CƠ SỞ AN TOÀN THÔNG TIN

Bài 05: Kiểm soát truy cập

1 Cấp quyền

2 Mô hình kiểm soát truy cập

Cấp quyền

- **Cấp quyền (Authorization)** là việc xác định một chủ thể (subject) đã được xác thực được phép thực hiện những thao tác nào lên những đối tượng (object) nào trong hệ thống

So sánh Authorization và Authentication

- **Authentication**: cho phép/từ chối truy cập
  - Ví dụ 1: xuất trình giấy tờ và đi qua cổng kiểm soát
  - Ví dụ 2: nhập định danh, mật khẩu và đăng nhập vào hệ thống
- **Authorization**: cho phép/từ chối thao tác khi đã được phép truy cập
  - Ví dụ 1: sau khi vào cơ quan thì có thể đi đến những khu vực nào, vào những phòng nào...
  - Ví dụ 2: sau khi đăng nhập thì được đọc file nào, thực thi file nào, sửa đổi file nào...

Nguyên tắc Đặc quyền tối thiểu

- **Nguyên tắc**: chỉ cấp cho chủ thể tập hợp tối thiểu các quyền truy cập đủ để chủ thể đó thực hiện chức trách/chức năng của mình trong hệ thống
- **Ví dụ:**
  - Bán hàng không được xem số liệu kế toán
  - Người dùng không được cài đặt phần mềm, cấu hình mạng...

Kiểm soát truy cập

- **Kiểm soát truy cập (Access control)** là tập hợp các cơ chế cho phép người quản trị hệ thống tác động lên hành vi, công dụng và nội dung của hệ thống đó.

- Nó cho phép xác định người dùng được làm những gì, được truy cập những tài nguyên nào, và được thực thi những tác vụ nào trong hệ thống.

Kiểm soát truy cập

❑Thực thể trong kiểm soát truy cập

- Tập các chủ thể truy cập (subject):

$$S = \{s\}$$

- Tập các đối tượng truy cập (object):

$$O = \{o\}$$

- Mỗi một chủ thể cũng là đối tượng

$$S \subset O$$

Mô hình kiểm soát truy cập

- Kiểm soát truy cập tùy chọn (DAC - Discretionary Access Control)
- Kiểm soát truy cập bắt buộc (MAC – Mandatory Access Control)
- Kiểm soát truy cập dựa trên vai trò (RBAC – Role Based Access Control)
- ...(còn nữa)...

Mô hình kiểm soát truy cập

1. Kiểm soát truy cập tùy chọn
2. Kiểm soát truy cập bắt buộc
3. Kiểm soát truy cập dựa trên vai trò

Mô hình kiểm soát truy cập

1. Kiểm soát truy cập tùy chọn
2. Kiểm soát truy cập bắt buộc
3. Kiểm soát truy cập dựa trên vai trò

Kiểm soát truy cập tùy chọn

- DAC = Discretionary Access Control
- Kiểm soát truy cập dựa trên định danh của chủ thể hoặc định danh của nhóm
- "Tùy chọn": chủ thể với một số quyền nhất định có thể chuyển quyền của mình cho chủ thể khác (có thể gián tiếp)
- Được biểu diễn bởi ma trận kiểm soát truy cập (ACM: Access Control Matrix)

Lampson's Access Control Matrix

- Đề xuất bởi Lampson năm 1971
- Dòng = subject, Cột = object

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Đặc điểm của ACM

❑Đặc điểm của ACM

- Mô tả đầy đủ, chi tiết các quyền truy cập
- Khó quản lý, có thể cấu hình sai
- Không phù hợp cho những hệ thống có số lượng lớn người dùng và số lượng lớn tài nguyên

Biến thể của ACM

❑Biến thể

- Lưu ACM theo từng cột

  ➔ Access Control List

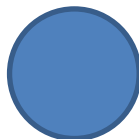
- Lưu ACM theo từng dòng

  ➔ Access Capbability (Profile)

