

Bài 6.
Phân quyền truy cập


ONE LOVE. ONE FUTURE.

1

1

Nội dung

- Các khái niệm cơ bản
- Mô hình ma trận điều khiển truy cập
- Một số phương pháp điều khiển truy nhập

 ĐAI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

2


2



3

Khái niệm

- Điều khiển truy cập (Access Control): Là chức năng của hệ thống được thi hành để cho phép chủ thể (người dùng, tiến trình, thiết bị) được truy cập đến một mức nào đó (quyền truy cập) tới tài nguyên của hệ thống và chia sẻ quyền truy cập này cho chủ thể khác
- Mô hình điều khiển truy cập AAA
 - Authentication (Xác thực): Xác định đúng chủ thể thực hiện hành vi truy nhập
 - Authorization (Ủy quyền): phân quyền truy cập
 - Auditing (Kiểm toán): kiểm tra, giám sát các hành vi truy cập
- Có mặt trong hầu hết các ứng dụng, hệ thống công nghệ thông tin

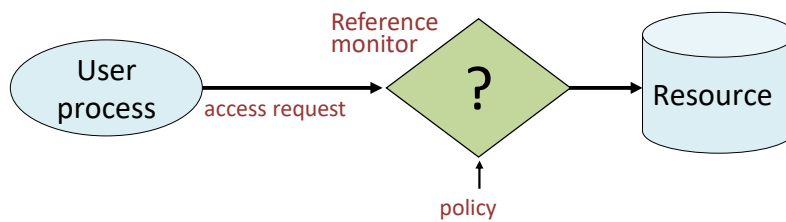
 ĐAI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

4

4

Kiểm soát hoàn toàn (nhắc lại)

- Reference Monitor: Module kiểm tra quyền truy cập
 - Không thể vòng tránh
 - Chống sửa đổi
 - Có thể thẩm tra
- là 1 thể hiện của TCB

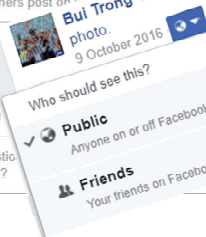


5

Ví dụ 1: chia sẻ thông tin trên MXH Facebook

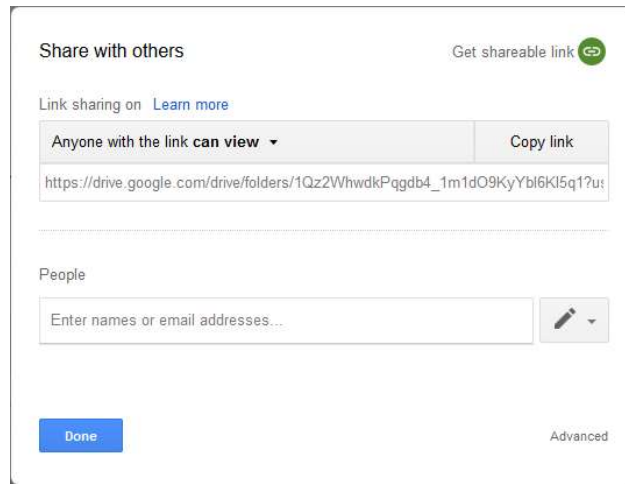
Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Only me
	Review posts that friends tag you in before they appear on your Timeline?	Off
Who can see things on my Timeline?	Review what other people see on your Timeline	
	Who can see posts you've been tagged in on your Timeline?	Only me
	Who can see what others post on...	
How can I manage tags people add and tagging suggestions?	Review tags people add and tagging suggestions?	
	When you're tagged add to the audience if...	
	Who sees tag suggestions you are uploaded?	



