BỘ CÔNG THƯƠNG

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO BÀI TẬP LỚN

MÔN: NGUYÊN LÝ HỆ ĐIỀU HÀNH

ĐỀ TÀI: NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS

Giáo Viên Hướng Dẫn: **Ths Nguyễn Thanh Hải**

Lớp: **IT6025.4**

Nhóm Thực Hiện: **Nhóm 11**

Hà Nội, tháng 06 năm 2022

BỘ CÔNG THƯƠNG

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO BÀI TẬP LỚN

MÔN: NGUYÊN LÝ HỆ ĐIỀU HÀNH

ĐỀ TÀI: NGHIÊN CỨU VÀ TÌM HIỂU VỀ HỆ THỐNG BẢO VỆ TRONG HỆ ĐIỀU HÀNH WINDOWS

Giáo Viên Hướng Dẫn: **Ths Nguyễn Thanh Hải**

Sinh Viên Thực Hiện:

1. **Ngô Thị Mai**
2. **Nguyễn Thông Tiến**
3. **Lê Ngọc Trường**
4. **Dương Trung Tú**
5. **Nguyễn Xuân Xoan**

Hà Nội, tháng 06 năm 2022

MỤC LỤC

MỞ ĐẦU

Như chúng ta đã biết, bất cứ một chương trình nào khi được thiết kế để chạy trên máy tính thì không chỉ chú tâm đến nội dung, hình thức...của chương trình đó mà có một thành phần cấu thành nên chương trình đó và phải có thành phần này thì chương trình mới hoạt động ổn định và hiệu quả. Đó chính là hệ thống bảo mật, cũng như bất kể các chương trình máy tính nào đó thì chính hệ điều hành mà chúng ta sử dụng để vận hành các chương trình đó cũng cần có hệ thống bảo mật và nó là một thành phần quyết định là hệ điều hành đó có tồn tại được và phát triển được hay không?

Trong đề tài này, chúng ta sẽ nghiên cứu và tìm hiểu một cách chi tiết nhất về hệ thống bảo vệ trong Windows và an toàn hệ thống trong Windows

An toàn và bảo vệ hệ thống là chức năng không thể thiếu của các hệ điều hành. Trong đề tài này, chúng ta sẽ làm quen và tìm hiểu rõ hơn về tính năng này trong hệ điều hành windows và liên hệ vào những gì đã được học.

CHƯƠNG 1: TỔNG QUAN VỀ BẢO VỆ HỆ THỐNG

1.1 Thế nào là bảo vệ hệ thống trong hệ điều hành ?

Cơ chế kiểm soát quyền truy nhập của các chương trình, quy trình hoặc người dùng vào các tài nguyên được xác định bởi hệ thống máy tính được gọi là bảo vệ. Bạn có thể sử dụng bảo vệ như một công cụ cho các hệ điều hành đa lập trình, cho phép nhiều người dùng chia sẻ một cách an toàn không gian tên logic chung, bao gồm một thư mục hoặc các tệp.

Nó cần được bảo vệ các tài nguyên máy tính như phần mềm, bộ nhớ, bộ xử lý, v.v. Người dùng nên thực hiện các biện pháp bảo vệ như một người trợ giúp cho hệ điều hành đa chương trình để nhiều người dùng có thể sử dụng một cách an toàn không gian tên logic chung như thư mục hoặc dữ liệu. Có thể đạt được sự bảo vệ bằng cách duy trì tính bảo mật, tính trung thực và tính khả dụng trong Hệ điều hành. Điều quan trọng là phải bảo mật thiết bị khỏi truy nhập trái phép, vi rút, worms (sâu) và phần mềm độc hại khác.

1.2 Cần được bảo vệ trong hệ điều hành

Các nhu cầu bảo vệ khác nhau trong hệ điều hành như sau:

- Có thể có các rủi ro bảo mật như đọc, ghi, sửa đổi trái phép hoặc ngăn hệ thống hoạt động hiệu quả đối với người dùng được ủy quyền.
- Nó giúp đảm bảo an ninh dữ liệu, bảo mật quy trình và bảo mật chương trình chống lại sự truy cập trái phép của người dùng hoặc truy cập chương trình.
- Điều quan trọng là đảm bảo không vi phạm quyền truy cập, không vi rút, không truy cập trái phép vào dữ liệu hiện có.
- Mục đích của nó là đảm bảo rằng chỉ các chính sách của hệ thống mới truy cập vào các chương trình, tài nguyên và dữ liệu.

1.3 Mục tiêu của bảo vệ hệ thống

Một hệ điều hành đa nhiệm có thể thực hiện đồng thời nhiều tiến trình tại cùng một thời điểm. Khi đó chắc chắn sẽ có hai hay nhiều tiến trình hoạt động song

hành trong hệ thống, ngẫu nhiên có thể phát sinh lỗi của một tiến trình và lỗi của tiến trình đó có thể gây ảnh hưởng đến các tiến trình khác đang hoạt động đồng thời trong hệ thống. Vì vậy, để bảo vệ hệ thống khỏi sự lây lan lỗi của một tiến trình đến các tiến trình khác thì hệ thống phải có chức năng ngăn chặn không cho lan truyền trên hệ thống làm ảnh hưởng đến các tiến trình khác. Đặc biệt, qua việc phát hiện các lỗi tiềm ẩn trong các thành phần của hệ thống có thể tăng cường độ tin cậy của hệ thống.

Hệ thống đảm bảo các bộ phận của tiến trình sử dụng tài nguyên theo một cách thức hợp lệ được quy định cho nó trong việc khai thác tài nguyên này.

Vai trò của bộ phận bảo vệ trong hệ thống là cung cấp một cơ chế để áp dụng các chiến lược quản trị việc sử dụng tài nguyên. Cần phân biệt rõ giữa khái niệm cơ chế và chiến lược của bộ phận bảo vệ trong hệ thống:

Cơ chế: xác định làm thế nào để thực hiện việc bảo vệ, có thể có các cơ chế phần mềm hoặc cơ chế phần cứng.

Chiến lược: quyết định việc bảo vệ được áp dụng như thế nào: Những đối tượng nào trong hệ thống cần được bảo vệ, và các thao tác thích hợp trên các đối tượng này.

Để hệ thống có độ tương thích cao, cần phân tách các cơ chế và chiến lược được sử dụng trong hệ thống. Các chiến lược sử dụng tài nguyên là khác nhau tùy theo ứng dụng, và thường để thay đổi. Thông thường các chiến lược được lập trình viên vận dụng vào ứng dụng của mình để chống lỗi truy xuất bất hợp lệ đến các tài nguyên trong khi đó hệ thống cung cấp các cơ chế giúp người sử dụng có thể thực hiện được chiến lược bảo vệ của mình.

1.4 Vai trò bảo vệ trong hệ điều hành

Vai trò chính của nó là cung cấp cơ chế thực hiện các chính sách xác định việc sử dụng tài nguyên trong hệ thống máy tính. Một số quy tắc được đặt ra trong quá trình thiết kế hệ thống, trong khi các quy tắc khác được quản trị viên hệ thống xác định để bảo mật các tệp và chương trình của họ.

Mỗi chương trình đều có các chính sách riêng biệt để sử dụng tài nguyên và các chính sách này có thể thay đổi theo thời gian. Do đó, bảo mật hệ thống không

thuộc trách nhiệm của người thiết kế hệ thống, và người lập trình cũng phải thiết kế kỹ thuật bảo vệ để bảo vệ hệ thống của họ chống lại sự xâm nhập.

1.5 Nguyên tắc bảo vệ (Principles of Protection)

Các nguyên tắc bắt buộc đặc quyền tối thiểu (The principle of least privilege dictates) là một loạt các quy tắc cho rằng các chương trình, người sử dụng, và các hệ thống chỉ đủ quyền để thực hiện các nhiệm vụ của các chương trình, người sử dụng và các hệ thống đó.