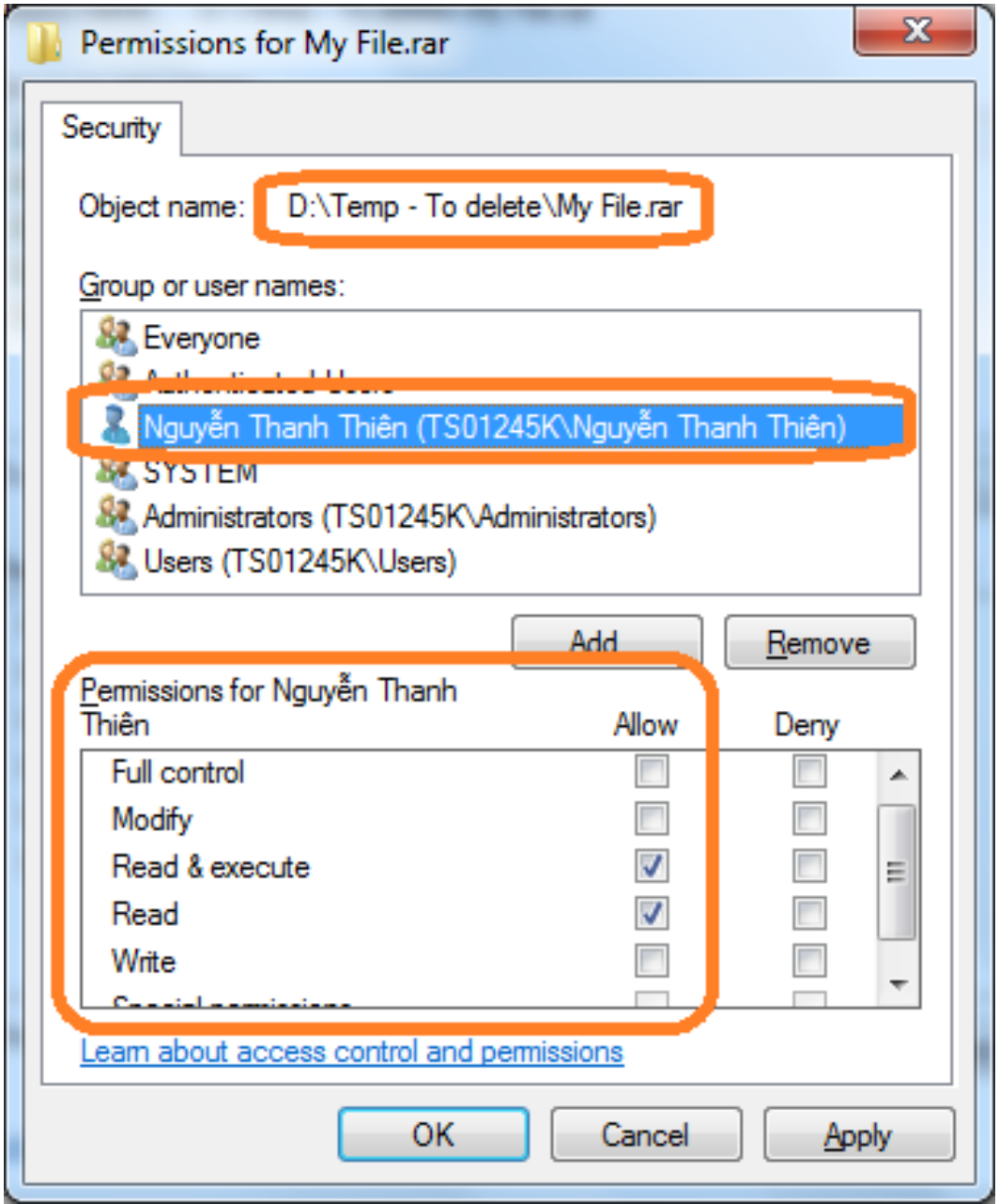
Access Control Lists (ACLs)

- ACL: store access control matrix by **column**
- Example: ACL for **insurance data** is in **blue**

	OS	Accounting program	Accounting data	**Insurance data**	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw



Access Control Lists (ACLs)