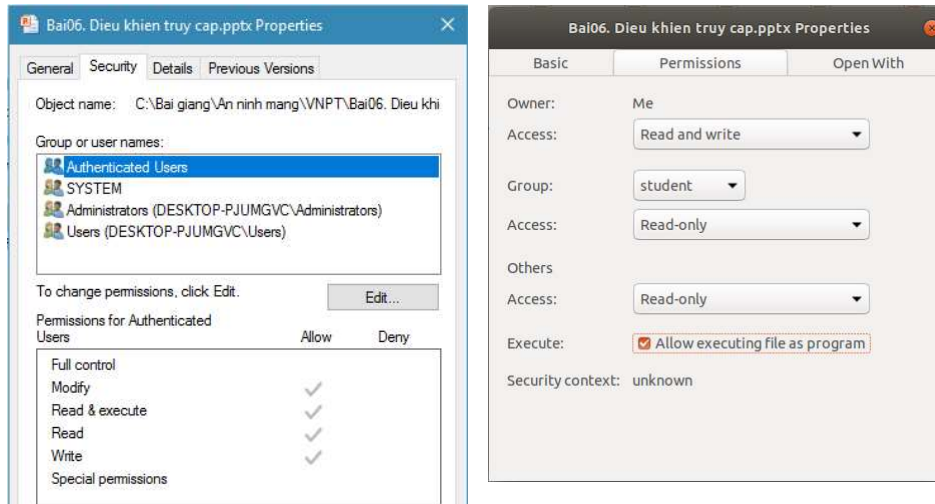
6

Ví dụ 2: Chia sẻ trong Google Drive



7

Ví dụ 3: Điều khiển truy cập trên tệp tin



Microsoft Windows

Linux Ubuntu

8

Ma trận điều khiển truy cập

- Access Control Matrix (ACM)
- Thể hiện các quyền đã cấp phát cho các chủ thể sử dụng tới từng tài nguyên của hệ thống
- S: Tập các chủ thể
- O: Tập các tài nguyên
- R: Tập các quyền truy cập

$A(s_i, o_j)$: các quyền truy cập của chủ thể s_i lên tài nguyên o_j

	O			
	o_1	...	o_m	
s_1				S
s_2	$r_x, r_y \dots$			
...				
s_n				

Ma trận điều khiển truy cập

- Không thể cài đặt trực tiếp ACM với đầy đủ các thành phần:
 - Số lượng tài nguyên cần phải quản lý quá lớn
 - Kích thước ma trận tăng \rightarrow tăng bộ nhớ lưu trữ, thời gian tìm kiếm
- Cài đặt gián tiếp ACM:
 - Phân rã theo cột: Danh sách điều khiển truy cập (Access Control List - ACL)
 - Phân rã theo dòng: Danh sách năng lực (Capability List - CL)
 - Các biểu diễn gián tiếp khác

Danh sách điều khiển truy cập

- Tiếp cận hướng tài nguyên: mỗi tài nguyên có một ACL định nghĩa các chủ thể và quyền truy cập của mỗi chủ thể trên tài nguyên đó

- Cần phải xác thực danh tính chủ thể

→ Chống giả mạo danh tính

- Các vấn đề cần giải quyết:

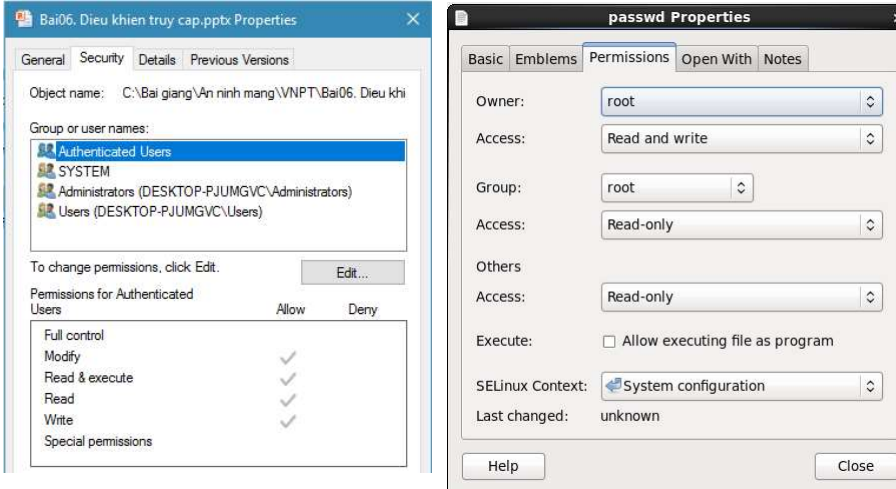
- Quyền cập nhật ACL
- Loại cập nhật được phép
- Các thủ tục rút phép