Các nguyên tắc trên được đặt ra và nó đảm bảo sự thiệt hại do các lỗi của 1 hay nhiều tiến trình phát sinh là ít nhất và hầu như không xảy ra nếu các tiến trình thực hiện đúng các quy tắc đó.

Thông thường, mỗi một tiến trình được cấp những quyền đã được quy định cho tiến trình đó thì những gì tiến trình có thể thực hiện được chỉ nằm trong phạm vi quyền của tiến trình đó.

1.6 Miền bảo vệ (Domain of Protection)

1.6.1 Khái niệm miền bảo vệ

Một hệ thống máy tính bao gồm tập hợp các chủ thể (subject’s) và tập hợp các khách thể (object’s). Chủ thể bao gồm các tiến trình và người sử dụng còn khách thể có thể coi là các tài nguyên của máy tính (như bộ nhớ, ổ đĩa, dữ liệu…).

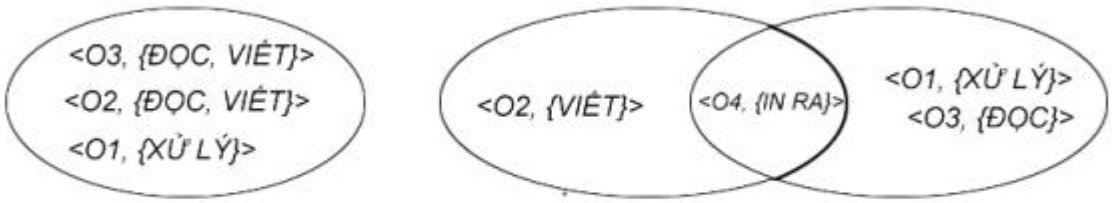
Để có thể kiểm soát được tình trạng sử dụng tài nguyên trong hệ thống, hệ điều hành chỉ cho phép các chủ thể truy cập tới các khách thể mà nó có quyền sử dụng và vào những thời điểm cần thiết (nguyên lý need – to - know) nhằm hạn chế các lỗi xảy ra do tranh chấp tài nguyên.

Mỗi chủ thể trong hệ thống sẽ hoạt động trong một miền bảo vệ (protection domain) nào đó. Một miền bảo vệ sẽ xác định các khách thể mà chủ thể trong miền đó được phép truy nhập và thực hiện thao tác.

1.6.2 Cấu trúc miền bảo vệ

Các khả năng thao tác mà chủ thể có thể thực hiện trên khách thể được gọi là quyền truy cập (Access Right), mỗi miền định nghĩa một tập hợp các đối tượng và các hoạt động mà có thể thể hiện trên từng đối tượng. Mỗi quyền truy nhập được

định nghĩa bởi một bộ hai thành phần <đối tượng, {quyền thao tác}> (<object, {access right}>). Như vậy, ta có thể hình dung miền bảo vệ là một tập hợp các quyền truy nhập, xác định các thao tác mà chủ thể có thể thực hiện trên các khách thể. Các miền bảo vệ khác nhau có thể giao nhau một số quyền truy cập.



HÌNH 1: HỆ THỐNG VỚI 3 MIỀN BẢO VỆ

Sự liên kết giữa một quá trình và một miền có thể là ***tĩnh*** hoặc ***động***:

Liên kết tĩnh: trong suốt thời gian tồn tại của tiến trình trong hệ thống, tiến trình chỉ hoạt động trong một miền bảo vệ. Trong trường hợp tiến trình trải qua các giai đoạn xử lý khác nhau, ở mỗi giai đoạn nó có thể thao tác trên những tập tài nguyên khác nhau. Như vậy trong liên kết tĩnh, miền bảo vệ phải xác định ngay từ đầu các quyền truy nhập cho các tiến trình trong tất cả các giai đoạn xử lý. Điều này khiến cho tiến trình sẽ được dư thừa quyền trong một giai đoạn xử lý nào đó và vi phạm nguyên lý need – to – know. Để đảm bảo được nguyên lý này cần phải có khả năng cập nhật nội dung miền bảo vệ qua các giai đoạn xử lý khác nhau để đảm bảo các quyền tối thiểu của tiến trình trong miền bảo vệ tại một thời điểm.

Liên kết động: cơ chế này cho phép tiến trình chuyển đổi từ miền bảo vệ này sang miền bảo vệ khác trong suốt thời gian tồn tại trong hệ thống của nó. Để tuân thủ nguyên lý need – to – know, thay vì phải sửa đổi nội dung miền bảo vệ hệ thống có thể tạo ra các miền bảo vệ mới với nội dung thay đổi tùy theo từng giai đoạn xử lý của tiến trình và chuyển tiến trình sang hoạt động tại các miền bảo vệ phù hợp với từng thời điểm.

Một miền bảo vệ có thể được xây dựng cho:

Một người sử dụng : trong trường hợp này, tập các đối tượng được phép truy xuất phụ thuộc vào định danh của người sử dụng, miền bảo vệ được chuyển khi thay đổi người sử dụng.

Một tiến trình : trong trường hợp này, tập các đối tượng được phép truy xuất phụ thuộc vào định danh của tiến trình, miền bảo vệ được chuyển khi quyền điều khiển được chuyển sang tiến trình khác.

Một thủ tục : trong trường hợp này, tập các đối tượng được phép truy xuất là các biến cục bộ được định nghĩa bên trong thủ tục, miền bảo vệ được chuyển khi thủ tục được gọi.

1.7 Ma trận quyền truy nhập

1.7.1 Khái niệm về ma trận quyền truy nhập

Để biểu diễn miền bảo vệ, các hệ điều hành sẽ cài đặt các ma trận quyền truy nhập trong đó các hàng của ma trận biểu diễn các miền bảo vệ, các cột biểu diễn khách thể. Phần tử (i,j) của ma trận xác định quyền truy nhập của chủ thể miền bảo vệ D_i, có thể thao tác đối với khách thể O_j.

Một cách trừu tượng, có thể biểu diễn mô hình bảo vệ trên đây như một ma trận quyền truy nhập (access matrix). Các dòng của ma trận biểu diễn các miền bảo vệ và các cột tương ứng với các đối tượng trong hệ thống. Phần tử truy nhập [i,j] của ma trận xác định các quyền truy nhập mà một tiến trình hoạt động trong miền bảo vệ Di có thể thao tác trên đối tượng khách thể Oj.

Object \ Domain	**F1**	**F2**	**F3**	**Máy in**
D1	Đọc/ Ghi	Xử lý	Đọc	
D2	Xử lý			In
D3		Ghi		
D4	Đọc/ghi		Đọc/ghi	In

Hình 2. Ma trận quyền truy nhập

Cơ chế bảo vệ được cung cấp khi ma trận quyền truy nhập được cài đặt (với đầy đủ các thuộc tính ngữ nghĩa đả mô tả trên lý thuyết), lúc này người sử dụng có thể áp dụng các chiến lược bảo vệ bằng cách đặc tả nội dung các phần tử tương ứng

trong ma trận - xác định các quyền truy nhập ứng với từng miền bảo vệ, và cuối cùng, hệ điều hành sẽ quyết định cho phép tiến trình hoạt động trong miền bảo vệ thích hợp. Ma trận quyền truy nhập cũng cung cấp một cơ chế thích hợp để định nghĩa và thực hiện một sự kiểm soát nghiêm ngặt cho cả phương thức liên kết tĩnh và động các tiến trình với các miền bảo vệ: Có thể kiểm soát việc chuyển đổi giữa các miền bảo vệ nếu quan niệm miền bảo vệ cũng là một đối tượng trong hệ thống, và bổ sung các cột mô tả cho nó trong ma trận quyền truy xuất. Khi đó tiến trình được phép chuyển từ miền bảo vệ Di sang miền bảo vệ Dj nếu phần tử truy nhập(i,j) chứa đựng quyền "chuyển" (switch).

