TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**TIỂU LUẬN GIỮA KỲ MÔN HỆ ĐIỀU HÀNH**

**SỰ BẢO MẬT - PROTECTION**

**(CHƯƠNG 13.4)**

*Người hướng dẫn*: **TRẦN TRUNG TÍN**

*Người thực hiện*: **TRẦN QUỐC ANH - 51900007**

Lớp **: 19050201**

Khoá  **: 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020**

**CHƯƠNG 1. NỘI DUNG SINH VIÊN THỰC HIỆN**

**13.4 Sự bảo mật**

Khi thông tin được lưu trữ trong hệ thống máy tính, chúng ta muốn giữ chi nó an toàn khỏi những hư hỏng vật lý (vấn đề về sự xác thực) và những truy cập không đáng tin (vấn đề về sự bảo mật).

Sự xác thực thông thường được cung cấp bởi nhiều bản san của tập tin. Nhiều máy vi tính có nhiều chương trình hệ thống tự động hoàn toàn ( hoặc là thông qua sự can thiệp của người điều hành máy tính), sao chép ổ đĩa tập tin vào đĩa băng vào khoảng thời gian thông thường nào đó (một lần một ngày hay tuần hoặc cả tháng), để phòng hờ cái bản sao đó vô tình bị phá hủy. Hệ thống quản lý tập tin có thể gây hại bởi các vấn đề về phần cứng (như là lỗi đọc hay ghi), dòng năng lượng tăng hoặc giảm, va đập phần cứng, bị bụi bẩn, tác động của nhiệt độ, và thậm chí là kẻ phá hoại. Những tập tin có thể vô tình vị xóa. Những lỗi trong hệ thống phần mềm quản lý tập tin có thể cũng gây ra việc mất mát của nội dung tập tin. Sự xác thực đã được bao quát nhiều chi tiết hơn trong Chương 11.

Sự bảo mật có thể được cung cấp bằng nhiều cách. Như một hệ thống máy tính chạy bằng hệ điều hành hiện đại, chúng ta có thể chu cấp bảo mật bởi việc phản hồi tài khoản của người dùng và mật mã xác thực để truy cập chúng, lưu trữ mã hóa thứ cấp thậm chí có thể một người nào đó mở máy và việc xóa ổ đĩa có thể gây mấy thời gian và khó khăn để truy cập dữ liệu, và việc truy cập tường lửa khi sử dụng, sẽ gây khó khăn cho việc xâm nhập thông qua kết nối mạng. Trong hệ thống đa người dùng, ngay cả việc truy cập hợp lệ của hệ thống cũng cần nhiều cơ chế tiên tiến để cho phép chỉ được truy cập hợp lệ trên dữ liệu.

**13.4.1 Các loại truy cập**

Sự cần thiết khi bảo mật các tập tin và là kết quả trực tiếp của khả năng truy cập tập tin. Hệ thống không cho phép truy cập đến tập tin của người dùng khác mà không có sự bảo mật nào. Vì vậy, chúng ta có thể cung cấp bảo mật hoàn toàn bằng cách cấm truy cập. Ngoài ra, chúng ta có thể cấp quyền truy cập tự do mà không cần bảo mật. Cả hai cách tiếp cận đều quá cùng cực cho việc sử dụng thông thường. Quả là những điều cần thiết trong việc kiểm soát truy cập.

Các máy móc bảo vệ cấp quyền kiểm soát truy cập bằng việc giới hạn các kiểu tập tin truy cập. Truy cập là cho phép hoặc không cho phép đều phụ thuộc vào một số yếu tố, một trong số đó là loại yều cầu truy cập. Một số loại hoạt động khác nhau có thể được kiểm soát:

* **Đọc**. Đọc từ tập tin.
* **Ghi.** Ghi hoặc ghi lại tập tin.
* **Thực thi**. Tải tập tin vào bộ nhớ và thực thi nó.
* **Viết thêm**. Ghi thêm thông tin mới vào cuối tập tin.
* **Xóa**. Xóa tập tin và mở rộng không gian để tiện cho việc sử dụng lại.
* **Liệt kê**. Liệt kê tên và thuộc tính của tập tin.
* **Thay đổi thuộc tính**. Thay đổi thuộc tính của tập tin.

