LOGO

CHƯƠNG 2
CÁC MÔ HÌNH VÀ CHÍNH SÁCH AN TOÀN

TS. Trần Thị Lượng
* Khoa An toàn thông tin *

MỤC TIÊU

- **Kiến thức:**
  - Hiểu và trình bày được các kiến thức cơ bản về các mô hình và chính sách an toàn cơ sở dữ liệu (MAC và DAC)
- **Kỹ năng:**
  - Triển khai được một số cơ chế an toàn theo hai mô hình MAC, DAC trong Oracle, SQL Server, MySQL

TÀI LIỆU THAM KHẢO

- [1] TS. Nguyễn Nam Hải, TS. Lương Thế Dũng, ThS. Trần Thị Lượng, *Giáo trình An toàn cơ sở dữ liệu,* Học viện Kỹ thuật Mật mã, 2013.
- [2] GÜNTHER PERNUL, *Database Security*, Advances in Computers, Vol. 38. M. C. Yovits (Ed.), Academic Press, 1994, pp. 1 - 74.
- [3] Ravi S. Sandhu, Sushil Jajodia, *Data and database security and controls*, Handbook of Information Security Management, Auerbach Publishers, 1993, pages, 481-499.
- [4] Scott Gaetjen, David Knox, William Maroulis, "*Oracle database 12c security",* Oracle Press, 2015.

NỘI DUNG

1. Các khái niệm cơ bản
2. Các mô hình và chính sách an toàn tùy ý
3. Các mô hình và chính sách an toàn bắt buộc
4. Các mô hình an toàn khác

NỘI DUNG

1. *Các khái niệm cơ bản*
2. Các mô hình và chính sách an toàn tùy ý
3. Các mô hình và chính sách an toàn bắt buộc
4. Các mô hình an toàn khác

CÁC KHÁI NIỆM CƠ BẢN

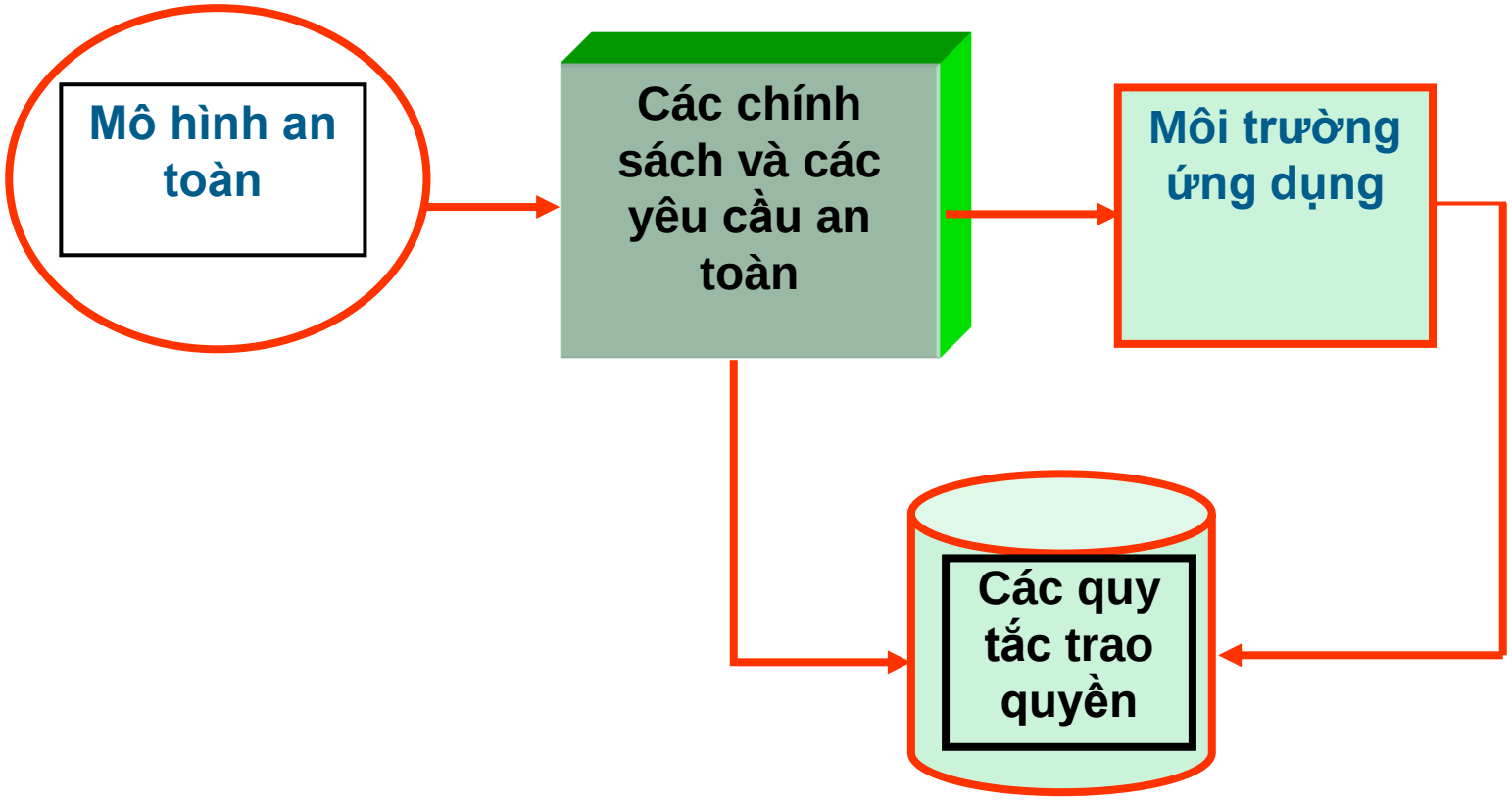
- Câu hỏi:
  - *Mô hình an toàn (Security model) là gì?*
  - *Chính sách an toàn (Security policy) là gì?*