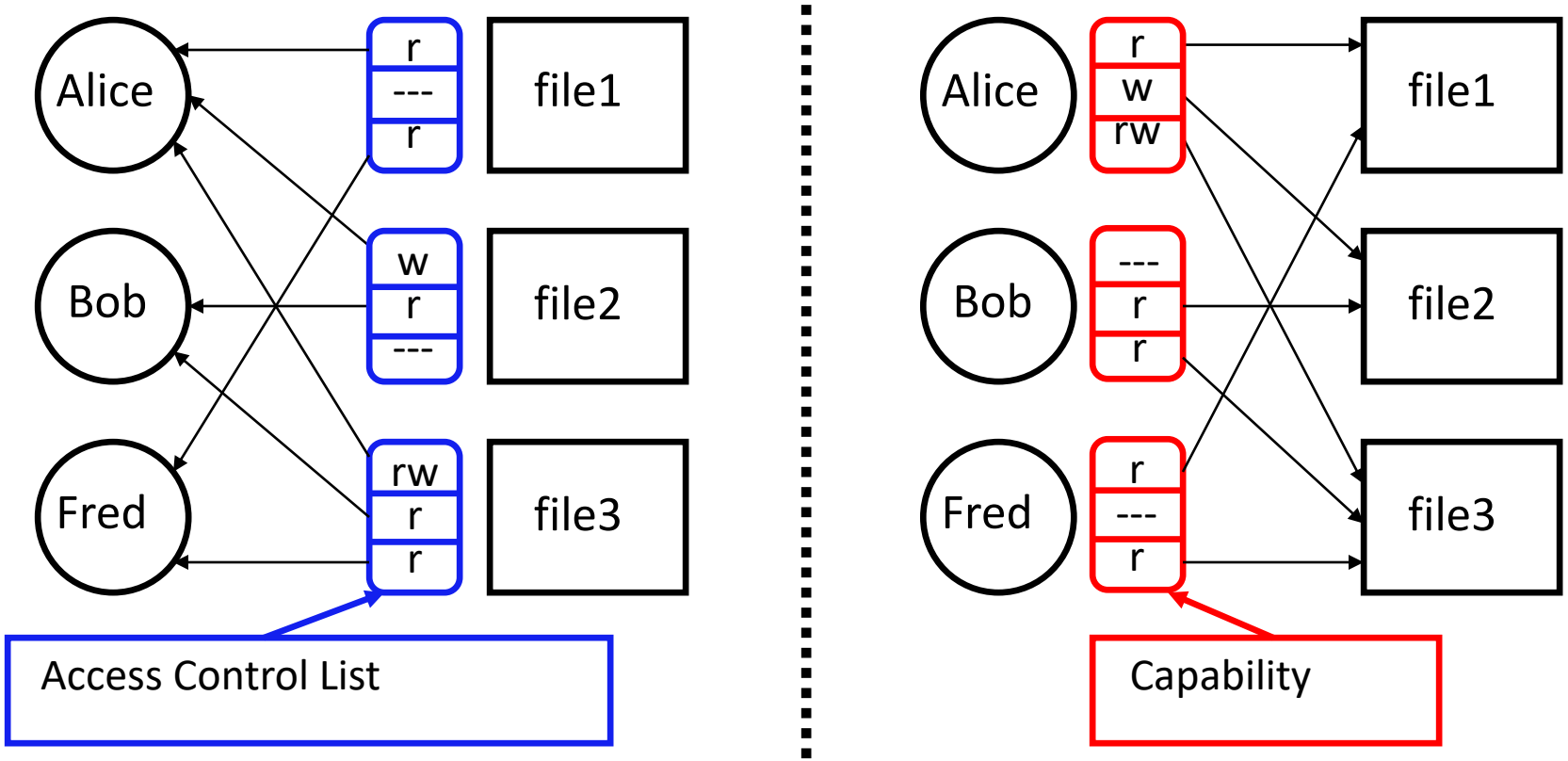
Capabilities (or C-Lists)

- Store access control matrix by **row**
- Example: Capability for **Alice** is in **red**

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

ACLs vs Capabilities

- Note that arrows point in opposite directions!
- With ACLs, still need to associate users to filess



DAC trong thực tế

❑Mô hình với "owner"

- Có một chủ thể là "owner"
- Owner có thể cấp quyền cho mọi chủ thể khác (Linux, Windows)