Object Domain	**F1**	**F2**	**F3**	**Máy in**	**D1**	**D2**	**D3**	**D4**
D1	Đọc		Đọc			Chuyển		
D2				In			Chuyển	Chuyển
D3		Đọc	Xử lý					
D4	Đọc/ghi		Đọc/ghi		Chuyển			

Hình 3. Ma trận quyền truy xuất với domain là một đối tượng

Có thể kiểm soát việc sửa đổi nội dung ma trận (thay đổi các quyền truy nhập trong một miền bảo vệ) nếu quan niệm bản thân ma trận cũng là một đối tượng. Các thao tác sửa đổi nội dung ma trận được phép thực hiện bao gồm: sao chép quyền (**copy**), chuyển quyền (**transfer**), quyền sở hữu (**owner**), và quyền kiểm soát (**control**)

- Copy: nếu một quyền truy nhập R trong truy nhập [i,j] được đánh dấu là R* thì có thể sao chép nó sang một phần tử truy nhập [k,j] khác (mở rộng quyền truy xuất R trên cùng đối tượng Oj nhưng trong miền bảo vệ Dk).

- Transfer: nếu một quyền truy xuất R trong truy nhập [i,j] được đánh dấu là R+ thì có thể chuyển nó sang một phần tử truy nhập [k,j] khác (chuyển quyền truy xuất R+ trên đối tượng Oj sang miền bảo vệ Dk).

- Owner: nếu truy nhập [i,j] chứa quyền truy nhập owner thì tiến trình hoạt động trong miền bảo vệ Di có thể thêm hoặc xóa các quyền truy nhập trong bất kỳ

phần tử nào trên cột j (có quyền thêm hay bớt các quyền truy nhập trên đối tượng Oj trong những miền bảo vệ khác).

- Control: nếu truy nhập [i,j] chứa quyền truy xuất control thì tiến trình hoạt động trong miền bảo vệ Di có thể xóa bất kỳ quyền truy nhập nào trong các phần tử trên dòng j (có quyền bỏ bớt các quyền truy nhập trong miền bảo vệ Dj).

Object domain	**F1**	**F2**	**F3**
D1	xử lý		ghi+
D2	xử lý	đọc*	xử lý
D3	xử lý		

(a)

Object domain	**F1**	**F2**	**F3**
D1	xử lý		
D2	xử lý	đọc*	xử lý
D3	xử lý	đọc	ghi+

(b)

Hình 4. Ma trận quyền truy nhập với quyền copy, transfer (a) trước, (b) sau cập nhật

Object domain	**F1**	**F2**	**F3**
D1	Owner xử lý		ghi
D2		đọc*/owner	Đọc*/owner/ghi*
D3	xử lý		

(a)

Object domain	**F1**	**F2**	**F3**
D1	Owner xử lý		
D2		Owner/đọc*/ghi*	Đọc*/owner/ ghi*
D3		ghi	

(b)

Hình 5. Ma trận quyền truy nhập với quyền owner (a) trước, (b) sau cập nhật

object domain	F1	F2	F3	Máy in	D1	D2	D3	D4
D1	đọc		đọc			chuyển		
D2				in			chuyển	control chuyển
D3		đọc	xử lý					
D4	ghi		Ghi		chuyển			

Hình 6. Ma trận quyền truy nhập đã sửa đổi nội dung so với H5.3 nhờ quyền control

1.7.2 Các phương pháp cài đặt ma trận quyền truy cập

Bảng toàn cục (Global Table): Phương pháp này đơn giản nhất, để cài đặt ma trận quyền truy cập, hệ thống sử dụng một bảng toàn cục bao gồm các bộ ba thành phần <miền bảo vệ, khách thể, quyền truy cập> (<domain,object,rights>). Mỗi khi thực hiện quyền thao tác M trên khách thể O_j trong miền bảo vệ D_i, cần tìm trong bảng toàn cục một bộ ba $<D_i,O_j,R_k>$ mà M thuộc R_k (truy cập các quyền truy nhập). Nếu tìm thấy thao tác M được phép ghi thành công, ngược lại sẽ xảy ra lỗi. Tuy nhiên phương pháp bảng toàn cục (Global table) có kích thước rất lớn nên không thể giữ trong bộ nhớ.

Danh sách quyền truy nhập (Access Control List for Objects - ACL): Có thể cài đặt mỗi cột trong ma trận quyền truy xuất như một danh sách quyền truy xuất đối với một đối tượng. Mỗi đối tượng trong hệ thống sẽ có một danh sách bao gồm các phần tử là các bộ hai thứ tự <miền bảo vệ, các quyền truy xuất>, danh sách này sẽ xác định các quyền truy xuất được quy định trong từng miền bảo vệ có thể tác động trên đối tượng. Mỗi khi thực hiện thao tác M trên đối tượng O_j trong miền bảo vệ D_i, cần tìm trong danh sách quyền truy xuất của đối tượng O_j một bộ hai $< D_i,R_k >$ mà M ở R_k. Nếu tìm thấy, thao tác M được phép thi hành, nếu không, xảy ra lỗi truy xuất.

Ví dụ : Một miền bảo vệ trong hệ thống UNIX được xác định tương ứng với một người sử dụng (uid) trong một nhóm (gid) nào đó. Giả sử có 4 người dùng : A,B,C,D thuộc các nhóm tương ứng là system, staff, student, student. Khi đó các tập tin trong hệ thống có thể có các ACL như sau :

File0 : (A,*,RWX)

File1 : (A,system,RWX)

File2 : (A,*,RW-),(B,staff,R--),(D,*,RW-)

File3 : (*,student,R--)

File4 : (C,*,---),(*,student,R--)

Thực tế, hệ thống tập tin trong UNIX được bảo vệ bằng cách mỗi tập tin được gán tương ứng 9 bit bảo vệ , từng 3 bit sẽ mô tả quyền truy xuất R(đọc), W(ghi) hay X(xử lý) của các tiến trình trên tập tin này theo thứ tự : tiến trình sở hữu các tiến trình cùng nhóm với tiến trình sở hữu, các tiến trình khác. Đây là một dạng ACL nhưng được nén thành 9 bit.

Danh sách khả năng (Capability List for Domain): Mỗi dòng trong ma trận quyền truy xuất tương ứng với một miền bảo vệ sẽ được tổ chức thành một danh sách tiềm năng (capabilities list) :

Một danh sách tiềm năng của một miền bảo vệ là một danh sách các đối tượng và các thao tác được quyền thực hiện trên đối tượng khi tiến trình hoạt động trong miền bảo vệ này.

Một phần tử của C-List được gọi là một tiềm năng (capability) là một hình thức biểu diễn được định nghĩa một cách có cấu trúc cho một đối tượng trong hệ thống và các quyền truy xuất hợp lệ trên đối tượng này.

Ví dụ:

Kiểu	Quyền	Đối tượng
File	R--	File 3
File	RWX	File 4
File	RW-	File 5
Printer	-W-	File 3

Tiến trình chỉ có thể thực hiện thao tác M trên đối tượng O_j trong miền bảo vệ D_i, nếu trong C_List của D_i có chứa tiềm năng tương ứng của O_j.

Danh sách tiềm năng được gán tương ứng với từng miền bảo vệ, thực chất nó cũng là một đối tượng được bảo vệ bởi hệ thống, và tiến trình của người sử dụng chỉ có thể truy xuất đến nó một cách gián tiếp để tránh làm sai lạc C_List.

Hệ điều hành cung cấp các thủ tục cho phép tạo lập, hủy bỏ và sửa đổi các tiềm năng của một đối tượng, và chỉ các tiến trình đóng vai trò server (thường là tiến trình hệ điều hành) mới có thể sửa đổi nội dung C_List.