CÁC KHÁI NIỆM CƠ BẢN

- ***Mô hình an toàn:*** là một mô hình khái niệm mức cao, độc lập phần mềm và xuất phát từ các đặc tả yêu cầu của tổ chức để mô tả nhu cầu bảo vệ của một hệ thống.
- ***Chính sách an toàn*:** là những phát biểu mức tổng quát về ATTT từ phía nhà quản lý

CÁC KHÁI NIỆM CƠ BẢN

❖Quy tắc trao quyền trong tổ chức:



CÁC KHÁI NIỆM CƠ BẢN

Trong Oracle:

- Có thể đạt được một danh sách tất cả các chính sách bằng cách truy vấn vào khung nhìn DBA_POLICIES.
- Ngoài ra các khung nhìn ALL_POLICIES và USER_POLICIES cung cấp thông tin về các chính sách đã được định nghĩa.

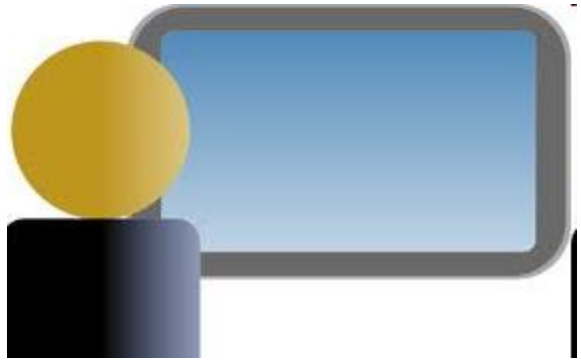
CÁC MÔ HÌNH AN TOÀN

Chủ thể an toàn (Security Subject)

- Là một thực thể chủ động
- Là user hay các tiến trình (process)

Đối tượng an toàn (Security Object)

- Là một thực thể thụ động
- Là file, CSDL, bảng, khung nhìn, cột, hàng, ô (entry)



CÁC MÔ HÌNH AN TOÀN

- Hai loại mô hình an toàn là:
  - ***Mô hình an toàn tùy ý***

    (Discretionary security models - DAC)
  - ***Mô hình an toàn bắt buộc***

    (Mandatory security models - MAC).

