiation). Cụ thể, các kỹ thuật mã hóa được ứng dụng rộng rãi trong các hệ thống, công cụ và dịch vụ bảo mật như:

- Dịch vụ xác thực (Kerberos, SSO, RADIUS,...)

- Điều khiển truy nhập
- Các công cụ cho đảm bảo an toàn cho truyền thông không dây
- Các nền tảng bảo mật như PKI, PGP
- Các giao thức bảo mật như SSL/TLS, SSH, SET, IPSec
- Các hệ thống bảo mật kênh truyền, như VPN.

4.2. Các phương pháp mã hóa

4.2.1. Phương pháp thay thế

Có hai loại mã cổ điển là mã thay thế và mã hoán vị (hay còn gọi là dịch chuyển). Mã thay thế là phương pháp mà từng kí tự (nhóm kí tự) trong bản rõ được thay thế bằng một kí tự (một nhóm kí tự) khác để tạo ra bản mã. Bên nhận chỉ cần thay thế ngược lại trên bản mã để có được bản rõ ban đầu. Trong phương pháp mã hoán vị, các kí tự trong bản rõ vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra bản mã. Tức là các kí tự trong bản rõ hoàn toàn không bị thay đổi bằng kí tự khác mà chỉ đảo chỗ của chúng để tạo thành bản mã.

Trước hết ta xét các mã cổ điển sử dụng phép thay thế các chữ của bản rõ bằng các chữ khác của bảng chữ để tạo thành bản mã.

- Ở đây các chữ của bản rõ được thay bằng các chữ hoặc các số hoặc các ký tự khác.
- Hoặc nếu xem bản rõ như môt dãy bít, thì phép thế thay các mẫu bít bản rõ bằng các mẫu bít bản mã.

** Mã Ceasar*

Đây là mã thế được biết sớm nhất, được sáng tạo bởi Julius Ceasar. Lần đầu tiên được sử dụng trong quân sự. Việc mã hoá được thực hiện đơn giản là thay mỗi chữ trong bản rõ bằng chữ thứ ba tiếp theo trong bảng chữ cái.

- Ví dụ:
  - Meet me after the toga party
  - PHHW PH DIWHU WKH WRJD SDUWB

Ở đây thay chữ m bằng chữ đứng thứ 3 sau m là p (m, n, o, p); thay chữ e bằng chữ đứng thứ 3 sau e là h (e, f, g, h).

- Có thể định nghĩa việc mã hoá trên qua ánh xạ trên bảng chữ cái sau: các chữ ở dòng dưới là mã của các chữ tương ứng ở dòng trên:

  a b c d e f g h i j k l m n o p q r s t u v w x y z

  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Về toán học, nếu ta gán số thứ tự cho mỗi chữ trong bảng chữ cái. Các chữ ở dòng trên có số thứ tự tương ứng là số ở dòng dưới:

  a b c d e f g h i j k l m

0 1 2 3 4 5 6 7 8 9 10 11 12

n o p q r s t u v w x y z

13 14 15 16 17 18 19 20 21 22 23 24 25

thì mã Ceasar được định nghĩa qua phép tịnh tiến các chữ như sau:

$$c = E(p) = (p + k) \bmod (26)$$

$$p = D(c) = (c - k) \bmod (26)$$

Ở đây, p là số thứ tự của chữ trong bản rõ và c là số thứ tự của chữ tương ứng của bản mã; k là khoá của mã Ceasar. Có 26 giá trị khác nhau của k, nên có 26 khoá khác nhau. Thực tế độ dài khoá ở đây chỉ là 1, vì mọi chữ đều tịnh tiến đi một khoảng như nhau.

- Thám mã Ceasar là việc làm đơn giản, do số khoá có thể có là rất ít.

  Chỉ có 26 khoá có thể, vì A chỉ có thể ánh xạ vào một trong số 26 chữ cái của bảng chữ cái tiếng Anh: A, B, C, …Các chữ khác sẽ được xác định bằng số bước tịnh tiến tương ứng của A. Kẻ thám mã có thể thử lần lượt từng khoá một, tức là sử dụng phương pháp tìm duyệt tổng thể. Vì số khoá ít nên việc tìm duyệt là khả thi. Cho trước bản mã, thử 26 cách dịch chuyển khác nhau, ta sẽ đoán nhận thông qua nội dung các bản rõ nhận được.

Ví dụ. Bẻ bản mã "GCUA VQ DTGCM" bằng cách thử các phép tịnh tiến khác nhau của bảng chữ, ta chọn được bước tịnh tiến thích hợp là 24 và cho bản rõ là "easy to break".

* *Các mã bảng chữ đơn*

Bây giờ ta khắc phục nhược điểm của mã Ceasar bằng cách mã hoá các chữ không chỉ là dịch chuyển bảng chữ, mà có thể tạo ra các bước nhảy khác nhau cho các chữ. Trong một mã mỗi chữ của bản rõ được ánh xạ đến một chữ khác nhau của bản mã. Do đó mỗi cách mã như vậy sẽ tương ứng với một hoán vị của bảng chữ và hoán vị đó chính là khoá của mã đã cho. Như vậy độ dài khoá ở đây là 26 và số khoá có thể có là 26!. Số khoá như vậy là rất lớn.

Ví dụ. Ta có bản mã tương ứng với bản rõ trong mã bảng chữ đơn như sau:

Plain: abcdefghijklmnopqrstuvwxyz

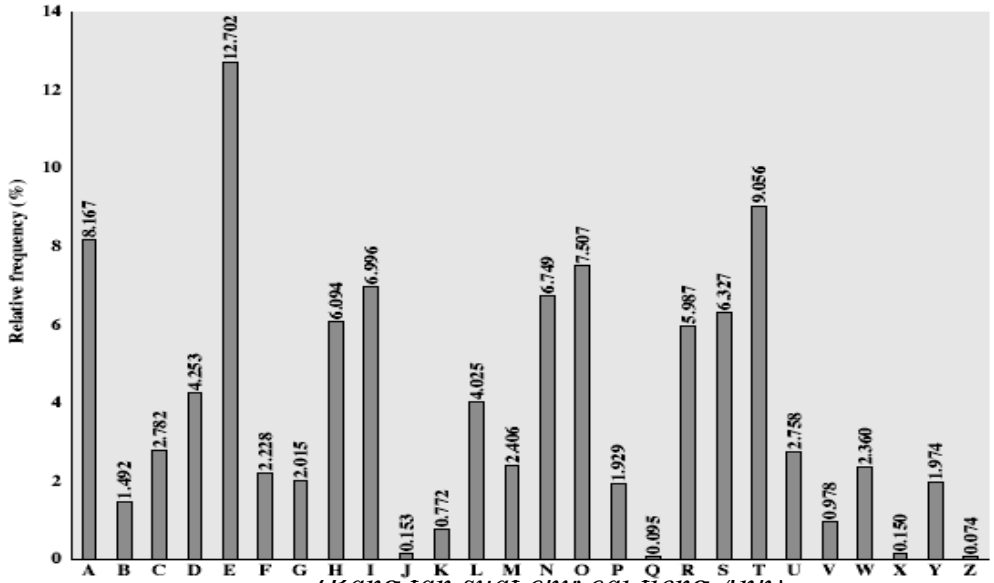
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

- Tính an toàn của mã trên bảng chữ đơn. Tổng cộng có 26! xấp xỉ khoảng 4×10^{26} khoá. Với khá nhiều khoá như vậy nhiều người nghĩ là mã trên bảng chữ đơn sẽ an toàn. Nhưng không phải như vậy. Vấn đề ở đây là do các đặc trưng về ngôn ngữ. Tuy có số lượng khoá lớn, nhưng do các đặc trưng về tần suất xuất hiện của các chữ trong bản rõ và các chữ tương ứng trong bản mã là như nhau, nên kẻ thám mã có thể đoán được ánh xạ của một số chữ và từ đó mò tìm ra chữ mã cho các chữ khác. Ta sẽ xét khía cạnh này cụ thể trong mục sau.

- Tính dư thừa của ngôn ngữ và thám mã. Ngôn ngữ của loài người là dư thừa. Có một số chữ hoặc các cặp chữ hoặc bộ ba chữ được dùng thường xuyên hơn các bộ chữ cùng độ dài khác. Chẳng hạn như các bộ chữ sau đây trong tiếng Anh "th lrd s m shphrd shll nt wnt". Tóm lại trong nhiều ngôn ngữ các chữ không được sử dụng thường xuyên như nhau. Trong tiếng Anh chữ E được sử dụng nhiều nhất; sau đó đến các chữ T, R, N, I, O, A, S. Một số chữ rất ít dùng như: Z, J, K, Q, X. Bằng phương pháp thống kê, ta có thể xây dựng các bảng các tần suất các chữ đơn, cặp chữ, bộ ba chữ.



(Bảng tần suất chữ cái tiếng Anh)

Sử dụng bảng tần suất vào việc thám mã. Điều quan trọng là mã thế trên bảng chữ đơn không làm thay đổi tần suất tương đối của các chữ, có nghĩa là ta vẫn có bảng tần suất trên nhưng đối với bảng chữ mã tương ứng. Điều đó được phát hiện bởi các nhà khoa học Ai cập từ thế kỷ thứ 9. Do đó có cách thám mã trên bảng chữ đơn như sau:
- Tính toán tần suất của các chữ trong bản mã
- So sánh với các giá trị đã biết
- Tìm kiếm các chữ đơn hay dùng A-I-E, bộ đôi NO và bộ ba RST; và các bộ ít dùng JK, X-Z..
- Trên bảng chữ đơn cần xác định các chữ dùng các bảng bộ đôi và bộ ba trợ giúp.

Ví dụ. Thám mã bản mã trên bảng chữ đơn, cho bản mã:
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEP
OPDZSZUFPOUDTMOHMQ

- Tính tần suất các chữ
- Đoán P và Z là e và t.
- Khi đó ZW là th và ZWP là the.
- Suy luận tiếp tục ta có bản rõ:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives in moscow

* *Mã Playfair*

Như chúng ta đã thấy không phải số khoá lớn trong mã bảng chữ đơn đảm bảo an toàn mã. Một trong các hướng khắc phục là mã bộ các chữ, tức là mỗi chữ sẽ được mã bằng một số chữ khác nhau tùy thuộc vào các chữ mà nó đứng cạnh. Playfair là một trong các mã như vậy, được sáng tạo bởi Charles Wheastone vào năm 1854 và mang tên người bạn là Baron Playfair. Ở đây mỗi chữ có thể được mã bằng một trong 7 chữ khác nhau tùy vào chữ cặp đôi cùng nó trong bản rõ.

Ma trận khoá Playfair. Cho trước một từ làm khoá, với điều kiện trong từ khoá đó không có chữ cái nào bị lặp. Ta lập ma trận Playfair là ma trận cỡ 5 x 5 dựa trên từ khoá đã cho và gồm các chữ trên bảng chữ cái, được sắp xếp theo thứ tự như sau:

- Trước hết viết các chữ của từ khoá vào các hàng của ma trận bắt từ hàng thứ nhất.

- Nếu ma trận còn trống, viết các chữ khác trên bảng chữ cái chưa được sử dụng vào các ô còn lại. Có thể viết theo một trình tự qui ước trước, chẳng hạn từ đầu bảng chữ cái cho đến cuối.

- Vì có 26 chữ cái tiếng Anh, nên thiếu một ô. Thông thường ta dồn hai chữ nào đó vào một ô chung, chẳng hạn I và J.

- Giả sử sử dụng từ khoá MORNACHY. Lập ma trận khoá Playfair tương ứng như sau:

MONAR

CHYBD

EFGIK

LPQST

UVWXZ

Mã hoá và giải mã: bản rõ được mã hoá 2 chữ cùng một lúc theo qui tắc như sau:

- Chia bản rõ thành từng cặp chữ. Nếu một cặp nào đó có hai chữ như nhau, thì ta chèn thêm một chữ lọc chẳng hạn X. Ví dụ, trước khi mã **"balloon"** biến đổi thành **"ba lx lo on".**

- Nếu cả hai chữ trong cặp đều rơi vào cùng một hàng, thì mã mỗi chữ bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn "**ar"** biến đổi thành "RM"

- Nếu cả hai chữ trong cặp đều rơi vào cùng một cột, thì mã mỗi chữ bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn "**mu"** biến đổi thành "CM"

- Trong các trường hợp khác, mỗi chữ trong cặp được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó trong ma trận khóa. Chẳng hạn, **"hs"** mã thành **"BP"**, và **"ea"** mã thành **"IM"** hoặc **"JM"** (tuỳ theo sở thích)

An toàn của mã Playfair:

- An toàn được nâng cao so hơn với bảng đơn, vì ta có tổng cộng 26 x 26 = 676 cặp. Mỗi chữ có thể được mã bằng 7 chữ khác nhau, nên tần suất các chữ trên bản mã khác tần suất của các chữ cái trên văn bản tiếng Anh nói chung.