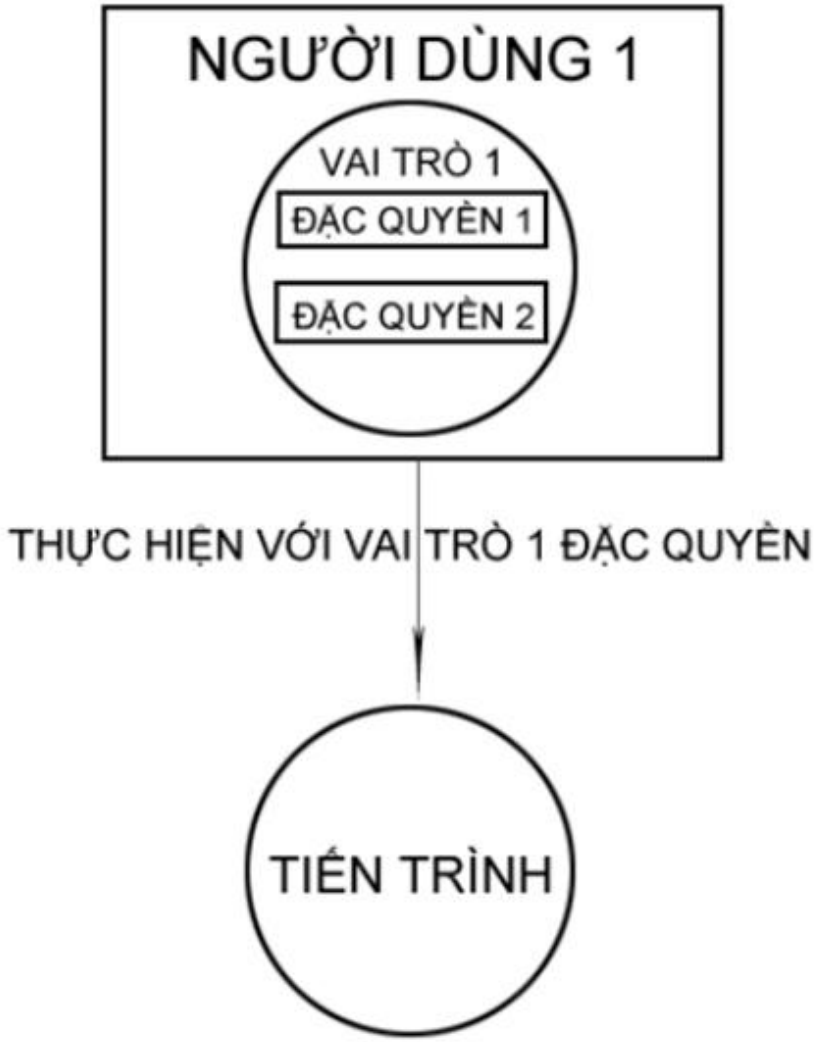
Cơ chế khóa-chìa (A Lock-Key Mechanism): Phương pháp này thực chất là sự kết hợp giữa danh sách quyền truy nhập và danh sách khả năng . Mỗi khách thể sở hữu một danh sách các mã nhị phân gọi là chìa (key). Một chủ thể hoạt động trong miền bảo vệ sở hữu một chìa tương ứng với một khóa trong danh sách của khách thể.

Cũng như phương pháp danh sách khả năng, phương pháp khóa và chìa được quản lý bởi hệ điều hành,người sử dụng không thể truy nhập trực tiếp để thấy được nội dung của nó.

1.8 Kiểm soát quyền truy nhập (Access Control)

Access Control có thể sử dụng trên các file với một tập tin hệ thống. Mỗi tập tin và thư mục được chỉ định một chủ sở hữu riêng, một nhóm hoặc một danh sách các người dùng, và cho các đơn vị, kiểm soát truy cập thông tin được giao. Một chức năng tương tự có thể được thêm vào các khía cạnh khác của một hệ thống máy tính.

Ví dụ: Những tính năng kiểm soát truy nhập được tích hợp sẵn trong Solaris 10 thể hiện qua các đặc quyền trong quy định về quyền cho user 1.



HÌNH 7: VAI TRÒ KIỂM SOÁT TRUY CẬP TRONG SOLIRIS 10

1.9 Thu hồi quyền truy nhập (Revocation of Access Rights)

Trong nội dung bảo vệ hệ thống,đôi khi việc thu hồi một số quyền thao tác trên các khách thể của các chủ thể cũng được xem là một biện pháp bảo vệ. Khi thu hồi quyền truy nhập cần chú ý tới một số vấn đề sau :

- Thu hồi tức khách hay trì hoãn và nêu trì hoãn thì tới bao giờ ?
- Nếu loại bỏ một quyền truy cập của chủ thể tới một khách thể thì loại bỏ tất cả hay chỉ áp dụng với một số chủ đề.
- Thu hồi một số quyền hay toàn bộ quyền trên một khách thể ?
- Thu hồi tạm thời hay vĩnh viễn một quyền truy cập ?

Đối với các hệ thống sử dụng danh sách quyền truy nhập.việc thưc hiện quyền thu hồi truy nhập có thể thực hiện một cách dễ dàng bằng cách tìm và hủy trong ACL. Như vậy viêc thu hồi sẽ có hiệu lực tức thời và có thể áp dụng cho tất cả các chủ thể hoặc một nhóm các chủ thể :thu hồi một cách vĩnh viễn hay tạm thời đều được.

Tuy nhiên, trong các hệ thống sử dụng danh sách khả năng, vấn đề thu hồi sẽ gặp nhiều khó khăn vì các khả năng được phát tán trên khách các miền bảo vệ trong hệ thống, do đó cần phải tìm ra đúng trước khi loại bỏ. Để giải quyết vấn đề này có thể tiến hành theo các phương pháp:

- ***Tái yêu cầu***: loại bỏ các khả năng ra khỏi miền bảo vệ sau mỗi chu kì .nếu miền bảo vệ vẫn còn khả năng nào thì nó sẽ tái yêu câu khả năng đó.
- ***Sử dụng con trỏ ngược***: Với mỗi khách thể sẽ tồn tại các con trỏ,trỏ đến các khả năng tương ứng của khách thể. Khi cần thu hồi quyền truy nhập nào trên khách thể hệ thống sẽ dựa vào các con trỏ để tìm kiếm các khả năng tương ứng.
- ***Sử dụng con trỏ gián tiếp***: trong phương pháp này con trỏ không trỏ trực tiếp tới các khả năng của khách thể mà trỏ tới một bảng toàn cục được quản lý bởi hệ điều hành. Khi cần thu hồi quyền truy nhập chỉ cần xóa phần tử tương ứng trong bảng này.

Trong các hệ thống sử dụng cơ chế khóa và chìa, khi cần thu hồi quyền chỉ cần thay đổi khóa và bắt buộc chủ thể thay đổi chìa khóa mới.

CHƯƠNG 2: TỔNG QUAN VỀ AN TOÀN HỆ THỐNG

Bảo vệ hệ thống là một cơ chế kiểm soát việc sử dụng tài nguyên của các chủ thể (tiến trình và người sử dụng) Để đối phó với các tình huống lỗi có thể phát sinh trong hệ thống. Trong khi đó khái niệm an toàn hệ thống muốn đề cập tới mức độ tin cậy mà hệ thống cần duy trì khi phải đối phó không những với các vấn đề nội bộ mà cả với những tác động đến từ môi trường bên ngoài.

2.1 Các vấn đề về bảo mật hệ thống

Hệ thống được coi là an toàn nếu các tài nguyên được sử dụng đúng quy định trong mọi hoàn cảnh. Điều này khó có thể đạt được trong thực tế. Thông thường, cơ chế an toàn hệ thống bị vi phạm vì các nguyên nhân vô tình hoặc cố ý. Việc ngăn chặn các hành vi cố ý là rất khó khăn vi hầu như không thể đạt hiệu quả hoàn toàn.

Bảo đảm an toàn hệ thống ở cấp cao như chống lại các nguyên nhân hỏa hoạn, thiên tai, mất điện... cần được thực hiện ở mức độ vật lý (trang bị các thiết bị đảm bảo an toàn cho hệ thống) và nhân sự (chọn lựa các nhân viên tin cậy làm việc trong hệ thống). Nếu an toàn môi trường được đảm bảo thì an toàn của hệ thống sẽ được duy trì tốt nhờ các cơ chế của hệ điều hành.