❑Mô hình với "capabilities"

- Một chủ thể có thể chuyển giao cho chủ thể khác mọi quyền mình có
- Phải có quyền đối với chủ thể nhận

Mô hình kiểm soát truy cập

1. Kiểm soát truy cập tùy chọn
2. Kiểm soát truy cập bắt buộc
3. Kiểm soát truy cập dựa trên vai trò

Mandatory Access Control

❑Cơ chế kiểm soát

- Tất cả các thực thể trong hệ thống đều được gắn một **Mức an toàn** tương ứng với độ nhạy cảm an toàn cao nhất của thực thể đó (Có thứ bậc)
- **Hạng mục an toàn** được định nghĩa như sự phân nhóm không thứ bậc các thực thể của hệ thống để giúp chỉ ra mức độ nhạy cảm an toàn của chúng
- Tất cả thực thể trong hệ thống sẽ được gắn một **Nhãn an toàn = Mức AT x Hạng mục AT**

Mandatory Access Control

❑Cơ chế kiểm soát

- Người dùng sẽ được phép truy cập tới những tài liệu dựa vào việc *tính trội nhãn AT* của người dùng với nhãn AT của tài liệu và các *quy tắc truy cập của HT.*

➔ Chỉ phù hợp với hệ thống đòi hỏi tính bảo mật cao, ví dụ như trong quân sự.

Mandatory Access Control

❑ Tính trội

$\forall x1,x2 \in$ "Nhãn AT" : x1 trội hơn x2

$\Leftrightarrow$ lev(x1) > lev(x2) và

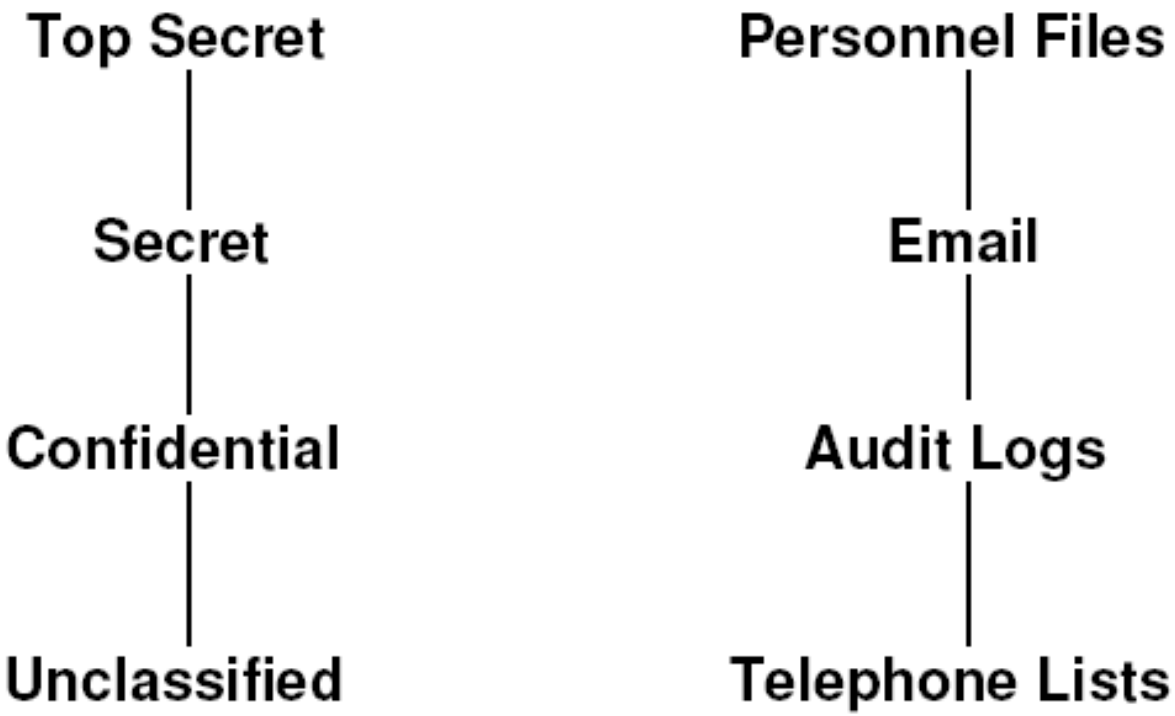
cats(x1) $\supseteq$ cats(x2)

lev(x) – mức AT của thực thể x

cats(x) – hạng mục AT của thực thể x.