- Muốn sử dụng thống kê tần suất, cần phải có bảng tần suất của 676 cặp để thám mã (so với 26 của mã bảng đơn). Như vậy phải xem xét nhiều trường hợp hơn và tương ứng sẽ có thể có nhiều bản mã hơn cần lựa chọn. Do đó khó thám mã hơn mã trên bảng chữ đơn.

- Mã Playfair được sử dụng rộng rãi nhiều năm trong giới quân sự Mỹ và Anh trong chiến tranh thế giới thứ 1. Nó có thể bị bẻ khoá nếu cho trước vài trăm chữ, vì bản mã vẫn còn chứa nhiều cấu trúc của bản rõ.

* *Các mã đa bảng*

Một hướng khác làm tăng độ an toàn cho mã trên bảng chữ là sử dụng nhiều bảng chữ để mã. Ta sẽ gọi chúng là các mã thế đa bảng. Ở đây mỗi chữ có thể được mã bằng bất kỳ chữ nào trong bản mã tùy thuộc vào ngữ cảnh khi mã hoá. Làm như vậy để trải bằng tần suất các chữ xuất hiện trong bản mã. Do đó làm mất bớt cấu trúc của bản rõ được thể hiện trên bản mã và làm cho thám mã đa bảng khó hơn. Ta sử dụng từ khoá để chỉ rõ chọn bảng nào được dùng cho từng chữ trong bản tin. Sử dụng lần lượt các bảng theo từ khóa đó và lặp lại từ đầu sau khi kết thúc từ khoá. Độ dài khoá là chu kỳ lặp của các bảng chữ. Độ dài càng lớn và nhiều chữ khác nhau được sử dụng trong từ khoá thì càng khó thám mã.

* *Mã Vigenere*

Mã thế đa bảng đơn giản nhất là mã Vigenere. Thực chất quá trình mã hoá Vigenere là việc tiến hành đồng thời dùng nhiều mã Ceasar cùng một lúc trên bản rõ với nhiều khoá khác nhau. Khoá cho mỗi chữ dùng để mã phụ thuộc vào vị trí của chữ đó trong bản rõ và được lấy trong từ khoá theo thứ tự tương ứng.

Giả sử khoá là một chữ có độ dài d được viết dạng $K = K_1K_2\ldots K_d$, trong đó K_i nhận giá trị nguyên từ 0 đến 25. Khi đó ta chia bản rõ thành các khối gồm d chữ. Mỗi chữ thứ i trong khối chỉ định dùng bảng chữ thứ i với tịnh tiến là K_i giống như trong mã Ceasar. Trên thực tế khi mã ta có thể sử dụng lần lượt các bảng chữ và lặp lại từ đầu sau d chữ của bản rõ. Vì có nhiều bảng chữ khac nhau, nên cùng một chữ ở các vị trí khác nhau sẽ có các bước nhảy khác nhau, làm cho tần suất các chữ trong bản mã dãn tương đối đều.

Giải mã đơn giản là quá trình làm ngược lại. Nghĩa là dùng bản mã và từ khoá với các bảng chữ tương ứng, nhưng với mỗi chữ sử dụng bước nhảy lui lại về đầu.

Ví dụ: Để sử dụng mã Vigenere với từ khóa và bản rõ cho trước ta có thể làm như sau:

- Viết bản rõ ra
- Viết từ khoá lặp nhiều lần phía trên tương ứng của nó
- Sử dụng mỗi chữ của từ khoá như khoá của mã Ceasar
- Mã chữ tương ứng của bản rõ với bước nhảy tương ứng.
- Chẳng hạn sử dụng từ khoá deceptive

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext:ZICVTWQNGRZGVTWAVZHCQYGL

Để mã chữ w đầu tiên ta tìm chữ đầu của khóa là d, như vậy w sẽ được mã trên bảng chữ tịnh tiến 3 (tức là a tịnh tiến vào d). Do đó chữ đầu w được mã bởi chữ Z. Chữ thứ hai trong từ khóa là e, có nghĩa là chữ thứ hai trong bản rõ sẽ được tịnh tiến 4 (từ a tịnh tiến đến e). Như vậy thứ hai trong bản rõ e sẽ được mã bởi chữ I. Tương tự như vậy cho đến hết bản rõ.

Trên thực tế để hỗ trợ mã Vigenere, người ta đã tạo ra trang Saint – Cyr để trợ giúp cho việc mã và giải mã thủ công. Đó là một bảng cỡ 26 x 26 có tên tương ứng là các chữ cái trong bảng chữ tiếng Anh. Hàng thứ i là tịnh tiến i chữ của bảng chứ cái. Khi đó chữ ở cột đầu tiên chính là khoá của bảng chữ ở cùng hàng. Do đó chữ mã của một chữ trong bản rõ nằm trên cùng cột với chữ đó và nằm trên hàng tương ứng với chữ khoá.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
H HIJKLMNOPQRSTUVWXYZABCDEFG
I IJKLMNOPQRSTUVWXYZABCDEFGH
J JKLMNOPQRSTUVWXYZABCDEFGHI
K KLMNOPQRSTUVWXYZABCDEFGHIJ
L LMNOPQRSTUVWXYZABCDEFGHIJK
M MNOPQRSTUVWXYZABCDEFGHIJKL
N NOPQRSTUVWXYZABCDEFGHIJKLM
O OPQRSTUVWXYZABCDEFGHIJKLMN
P PQRSTUVWXYZABCDEFGHIJKLMNO
Q QRSTUVWXYZABCDEFGHIJKLMNOP
R RSTUVWXYZABCDEFGHIJKLMNOPQ
S STUVWXYZABCDEFGHIJKLMNOPQR
T TUVWXYZABCDEFGHIJKLMNOPQRS
U UVWXYZABCDEFGHIJKLMNOPQRST
V VWXYZABCDEFGHIJKLMNOPQRSTU
W WXYZABCDEFGHIJKLMNOPQRSTUV
X XYZABCDEFGHIJKLMNOPQRSTUVW
Y YZABCDEFGHIJKLMNOPQRSTUVWX
Z ZABCDEFGHIJKLMNOPQRSTUVWXY

(*Bảng Saint Cyr)*

An toàn của mã Vigenere. Như vậy có chữ mã khác nhau cho cùng một chữ của bản rõ. Suy ra tần suất của các chữ bị là phẳng, nghĩa là tần suất xuất hiện các chữ trên bản mã tương đối đều nhau**.** Tuy nhiên chưa mất hoàn toàn**,** do độ dài của khoá có hạn, nên có thể tạo nên chu kỳ vòng lặp. Kẻ thám mã bắt đầu từ tần suất của chữ để xem có phải đây là mã đơn bảng chữ hay không. Giả sử đây là mã đa bảng chữ, sau đó xác định số bảng chữ trong từ khoá và lần tìm từng chữ. Như vậy cần tăng độ dài từ khoá để tăng số bảng chữ dùng khi mã để "là" tần suất của các chữ.

***** *Mã Hill*

Tác giả mã này là Lester S. Hill năm 1929. Mã này cũng được thực hiện trên từng bộ m ký tự, mỗi ký tự trong bản mã là tổ hợp của m ký tự trong bản rõ. Cụ thể là tổ hợp tuyến tính này là một ma trận $k \in Z_{26}^{mxm}$. Để dịch ngược lại mã từ bản mã sang bản rõ, thì ma trận k phải có ma trận nghịch đảo, tức là khi và chỉ khi định thức của k, ký hiệu là det(k) nguyên tố cùng nhau với m.

Định nghĩa: Mã Hill là bộ năm (P, C, K, E, D) thỏa mãn:

1. $P = C = Z_{26}^m$, $K = \{k \in Z_{26}^{m \times m} : (det(k), m) = 1\}$,

2. Với mỗi $k \in K$, $e_k(x_1, x_2, ..., x_m) = (x_1, x_2, ..., x_m)k$,

$$d_k(y_1, y_2, ..., y_m) = (y_1, y_2, ..., y_m)\, k^{-1}$$

Ví dụ: $m = 2, k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}, k^{-1} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

$$(y_1, y_2) = e_k(x_1, x_2) = (x_1, x_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (11x_1 + 3x_2, 8x_1 + 7x_2),$$

$$(x_1, x_2) = d_k(y_1, y_2) = (y_1, y_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = (7x_1 + 23x_2, 18x_1 + 11x_2).$$

Nhận xét: Mã Hill tổng quát hơn mã Vigenère

* *Phương pháp thám mã Kasiski*

Phương pháp phát triển bởi Babbage và Kasiski. Ta thấy các chữ như nhau trên bản rõ và cách nhau một khoảng đúng bằng độ dài từ khoá (chu kỳ), thì sẽ được mã bằng cùng một chữ. Như vậy từ độ lặp của các chữ trong bản mã có thể cho phép xác định chu kỳ. Tất nhiên không phải khi nào cũng tìm được độ dài từ khoá. Sau đó tìm các chữ trong từ khoá bằng cách tấn công từng bảng chữ đơn với cùng kỹ thuật dựa trên các bảng tần suất của các bộ chữ như trước.

4.2.2. Các mã thế cổ điển hoán vị

Trong các mục trước chúng ta đã xét một số mã thay thế, ở đó các chữ của bản rõ được thay thế bằng các chữ khác của bản mã. Bây giờ chúng ta xét đến loại mã khác, mã hoán vị, các chữ trong bản rõ không được thay thế bằng các chữ khác mà chỉ thay đổi vị trí, tức là việc mã hoá chỉ dịch chuyển vị trí tương đối giữa các chữ trong bản rõ. Như vậy, nó dấu bản rõ bằng cách thay đổi thứ tự các chữ, nó không thay đổi các chữ thực tế được dùng. Do đó bản mã có cùng phân bố tần suất xuất hiện các chữ như bản gốc. Như vậy có thể thám mã để phát hiện được.

* *Mã Rail Fence*

Đây là mã hoán vị đơn giản. Viết các chữ của bản rõ theo đường chéo trên một số dòng. Sau đó đọc các chữ theo theo từng dòng sẽ nhận được bản mã. Số dòng chính là khoá của mã. Vì khi biết số dòng ta sẽ tính được số chữ trên mỗi dòng và lại viết bản mã theo các dòng sau đó lấy bản rõ bằng cách viết lại theo các cột.

Ví dụ. Viết bản tin "meet me after the toga party" lần lượt trên hai dòng như sau:

m e m a t r h t g p r y

e t e f e t e o a a t

Sau đó ghép các chữ ở dòng thứ nhất với các chữ ở dòng thứ hai cho bản mã:

MEMATRHTGPRYETEFETEOAAT

* *Mã dịch chuyển vòng*

Mã có sơ đồ phức tạp hơn. Viết các chữ của bản tin theo các dòng với số cột xác định. Sau đó thay đổi thứ tự các cột theo một dãy số khoá cho trước, rồi đọc lại chúng theo các cột để nhận được bản mã. Quá trình giải mã được thực hiện ngược lại.

Ví dụ:

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ta đọc theo thứ tự các cột từ 1 đến 7 để nhận được bản mã:

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

* *Mã tích*

Mã dùng hoán vị hoặc dịch chuyển không an toàn vì các đặc trưng tần xuất của ngôn ngữ không thay đổi. Có thể sử dụng một số mã liên tiếp nhau sẽ làm cho mã khó hơn. Mã cổ điển chỉ sử dụng một trong hai phương pháp thay thế hoặc hoán vị. Người ta nghĩ đến việc kết hợp cả hai phương pháp này trong cùng một mã và có thể sử dụng đan xen hoặc lặp nhiều vòng. Đôi khi ta tưởng lặp nhiều lần cùng một loại mã sẽ tạo nên mã phức tạp hơn, nhưng trên thực tế trong một số trường hợp về bản chất chúng cũng tương đương với một lần mã cùng loại nào đó như: tích của hai phép thế sẽ là một phép thế; tích của hai phép hoán vị sẽ là một phép hoán vị. Nhưng nếu hai loại mã đó khác nhau thì sẽ tạo nên mã mới

phức tạp hơn, chính vì vậy phép thế được nối tiếp bằng phép dịch chuyển sẽ tạo nên mã mới khó hơn rất nhiều. Đây chính là chiếc cầu nối từ mã cổ điển sang mã hiện đại.