Cần chú ý nếu bảo vệ hệ thống có thể đạt độ tin cậy 100% thì các cơ chế an toàn hệ thống được cung cấp chỉ nhằm ngăn chặn bớt các tình huống bất lợi hơn là đạt đến độ an toàn hệ tuyệt đối.

2.2 Các cơ chế an toàn hệ thống

2.2.1 Kiểm định danh tính

Để đảm bảo an toàn, hệ điều hành cần phải giải quyết tốt vấn đề kiểm định danh tính (authentication). Hoạt động của hệ thống bảo vệ phụ thuộc vào khả năng xác định các tiến trình đang xử lý. Khả năng này, đến lượt nó lại phụ thuộc vào việc xác định người dùng đang sử dụng hệ thống để có thể kiểm tra người dùng này được phép thao tác trên những tài nguyên nào.

Cách tiếp cận phổ biến nhất để giải quyết vấn đề là sử dụng mật khẩu (password) để kiểm định danh tính người sử dụng. Mỗi khi người dùng muốn sử dụng một tài nguyên, hệ thống sẽ so sánh mật khẩu của họ nhập vào với mật khẩu được lưu trữ, nếu đúng họ mới được phép sử dụng tài nguyên. Mật khẩu có thể được

áp dụng để bảo vệ cho từng đối tượng trong hệ thống, thậm chí cùng một đối tượng sẽ có các mật khẩu khác nhau tương ứng với các quyền truy nhập khác nhau.

Cơ chế mật khẩu rất đơn giản và dễ sử dụng, do đó được các hệ điều hành sử dụng rộng rãi, tuy nhiên điểm yếu nghiêm trọng của nó là khả năng bảo mật mật khẩu rất khó đạt được sự hoàn hảo. Những tác nhân tiêu cực có thể tìm ra mật khẩu của người khác nhờ nhiều cách thức khác nhau.

2.2.2 Ngăn chặn nguyên nhân từ phía các chương trình

Trong môi trường hoạt động mà một chương trình được tạo lập bởi một người lại được người khác sử dụng rất có thể xảy ra các tình huống sử dụng sai chức năng, từ đó dẫn tới những hậu quả không lường trước. Hai trường hợp điển hình gây mất an toàn hệ thống có thể đề xuất là:

- ***Ngựa thành Troy:*** khi người sử dụng A kích hoạt một chương trình (do người sử dụng B viết) dưới danh nghĩa của mình (trong miền bảo vệ được gán tương ứng cho người sử dụng A), chương trình này có thể trở thành "chú ngựa thành Troy" vì khi các đoạn lệnh trong chương trình có thể thao tác với các tài nguyên người sử dụng A có quyền nhưng người sử dụng B lại bị cấm, Những chương trình kiểu này đã lợi dụng hoàn cảnh để gây ra các tác hại đáng tiếc.
- ***Cánh cửa nhỏ (Trap-door):*** mối đe dọa đặc biệt nguy hiểm và khó chống đỡ do vô tình hoặc cố ý của các lập trình viên khi xây dựng chương trình. Các lập trình viên có thể để lại một "cánh cửa nhỏ" trong phần mềm của họ để thông qua đó can thiệp vào hệ thống. Chính "cánh của nhỏ" này đã tạo cơ chế cho các hacker thâm nhập và phá hoại hệ thống của người sử dụng. Việc phát hiện các "cánh của nhỏ" để đối phó rất phức tạp vì chúng ta cần phải tiến hành phân tích chương trình nguồn để tìm ra chỗ sơ hở.

2.2.3 Ngăn chặn nguyên nhân từ phía hệ thống

Hầu hết các tính trình hoạt động trong hệ thống đều có thể tạo ra các tiến trình con. Trong các cơ chế hoạt động này, các tài nguyên hệ thống rất dễ bị sử dụng sai mục đích gây mất an toàn cho hệ thống. hai mối đe dọa phổ biến theo phương pháp này là:

- Các chương trình sâu (worm): một chương trình sâu là chương trình lợi dụng cơ chế phát sinh các bản sao trong hệ thống để đánh bại chính hệ thống sau đó chiếm dụng tài nguyên, làm ngưng trệ hoạt động của các tiến trình khác và toàn bộ hệ thống.
- Các chương trình virus: virus là một chương trình phá hoại khá nguy hiểm đối với các hệ thống thông tin. Khác với các chương trình sâu là những chương trình hoàn chỉnh, virus là những đoạn mã có khả năng lây nhiễm vào các chương trình hệ thống và từ đó tàn phá hệ thống.

2.2.4 Giám sát các nguyên nhân

Nhìn chung, việc đảm bảo an toàn hệ thống là rất phức tạp vì nó liên quan tới yếu tố con người. hệ điều hành chỉ có thể áp dụng một số biện pháp để giảm bớt thiệt hại như lập nhật ký sự kiện để ghi nhận các tình huống xảy ra trong hệ thống. Ví dụ như theo dõi:

- ✓ Người sử dụng cố gắng nhập mật khẩu nhiều lần.
- ✓ Các tiến trình với định danh nghi ngờ không được uỷ quyền.
- ✓ Các tiến trình lạ trong trong các thư mục hệ thống.
- ✓ Các chương trình kéo dài thời gian xử lý một cách đáng ngờ.
- ✓ Các tệp tin và các thư mục bị khóa không hợp lý.
- ✓ Kích thước các chương trình hệ thống bị thay đổi…

Việc kiểm tra thường kỳ và ghi nhận những thông tin này giúp hệ thống phát hiện kịp thời các nguy cơ, cho phép phân tích, dự đoán và tìm phương pháp đối phó.

CHƯƠNG 3: BẢO VỆ HỆ THỐNG TRONG WINDOWS

Hệ điều hành Windows giúp bảo vệ các tập tin, ứng dụng và các nguồn lực khác từ việc sử dụng trái phép thông qua một quá trình kết hợp các tài khoản người dùng và nhóm thành viên chống lại các quyền, đặc quyền và quyền liên quan đến các tài khoản và thành viên nhóm. Các chủ đề trong phần này sẽ cho bạn thấy làm thế nào để gán hoặc thiết lập các đặc quyền và quyền. Ngoài ra, sự hiểu biết đặc quyền và các quyền, tại sao sự bảo vệ là cần thiết, và làm thế nào mà có khả năng có thể giúp bạn quản lý tài nguyên chia sẻ có hiệu quả. Hiểu được những quá trình này cũng có thể giúp bạn tránh được những rủi ro không cần thiết và khắc phục mọi vấn đề kiểm soát truy cập, bạn có thể gặp phải.

3.1 Các chủ thể (miền bảo vệ) / User hoặc Group trong windows

- ✓ Full control: có toàn quyền trên folder.
- ✓ Modify (sửa đổi): có toàn quyền sửa chữa như sửa, tạo và xóa folder.
- ✓ Read & Execute (Đọc và thi hành): Quyền được phép đọc bao hàm cả việc gọi.
- ✓ Write (Viết): Quyền ghi.
- ✓ List folder contents (Nội dung danh sách các thư mục): Thấy được các folder bên trong.
- ✓ Special permission (Các quyền đặc biệt): Quyền đặc biệt

3.2 Các quyền tác động của User lên các đối tượng trong hệ thống máy tính

3.2.1 Access control overview (Tổng quan về kiểm soát truy cập)

Kiểm soát truy cập là quá trình cho phép người dùng, nhóm, và máy tính để truy cập vào các đối tượng trên mạng hoặc máy tính.