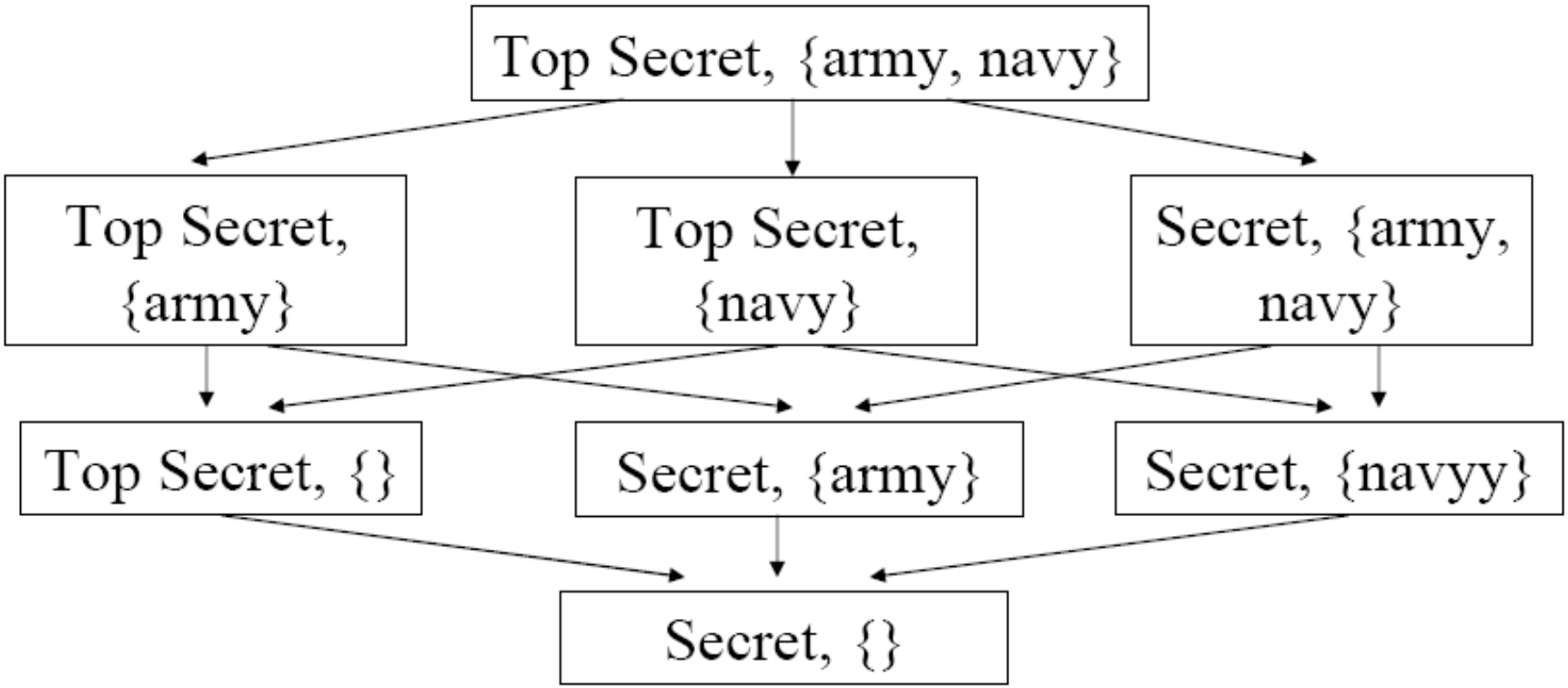
Mandatory Access Control

- **Mức an toàn:**



Mandatory Access Control

- levels={top secret, secret}
- categories={army,navy}