4.2.3. Phương pháp XOR

Phương pháp mã hóa XOR sử dụng phép toán logic XOR để tạo bản mã, trong đó từng bit của bản rõ được XOR với bit tương ứng của khóa. Để giải mã, ta thực hiện XOR từng bit của bản mã với bit tương ứng của khóa. Hình ảnh minh họa quá trình mã hóa bản rõ "CAT" với khóa "VVV". Theo đó, các ký tự của bản rõ và khóa được chuyển thành mã ASCII và biểu diễn dưới dạng nhị phân. Sau đó, thực hiện phép toán XOR trên các bit tương ứng của bản rõ và khóa để tạo bản mã (Cipher).

Text Value	Binary Value
CAT as bits	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 0
VVV as key	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Cipher	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0

(Mã hóa bằng phương pháp XOR)

4.2.4. Phương pháp Vernam

Phương pháp Vernam sử dụng một tập ký tự để nối vào các ký tự của bản rõ để tạo bản mã. Tập ký tự này được gọi là one-time pad và mỗi ký tự trong tập chỉ dùng 1 lần trong một tiến trình mã hóa. Với bộ chữ tiếng Anh có 26 chữ, mã hóa bằng phương pháp Vernam được thực hiện như sau:

- Các ký tự của bản rõ và các ký tự của tập nối thêm (one-time pad) được chuyển thành số trong khoảng 1-26;

- Cộng giá trị của ký tự trong bản rõ với giá trị tương ứng trong tập nối thêm;

- Nếu giá trị cộng lớn hơn 26 thì đem trừ cho 26 (đây chính là phép modulo - chia lấy phần dư).

- Chuyển giá trị số thành ký tự mã.

Plaintext:	s	A	c	K	G	A	u	L	s	p	A	R	E	N	o	o	N	E	
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05	
One-time pad text:	F	p	Q	R	N	s	B	I	E	H	T	z	L	A	c	D	G	J	
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10	
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15	
After modulo Subtraction:							03									18			
Ciphertext:	YQTCUTWUXXURQORSUO																		

(Mã hóa bằng phương pháp Vernam)

4.2.5. Phương pháp sách hoặc khóa chạy

Phương pháp sách, hoặc khóa chạy thực hiện việc mã hóa và giải mã sử dụng các khóa mã chứa trong các cuốn sách. Hiện nay phương pháp này thường được dùng trong các bộ phim trinh thám do tính chất kỳ bí của nó. Ví dụ như, với bản mã "259,19,8; 22,3,8; 375,7,4; 394,17,2" và cuốn sách được dùng chứa khóa là "A Fire Up on the Deep", ta có thể giải mã như sau:

- Trang 259, dòng 19, từ thứ 8 là sack
- Trang 22, dòng 3, từ thứ 8 là island
- Trang 375, dòng 7, từ thứ 4 là sharp
- Trang 394, dòng 17, từ thứ 2 là path

Bản rõ tương ứng của bản mã "259,19,8;22,3,8;375,7,4;394,17,2" là "sack island sharp path".

4.2.6. Phương pháp hàm băm

Các hàm băm (Hash functions) là các giải thuật để tạo các bản tóm tắt (digest) của thông điệp, thường được sử dụng để nhận dạng và đảm bảo tính toàn vẹn của thông điệp. Độ dài của thông điệp đầu vào là bất kỳ, nhưng đầu ra hàm băm thường có độ dài cố định. Chi tiết về các hàm băm được ở mục 4.4. Các hàm băm thông dụng gồm:

- Các hàm băm MD2, MD4, MD5 với độ dài chuỗi đầu ra là 128 bit;
- Hàm băm MD6 cho chuỗi đầu ra có độ dài trong khoảng 0 đến 512 bit;
- Các hàm băm SHA0, SHA1 với độ dài chuỗi đầu ra là 160 bit;
- Các hàm băm SHA2, gồm SHA256, SHA384, SHA512 cho phép một số lựa chọn chuỗi đầu ra tương ứng 256, 384 và 512 bit;
- Hàm băm SHA3 cho chuỗi đầu ra có độ dài trong khoảng 0 đến 512 bit;
- Hàm băm CRC32 với chuỗi đầu ra 32 bit sử dụng trong kiểm tra dư thừa mạch vòng.

❖ TÓM TẮT CHƯƠNG 4

Trong chương này, một số nội dung chính được giới thiệu:

- **Mã Hóa Thông Tin**: Chương này giới thiệu về mã hóa thông tin, bao gồm mã hóa đối xứng và mã hóa bất đối xứng.
- **Loại Hình Mã Hóa**: Chương này trình bày các loại hình mã hóa thông tin, bao gồm mã hóa dữ liệu trong truyền thông mạng, mã hóa ổ cứng, và mã hóa email.

- **Mã Hóa và Bảo Mật Thông Tin**: Chương này giải thích vai trò của mã hóa trong bảo mật thông tin và cách nó giúp ngăn chặn truy cập trái phép vào dữ liệu quan trọng.
- **Quy Định và Tuân Thủ**: Chương này trình bày về các quy định và tiêu chuẩn liên quan đến việc sử dụng mã hóa trong lĩnh vực an toàn thông tin và tại sao tuân thủ quy định này là quan trọng.

❖ CÁC BÀI TẬP HỆ THỐNG KIẾN THỨC

1) Mã hóa thông tin là gì? Nêu vai trò của mã hóa.
2) Mô tả các thành phần của một hệ mã hóa.
3) Mô tả các phương pháp mã hóa dòng và mã hóa khối.
4) Nêu các ứng dụng của mã hóa.
5) Mô tả phương pháp mã hóa thay thế (substitution).
6) Mô tả phương pháp mã hóa hoán vị (permutation).
7) Mô tả phương pháp mã hóa XOR.
8) Mô tả phương pháp mã hóa Vernam.
9) Mô tả phương pháp mã hóa Playfair.
10) Mô tả phương pháp mã hóa Vigenere

CHƯƠNG 5. CÁC KỸ THUẬT VÀ CÔNG NGHỆ ĐẢM BẢO AN TOÀN THÔNG TIN

❖ GIỚI THIỆU CHƯƠNG 5

Chương 5 của môn học "An Toàn Hệ Thống Thông Tin" tập trung vào việc tìm hiểu về các kỹ thuật và công nghệ được sử dụng để đảm bảo an toàn thông tin trong môi trường số hóa. Chương này giúp học viên hiểu về các công nghệ bảo mật, phương pháp xác thực và kiểm soát truy cập, cũng như cách triển khai các biện pháp bảo mật hiệu quả để bảo vệ thông tin và hệ thống thông tin.

❖ MỤC TIÊU CHƯƠNG 5

Sau khi học xong chương này, người học có khả năng:

➢ ***Về kiến thức:***

- *Hiểu các công nghệ bảo mật như tường lửa, mã hóa, kiểm soát truy cập, và phần mềm chống vi-rút.*
- *Hiểu cách thực hiện xác thực người dùng và kiểm soát quyền truy cập để đảm bảo chỉ người dùng được ủy quyền có thể truy cập thông tin quan trọng.*
- *Hiểu về các công nghệ đảm bảo dữ liệu như sao lưu, khôi phục, và giám sát dữ liệu.*
- *Biết cách triển khai các biện pháp bảo mật trong môi trường thực tế, bao gồm việc xây dựng tường lửa, cấu hình mã hóa, và quản lý quyền truy cập.*

➢ ***Về kỹ năng:***

- *Hiểu Biết về Công Nghệ Bảo Mật: Học viên sẽ nắm vững kiến thức về các công nghệ bảo mật như tường lửa, mã hóa, kiểm soát truy cập, và phần mềm chống vi-rút.*
- *Kỹ năng triển khai các công nghệ bảo mật như tường lửa, mã hóa, và phần mềm chống vi-rút trong môi trường hệ thống thông tin.*
- *Kỹ năng xác thực và kiểm soát quyền truy cập bằng cách cấu hình hệ thống để đảm bảo chỉ người dùng được ủy quyền có thể truy cập thông tin quan trọng.*
- *Kỹ năng bảo vệ dữ liệu bằng cách thực hiện các biện pháp như sao lưu, khôi phục, và giám sát dữ liệu một cách hiệu quả.*

➢ ***Về năng lực tự chủ và trách nhiệm:***

- *Năng lực về quản lý thời gian, trách nhiệm với công việc*
- *Năng lực học tập và làm việc độc lập*
- *Tự chủ trong việc giải quyết vấn đề*

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP CHƯƠNG 5

- *Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, dạy học theo vấn đề); yêu cầu người học thực hiện câu hỏi thảo luận và bài tập chương (cá nhân hoặc nhóm).*
- *Đối với người học: chủ động đọc trước giáo trình trước buổi học; hoàn thành đầy đủ câu hỏi thảo luận và bài tập tình huống chương 1 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.*

❖ **ĐIỀU KIỆN THỰC HIỆN CHƯƠNG 5**

- ***Phòng học chuyên môn hóa/nhà xưởng:*** Phòng học thực hành
- ***Trang thiết bị máy móc:*** Máy chiếu, máy tính và các thiết bị dạy học khác
- ***Học liệu, dụng cụ, nguyên vật liệu:*** Chương trình môn học, giáo trình, tài liệu tham khảo, giáo án, phim ảnh, và các tài liệu liên quan.
- ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ CHƯƠNG 5**

- **Nội dung:**

✓ *Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức*

✓ *Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.*

✓ *Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:*

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ ***Điểm kiểm tra thường xuyên:*** *1 điểm kiểm tra (hình thức: hỏi miệng)*

✓ ***Kiểm tra định kỳ lý thuyết:*** *không có*

❖ **NỘI DUNG CHƯƠNG 1**

5.1. Điều khiển truy nhập

5.1.1. Khái niệm điều khiển truy nhập

Điều khiển truy nhập (Access control) 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 (Authentication), Trao quyền, hoặc cấp quyền (Authorization) và Quản trị (Administration).

Xác thực là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người

dùng cung cấp. Đây là khâu đầu tiên cần thực hiện trong một hệ thống điều khiển truy nhập. Cần nhớ rằng, xác thực chỉ có khả năng khẳng định các thông tin nhận dạng mà người dùng cung cấp tồn tại trong hệ thống mà thường không thể xác minh chủ thể thực sự của thông tin đó. Sau khi người dùng đã được xác thực, trao quyền xác định các tài nguyên mà người dùng được phép truy nhập dựa trên chính sách quản trị tài nguyên của cơ quan, tổ chức và vai trò của người dùng trong hệ thống.

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. Mặc dù quản trị không trực tiếp tham gia vào quá trình xác thực và trao quyền cho người dùng, quản trị là dịch vụ không thể thiếu trong một hệ thống điều khiển truy nhập.

Mục đích chính của điều khiển truy nhập là để đảm bảo tính bí mật, toàn vẹn và sẵn dùng hoặc khả dụng của thông tin, hệ thống và các tài nguyên. Đây cũng là các yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin đã đề cập trong Chương 1.

5.1.2. Các biện pháp điều khiển truy nhập

Các biện pháp hay cơ chế (mechanism) điều khiển truy nhập là các phương pháp thực hiện điều khiển truy nhập, gồm 4 loại chính: Điều khiển truy nhập tuỳ chọn - Discretionary Access Control (DAC), Điều khiển truy nhập bắt buộc - Mandatory Access Control (MAC), Điều khiển truy nhập dựa trên vai trò - Role-Based Access Control (RBAC) và Điều khiển truy nhập dựa trên luật - Rule-Based Access Control.

* *Điều khiển truy nhập tùy chọn*

Điều khiển truy nhập tuỳ chọn (còn gọi là tùy quyền) được định nghĩa 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 (còn gọi là các nhân tố - factor) 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, ...)

Đặc điểm nổi bật của điều khiển truy nhập tuỳ chọn là cơ chế này cho phép người dùng có thể cấp hoặc huỷ quyền truy nhập cho các người dùng khác đến các đối tượng thuộc quyền điều khiển của họ. Điều này cũng có nghĩa là chủ sở hữu của các đối tượng (owner of objects) là người có toàn quyền điều khiển các đối tượng này. Chẳng hạn, trong một hệ thống nhiều người dùng, mỗi người dùng được cấp 1 thư mục riêng (home directory) và là chủ sở hữu của thư mục này. Người dùng có quyền tạo, sửa đổi và xoá các file trong thư mục của riêng mình. Người dùng cũng có khả năng cấp hoặc huỷ quyền truy nhập vào các file của mình cho các người dùng khác.