Còn các hoạt động khác, ví dụ như đổi tên, sao chép, và chỉnh sửa tập tin, có thể cũng được kiểm soát. Tuy vậy đối với nhiều hệ thống, những chức năng cao cấp có thể được thực thị bởi chương trình hệ thống, điều mà tạo ra nhiều lời gọi hệ thống cơ bản hay còn gọi là cấp thấp. Bảo mật chỉ được cấp ở mức độ thấp. Ví dụ, sao chép tập tin có thể được thực hiện một cách đơn giản bởi một chuỗi các yêu cầu. Trong trường hợp này, một người dùng với quyền đọc cũng có thể...sao chép, in…

Nhiều cơ chế bảo mật đã được đề xuất. Mỗi cái thuận lợi và bất lợi phải phù hợp với các ứng dụng đã được định sẵn. Hệ thống máy tính nhỏ có thể được dùng bởi rất ít thành viên của một nhóm nghiên cứu, ví dụ, có thể không cần thiết cho nhiều loại bảo mật cũng như một máy tính doanh nghiệp lớn được dùng để nghiên cứu, tài chính và nhân sự. Chúng ta thảo luận một vài cách tiếp cận bảo mật trong phần tiếp theo và được nói rõ hơn ở Chương 17.

**13.4.2 Kiểm soát quyền truy cập**

Cách tiếp cận phổ biến nhất cho vấn đề bảo mật cũng khiến cho quyền truy cập phụ thuộc đến người dùng. Nhiều người dùng khác nhau có thể cần nhiều loại truy cập tập tin hoặc thư mục cũng khác nhau. Chiến lược chung nhất để thực hiện truy cập là liên kết với mỗi tệp hoặc thư mục các danh sách kiểm soát quyền truy cập (ACL), chỉ định tên người dùng và các loại quyền truy cập được phép cho mỗi người dùng. Khi người dùng yêu cầu một quyền truy cập vào một tệp cụ thể nào đó, hệ điều hành sẽ kiểm tra danh sách truy cập có liên quan đến tập tin đó. Nếu người dùng được liệt kê trong danh sách quyền truy cập, quyền truy cập sẽ được cho phép.

Cách tiếp cận này có một điều có lợi là cho phép các phương thức truy cập phức tạp. Vấn đề chính với danh sách truy cập là độ dài của chúng. Nếu chúng ta muốn cho phép mọi người nào đó đọc một tệp, chúng ta phải liệt kê tất cả người dùng có quyền đọc. Cơ chế này sẽ có hai hậu quả không mong muốn xảy ra:

* Tạo dựng một danh sách như vậy có thể là một nhiệm vụ buồn chán và không được chuyển tiếp, đặc biệt là nếu chúng ta không biết trước danh sách người dùng trong hệ thống.
* Đi vào thư mục,có kích thước cố định trước, bây giờ phải có kích thước có thể thay đổi, dẫn đến quản lý không gian phức tạp hơn.

Những vấn đề này có thể được giải quyết bằng cách sử dụng phiên bản thu gọn của danh sách truy cập.

Để thu nhỏ độ dài của danh sách kiểm soát quyền truy cập, nhiều hệ thống phát hiện được ba tầng lớp người dùng liên quan đến mỗi tập tin:

* **Chủ sở hữu.** Người mà tạo ra tập tin là chủ sở hữu.
* **Nhóm**. Một bó người dùng chia sẻ tập tin và cần truy cập là một nhóm hoặc một nhóm làm việc.
* **Các thành phần khác**. Tất các những người dùng khác trong hệ thống

Cách tiếp cận phổ biến nhất là kết hợp các danh sách kiểm soát truy cập với kiểm soát truy cập chủ sở hữu, nhóm và vũ trụ chung hơn (và dễ thực hiện hơn) mà chúng ta vừa mô tả. Ví dụ, Solaris sử dụng ba loại truy cập nhưng cho phép danh sách kiểm soát truy cập được thêm vào các tập tin và thư mục cụ thể khi muốn kiểm soát truy cập chi tiết hơn.

Để minh họa, tưởng tượng như là 1 người, Sara, đang viết một quyển sách mới. Cô ấy đã thuê 3 học sinh tốt nghiệp (Jim,Dawn và Jill) để phụ cô ấy trong dự án. Văn bản của quyển sách được giữ trong một tập tin tên là book.text.

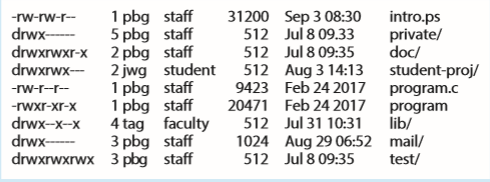
Sự bảo vệ liên kết với tập tin này được thể hiện như bên dưới:

* Sara có thể gọi tất cả các hoạt động trên tập tin.
* Jim, Dawn, và Jill có thể chỉ đọc và ghi tập tin; chúng không nên được cấp quyền xóa tập tin.
* Tất cả các người dùng khác nên được phép đọc, nhưng không dc được ghi lên tập tin (Sara quan tâm đến việc cho phép nhiều người đọc vì thế cô ấy có thể nhận được phản hồi)