- Các khái niệm hỗ trợ:

- Người sở hữu(Owner)
- Nhóm(Group)

	objectX
s1	r1,r2
s2	r3
..	..
..	
Sn	r1, r3

Danh sách điều khiển truy cập – Ví dụ



The image shows two side-by-side screenshots of Windows security dialog boxes. The left window, titled 'Bai06. Dieu khien truy cap.pptx Properties', shows the 'Security' tab with a list of users and groups including 'Authenticated Users', 'SYSTEM', 'Administrators', and 'Users'. Below, the 'Permissions for Authenticated Users' table shows 'Full control', 'Modify', 'Read & execute', 'Read', and 'Write' all checked under the 'Allow' column. The right window, titled 'passwd Properties', shows the 'Permissions' tab with 'root' as the owner and group, and 'Read and write' and 'Read-only' as access permissions for the owner and group respectively. The 'SELinux Context' is set to 'System configuration'.

Danh sách năng lực(Capability List)

- Tiếp cận hướng chủ thể: mỗi chủ thể có danh sách các tài nguyên và quyền truy cập trên tài nguyên đó
 - Không có danh tính của chủ thể trên đó
- Danh sách năng lực thường triển khai dưới dạng thẻ truy cập:
 - Có thể truyền từ chủ thể này tới chủ thể khác
 - Không cần xác thực chủ thể
- Vấn đề cần giải quyết: Chống giả mạo CL, chống dùng lại trái phép (replay attack)

13

2. Các mô hình điều khiển truy cập

14

Mô hình điều khiển truy cập DAC

- Discretionary Access Control: mô hình điều khiển truy cập tùy nghi
- Quyền truy cập định nghĩa cho mỗi cặp (chủ thể, tài nguyên) được quyết định bởi chủ sở hữu của tài nguyên
- Được sử dụng rộng rãi trong các hệ điều hành
- Hạn chế: khả năng quản trị lỏng lẻo, không quản lý được sự lan truyền của quyền dẫn đến sự mất an toàn của hệ thống
- Ví dụ: người dùng cấp quyền truy cập trên các thư mục chia sẻ

Case study: DAC trong SQL

- Cấp quyền: lệnh GRANT
GRANT <danh sách các quyền>
ON <danh sách đối tượng dữ liệu>
TO <danh sách người dùng>
[WITH GRANT OPTION] //lan truyền quyền
- Thu hồi quyền: lệnh REVOKE
REVOKE <danh sách các quyền>
ON <danh sách đối tượng dữ liệu>
FROM <danh sách người dùng>

Case study: DAC trong SQL

Lan truyền quyền

- Một người dùng A là chủ sở hữu của bảng quan hệ O: người dùng A có thể cấp quyền R trên O cho người dùng B với tùy chọn WITH GRANT OPTION hoặc không
 - Nếu trong lệnh cấp quyền có tùy chọn WITH GRANT OPTION, B có thể cấp quyền R cho người dùng C khác
- chủ sở hữu của O không biết sự lan truyền của quyền R từ B tới C
- Khi A thu hồi quyền R đã cấp cho B, tất cả những quyền đã cấp cho người dùng khác do sự lan truyền đều được thu hồi

DAC và điều khiển dòng thông tin

- Hạn chế của DAC: cho phép thông tin truyền từ chủ thể này sang chủ thể khác mà không có chính sách kiểm soát
- Ví dụ: Bob không được phép xem nội dung tệp tin A. Anh ta có thể nhờ Alice (hoặc đánh lừa Alice thực thi chương trình) đọc nội dung tệp tin A và sao chép vào tệp tin B là file mà anh ta có quyền đọc

Mô hình điều khiển truy cập MAC

- Mandatory Access Control: điều khiển truy cập cưỡng bức
- Quyền truy cập được cấp phát theo chính sách chung của hệ thống dựa trên phân loại người dùng và tài nguyên
- Phân loại chủ thể: mức độ tin cậy và lĩnh vực hoạt động
- Phân loại tài nguyên: mức độ nhạy cảm và lĩnh vực của tài nguyên