Có nhiều kỹ thuật thực hiện cơ chế điều khiển truy nhập tuỳ chọn trên thực tế, trong đó 2 kỹ thuật được sử dụng rộng rãi nhất là Ma trận điều khiển truy nhập (Access Control

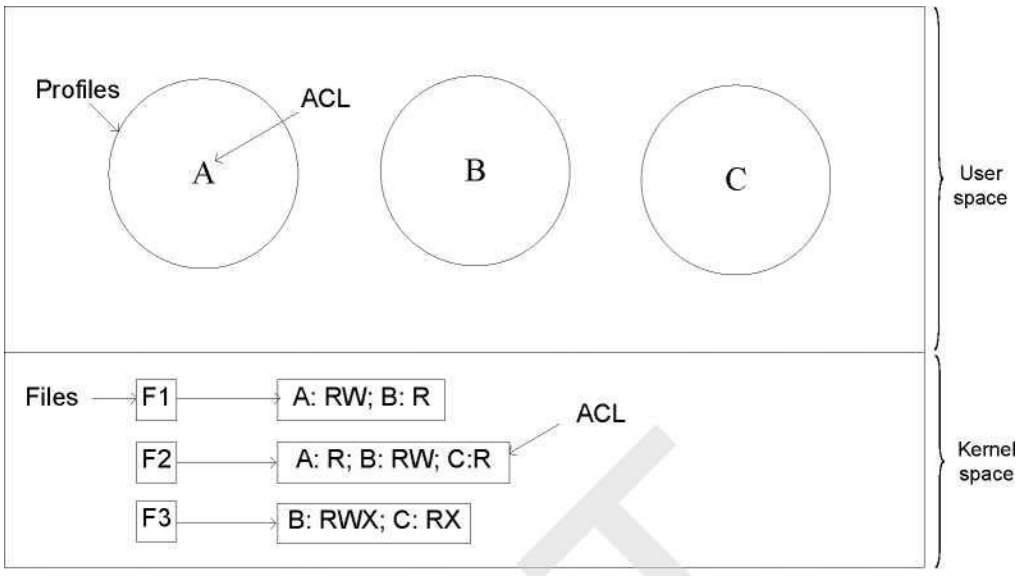
Matrix - ACM) và Danh sách điều khiển truy nhập (Access Control List - ACL). Ma trận điều khiển truy nhập là một phương pháp thực hiện điều khiển truy nhập thông qua 1 ma trận 2 chiều gồm chủ thể (subject), đối tượng (object) và các quyền truy nhập, như biểu diễn trên Hình 5.1. Các đối tượng, hay khách thể (Objects) là các thực thể cần bảo vệ, được ký hiệu là O1, O2, O3, Các đối tượng có thể là các file, các thư mục hay các tiến trình (process). Các chủ thể (Subjects) là người dùng (users), hoặc các tiến trình tác động lên các đối tượng, được ký hiệu là S1, S2, S3,... Quyền truy nhập là hành động mà chủ thể thực hiện trên đối tượng. Các quyền bao gồm r (read - đọc), w (write - ghi), x (execute - thực hiện) và o (own - chủ sở hữu).

Objects / Subjects	O1	O2	O3	O4
S1	rw	rwxo	r	rwxo
S2	rw	rx	rw	rwx
S3	r	rw	rwo	rw

(Mô hình ma trận điều khiển truy nhập)

Ưu điểm của ma trận điều khiển truy nhập là đơn giản, trực quan, dễ sử dụng. Tuy nhiên, khi số lượng các đối tượng và số lượng các chủ thể lớn, kích thước của ma trận sẽ rất lớn. Hơn nữa, quyền truy nhập của các chủ thể vào các đối tượng là khác nhau, trong đó một số chủ thể không có quyền truy nhập vào một số đối tượng, và như vậy ô nhớ chứa quyền truy nhập của chủ thể vào đối tượng là rỗng. Trong ma trận điều khiển truy nhập có thể tồn tại rất nhiều ô rỗng và điều này làm giảm hiệu quả sử dụng bộ nhớ của phương pháp này. Do vậy, ma trận điều khiển truy nhập ít được sử dụng hiện nay trên thực tế.

Danh sách điều khiển truy nhập (ACL) là một danh sách các quyền truy nhập của một chủ thể đối với một đối tượng. Một danh sách điều khiển truy nhập chỉ ra các người dùng hoặc tiến trình được truy nhập vào đối tượng nào và các thao tác cụ thể (hay quyền) được thực hiện trên đối tượng đó. Một bản ghi điển hình của ACL có dạng (subject, operation). Ví dụ bản ghi (Alice, write) của 1 file có nghĩa là Alice có quyền ghi vào file đó. Khi chủ thể yêu cầu truy nhập, hệ điều hành sẽ kiểm tra ACL xem yêu cầu đó có được phép hay không. ACL có thể được áp dụng cho một hoặc 1 nhóm đối tượng.



(Mô hình danh sách điều khiển truy nhập)

Hình mô hình danh sách điều khiển truy nhập trong không gian người dùng (user space) và không gian nhân (kernel space) tổ chức bởi hệ điều hành. Mỗi file (F1, F2, F3,...) có một danh sách điều khiển truy nhập (ACL) của riêng mình lưu trong hồ sơ (profile) của file. Quyền truy nhập vào file được tổ chức thành một chuỗi gồm nhiều cặp (subject, operation), với A, B, C là ký hiệu biểu diễn chủ thể (subject) và các thao tác (operation) hay quyền gồm R (Read - đọc), W (Write - ghi), và X (eXecute - thực hiện). Chẳng hạn, trong danh sách điều khiển truy nhập F1(A: RW; B: R) thì chủ thể A được quyền đọc (R) và ghi (W) đối với F1, còn chủ thể B chỉ có quyền đọc (R).

** Điều khiển truy nhập bắt buộc*

Điều khiển truy bắt buộc (MAC) được định nghĩa là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên hai yếu tố chính:

- Tính nhạy cảm (sensitivity) của thông tin chứa trong các đối tượng, và
- Sự trao quyền chính thức (formal authorization) cho các chủ thể truy nhập các thông tin nhạy cảm này.

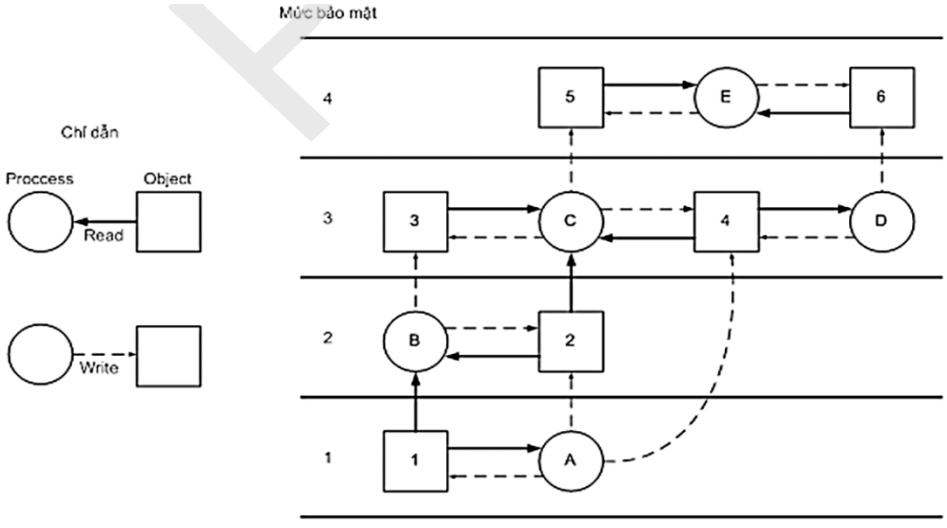
Các thông tin nhạy cảm thường được gán nhãn với các mức nhạy cảm (Sensitivity level). Có nhiều phương pháp phân chia các mức nhạy cảm của các thông tin tùy thuộc vào chính sách an toàn thông tin của các cơ quan, tổ chức. Các mức nhạy cảm thường được sử dụng gồm:

- Tối mật (Top Secret - T): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến những thiệt hại trầm trọng đối với an ninh quốc gia.
- Tuyệt mật (Secret - S): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến một loạt thiệt hại đối với an ninh quốc gia.
- Mật (Confidential - C): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến thiệt hại đối với an ninh quốc gia.
- Không phân loại (Unclassified - U): Những thông tin không gây thiệt hại đối với an

ninh quốc gia nếu bị tiết lộ.

Đặc điểm nổi bật của cơ chế điều khiển truy nhập bắt buộc là nó không cho phép người tạo ra các đối tượng (thông tin, hoặc tài nguyên) có toàn quyền truy nhập các đối tượng này. Quyền truy nhập đến các đối tượng do người quản trị hệ thống định ra trước trên cơ sở chính sách an toàn thông tin của tổ chức đó. Đây cũng là điểm khác biệt hoàn toàn với cơ chế điều khiển truy nhập tùy chọn, trong đó người tạo ra các đối tượng là chủ sở hữu và có toàn quyền đối với các đối tượng họ tạo ra. Ví dụ như, một tài liệu được tạo ra và được đóng dấu "Mật" thì chỉ những người có trách nhiệm trong cơ quan, tổ chức mới được quyền xem và phổ biến cho người khác, còn bản thân tác giả của tài liệu không được quyền phổ biến đến người khác. Cơ chế điều khiển truy nhập bắt buộc thường được sử dụng phổ biến trong các cơ quan an ninh, quân đội và ngân hàng.

Có nhiều kỹ thuật thực hiện cơ chế điều khiển truy nhập bắt buộc, trong đó mô hình điều khiển truy nhập Bell-LaPadula là một trong các kỹ thuật được sử dụng rộng rãi nhất. Mô hình Bell-LaPadula là mô hình bảo mật đa cấp thường được sử dụng trong quân sự, nhưng nó cũng có thể áp dụng cho các lĩnh vực khác. Theo mô hình này trong quân sự, các tài liệu được gán một mức độ bảo mật, chẳng hạn như không phân loại, mật, bí mật và tối mật. Người dùng cũng được ấn định các cấp độ bảo mật, tùy thuộc vào những tài liệu mà họ được phép xem. Chẳng hạn, một vị tướng quân đội có thể được phép xem tất cả các tài liệu, trong khi một trung úy có thể bị hạn chế chỉ được xem các tài liệu mật và thấp hơn. Đồng thời, một tiến trình chạy nhân danh một người sử dụng có được mức độ bảo mật của người dùng đó.



(Mô hình điều khiển truy nhập Bell-LaPadula)

Mô hình Bell-LaPadula sử dụng nguyên tắc "đọc xuống" (read down) và nguyên tắc "ghi lên" (write up) để đảm bảo an toàn trong việc cấp quyền truy nhập cho người dùng đến các đối tượng. Với nguyên tắc "đọc xuống", một người dùng ở mức độ bảo mật k chỉ có thể đọc các đối tượng ở cùng mức bảo mật hoặc thấp hơn. Ví dụ, một vị tướng

có thể đọc các tài liệu của một trung úy, nhưng một trung úy không thể đọc các tài liệu của vị tướng đó. Ngược lại, nguyên tắc "ghi lên" quy định, một người dùng ở mức độ bảo mật k chỉ có thể ghi các đối tượng ở cùng mức bảo mật hoặc cao hơn. Ví dụ, một trung úy có thể nối thêm một tin nhắn vào hộp thư của chung của đơn vị về tất cả mọi thứ ông biết, nhưng một vị tướng không thể ghi thêm một tin nhắn vào hộp thư của trung úy với tất cả mọi thứ ông ấy biết vì vị tướng có thể đã nhìn thấy các tài liệu có mức bảo mật cao mà không thể được tiết lộ cho một trung úy.