CÁC MÔ HÌNH AN TOÀN

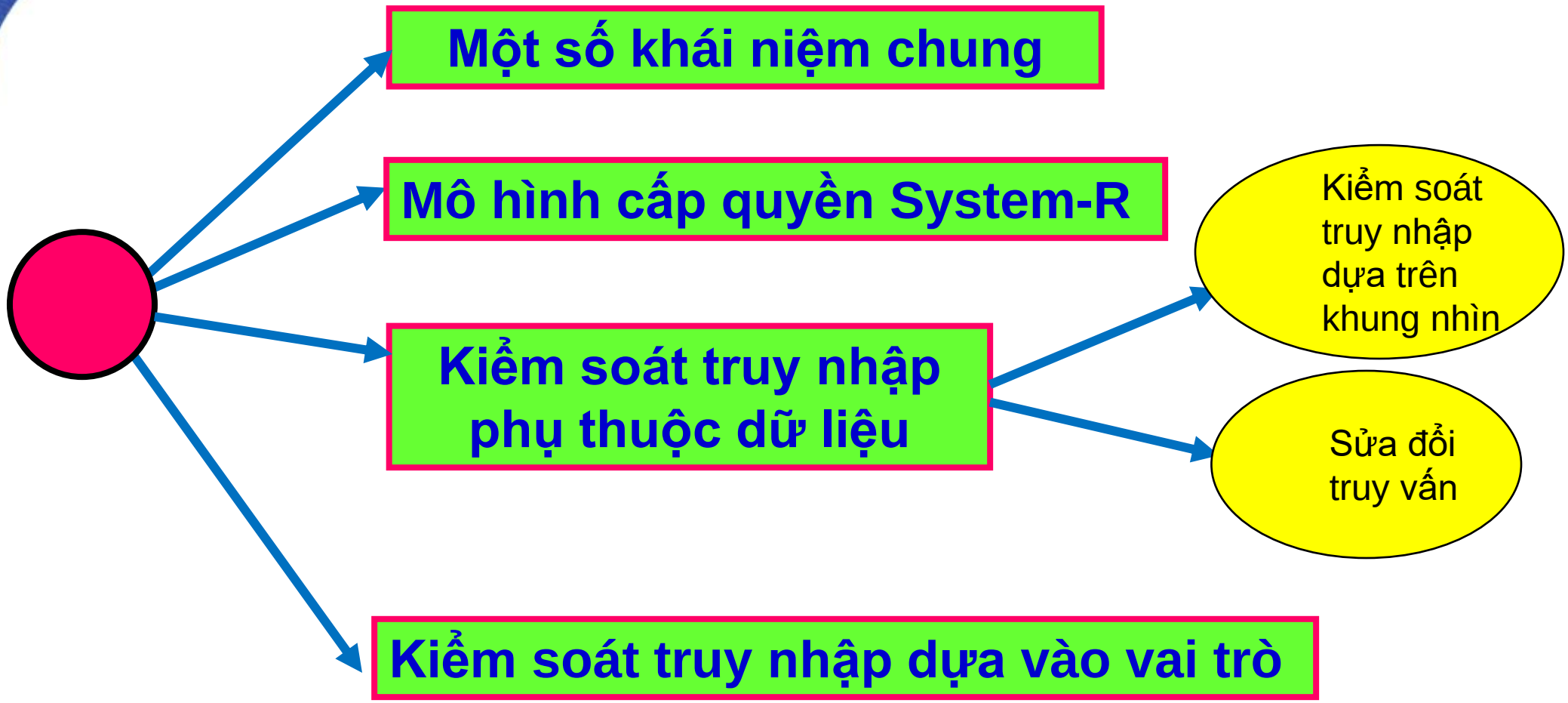
- ***Một số mô hình an toàn tùy ý:*** *Mô hình ma trận truy nhập* (Lampson,1971; Graham-Denning, 1973; Harrison, 1976), mô hình Take-Grant (Jones, 1976), mô hình Action-Entity (Bussolati, 1983; Fugini-Martella, 1984), mô hình của Wood-1979 như kiến trúc ANSI/SPARC đề cập đến vấn đề cấp quyền trong các cơ sở dữ liệu quan hệ lược đồ - nhiều mức,...

- ***Một số mô hình an toàn bắt buộc:*** *mô hình Bell – Lapadula* (1973, 1974, 1975), mô hình Biba (1977), mô hình Sea View (Denning, 1987), mô hình Dion (1981),…

NỘI DUNG

1. Các khái niệm cơ bản
2. *Các mô hình và chính sách an toàn tùy ý*
3. Các mô hình và chính sách an toàn bắt buộc
4. Các mô hình an toàn khác

MÔ HÌNH, CHÍNH SÁCH AN TOÀN TÙY Ý (DAC)