Để hiểu và quản lý kiểm soát truy cập, chúng ta cần phải hiểu các mối quan hệ :

- ✓ Đối tượng (file, máy in, và các nguồn lực khác)
- ✓ Thẻ truy cập
- ✓ Danh sách điều khiển truy cập (ACL) và các mục kiểm soát truy cập (ACE)
- ✓ Đối tượng (sử dụng hoặc ứng dụng)
- ✓ Hệ điều hành

- ✓ Các quyền
- ✓ Quyền người dùng và đặc quyền

- Trước khi một chủ có thể được truy cập vào một khách thể, chủ thể phải xác định chính nó vào hệ thống phụ bảo mật cho hệ điều hành. danh tính này được chứa trong một thẻ truy cập được tái tạo mỗi lần một chủ thể đăng nhập vào. Trước khi cho phép các chủ thể để truy cập vào một khách thể, kiểm tra hệ thống điều hành để xác định xem các thẻ truy cập cho chủ thể phép truy cập đến khách thể và hoàn thành nhiệm vụ mong muốn. Nó làm điều này bằng cách so sánh thông tin trong thẻ truy cập với mục kiểm soát truy cập (ACE) cho các chủ thể.
- Các ACE có thể cho phép hoặc từ chối một số hành vi khác nhau, tùy thuộc vào loại khách thể. Ví dụ, tùy chọn trên một khách thể tập tin có thể bao gồm đọc, viết, và thi hành. Trên một máy in, các ACE có sẵn bao gồm in, Quản lý máy in, và quản lý tài liệu.
- ACE cá nhân cho một đối tượng được kết hợp trong một danh sách điều khiển truy cập (ACL). Các hệ thống phụ an ninh kiểm tra ACL(Acsess Control List) của đối tượng cho ACE áp dụng cho người sử dụng và nhóm người sử dụng thuộc. Qua từng bước ACE cho đến khi nó tìm thấy một trong số đó, hoặc cho phép hoặc từ chối truy cập cho người sử dụng hoặc một trong các nhóm của người dùng, hoặc cho đến khi không có nhiều ACE để kiểm tra. Nếu nói đến sự kết thúc của ACL và truy cập mong muốn vẫn không cho phép một cách rõ ràng hoặc bị từ chối, các hệ thống phụ an ninh từ chối truy cập đến đối tượng.

✓ Quyền

Quyền xác định các loại hình truy cập cấp cho người dùng hoặc nhóm cho một đối tượng hoặc đối tượng sở hữu. Ví dụ, nhóm Tài chính có thể được cấp Đọc và Viết quyền cho một tập tin có tên Payroll.dat.

Sử dụng giao diện người dùng kiểm soát truy cập, bạn có thể thiết lập quyền truy cập NTFS cho các đối tượng như: các tập tin, thư mục hoạt động, đăng ký, hoặc hệ thống các đối tượng như quy trình. Quyền có thể được cấp cho bất kỳ người sử

dụng, nhóm, hoặc máy tính. Đó là một thực hành tốt để gán quyền cho các nhóm vì nó cải thiện hiệu năng hệ thống khi kiểm tra quyền truy cập vào một đối tượng.

Đối với một đối tượng, bạn có thể cấp quyền truy cập đến:

- Nhóm, người sử dụng, và các đối tượng khác với định danh an ninh trong miền
- Nhóm và người dùng trong miền đó và bất kỳ tên miền tin cậy
- Các nhóm địa phương và người sử dụng trên máy tính, nơi các đối tượng cư trú.

Các quyền gắn liền với một đối tượng phụ thuộc vào loại đối tượng. Ví dụ, các điều khoản có thể được gắn vào một tập tin khác nhau từ những người có thể được gắn vào một khóa registry. Một số cho phép, tuy nhiên, được phổ biến với hầu hết các loại đối tượng. Những điều khoản chung là:

- Đọc
- Sửa đổi
- Thay đổi quyền sở hữu
- Xóa

Khi bạn thiết lập quyền, bạn chỉ rõ mức độ truy cập cho các nhóm và người sử dụng. Ví dụ, bạn có thể cho một người sử dụng đọc nội dung của một tập tin, cho phép người dùng khác thay đổi các tập tin, và ngăn chặn tất cả người dùng khác truy cập các tập tin. Bạn có thể thiết lập quyền tương tự như trên các máy in để người dùng nhất định có thể cấu hình các máy in và những người dùng khác chỉ có thể in.

Khi bạn cần thay đổi các điều khoản trên một tập tin, bạn có thể chạy Windows Explorer, kích chuột phải vào tên file và kích Properties. Trên tab Security, bạn có thể thay đổi quyền truy cập vào các tập tin.

✓ Quyền sở hữu của các đối tượng

Chủ sở hữu được gán cho một đối tượng khi đối tượng được tạo ra. Theo mặc định, các chủ sở hữu là tác giả của các đối tượng. Không có vấn đề gì đặt quyền trên một đối tượng, chủ sở hữu của các đối tượng luôn luôn có thể thay đổi các điều khoản trên một đối tượng. Để biết thêm thông tin,xem Managing Object Ownership.

✓ Quyền thừa kế

Thừa kế cho phép các quản trị viên dễ dàng ấn định và quản lý quyền. Tính năng này sẽ tự động gây ra các đối tượng trong một container để thừa hưởng tất cả các quyền thừa kế của container. Ví dụ, các tập tin trong một thư mục, khi tạo ra, kế thừa quyền truy cập của thư mục. Chỉ cho phép đánh dấu để được thừa hưởng sẽ được thừa hưởng.

✓ Quyền người dùng và đặc quyền

- Quyền sử dụng cấp đặc quyền cụ thể và quyền đăng nhập cho người dùng và các nhóm trong môi trường máy tính của bạn. Người quản trị có thể gán các quyền cụ thể vào các tài khoản nhóm hoặc tài khoản người dùng cá nhân. Những quyền này cho phép người dùng thực hiện các hành động cụ thể, chẳng hạn như đăng nhập vào một hệ thống tương tác hoặc sao lưu các tập tin và thư mục.
- Quyền người dùng khác với quyền vì quyền người dùng áp dụng cho tài khoản người dùng, và quyền được gắn vào các đối tượng. Mặc dù quyền sử dụng có thể áp dụng cho các tài khoản người dùng cá nhân, quyền người dùng được quản lý tốt nhất trên cơ sở tài khoản nhóm. Không có hỗ trợ trong giao diện người sử dụng kiểm soát truy cập để cấp quyền sử dụng; Tuy nhiên, chuyển nhượng quyền sử dụng có thể được quản lý thông qua Local Security Policy snap-in dưới Local Policies \ Quyền tài nhượng. Để biết thêm thông tin, xem User Rights and Privileges.

✓ Kiểm toán đối tượng

Với quyền quản trị, bạn có thể kiểm tra người sử dụng thành công hay thất bại trong tiếp cận với các đối tượng. Bạn có thể lựa chọn truy cập đối tượng kiểm toán bằng cách sử dụng giao diện người dùng kiểm soát truy cập, nhưng trước tiên bạn phải kích hoạt các chính sách kiểm toán bằng cách chọn truy cập đối tượng kiểm toán theo Chính sách Local \ Kiểm toán Chính sách \ Local Policies trong Local Security Policy snap-in. Sau đó bạn có thể xem các sự kiện bảo mật liên quan đến trong bản ghi Security trong Event Viewer.

3.2.2 Permission Entry Dialog Box (Cho phép truy nhập vào hội thoại)

Thư mục có các quyền : cài đặt đầy đủ, sửa đổi, đọc và thực thi, liệt kê nội dung thư mục,đọc và viết. Để biết thông tin về các quyền này, xem ở mục tập tin và quyền thư mục. Mỗi một quyền bao gồm một nhóm những quyền đặc biệt, được liệt kê và định nghĩa dưới đây. Không phải tất cả các điều khoản đặc biệt sẽ áp dụng cho tất cả các đối tượng.

- ✓ Traverse folder/ execute file(thực thi tập tin/ đi vào thư mục): tập tin thực thi cho phép hoặc từ chối di chuyển các thư mục tới các tập tin hoặc thư mục khác ngay cả khi người dùng không có quyền truy cập các thư mục đi qua. tập tin thực thi có hiệu lực chỉ khi nhóm hay người dùng không được cấp các vượt qua các tập tin thực thi người sử dụng ngay trong Console Management Group Policy(bảng điều khiển nhóm chính sách).