Hình ảnh minh họa việc thực hiện các nguyên tắc "đọc xuống" và nguyên tắc "ghi lên" trong mô hình Bell-LaPadula. Trong đó, các tiến trình chạy bởi người dùng (Process) được ký hiệu A, B, C, D, E được biểu diễn bởi các hình tròn và các đối tượng (Object) được đánh số 1, 2, 3, 4, 5. Mũi tên liền nét biểu diễn quyền đọc (Read), mũi tên đứt nét biểu diễn quyền ghi (Write) và các mức bảo mật cho cả tiến trình và đối tượng được đánh số 1, 2, 3, 4. Theo mô hình này, tiến trình B có mức bảo mật là 2 chỉ được phép đọc các đối tượng số 1 và 2 - là các đối tượng có cùng mức bảo mật và thấp hơn 2. B không được phép đọc đối tượng số 3 do đối tượng này có mức bảo mật cao hơn. Ngược lại, B có quyền ghi các đối tượng số 2 và 3 - là các đối tượng có cùng mức bảo mật và cao hơn 2. Tuy nhiên, B không được phép ghi đối tượng số 1 do đối tượng này có mức bảo mật thấp hơn.

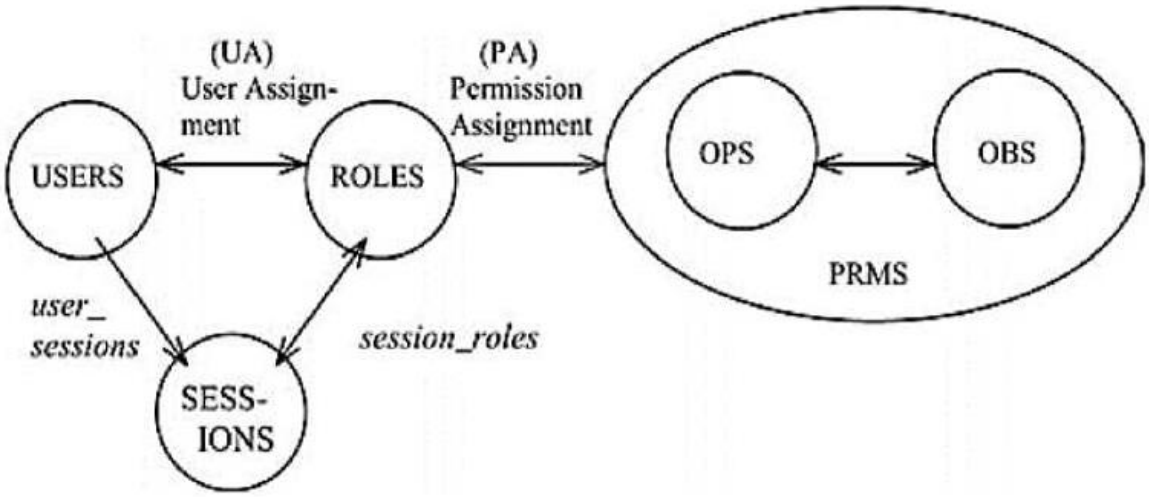
* *Điều khiển truy nhập dựa trên vai trò*

Điều khiển truy nhập dựa trên vai trò (RBAC) cho phép người dùng truy nhập vào hệ thống và thông tin dựa trên vai trò (role) của họ trong cơ quan, tổ chức đó. Điều khiển truy nhập dựa trên vai trò có thể được áp dụng cho một nhóm người dùng hoặc từng người dùng riêng lẻ. Quyền truy nhập vào các đối tượng trong hệ thống được tập hợp thành các nhóm "vai trò" với các mức quyền truy nhập khác nhau. Các vai trò được tổ chức thành một cây theo mô hình phân cấp tự nhiên của các cơ quan, tổ chức. Ví dụ như, hệ thống thông tin trong một trường học chia người dùng thành các nhóm gán sẵn quyền truy nhập vào các phần trong hệ thống như sau:

- Nhóm Quản lý được quyền truy nhập vào tất cả các thông tin trong hệ thống;
- Nhóm Giáo viên được truy nhập vào cơ sở dữ liệu các môn học, bài báo khoa học, cập nhật điểm các lớp do mỗi giáo viên phụ trách;
- Nhóm Sinh viên chỉ được quyền xem nội dung các môn học, tải tài liệu học tập và xem điểm của mình.

Việc liên kết giữa người dùng và nhóm vai trò có thể được tạo lập và huỷ bỏ dễ dàng và được thực hiện theo nguyên tắc: Người dùng được cấp "thẻ thành viên" của các nhóm "vai trò" trên cơ sở năng lực và vai trò, cũng như trách nhiệm của họ trong một tổ chức. Trong nhóm "vai trò", người dùng được cấp vừa đủ quyền để thực hiện các thao tác cần thiết cho công việc được giao. Hình 5.4 minh họa một mô hình RBAC đơn

giản, trong đó quyền truy nhập vào các đối tượng (PRMS) được tập hợp thành các nhóm vai trò (Roles) và việc cấp quyền truy nhập các đối tượng cho người dùng (Users) được thực hiện thông qua thao tác gán quyền (UA - User Assignment). Việc cấp quyền truy nhập các đối tượng cho người dùng có thể có hiệu lực trong dài hạn, hoặc cũng có thể có hiệu lực trong ngắn hạn, như theo phiên làm việc (Session).



(Một mô hình RBAC đơn giản)

* Điều khiển truy nhập dựa trên luật

Điều khiển truy nhập dựa trên luật (Rule-based Access Control) là cơ chế cho phép người dùng truy nhập vào hệ thống và thông tin dựa trên các luật (rules) 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 tường lửa (firewalls), hoặc proxies là ví dụ điển hình về việc thực hiện cơ chế điều khiển truy nhập dựa trên luật. 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.

5.1.3. Một số công nghệ điều khiển truy nhập

Mục này trình bày một số công nghệ điều khiển truy nhập được ứng dụng rộng rãi trên thực tế. Các công nghệ điều khiển truy nhập được đề cập gồm:

- Điều khiển truy nhập dựa trên mật khẩu (password)
- Điều khiển truy nhập dựa trên các khoá mã (encrypted keys)
- Điều khiển truy nhập dựa trên thẻ thông minh (smartcard)
- Điều khiển truy nhập dựa trên thẻ bài (token)
- Điều khiển truy nhập dựa trên các đặc điểm sinh trắc (biometric).

** Điều khiển truy nhập dựa trên mật khẩu*

Điều khiển truy nhập dựa trên mật khẩu là công nghệ điều khiển truy nhập được sử dụng từ lâu và vẫn đang được sử dụng rộng rãi do tính dễ dùng và rẻ tiền. Thông thường, mỗi người dùng được cấp 1 tài khoản (account) để truy nhập vào hệ thống. Mỗi tài khoản người dùng thường gồm 2 thành tố: tên người dùng (username) và mật khẩu (password), trong đó mật khẩu cần được giữ bí mật. Trong một số hệ thống, tên người dùng có thể được thay thế bằng địa chỉ email, số điện thoại,... Mật khẩu có thể lưu trong hệ thống ở dạng rõ (plaintext) hoặc dạng mã hóa (encrypted text - thường dưới dạng giá trị băm).

Tính bảo mật của điều khiển truy nhập sử dụng mật khẩu dựa trên 2 yếu tố: (1) độ khó đoán của mật khẩu và (2) tuổi thọ của mật khẩu. Độ khó đoán của mật khẩu lại phụ thuộc vào số bộ ký tự sử dụng trong mật khẩu và độ dài của mật khẩu. Nhìn chung, mật khẩu càng an toàn nếu càng nhiều bộ ký tự được sử dụng và có kích thước đủ lớn. Với các tài khoản của ứng dụng thông thường, khuyến nghị nên sử dụng cả ký tự in thường, ký tự in hoa, chữ số và ký tự đặc biệt trong mật khẩu với độ dài từ 8 ký tự trở lên. Theo tuổi thọ, mật khẩu gồm 3 loại: không hết hạn, có thời hạn sống và mật khẩu sử dụng 1 lần. Để đảm bảo an toàn, khuyến nghị định kỳ đổi mật khẩu. Khoảng thời gian sống của mật khẩu có thể được thiết lập từ 3 tháng đến 6 tháng phụ thuộc chính sách an toàn thông tin của cơ quan, tổ chức.

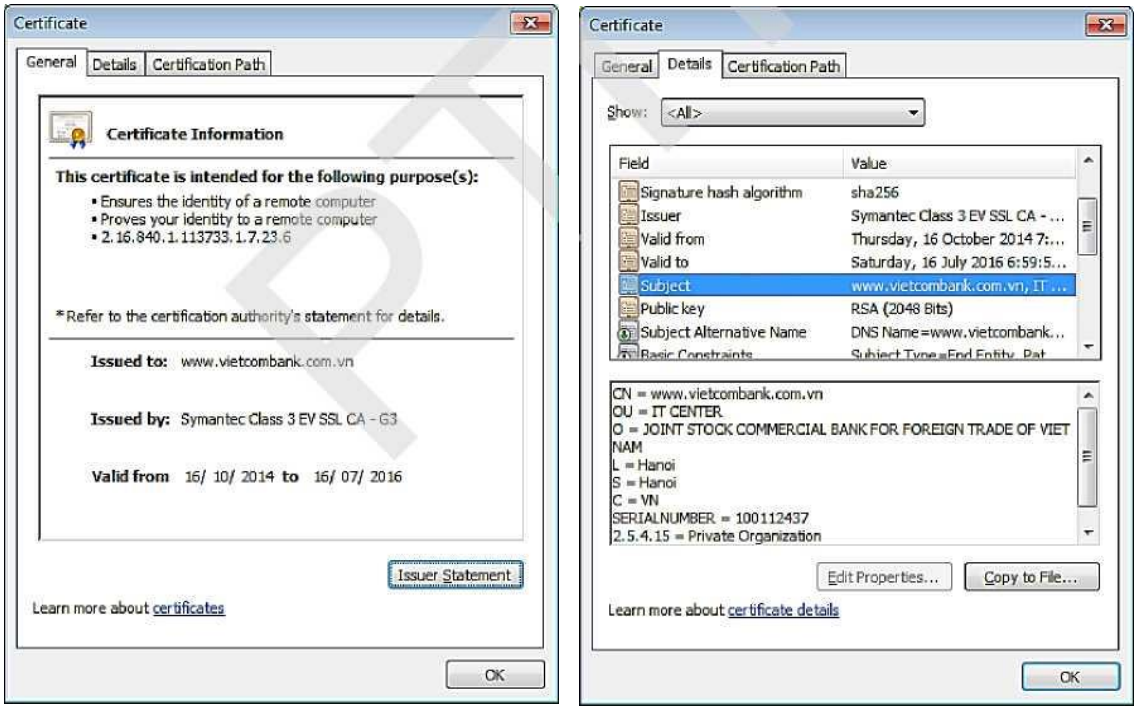
Nhìn chung, điều khiển truy nhập dựa trên mật khẩu có độ an toàn thấp do người dùng có xu hướng chọn các từ đơn giản, dễ nhớ làm mật khẩu. Ngoài ra, mật khẩu có thể bị nghe lén khi được truyền trên môi trường mạng mở như Internet. Do vậy, để đảm bảo an toàn, cần có chính sách quản lý tài khoản và sử dụng mật khẩu phù hợp với từng hệ thống cụ thể.

** Điều khiển truy nhập dựa trên các khoá mã*

Điều khiển truy nhập dựa trên các khoá mã cho phép đảm bảo tính bí mật của thông tin và đồng thời cho phép kiểm tra thông tin nhận dạng của các bên tham gia giao dịch. Một trong các ứng dụng rộng rãi nhất của khóa mã là chứng chỉ số khóa công khai (Public Key Digital Certificate). Một chứng chỉ số khóa công khai thường gồm 3 thông tin quan trọng nhất:

- Thông tin nhận dạng của chủ thể (Subject);
- Khoá công khai của chủ thể (Public key);
- Chữ ký số của nhà cung cấp chứng chỉ số (Certificate Authority - CA).

Hình ảnh dưới đây là giao diện của một chứng chỉ số khóa công khai cấp cho tên miền www.vietcombank.com.vn. Chứng chỉ số khóa công khai có thể được sử dụng để xác thực các thực thể tham gia phiên truyền thông, đồng thời hỗ trợ trao đổi khóa cho các khâu mã hóa - giải mã thông điệp, nhằm đảm bảo tính bí mật thông điệp truyền.