MỘT SỐ KHÁI NIỆM CHUNG

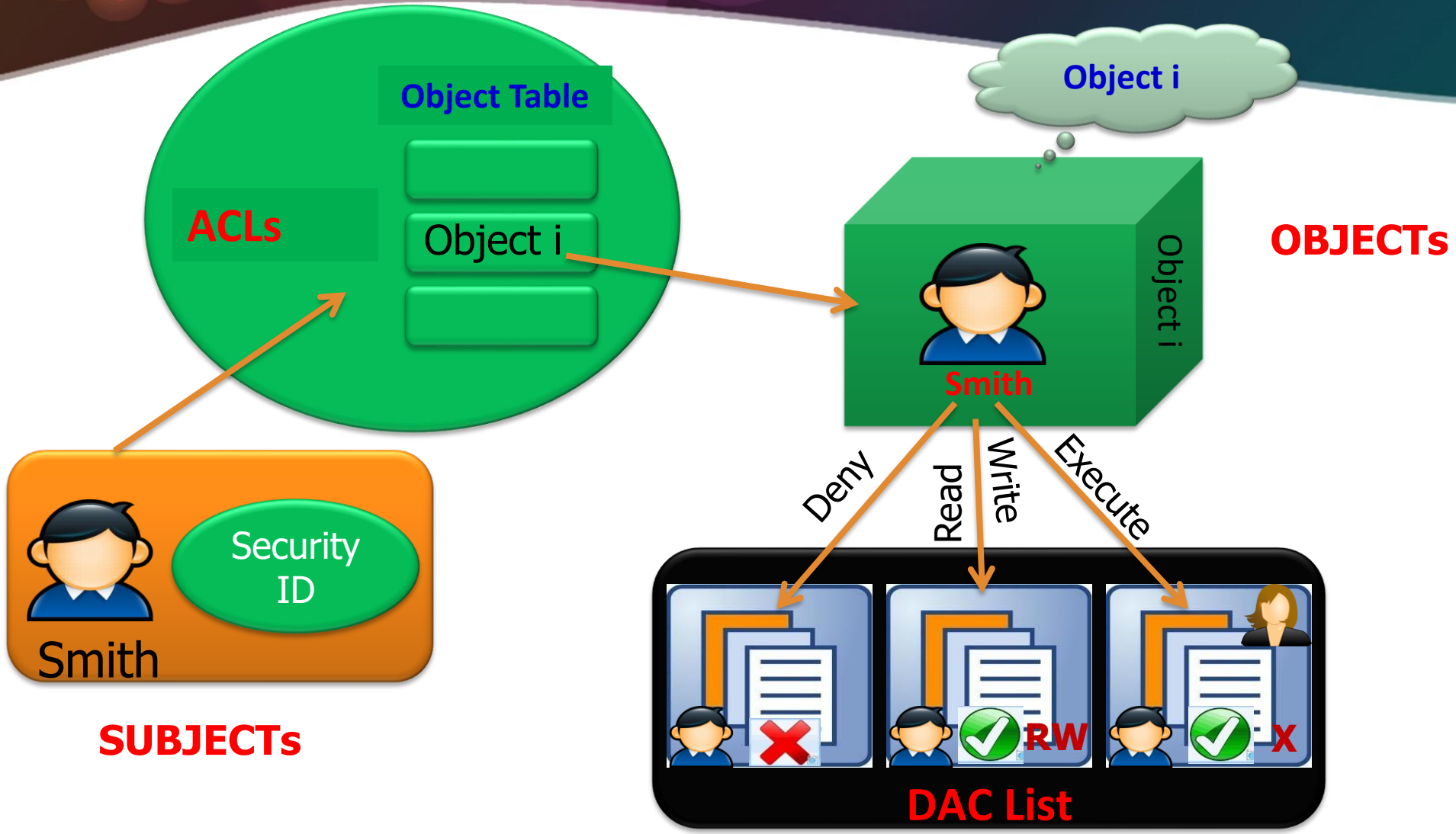
- Mô hình an toàn tùy ý đã được nghiên cứu trong một thời gian dài và là nền tảng cho các hệ điều hành và các DBMS.
- ***Chính sách tùy ý (DAC):*** chỉ rõ những đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống (object prilvilege, system prilvilege).
- ***Được định nghĩa trên một tập:***
  - Các đối tượng an toàn (security objects)
  - Các chủ thể an toàn (security subjects)
  - Và các đặc quyền truy nhập (access prilvilege)

(Quyền truy nhập gồm: object prilvilege, system prilvilege

MỘT SỐ KHÁI NIỆM CHUNG

- Đặc điểm:
  - Người dùng có thể bảo vệ dữ liệu mà họ sở hữu
  - Người chủ sở hữu (owner) có thể gán quyền truy nhập (read , write, execute…) tới các user khác.
  - Việc gán và thu hồi quyền truy nhập là “tùy ý” do những người dùng này.
- Các yêu cầu truy nhập được kiểm tra, thông qua một cơ chế kiểm soát tuỳ ý, truy nhập chỉ được trao cho các chủ thể thoả mãn các quy tắc cấp quyền của hệ thống.