Mặc định, tất cả các nhóm được cấp vượt qua các tập tin thực thi người sử dụng ngay (Áp dụng cho các thư mục mà thôi).

Thực hiện tập tin cho phép hay phủ nhận chạy tập tin chương trình (Áp dụng cho các tập tin chỉ).

Thiết lập sự cho phép thư mục thi hành vào một thư mục không tự động thiết lập các thực thi tập tin trên tất cả các tập tin trong thư mục đó.

- ✓ List Folder/Read Data(Danh sách thư mục / đọc dữ liệu): Danh sách thư mục cho phép hoặc từ chối xem tên tập tin và tên thư mục con trong thư mục. Danh sách thư mục ảnh hưởng đến nội dung của chỉ thư mục đó và không ảnh hưởng đến việc thư mục mà bạn đang thiết lập sự cho phép trên sẽ được liệt kê (Áp dụng cho các thư mục mà thôi).

Đọc dữ liệu cho phép hoặc từ chối xem dữ liệu trong các tập tin (Áp dụng cho các tập tin chỉ).

- ✓ Read Attribute(đọc thuộc tính): Cho phép hoặc từ chối xem các thuộc tính của một tập tin hoặc thư mục, chẳng hạn như chỉ đọc và ẩn. Các thuộc tính được định nghĩa bởi NTFS.
- ✓ Read Extended Attributes (đọc thuộc tính mở rộng): Cho phép hoặc từ chối xem các thuộc tính mở rộng của một tập tin hoặc thư mục. Thuộc tính mở

rộng được định nghĩa bởi các chương trình và có thể thay đổi theo từng chương trình.

- ✓ Create Files/Write Data(Tạo tập tin / ghi dữ liệu): Tạo tập tin cho phép hoặc từ chối việc tạo ra các tập tin trong thư mục. (Áp dụng cho các thư mục mà thôi.)

Viết dữ liệu cho phép hoặc từ chối làm thay đổi các tập tin và ghi đè lên nội dung hiện có. (Áp dụng cho các tập tin chỉ.)

- ✓ Create Folders/Append Data(Tạo thư mục / Nối dữ liệu): Tạo thư mục cho phép hoặc từ chối việc tạo ra các thư mục trong thư mục. (Áp dụng cho các thư mục mà thôi.)

Nối dữ liệu cho phép hoặc từ chối làm thay đổi kết thúc của tập tin nhưng không thay đổi, xóa hoặc ghi đè lên dữ liệu hiện có. (Áp dụng cho các tập tin chỉ.)

- ✓ Write Extended Attributes(Write Attributes): Cho phép hoặc từ chối thay đổi các thuộc tính của một tập tin hoặc thư mục, chẳng hạn như chỉ đọc hoặc ẩn. Các thuộc tính được định nghĩa bởi NTFS. Quyền Write Attributes không bao hàm việc tạo hoặc xóa các tập tin hoặc thư mục; nó chỉ bao gồm việc cho phép thay đổi các thuộc tính của một tập tin hoặc thư mục. Để cho phép (hoặc từ chối) tạo hoặc xóa các hoạt động, xem Tạo tập tin / ghi dữ liệu, Tạo thư mục / Nối dữ liệu, Xóa thư mục con và tập tin, và Xóa .
- ✓ Write Extended Attributes(Viết thuộc tính mở rộng):Cho phép hoặc từ chối thay đổi các thuộc tính mở rộng của một tập tin hoặc thư mục. thuộc tính mở rộng được định nghĩa bởi các chương trình và có thể thay đổi theo từng chương trình. Các thuộc tính Viết Mở rộng phép nào không bao hàm việc tạo hoặc xóa các tập tin hoặc thư mục; nó chỉ bao gồm việc cho phép thay đổi các thuộc tính của một tập tin hoặc thư mục. Để cho phép (hoặc từ chối) tạo hoặc xóa các hoạt động, xem Tạo tập tin / ghi dữ liệu, Tạo thư mục / Nối dữ liệu, Xóa thư mục con và tập tin, và Xóa .

- ✓ Delete Subfolders and Files(Xóa thư mục con và tập tin) :Cho phép hoặc từ chối các thư mục con và các tập tin xóa, thậm chí nếu các phép Xóa đã không được cấp trên thư mục hoặc tập tin.
- ✓ Delete(Xóa bỏ):Cho phép hoặc từ chối xóa các tập tin hoặc thư mục. Nếu bạn không có sự cho phép xóa trên một tập tin hoặc thư mục, bạn vẫn có thể xóa nó nếu bạn đã được cấp Xóa thư mục con và tập tin trên thư mục mẹ.
- ✓ Read Permissions(đọc Quyền):Cho phép hoặc từ chối quyền đọc các tập tin hoặc thư mục, chẳng hạn như Full Control, Read, và write.
- ✓ Change Permissions(thay đổi quyền):Cho phép hoặc từ chối cho phép thay đổi các tập tin hoặc thư mục, chẳng hạn như Full Control, Read, và write.
- ✓ Take Ownership(Lấy quyền sở hữu):Cho phép hoặc từ chối nắm quyền sở hữu của tập tin hoặc thư mục. Chủ sở hữu của một tập tin hoặc thư mục luôn có thể thay đổi quyền truy cập vào nó, bất kể bất kỳ khoản đang tồn tại trên các tập tin hoặc thư mục.
- ✓ Synchronize(đồng bộ hóa):Cho phép hoặc từ chối đề khác nhau để chờ đợi trên tay cầm cho các tập tin hoặc thư mục và đồng bộ hóa với một chủ đề đó có thể là dấu hiệu nó. Sự cho phép này chỉ áp dụng cho các chương trình đa tiến đa luồng

CHƯƠNG 4: MỘT SỐ TÍNH NĂNG THỰC HIỆN CƠ CHẾ AN TOÀN TRÊN WINDOWS 10

4.1 Secure Boot – UEFI (Khởi động bảo mật)

Secure Boot là phần mềm ngăn chặn các tệp tin, mã nguồn đáng nghi, độc hại ngay từ khi bắt đầu khởi động máy tính. Những tệp, mã nguồn bị chặn là những tệp không nằm trong hệ điều hành Windows hoặc chưa được công ty Windows chấp nhận để hoạt động trên hệ điều hành của họ, nếu để những tệp này khởi động chung thì rất có thể sẽ gây lỗi cho máy tính của bạn.

Nói một cách dễ hiểu hơn là Secure Boot như một chốt chặn, những phần mềm, tệp tin, mã nguồn,... muốn qua chốt để có thể khởi động cùng hệ thống thì phải có giấy phép. Nếu không có sẽ bị buộc dừng ngay lập tức. Tuy nhiên, bạn có thể điều chỉnh Secure Boot để có thể cho qua những phần mềm đặc biệt theo ý muốn của bạn.

4.2 Early Antimalware (ELAM)

Cơ chế khởi động UEFI bảo vệ trình nạp khởi động và Trusted Boot đã bảo vệ nhân của Windows hoặc các thành phần khởi động Windows khác, do đó cơ hội để các phần mềm độc hại bắt đầu lây nhiễm vào trình điều khiển là tránh không liên quan tới khởi động của Microsoft. Các ứng dụng chống malware truyền thống không bắt đầu cho tới khi các trình điều khiển liên quan đến khởi động được nạp, nên cho phép rootkit giả mạo là một trình điều khiển có cơ hội được làm việc.

Early Antimalware được thiết kế cho phép giải pháp chống ma trận bắt đầu trước tất cả các trình điều khiển và ứng dụng không phải của Microsoft. ELAM kiểm tra tính toàn vẹn của các trình điều khiển ngoại lệ xem có đáng tin cậy hay không, Nếu phần mềm độc hại sửa đổi trình điều khiển liên quan tới khởi động, ELAM sẽ phát hiện sự thay đổi này và Windows sẽ ngăn không có trình điều khiển đó hoạt động, ngăn chặn được các rootkit. ELAM cũng cho phép các nhà cung cấp phần mềm antimalware đăng ký quét các trình điều khiển được nạp trong quá trình khởi động được hoàn tất.