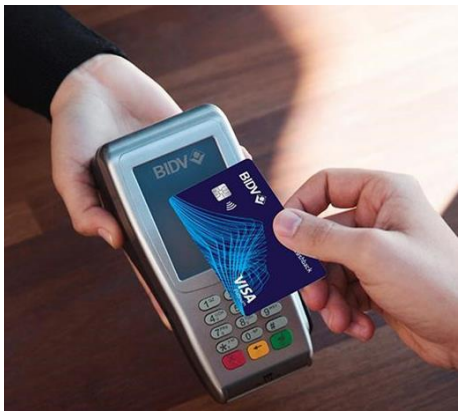


(iao diện của một chứng chỉ số khóa công khai)

* *Điều khiển truy nhập dựa trên thẻ thông minh*

Thẻ thông minh (Smartcard) là các thẻ nhựa có gắn các chip điện tử với khả năng tính toán và các thông tin lưu trong thẻ được mã hoá. Điều khiển truy nhập dựa trên thẻ thông minh là phương pháp có độ an toàn cao do smartcard sử dụng hai nhân tố (two-factors) để xác thực và nhận dạng chủ thể: (1) cái bạn có (what you have) - thẻ smartcard và (2) cái bạn biết (what you know) - số PIN. Hình (a) là hình ảnh thẻ thông minh tiếp xúc và (b) thẻ thông minh không tiếp xúc.

(a)



(b)

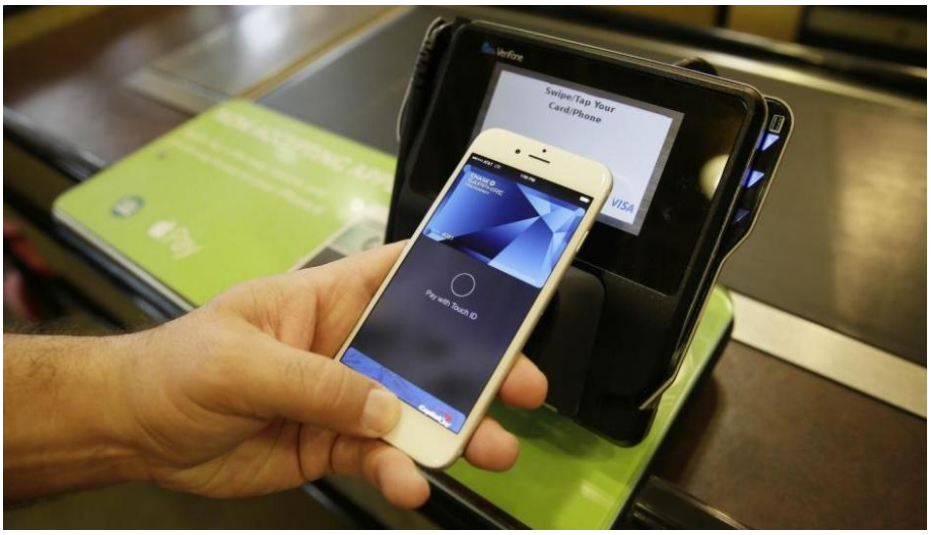
* *Điều khiển truy nhập dựa trên thẻ bài*

Các thẻ bài thường là các thiết bị cầm tay được thiết kế nhỏ gọn để có thể dễ dàng mang theo. Khác với thẻ thông minh, thẻ bài được tích hợp pin cung cấp nguồn nuôi. Thẻ bài có thể được sử dụng để lưu mật khẩu, các thông tin cá nhân và các thông tin quan trọng khác. Tương tự thẻ thông minh, thẻ bài thường được trang bị cơ chế xác thực 2 nhân tố,

gồm thẻ bài và mật khẩu, hoặc PIN (thường dùng 1 lần). Ưu điểm của thẻ bài là có cơ chế xác thực mạnh hơn thẻ thông minh do thẻ bài có CPU với năng lực xử lý cao hơn và bộ nhớ lưu trữ lớn hơn.

(Hình minh họa một số thẻ bài của hãng RSA Security)

(Ví điện tử của cổng thanh toán trực tuyến Paypal)



(Hệ thống ApplePay tích hợp vào điện thoại di động)

** Điều khiển truy nhập dựa trên các đặc điểm sinh trắc*

Các đặc điểm sinh trắc là các đặc điểm riêng có để nhận dạng người dùng, bao gồm dấu vân tay, tròng mắt, khuôn mặt, tiếng nói, chữ ký tay,... Điều khiển truy nhập sử dụng các đặc điểm sinh trắc để nhận dạng chủ thể là phương pháp có khả năng cung cấp độ

an toàn cao nhất và cho phép xác thực chủ thể do các đặc điểm sinh trắc luôn đi cùng chủ thể và khó bị đánh cắp hoặc làm giả.

(Hình minh họa Khóa vân tay)

(Hình minh họa Khe xác thực vân tay trên laptop)

(Hình minh họa Xác thực vân tay trên điện thoại thông minh Samsung)

(Hình minh họa việc quét võng mạc để nhận dạng tròng mắt)

Nhược điểm chính của điều khiển truy nhập sử dụng các đặc điểm sinh trắc là phương pháp này yêu cầu chi phí đầu tư lớn cho các thiết bị quét, đọc và xử lý các đặc điểm sinh trắc. Ngoài ra, phương pháp này tương đối chậm do thường liên quan đến xử lý ảnh - công việc đòi hỏi khối lượng tính toán lớn. Một vấn đề khác cần quan tâm là tỷ lệ nhận dạng sai cao do có nhiều yếu tố nhiễu ảnh hưởng.

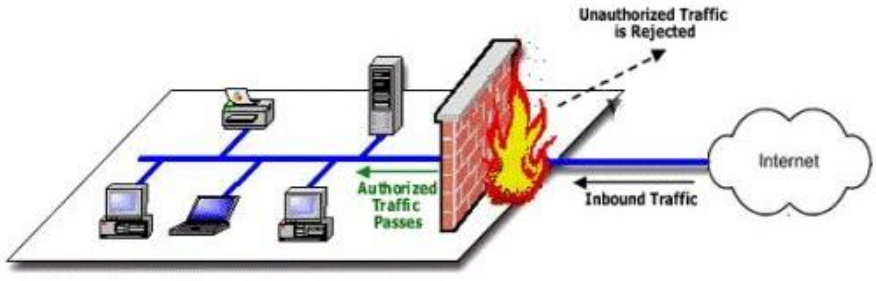
5.2. Tường lửa

5.2.1. Giới thiệu tường lửa

Tường lửa (Firewall) là một trong các kỹ thuật được sử dụng phổ biến nhất để bảo hệ thống và mạng cục bộ tránh các đe dọa từ bên ngoài. Tường lửa có thể là một thiết bị phần cứng chuyên dụng, hoặc mô đun phần mềm chạy trên máy tính.

(Hình ảnh một tường lửa phần cứng chuyên dụng của hãng Cisco)

Để đảm bảo hiệu quả bảo vệ, tường lửa phải miễn dịch với các loại tấn công, xâm nhập và thường được đặt ở vị trí cổng vào của mạng nội bộ cơ quan hoặc tổ chức. Nhờ vị trí đặt ở cổng mạng, tất cả các gói tin từ trong ra và từ ngoài vào đều phải đi qua tường lửa và chỉ các gói tin hợp pháp được phép đi qua tường lửa. Việc xác định một gói tin là hợp pháp hay không được thực hiện bởi thao tác lọc (filtering) dựa trên các luật (rules). Tập các luật sử dụng cho việc lọc các gói tin được tạo ra dựa trên chính sách an ninh của cơ quan, tổ chức.

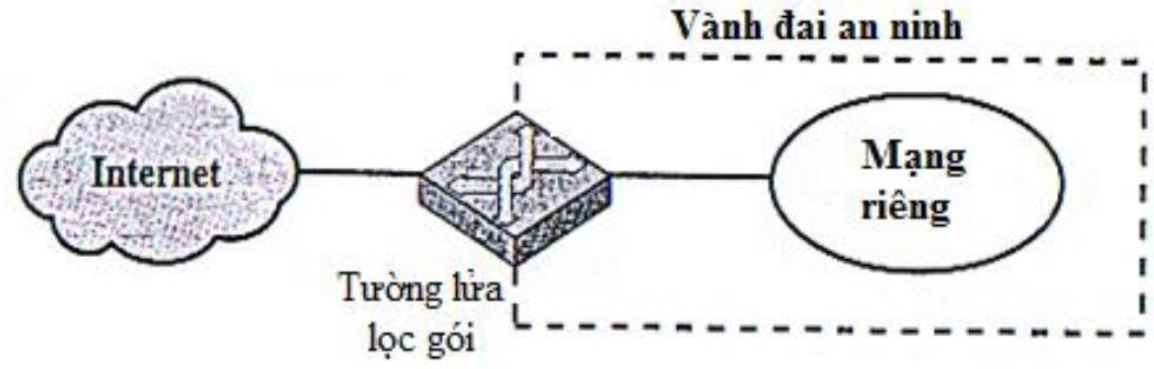


(Hình ảnh tường lửa bảo vệ mạng văn phòng nhỏ và mạng gia đình)

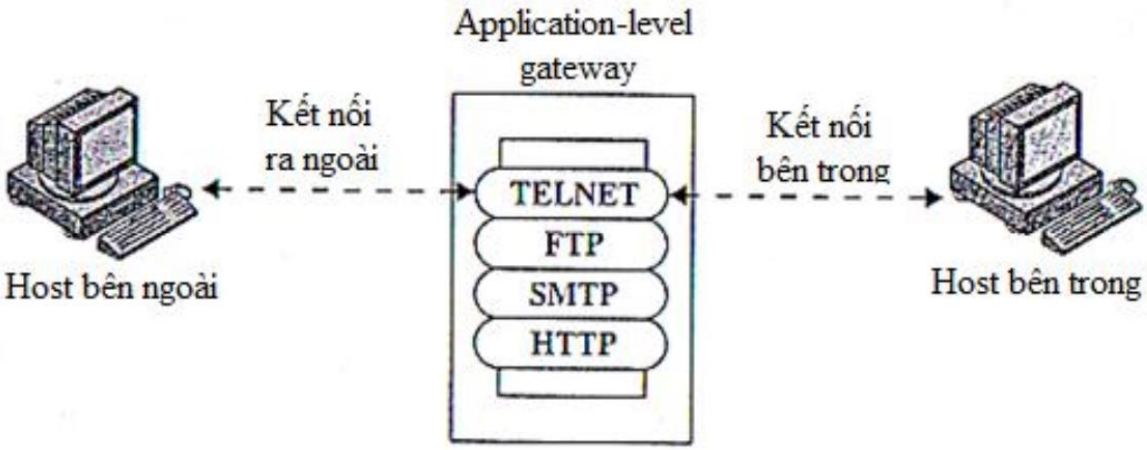
5.2.2. Các loại tường lửa

Có nhiều phương pháp phân loại các tường lửa, chẳng hạn như dựa trên vị trí các lớp giao thức mạng và khả năng lưu trạng thái của các kết nối mạng. Dựa trên vị trí các lớp giao thức mạng, có thể chia tường lửa thành 3 loại: tường lửa lọc gói (Packet-filtering),

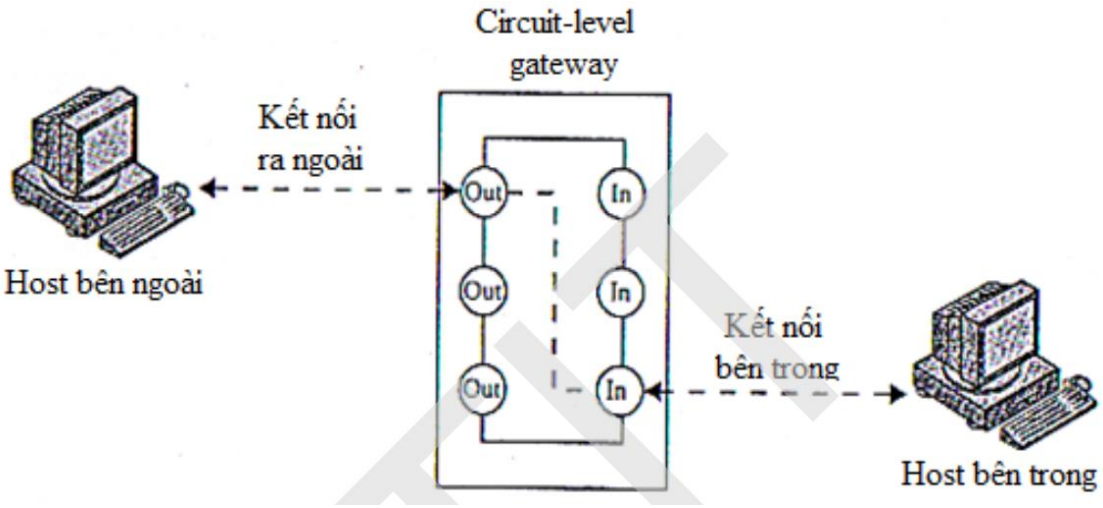
cổng ứng dụng (Application-level gateway) và cổng chuyển mạch (Circuit-level gateway). Tường lửa lọc gói thường thực hiện việc lọc các gói tin IP, theo đó một tập, hoặc một nhóm các luật được áp dụng cho mỗi gói tin gửi đi, hoặc chuyển đến để quyết định chuyển tiếp các gói tin hợp pháp, hay loại bỏ gói tin bất hợp pháp. Cổng ứng dụng, còn gọi là máy chủ proxy thường được sử dụng để phát lại lưu lượng mạng ở mức ứng dụng. Cổng ứng dụng thực hiện việc lọc các yêu cầu, hoặc hồi đáp (request/response) ở các giao thức ứng dụng phổ biến như HTTP, SMTP, FTP,... Cổng chuyển mạch hoạt động ở mức thấp nhất, với cơ chế tương tự như các bộ chuyển mạch (switch).