Mô hình Bell-LaPadula

- Mô hình kiểm soát truy cập cho mục tiêu bảo vệ tính bí mật
- Phân loại mức độ bí mật(Clearance Level):
Top Secret > Secret > Confidential > Unclassified
- Simple Security Property: chủ thể s chỉ có thể đọc đối tượng o nếu chủ thể có mức độ bí mật cao hơn hoặc bằng (nguyên tắc no-read-up)
- *-Property: chủ thể chỉ có quyền ghi đối tượng o nếu chủ thể có mức độ bí mật thấp hơn hoặc bằng (nguyên tắc no-write-down)

Bài tập: Mô hình Bell-LaPadula

TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

- Quyền của những người dùng?

Mô hình Biba

- Bảo vệ tính toàn vẹn
- Phân loại mức độ toàn vẹn:
Crucial > Very Important > Important
- Các nguyên tắc:
 - No-write-up: chủ thể s chỉ có thể chỉnh sửa được đối tượng o nếu mức độ toàn vẹn của chủ thể cao hơn hoặc bằng
 - No-read-down: s chỉ có thể đọc được o nếu mức độ toàn vẹn của chủ thể thấp hơn hoặc bằng
 - Thực thi: chủ thể s1 chỉ có thể thực thi chủ thể s2 nếu mức độ toàn vẹn của $s1 \geq s2$

Bài tập: Mô hình Biba

Crucial	Alice, Charlie	File A
Very Important	Bob	File B
Important	David	File C

23

Mô hình Chinese Wall

- Tài nguyên được chia thành các nhóm tranh chấp
- Chủ thể S có quyền truy cập tới mọi đối tượng trong một nhóm, tuy nhiên nếu S đã truy cập tới O thì S không còn quyền truy cập tới mọi $O' \neq O$ trong nhóm đó

24

Mô hình điều khiển truy cập MAC

- Ưu điểm:
 - Quản trị tập trung
 - Tính bảo mật cao
- Nhược điểm:
 - Đòi hỏi phải phân loại rõ ràng chủ thể và tài nguyên
 - Phạm vi ứng dụng hạn chế

25

Mô hình điều khiển truy cập RBAC

- Role-based Access Control: Điều khiển truy cập theo vai
- Việc cấp quyền truy cập không trực tiếp hướng tới người dùng cuối mà hướng tới nhóm người dùng có nhiệm vụ, vai trò trong hệ thống
- Phản ánh tốt hơn đặc trưng nghiệp vụ của hệ thống thông tin của tổ chức
- Vai trò(Role-Group): khái niệm tượng trưng cho một nhóm, một dạng nhiệm vụ xử lý
- Mỗi vai trò được gán các quyền truy cập, có tính lâu dài
- Mỗi người dùng được gán cho một hoặc nhiều vai trò và có quyền truy cập theo vai trò

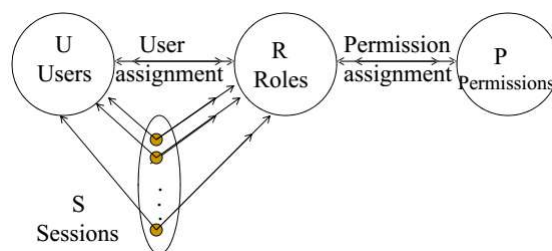
26

Mô hình điều khiển truy cập RBAC

- Có khả năng diễn tả cao các chính sách của tổ chức: phân công theo vai trò là cơ sở cho sự sự tách biệt các nhiệm vụ cũng như tạo ra cơ chế đại diện ủy nhiệm
- Linh hoạt và mềm dẻo: yêu cầu bảo mật mới sẽ chỉ dẫn đến thay đổi cách thức gán quyền truy nhập vào các vai trò
- Khả năng co giãn tốt do các quyền truy cập không gán trực tiếp cho người dùng cuối