ELAM phân loại các trình điều khiển như sau:

- Tốt: trình điều khiển đã được đăng kí và không bị làm giả mạo.

- Xấu: trình điều khiển đã được xác định là phần mềm độc hại. Khuyến cáo không nên kích hoạt điều khiển xấu được biết đến.
- Xấu nhưng cần thiết cho khởi động: trình điều khiển đã được xác định là phần mềm độc hại nhưng máy tính không thể khởi động thành công mà không tải trình điều khiển này.
- Không xác định: trình điều khiển chưa được chứng thực bởi ứng dụng phát triển phần mềm độc hại hoặc chưa được phân loại

4.3 User Account Control

Kiểm soát Tài khoản Người dùng (UAC) giúp ngăn phần mềm độc hại gây hại cho máy tính và giúp các tổ chức triển khai môi trường máy tính để bàn được quản lý tốt hơn. Với UAC, ứng dụng và nhiệm vụ luôn chạy trong bối cảnh bảo mật của một tài khoản không phải quản trị viên, trừ khi một quản trị viên đặc biệt cho phép quyền truy cập cấp quản trị vào hệ thống. UAC có thể chặn cài đặt tự động các ứng dụng trái phép và ngăn các thay đổi vô ý đối với cài đặt hệ thống. UAC cho phép tất cả người dùng đăng nhập vào máy tính của họ bằng tài khoản người dùng chuẩn. Các quy trình khởi chạy sử dụng token người dùng chuẩn có thể thực hiện các tác vụ sử dụng quyền truy cập được cấp cho người dùng chuẩn. Ví dụ: Windows Explorer tự động được thừa hưởng quyền người dùng cấp độ chuẩn. Ngoài ra, bất kỳ ứng dụng nào được bắt đầu sử dụng Windows Explorer (ví dụ bằng cách nhấp đúp vào một phím tắt) cũng chạy cùng với bộ quyền người dùng chuẩn. Nhiều ứng dụng, bao gồm cả những ứng dụng có trong hệ điều hành, được thiết kế để hoạt động theo cách này. Các ứng dụng khác, đặc biệt là các ứng dụng không được thiết kế đặc biệt với các cài đặt bảo mật, thường đòi hỏi phải có thêm quyền để chạy thành công. Những loại ứng dụng này được gọi là ứng dụng cũ. Ngoài ra, các hành động như cài đặt phần mềm mới và thay đổi cấu hình cho Windows Firewall, cần nhiều quyền hơn những gì có sẵn cho tài khoản người dùng chuẩn. Khi ứng dụng cần chạy với nhiều quyền người dùng chuẩn, UAC có thể khôi phục các nhóm người dùng bổ sung vào mã thông báo. Điều này cho phép người dùng kiểm soát rõ ràng các ứng dụng đang thực hiện thay đổi mức hệ thống đối với máy tính hoặc thiết bị của họ.

Theo mặc định, UAC được đặt để thông báo cho bạn bất cứ khi nào ứng dụng cố gắng thay đổi máy tính của bạn, nhưng bạn có thể thay đổi tần suất UAC thông báo cho bạn.

Trong Windows 10, User Account Control đã bổ sung một số cải tiến:

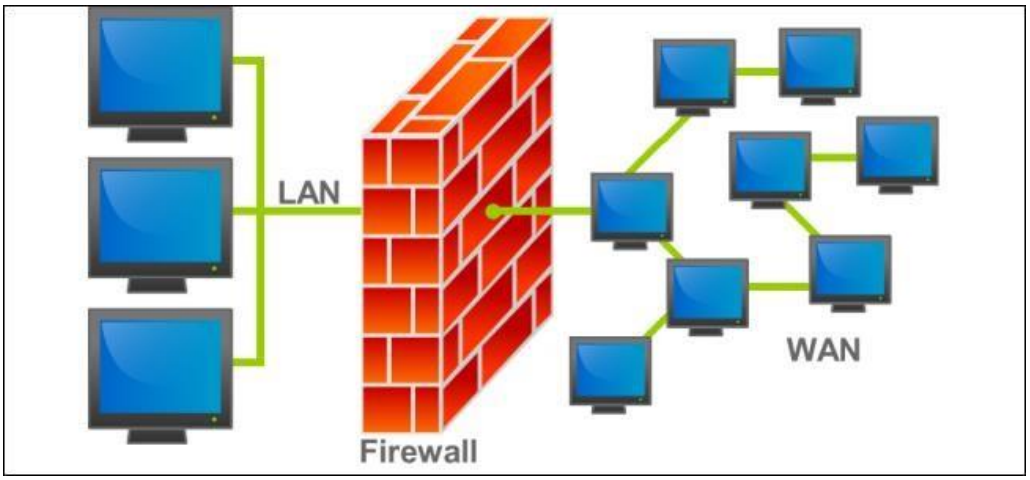
• Tích hợp với giao diện quét Antimalware (AMSI). AMSI quét tất cả các yêu cầu độ cao UAC cho phần mềm độc hại. Nếu phát hiện phần mềm độc hại, đặc quyền quản trị viên sẽ bị chặn.

4.4 Tường lửa

Tường lửa có thể là phần cứng, có thể là phần mềm, nhằm giúp bảo vệ an toàn cho máy tính của bạn.

Những người dùng máy tính từ trước tới nay hầu hết đều đã từng nghe qua từ "Tường lửa" (Firewall), và thường hiểu rằng đây là một biện pháp bảo vệ an toàn cho máy tính. Tuy nhiên, khái niệm tường lửa là gì? Chức năng của nó như thế nào thì không phải ai cũng biết.

Tường lửa được xem như một bức rào chắn giữa máy tính (hoặc mạng cục bộ - local network) và một mạng khác (như Internet), điều khiển lưu lượng truy cập dữ liệu vào ra. Nếu không có tường lửa, các luồng dữ liệu có thể ra vào mà không chịu bất kỳ sự cản trở nào. Còn với tường lửa được kích hoạt, việc dữ liệu có thể ra vào hay không sẽ do các thiết lập trên tường lửa quy định.



HÌNH 8: Mô phỏng tường lửa cơ bản

KẾT LUẬN

Thông qua bài tập lớn chúng ta nắm vững các kiến thức tổng quan về bảo vệ hệ thống của các hệ điều hành như mục tiêu của bảo vệ hệ thống, các cơ chế an toàn… Từ đó ta liên hệ với hệ điều hành windows.

Bài tập lớn này được tổng hợp từ nhiều nguồn tài liệu trong và ngoài nước được nhóm tìm hiểu và đúc kết lại. Việc dịch từ các nguồn tài liệu nước ngoài sẽ không tránh khỏi sai sót trong quá trình làm bài rất mong nhận được những góp ý và nhận xét từ thầy và các bạn đọc.

Chúng em trân thành cảm ơn thầy giáo Nguyễn Thanh Hải đã hướng dẫn tận tình cho chúng em để chúng em có thể hoàn thành tốt bài tập này.

TÀI LIỆU THAM KHẢO

- ✓ Giáo trình Nguyên Lý Hệ Điều Hành, Tác giả: Nguyễn Thanh Hải
- ✓ Giáo trình Nguyên Lý Hệ Điều Hành, Tác giả: Hà Quang Thụy
- ✓ "Khái niệm hệ điều hành, ấn bản thứ chín", Chương 14, Abraham Silberschatz, Greg Gagne và Peter Baer Galvin
- ✓ Tài liệu tìm hiểu trong windows
- ✓ Operating Systems: Internals and Design Principles (7th Edition), Author: William Stallings.
- ✓ Operating Systems Design and Implementation (3rd Edition), Author: Andrew S Tanenbaum & Albert S Woodhull.
- ✓ Operating System Concepts Ninth Edition, Author: Avi Silberschatz, Peter Baer Galvin, Greg Gagne, Copyright © John Wiley & Sons, Inc.