(Hình minh họa mô hình tường lửa lọc gói)

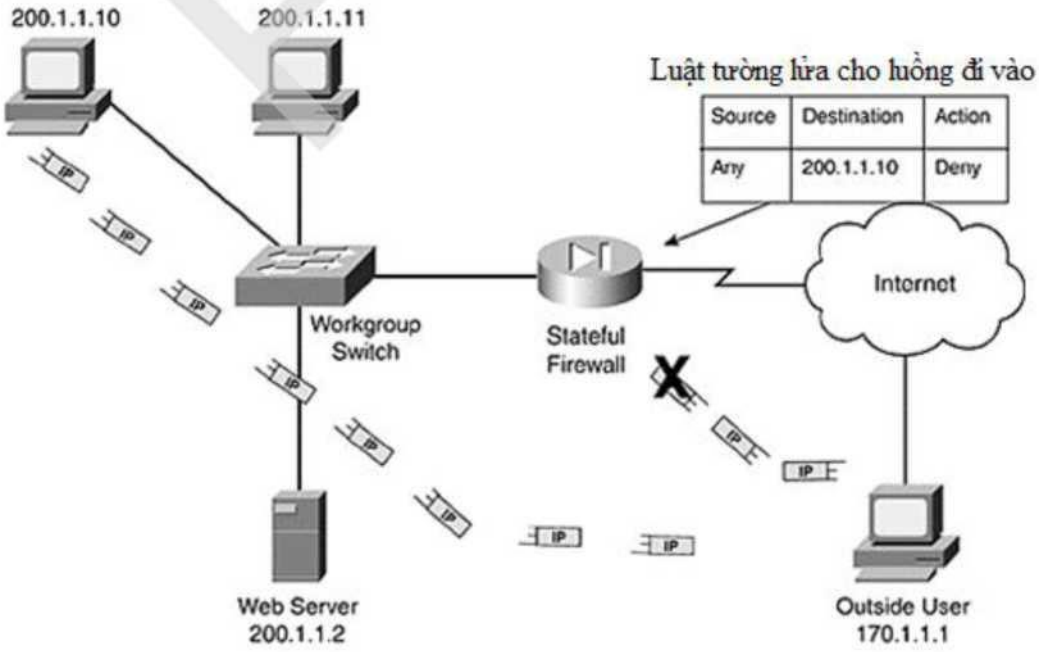


(Hình minh họa cổng ứng dụng)



(Hình minh họa cổng chuyển mạch)

Dựa trên khả năng lưu trạng thái của các kết nối mạng, tường lửa được chia thành 2 loại: tường lửa có trạng thái (Stateful firewall) và tường lửa không trạng thái (Stateless firewall). Tường lửa có trạng thái có khả năng lưu trạng thái của các kết nối mạng đi qua và được lập trình để phân biệt các gói tin thuộc về các kết nối mạng khác nhau. Theo đó, chỉ những gói tin thuộc một kết nối mạng đang hoạt động mới được đi qua tường lửa, còn các gói tin khác không thuộc kết nối đang hoạt động sẽ bị chặn lại.



(Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động)

Hình ảnh trên minh hoạt một tường lửa có trạng thái chặn các gói tin IP gửi từ người dùng ngoài (Outside User) đến địa chỉ IP 200.1.1.10 do chúng không thuộc kết nối đang hoạt động. Ngược lại, tường lửa không trạng thái thực hiện việc lọc các gói tin riêng rẽ mà không quan tâm mỗi gói tin thuộc về kết nối mạng nào. Tường lửa dạng này dễ bị tấn công bởi kỹ thuật giả mạo địa chỉ, giả mạo nội dung gói tin do tường lửa không có khả năng nhớ các gói tin đi trước thuộc cùng một kết nối mạng.

5.2.3. Các kỹ thuật kiểm soát truy nhập

Hầu hết các tường lửa hỗ trợ nhiều kỹ thuật kiểm soát truy nhập, gồm kiểm soát dịch vụ, kiểm soát hướng, kiểm soát người dùng và kiểm soát hành vi. Cụ thể:

- Kiểm soát dịch vụ xác định dịch vụ nào có thể được truy nhập và thường được thực hiện thông qua việc mở hoặc đóng một cổng dịch vụ nào đó. Chẳng hạn, để cung cấp dịch vụ web và cấm tất cả các dịch vụ khác, tường lửa mở cổng HTTP 80 và HTTPS 443, còn đóng tất cả các cổng dịch vụ khác.
- Kiểm soát hướng điều khiển hướng được phép đi của các gói tin của mỗi dịch vụ. Hướng có thể gồm luồng từ mạng nội bộ đi ra (outgoing) và luồng từ ngoài đi vào mạng nội bộ (incoming).
- Kiểm soát người dùng xác định người dùng nào được quyền truy nhập và thường áp dụng cho người dùng mạng nội bộ.
- Kiểm soát hành vi thực hiện kiểm soát việc sử dụng các dịch vụ cụ thể. Ví dụ như, tường lửa có thể được cấu hình để lọc loại bỏ các thư rác, hoặc hạn chế truy nhập đến một bộ phận thông tin của máy chủ web.

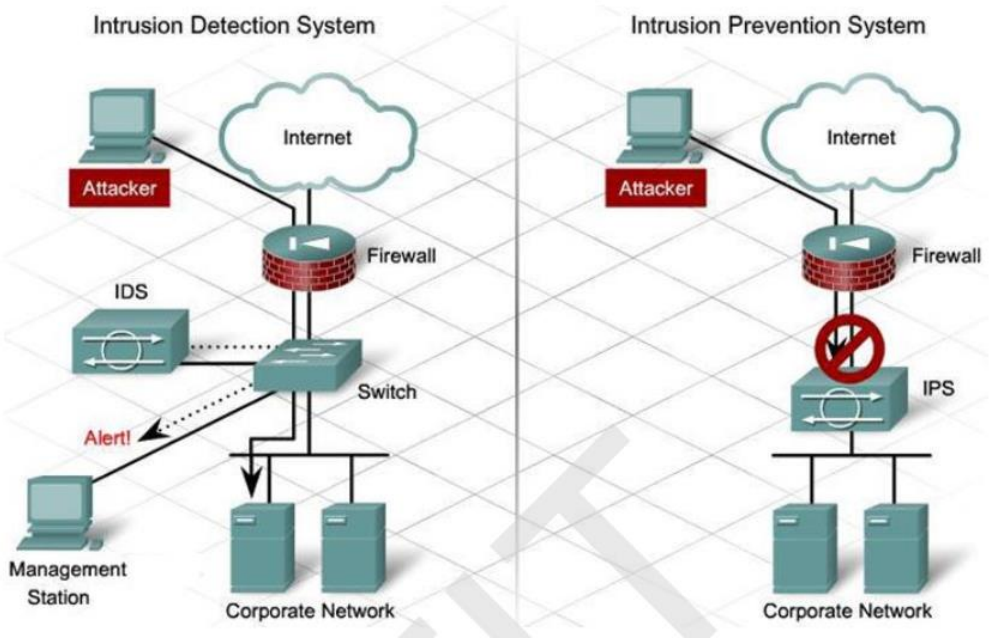
5.2.4. Các hạn chế tường lửa

Mặc dù tường lửa được sử dụng rộng rãi để bảo vệ mạng nội bộ khỏi các cuộc tấn công, xâm nhập, nhưng cũng như hầu hết các kỹ thuật và công cụ đảm bảo an toàn khác, tường lửa cũng có những hạn chế. Các hạn chế của tường lửa gồm:

- Không thể chống lại các tấn công không đi qua tường lửa. Đó có thể là các dạng tấn công khai thác yếu tố con người, hoặc kẻ tấn công có thể xâm nhập trực tiếp vào hệ thống mạng nội bộ mà không đi qua tường lửa.
- Không thể chống lại các tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng bảo mật của các phần mềm.
- Không thể chống lại các hiểm hoạ từ bên trong, như từ người dùng trong mạng nội bộ.
- Không thể ngăn chặn việc vận chuyển các chương trình hoặc các file bị nhiễm vi rút hoặc các phần mềm độc hại (thường ở dạng nén hoặc mã hóa).

5.3. Các hệ thống phát hiện và ngăn chặn xâm nhập

5.3.1. Giới thiệu



(Vị trí các hệ thống IDS và IPS trong sơ đồ mạng)

Các hệ thống phát hiện, ngăn chặn tấn công, xâm nhập (IDS/IPS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ có chiều sâu (defence in depth). IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập và IPS (Intrusion Prevention System) là hệ thống ngăn chặn tấn công, xâm nhập. Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa trong mô hình mạng, tùy theo mục đích sử dụng. Hình ảnh trên cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ switch phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa. Nhiệm vụ chính của các hệ thống IDS/IPS bao gồm:

- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập;
- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này;
- Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập;
- Gửi thông báo cho người quản trị về các các hành vi tấn công, xâm nhập đã phát hiện được.

Về cơ bản IPS và IDS giống nhau về chức năng giám sát lưu lượng mạng hoặc các sự kiện trong hệ thống. Tuy nhiên, IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công, xâm nhập bị phát hiện. Trong khi đó, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh bảo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

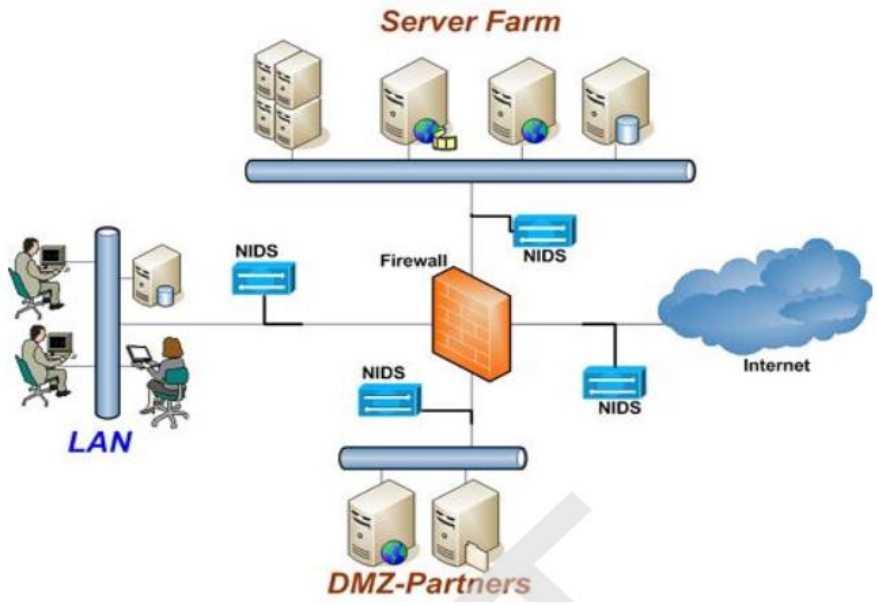
5.3.2. Phân loại

Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, gồm (1) phân loại theo

nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu. Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

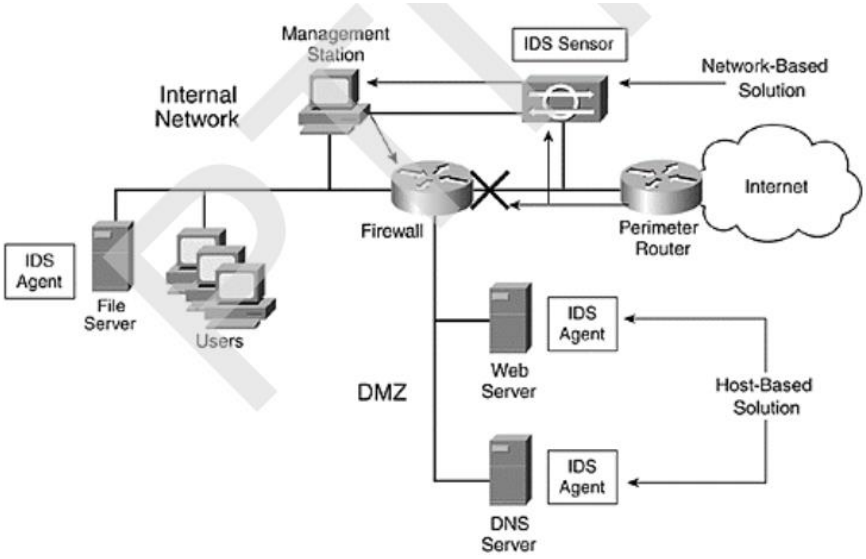
- Hệ thống phát hiện xâm nhập mạng (NIDS - Network-based IDS): NIDS phân tích lưu

lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng. Hình ảnh sau biểu diễn một sơ đồ mạng, trong đó các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng.