Mô hình kiểm soát truy cập

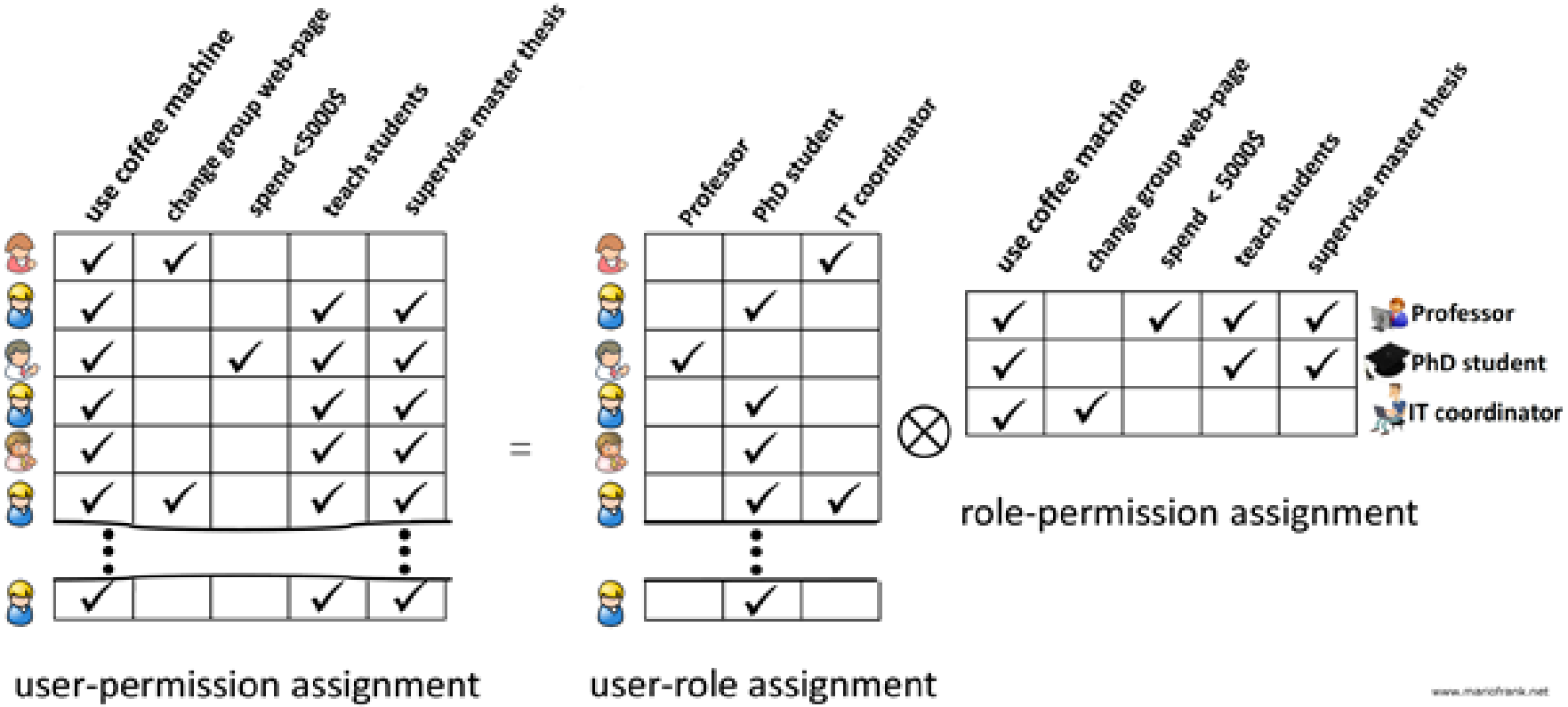
1. Kiểm soát truy cập tùy chọn
2. Kiểm soát truy cập bắt buộc
3. Kiểm soát truy cập dựa trên vai trò