27

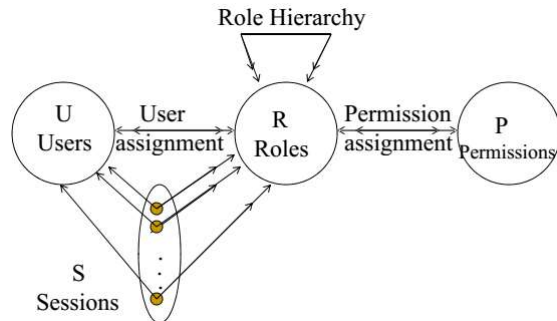
RBAC₀



- Ánh xạ $UA \subseteq U \times R$: Gán vai trò cho người dùng
- Ánh xạ $PA \subseteq P \times R$: Gán quyền cho vai trò
- Tập S: phiên truy cập của người dùng với các vai trò khác nhau. Trong mỗi phiên, người dùng có thể sử dụng một hoặc đồng thời nhiều vai trò

28

RBAC₁



- Tổ chức phân cấp các vai trò
- Vai trò ở cấp cao hơn được thừa hưởng các quyền ở vai trò cấp thấp hơn

3. Case study: Điều khiển truy cập trong hệ điều hành unix


Các khái niệm

- Định danh người dùng: UID
- Định danh nhóm người dùng: GID
- Định danh tiến trình: PID
- Đối tượng cần điều khiển truy cập: tệp tin, thư mục
 - Lưu ý: mọi thiết bị ngoại vi được Unix coi là tệp tin hoặc thư mục
- Tổ chức lưu trữ tệp tin, thư mục
 - Thư mục là một loại tệp tin đặc biệt
 - Tệp tin phải nằm trong một thư mục
 - Cấu trúc phân cấp
 - Quyền truy cập trên thư mục không có tính kế thừa

Điều khiển truy cập trong Unix

- Sử dụng ACL rút gọn
- Sử dụng mô hình RBAC + DAC
- Các quyền: Đọc(r-Read), Ghi(w-Write), Thực thi(x-Execute)
- Khi truy cập một tệp tin/thư mục: cần có quyền truy cập tương ứng trong tất cả các thư mục trong đường dẫn

	File 1	File 2	...
User 1	read	write	-
User 2	write	write	-
User 3	-	-	read
...			
User n	Read	write	write



	File 1	File 2	...
Owner	read	write	-
Group	write	write	-
Other	-	-	read

Điều khiển truy cập trong Unix

- Mỗi quyền được đại diện bởi 1 bit:
 - Có quyền: 1
 - Không có quyền: 0
- Thông tin quyền truy cập được lưu trữ trong 10 bit:
 - Bit 1: Tập tin(hiển thị '-') hay thư mục(hiển thị 'd').
 - Bit 2, 3, 4: Quyền truy cập cho tài khoản sở hữu
 - Bit 5, 6, 7: Quyền truy cập cho nhóm sở hữu
 - Bit 8, 9, 10: Quyền truy cập cho các nhóm người dùng khác
- Biểu diễn::
 - Số: 3 chữ số thập phân tương ứng với 3 nhóm quyền
 - Chuỗi: hiển thị các ký tự viết tắt cho quyền, dấu '-' biểu thị không có quyền

Biểu diễn quyền: Ví dụ

- Dạng số: 777
 - Nhị phân: (?)111 111 111
 - Chuỗi ký tự: (?) rwx rwx rwx
- Dạng số: 640
 - Nhị phân: (?)110 100 000
 - Chuỗi ký tự: (?)rw-r-----

Điều khiển truy cập trong Unix

- Gán quyền sở hữu file/thư mục

chown *user:group filename*

- Gán quyền truy cập file/thư mục

chmod *permission filename*

- Xem thông tin phân quyền trên file/thư mục

```
student@ubuntu:~$ ls -l
total 76
-rwxr-xr-x 1 student student 2126 Oct  2  2018 'Bai06. Dieu khien truy cap.pptx'
drwxr-xr-x 2 student student 4096 Aug 15  2018 Desktop
drwxr-xr-x 2 student student 4096 Feb  6 18:31 Documents
```

Điều khiển truy cập trong Unix

- Unix phân biệt quyền truy cập thư mục và truy cập file trong thư mục
- Người dùng có thể xóa file nằm trong thư mục mà họ có quyền truy cập thư mục nhưng không có quyền truy cập file?