**SỰ CHO PHÉP TRONG HỆ THỐNG UNIX**

Trong hệ thống UNIX, bảo vệ thư mục và bảo vệ tập tin được giải quyết khá giống nhau. Liên quan đến mỗi thư mục và tập tin gồm 3 nhóm – người sở hữu (owner), nhóm (group), vũ trụ (universe) – mỗi lĩnh vực bao gồm có 3 bit rwx, trong đó, “r” điều khiển việc truy cập đọc, “w” điều khiển việc ghi, “x” điều khiển việc thực thi. Do đó, một người dùng có thể liệt kê nội dung của thư mục con chỉ với việc đặt bit “r” vào nhóm thích hợp. Cũng giống như vậy, người dùng có thể thay đổi thư mục hiện tại của họ thành một một thư mục khác (gọi là foo) chỉ bằng cách đặt bit “x” liên quan đến thư mục con foo vào nhóm thích hợp.

Một ví dụ thư mục được liệt từ một môi trường hệ thống UNIX được đưa ra như sau:



Miền (cột) đầu tiên mô tả cách bảo vệ file hoặc thư mục. Kí tự đầu tiên “d” chỉ ra thư mục con. Nó còn cho ta thấy ra số lượng đường liên kết đến tập tin, tên của người sở hữu, tên của nhóm, kích thước của tập tin được tính bằng byte, thời gian chỉnh sửa lần cuối, và cuối cùng là tên của file (với phần mở rộng tùy chọn) .

Để đạt được sự bảo mật như thế này, chúng ta phải tạo một nhóm mới – nói, “text” – với thành viện Jim, Dawn, và Jill. Tên của nhóm là “text” , phải liên quan đến bộ sách.tex, và những truy cập đúng đắn phải được đặt trong chính sách mà chúng ta đã đặt ra.

Bây giờ thử cùng cân nhắc một người tới thăm mà Sara sẽ muốn giao cho quyền truy cập tạm thời tới Chương 1. Người tới thăm này không thể được thêm vào nhóm “text” bởi vì như vậy sẽ cho anh ta quyền truy cập tới tất cả các chương. Và bởi vì một tập tin chỉ có thể ở trong một nhóm, Sara không thể thêm nhóm nào khác vào Chương 1.

Với sự thêm vào của tính năng danh sách quyền điều khiển truy cập, điều này sẽ giúp người tới thăm có thể được thêm vào danh sách điều khiển truy cập của Chương 1.

Để viễn cảnh này có thể hoạt động một cách đúng đắn, các quyền và các danh sách truy cập cần phải được điều khiển một cách chặt chẽ. Việc điều khiển có thể được

hiện thực bằng một số cách. Ví dụ như, trong hệ thống UNIX, các nhóm có thể được tạo ra và được chỉnh sửa bởi duy nhất người quản lý của các tính năng (hoặc bởi bất kỳ siêu người dùng nào). Do đó, việc điều khiển sẽ đạt được thông qua sự tương tác với người dùng. Các danh sách truy cập sẽ được thảo luận kỹ càng hơn ở Mục 17.6.2.

**CHƯƠNG 2. NỘI DUNG CỦA SÁCH**

**13.4 Protection**

When information is stored in a computer system, we want to keep it safe from physical damage (the issue of reliability) and improper access (the issue of protection).

Reliability is generally provided by duplicate copies of files. Many computers have systems programs that automatically (or through computer-operator intervention) copy disk files to tape at regular intervals(once per day or week or month) to maintain a copy should a file system be accidentally destroyed. File systems can be damaged by hardware problems(such as errors in reading or writing), power surges or failures, head crashes, dirt, temperature extremes, and vandalism. Files may be deletedaccidentally. Bugs in the file-systemsoftware can also cause file contents to be lost. Reliability was covered in more detail in Chapter 11.

Protection can be provided in many ways. For a laptop system running a modern operating system, we might provide protection by requiring a user name and password authentication to access it, encrypting the secondary storage so even someone opening the laptop and removing the drive would have a difficult time accessing its data, and firewalling network access so that when it is in use it is difficult to break in via its network connection. In multiuser system, even valid access of the system needs more advanced mechanisms to allow only valid access of the data.

**13.4.1 Types of Access**

The need to protect files is a direct result of the ability to access files. Systems that do not permit access to the files of other users do not need protection.Thus, we could provide complete protection by prohibiting access.Alternatively,we could provide free access with no protection. Both approaches are too extreme for general use. What is needed is controlled access.

Protection mechanisms provide controlled access by limiting the types of file access that can be made. Access is permitted or denied depending on several factors, one of which is the type of access requested. Several different typesof operations may be controlled:

* Read. Read from the file.
* Write. Write or rewrite the file.

• Execute. Load the file into memory and execute it.

• Append.Write new information at the end of the file.

• Delete. Delete the file and free its space for possible reuse.

• List. List the name and attributes of the file.

• Attribute change. Changing the attributesof the file.