Role Based Access Control

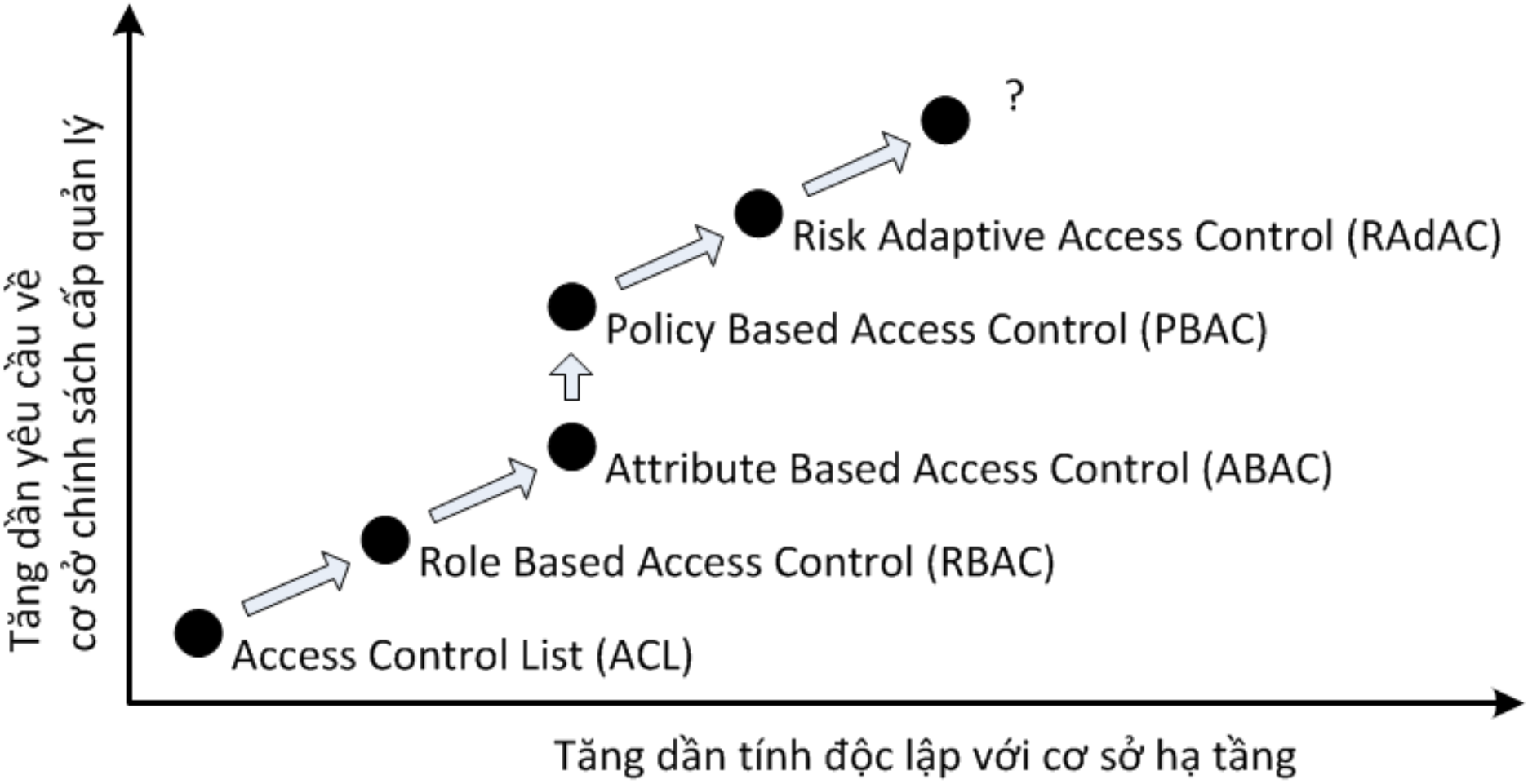
❑RBAC – Role-Based Access Control

- Trong hệ thống, xác định các vai trò có thể có đối với mọi chủ thể.
- Đối với mỗi đối tượng O, liệt kê danh sách các nhóm G với các quyền truy cập tới O
- Mỗi chủ thể có thể là thành viên của một hoặc một số nhóm (có một hoặc nhiều vai trò)
- Chủ thể có tất cả các quyền của tất cả các nhóm mà nó thuộc về

Role Based Access Control



Mô hình kiểm soát truy cập khác




THANK YOU FOR LISTENING
ANY QUESTIONS?