MỘT SỐ KHÁI NIỆM CHUNG



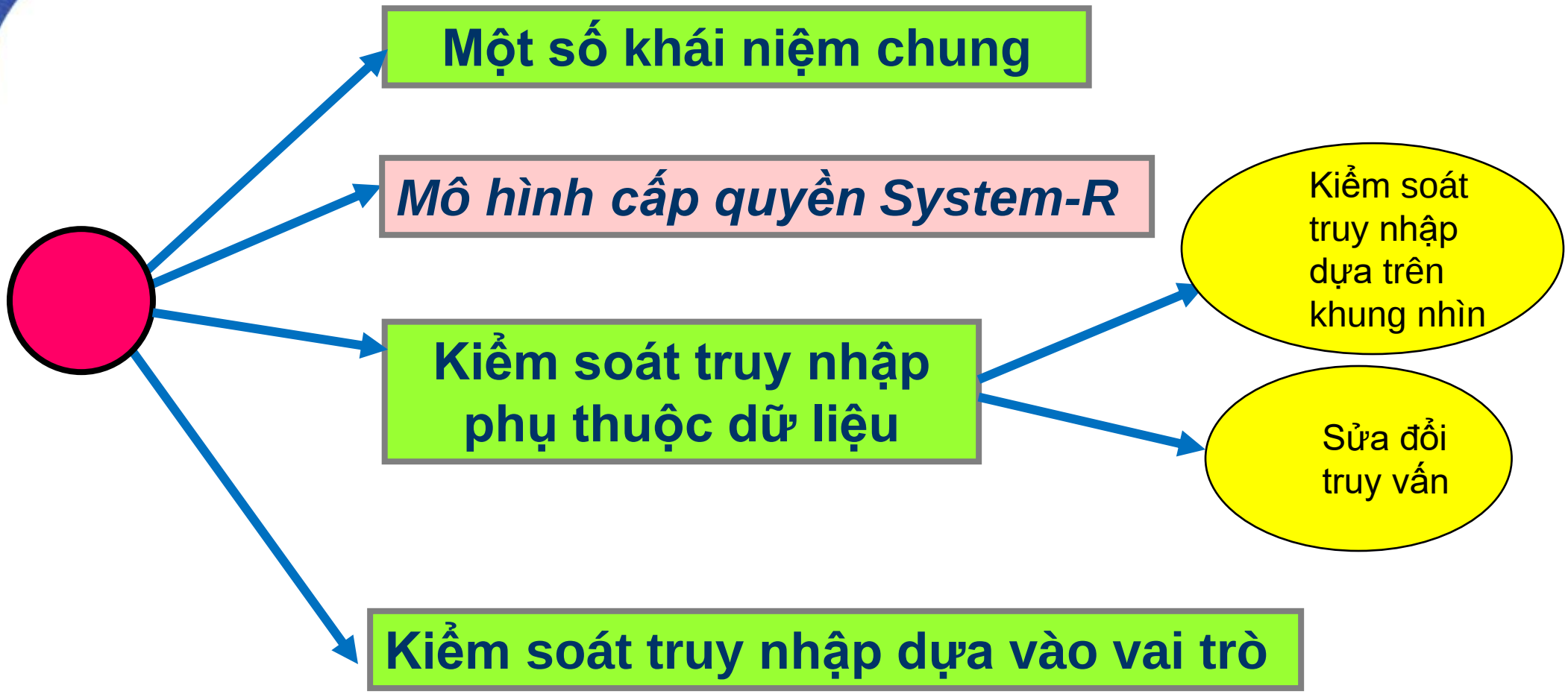
MỘT SỐ KHÁI NIỆM CHUNG

- ***Trao quyền:*** Việc trao quyền do người sở hữu đối tượng. Tuy nhiên, trong DAC có thể lan truyền các quyền. Ví dụ: trong Oracle có GRANT OPTION, ADMIN OPTION.
- ***Thu hồi quyền*:** Người dùng muốn thu hồi quyền (người đã được trao quyền đó) phải có đặc quyền để thu hồi quyền. Trong Oracle, nếu 1 user có GRANT OPTION/ADMIN OPTION, anh ta có thể thu hồi quyền đã truyền cho người khác.
- ***DAC*** dựa vào định danh của người dùng có yêu cầu truy nhập.
- ***'Tùy ý*** có nghĩa rằng người sử dụng có khả năng cấp phát hoặc thu hồi quyền truy nhập trên một số đối tượng.