(Các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào
và cho từng phân đoạn mạng)

- Hệ thống phát hiện xâm nhập cho host (HIDS - Host-based IDS): HIDS phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó. Hình sau minh họa một sơ đồ mạng, trong đó sử dụng NIDS để giám sát lưu lượng tại cổng mạng và HIDS để giám sát các host thông qua các IDS agent. Một trạm quản lý (Management station) được thiết lập để thu nhập các thông tin từ các NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng.



(Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host)

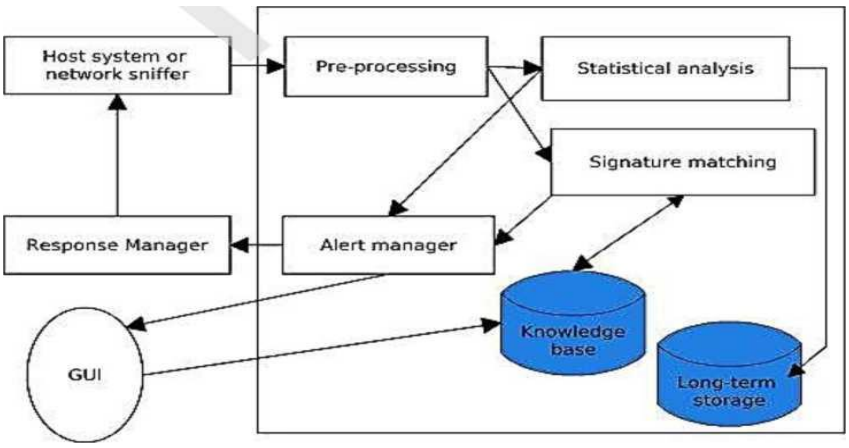
Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính, gồm (1) phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection) và (2) phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection). Mục tiếp theo trình bày chi tiết hơn về hai kỹ thuật phát hiện này.

5.3.3. Các kỹ thuật phát hiện xâm nhập

* *Phát hiện xâm nhập dựa trên chữ ký*

Phát hiện xâm nhập dựa trên chữ ký trước hết cần xây dựng cơ sở dữ liệu các chữ ký, hoặc các dấu hiệu của các loại tấn công, xâm nhập đã biết. Hầu hết các chữ ký, dấu hiệu được nhận dạng và mã hóa thủ công và dạng biểu diễn thường gặp là các luật phát hiện (Detection rule). Bước tiếp theo là sử dụng cơ sở dữ liệu các chữ ký để giám sát các hành vi của hệ thống, hoặc mạng, và cảnh báo nếu phát hiện chữ ký của tấn công, xâm nhập.

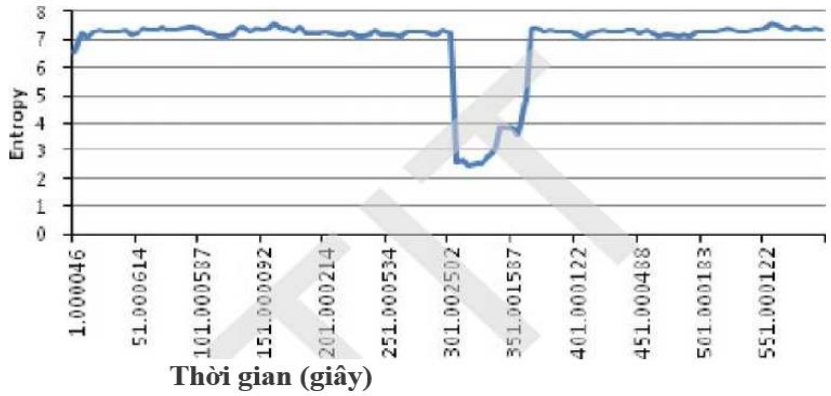
Ưu điểm lớn nhất của phát hiện xâm nhập dựa trên chữ ký là có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả. Ngoài ra, phương pháp này cho tốc độ xử lý cao, đồng thời yêu cầu tài nguyên tính toán tương đối thấp. Nhờ vậy, các hệ thống phát hiện xâm nhập dựa trên chữ ký được ứng dụng rộng rãi trong thực tế. Tuy nhiên, nhược điểm chính của phương pháp này là không có khả năng phát hiện các tấn công, xâm nhập mới, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu các chữ ký. Hơn nữa, nó cũng đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.



Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

** Phát hiện xâm nhập dựa trên bất thường*

Phát hiện xâm nhập dựa trên bất thường dựa trên giả thiết: các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường. Quá trình xây dựng và triển khai một hệ thống phát hiện xâm nhập dựa trên bất thường gồm 2 giai đoạn: (1) huấn luyện và (2) phát hiện. Trong giai đoạn huấn luyện, hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện này, cần giám sát đối tượng trong một khoảng thời gian đủ dài để thu thập được đầy đủ dữ liệu mô tả các hành vi của đối tượng trong điều kiện bình thường làm dữ liệu huấn luyện. Tiếp theo, thực hiện huấn luyện dữ liệu để xây dựng mô hình phát hiện, hay hồ sơ của đối tượng. Trong giai đoạn phát hiện, thực hiện giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và các hành vi lưu trong hồ sơ của đối tượng.



(*Giá trị entropy của IP nguồn của các gói tin từ lưu lượng hợp pháp - phần giá trị cao, đều và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS - phần giá trị thấp*)

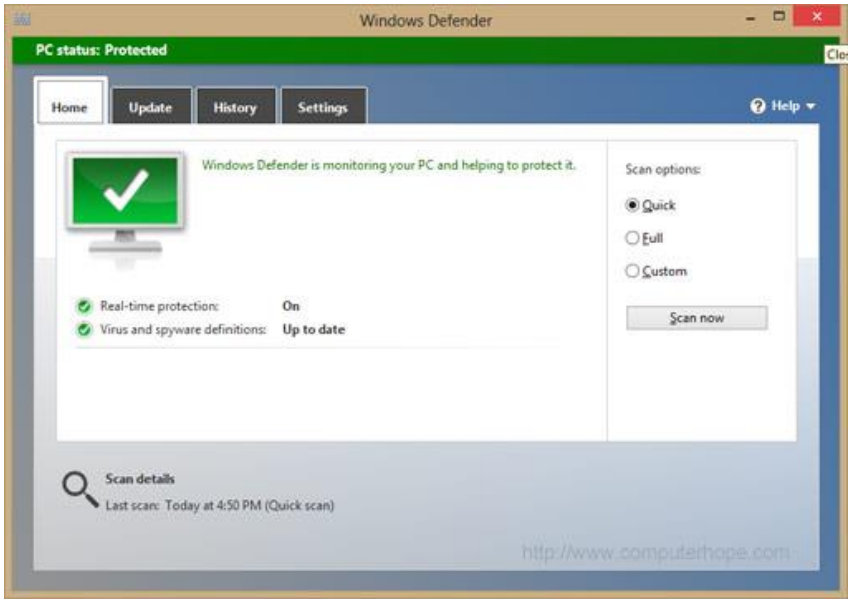
Hình trên biểu diễn giá trị entropy của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS. Có thể thấy sự khác biệt rõ nét giữa giá trị entropy của lưu lượng bình thường và lưu lượng tấn công và như vậy, nếu một ngưỡng entropy được chọn phù hợp ta hoàn toàn có thể phát hiện sự xuất hiện của cuộc tấn công DDoS dựa trên sự thay đổi đột biến của

giá trị entropy.

Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên, phương pháp này có tỷ lệ cảnh báo sai tương đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, nó cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

5.4. Các công cụ rà quét phần mềm độc hại

Các công cụ rà quét vi rút và các phần mềm độc hại (Antivirus software) là các phần mềm có khả năng rà quét, bảo vệ hệ thống khỏi vi rút và các phần mềm độc hại khác theo thời gian thực. Hầu hết các công cụ này đều cho phép thực hiện 2 chế độ quét: quét định kỳ từng phần hoặc toàn bộ hệ thống các file và bảo vệ hệ thống theo thời gian thực (Realtime protection). Chúng cho phép giám sát tất cả các thao tác đọc/ghi hệ thống file để phát hiện các phần mềm độc hại. Đa số công cụ rà quét vi rút và các phần mềm độc hại hoạt động dựa trên một cơ sở dữ liệu các mẫu, hoặc chữ ký của các phần mềm độc hại đã biết. Do vậy, để đảm bảo an toàn cơ sở dữ liệu này phải được cập nhật thường xuyên. Một số bộ công cụ cho phép quét theo hành vi hoặc heuristics.



Màn hình chính của Microsoft Windows Defender

Có thể liệt kê một số công cụ rà quét vi rút và các phần mềm độc hại thông dụng, như:

- Microsoft Security Essentials (Windows 7 trở lên)
- Microsoft Windows Defender (Windows 8 trở lên)
- Semantec Norton Antivirus
- Kaspersky Antivirus
- BitDefender Antivirus
- AVG Antivirus

- McAfee VirusScan

❖ TÓM TẮT CHƯƠNG 5

Trong chương này, một số nội dung chính được giới thiệu:

- **Công Nghệ Bảo Mật**: Chương này giới thiệu về các công nghệ bảo mật như tường lửa, mã hóa, phần mềm chống vi-rút, và phương pháp phát hiện xâm nhập. Học sinh sẽ hiểu cách các công nghệ này hoạt động và tại sao chúng quan trọng trong bảo vệ thông tin.
- **Xác Thực và Kiểm Soát Truy Cập**: Chương này trình bày về quá trình xác thực người dùng và kiểm soát quyền truy cập thông tin. Học sinh sẽ hiểu cách cấu hình hệ thống để đảm bảo chỉ người dùng được ủy quyền có thể truy cập thông tin quan trọng.
- **Bảo Vệ Dữ Liệu**: Chương này tập trung vào bảo vệ dữ liệu thông qua việc thực hiện các biện pháp như sao lưu, khôi phục dữ liệu, và giám sát dữ liệu.
- **Triển Khai Biện Pháp Bảo Mật**: Chương này hướng dẫn cách triển khai các biện pháp bảo mật trong môi trường thực tế, bao gồm xây dựng tường lửa, cấu hình mã hóa, và quản lý quyền truy cập.

❖ CÁC BÀI TẬP HỆ THỐNG KIẾN THỨC

1) Nêu khái niệm tài sản an toàn thông tin, khái niệm quản lý an toàn thông tin. Nêu vai trò và các khâu cần thực hiện của quản lý an toàn thông tin.
2) Đánh giá rủi ro an toàn thông tin là gì? Mô tả vắn tắt các phương pháp tiếp cận đánh giá rủi ro an toàn thông tin.
3) Nêu một số công nghệ điều khiển truy nhập
4) Tường lửa là gì? Có mấy loại tường lửa, kể tên.
5) Nêu các kĩ thuật kiểm soát truy nhập
6) Các hạn chế tường lửa
7) Nêu nhiệm vụ chính của các hệ thống IDS/IPS
8) Nêu các loại hệ thống phát hiện, xâm nhập
9) Các kĩ thuật phát hiện xâm nhập mạng nào?
10) Liệt kê một số công cụ và quét virut và các phần mềm độc hại thông dụng.