Other operations, such as renaming, copying, and editing the file, may also be controlled. For many systems, however, these higher-level functions may be implemented by a system program that makes lower-level system calls. Protection is provided at only the lower level. For instance, copying a file may be implemented simply by a sequence of read requests. In this case, a user with read access can also cause the file to be copied, printed, and so on.

Many protection mechanisms have been proposed. Each has advantages and disadvantages and must be appropriate for its intended application. A small computer system that isused by only a few members of a research group, for example, may not need the same types of protection as a large corporate computer that is used for research, finance, and personnel operations. We discuss some approaches to protection in the following sections and present a more complete treatment in Chapter 17.

**13.4.2 Access Control**

The most common approach to the protection problem is to make access dependent on the identity of the user. Different users may need different types of access to a file or directory. The most general scheme to implement identity dependent access is to associate with each file and directory an access-control list (ACL) specifying user names and the types of access allowed for each user. When a user requests access to a particular file, the operating system checks the access list associated with that file. If that user is listed for the requested access, the access is allowed. Otherwise, a protection violationoccurs, and the user job is denied access to the file.

This approach has the advantage of enabling complex access methodologies. The main problem with access lists is their length. If we want to allow everyone to read a file, we must list all users with read access. This technique has two undesirable consequences:

• Constructing such a list may be a tedious and unrewarding task, especially if we do not know in advance the list of users in the system.

•The directory entry, previously of fixed size, now must be of variable size, resulting in more complicated space management.

These problems can be resolved by use of a condensed version of the access list.

To condense the length of the access-control list, many systems recognize three classifications of users in connection with each file:

• Owner. The user who created the file is the owner.

• Group. Aset of users who are sharing the file and need similar access is a group, or work group.

• Other. All other users in the system.

The most common recent approach is to combine access-control lists with the more general (and easier to implement) owner, group, and universe access control scheme just described. For example, Solar isuses the three categories of access by default but allows access-controllists to be added to specific files and directories when more fine-grained access control is desired.

To illustrate, consider a person, Sara, who is writing a new book. She has hired three graduate students (Jim,Dawn, and Jill) to help with the project.The text of the book is kept in a file named book.tex. The protection associated with this file is as follows:

• Sara should be able to invoke all operations on the file.

• Jim, Dawn, and Jill should be able only to read and write the file; they should not be allowed to delete the file.

• All other users should be able to read, but not write, the file. (Sara is interested in letting as many people as possible read the text so that she can obtain feedback.)

PERMISSIONS IN AUNIX SYSTEM

In the UNIX system, directory protection and file protection are handled

similarly. Associated with each file and directory are three fields —owner,

group, and universe—each consisting of the three bits rwx, where r controls

read access, w controls write access, and x controls execution. Thus, a user can

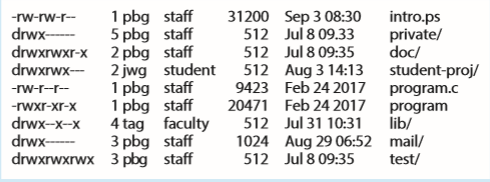
list the content of a subdirectory only if the r bit is set in the appropriate field.

Similarly, a user can change his current directory to another current directory

(say, foo) only if the x bit associated with the foo subdirectory is set in the

appropriate field.

A sample directory listing from a UNIX environment is shown in below:



The first field describes the protection of the file or directory. A d as the first

character indicates a subdirectory. Also shown are the number of links to the

file, the owner’s name, the group’s name, the size of the file in bytes, the date

of last modification, and finally the file’s name (with optional extension).

To achieve such protection, we must create a new group—say, text —

with members Jim, Dawn, and Jill. The name of the group, text, must then

be associated with the file book.tex, and the access rights must be set in

accordance with the policy we have outlined.

Now consider a visitor to whom Sara would like to grant temporary access

to Chapter 1. The visitor cannot be added to the text group because that would

give him access to all chapters. Because a file can be in only one group, Sara

cannot add another group to Chapter 1. With the addition of access-control-

list functionality, though, the visitor can be added to the access control list of

Chapter 1.

For this scheme to work properly, permissions and access lists must be con-

trolled tightly. This control can be accomplished in several ways. For example,

in the UNIX system, groups can be created and modified only by the manager

of the facility (or by any superuser). Thus, control is achieved through human

interaction. Access lists are discussed further in Section 17.6.2.

**CHƯƠNG 3. CÁC THUẬT NGỮ VÀ GHI CHÚ**

**Protection : sự bảo mật -> thông tin nào của chúng ta đều cần được an toàn, nên ta phải có bảo mật, cũng như là tài khoản Facebook, Instagram, Mail…**

**Access-control list (ACL): danh sách kiểm soát quyền truy cập -> là một danh sách tuần tự các câu lệnh mang tính kiểm soát và bảo mật.**