→ sticky bit:

- Off: Nếu người dùng có quyền truy cập thư mục, họ có thể đổi tên file, xóa file
- On: Chỉ có tài khoản sở hữu file, sở hữu thư mục hoặc tài khoản root mới có quyền đổi tên file, xóa file

Điều khiển truy cập trong Unix

- Trên thực tế, người dùng là chủ thể thao tác nhưng tiến trình là chủ thể truy cập tệp tin
 - Tiến trình được cấp quyền của người dùng đã kích hoạt nó
- Làm cách nào để tiến trình có quyền ở cấp cao hơn?
 - Ví dụ: **passwd** là tệp tin hệ thống nhưng người sử dụng thông thường có nhu cầu sửa nội dung khi họ thay đổi mật khẩu?
- Mỗi tiến trình được gắn với 3 giá trị UID, GID:
 - Real UID, GID: UID, GID của người dùng kích hoạt tiến trình
 - Effective UID, GID: UID, GID hiệu lực khi tiến trình truy cập tệp tin
 - Saved UID, GID: UID, GID quay lui khi tiến trình kết thúc truy cập
- Tệp tin/thư mục được gắn 1 bit **setuid** cho biết tiến trình truy cập có thể thay đổi effective UID không?

Điều khiển truy cập trong Unix

Cách thức gán ID cho tiến trình:

- Khi tiến trình được kích hoạt
 - Real UID: UID của người dùng thực thi tiến trình
 - Effective UID: UID của người dùng thực thi tiến trình
- Khi tiến trình truy cập tệp tin/thư mục:
 - Real UID: UID của người dùng thực thi tiến trình
 - Saved UID: UID cũ của Effective UID
 - Effective UID: thay đổi thành UID của người dùng sở hữu nếu **setuid = 1**, ngược lại không đổi
- Khi tiến trình kết thúc truy cập: trả lại các giá trị giống như khi tiến trình trước khi truy cập tệp tin/thư mục

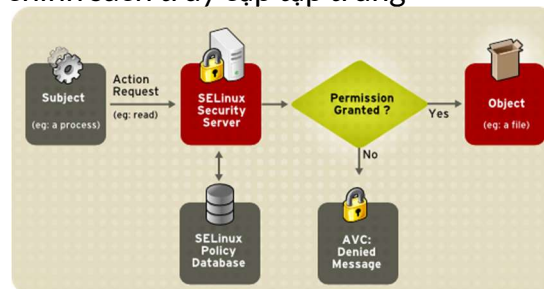
Điều khiển truy cập trong Unix

- Tài khoản root:
 - UID = 0
 - Có mọi quyền truy cập trên tất cả file
- fork() và exec(): tiến trình con thừa kế cả 3 giá trị ID, trừ file có thiết lập setuid = 1
- Lời gọi hệ thống setuid(int newid):
 - Có thể thiết lập Effective UID cho RealUID và Saved UID
- Các lời gọi hệ thống khác: seteuid(), setreuid(),...

39

MAC trong Linux

- Security-Enhanced Linux (SELinux): kernel module có chức năng thiết lập chính sách truy cập tập trung



- Các chế độ:
 - **Enforcing:** Chế độ mặc định, thực thi chính sách bảo mật SELinux trên hệ thống
 - **Permissive:** Không thực thi chính sách bảo mật, chỉ cảnh báo và ghi lại các hành động.
 - **Disabled:** Vô hiệu hóa SELinux

40

Một số lệnh quan trọng SELinux

- `setsebool policy = on/off`: Bật/tắt chính sách
- `getsebool`: Hiển thị trạng thái chính sách
- `setenforce mode`: Thiết lập chế độ hoạt động của SELinux

Hạn chế của Unix

- Các ứng dụng network daemon như `sshd`, `ftpd` có thể thực thi với quyền root
- Biến môi trường `LIBPATH` có thể bị kẻ tấn công thay đổi
- Tiến trình bất kỳ có thể truy cập và thực thi mọi file trong thư mục `/tmp`
- TOCTTOU:
 - 1) Tiến trình sử dụng quyền root để mở 1 file nào đó, ví dụ `/tmp/X`
 - 2) Trước khi file được mở, tiến trình thay đổi file `/tmp/X` thành một symbolic link tới file `/etc/shadow`