MỘT SỐ KHÁI NIỆM CHUNG

- ***Các chế độ kiểm soát truy nhập:*** Kiểm soát truy nhập có thể được áp dụng ở các mức độ chi tiết khác nhau trong hệ thống, bao gồm:
  - Toàn bộ cơ sở dữ liệu
  - Một tập các quan hệ (bảng CSDL)
  - Một quan hệ (một bảng)
  - Một vài cột của một quan hệ
  - Một vài hàng của một quan hệ
  - Một vài cột của một vài hàng trong một quan hệ

MÔ HÌNH, CHÍNH SÁCH AN TOÀN TÙY Ý



MÔ HÌNH CẤP QUYỀN SYSTEM-R

MÔ HÌNH CẤP QUYỀN SYSTEM - R

1. Giới thiệu
2. Quyền trong System R
3. Gán/thu hồi quyền trong System R

MÔ HÌNH CẤP QUYỀN SYSTEM - R

Câu hỏi:

- *Ý nghĩa của mô hình System R?*

Trả lời:

- Các mô hình cấp quyền theo cơ chế DAC hiện tại đều dựa trên mô hình System R.
- Là một trong những mô hình ra đời đầu tiên cho hệ quản trị cơ sở dữ liệu quan hệ.
- System R dựa trên nguyên lý cấp quyền quản trị cho người sở hữu.

MÔ HÌNH CẤP QUYỀN SYSTEM - R

❖Giới thiệu:

- System R là một hệ quản trị CSDL quan hệ đầu tiên của IBM được bắt đầu năm 1974 thuộc phòng thí nghiệm nghiên cứu San Jose. Việc bảo vệ được thực hiện tại mức table.

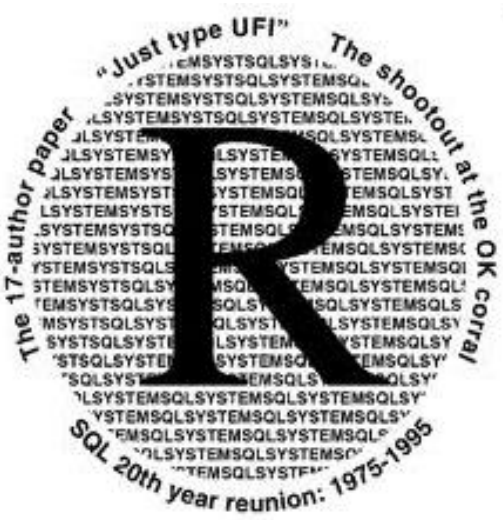
  + Chủ thể: người dùng

  + Đối tượng: các bảng và khung nhìn

- Khách hàng đầu tiên của System R là hãng Pratt & Whitney năm 1977.

MÔ HÌNH CẤP QUYỀN SYSTEM - R

- 5 chế độ truy nhập vào một table:
  - **Select**
  - **Insert**.
  - **Delete**
  - **Update**
  - **Drop**.



MÔ HÌNH CẤP QUYỀN SYSTEM – R (..)

- System R hỗ trợ ***quản trị quyền phi tập trung:***
  - Người tạo ra bảng có mọi đặc quyền trên bảng đó và có thể trao/thu hồi (grant/revoke) quyền cho các user khác.
  - Điều này có thể không đúng với các khung nhìn.
- Việc trao và thu hồi quyền của System R được thực hiện bằng các lệnh SQL.

MÔ HÌNH CẤP QUYỀN SYSTEM R

1. Giới thiệu
2. Quyền trong System R
3. Gán/thu hồi quyền trong System R

QUYỀN TRONG SYSTEM - R

- Người tạo ra bảng có mọi đặc quyền trên bảng đó và có thể trao/thu hồi quyền cho các user khác, mỗi quyền là một bộ sau:

  <s, p, t, ts, g, go>

  - **s**: chủ thể được gán quyền (***grantee***).
  - **p**: đặc quyền được gán (select, update…).
  - **t**: tên bảng, trên đó truy nhập được gán.
  - **ts**: thời điểm quyền được gán.
  - **g**: người gán quyền (***grantor***).
  - **go** $\in$ {yes,no}: ***grant option*.**

QUYỀN TRONG SYSTEM – R...

- Ví dụ, trong Oracle, một bảng có tên là USER_TAB_PRIVS_RECD được dùng để xác định các quyền đã được gán cho một người dùng:

Cột	Kiểu dữ liệu	NULL	Mô tả
GRANTEE	VARCHAR2(30)	NOT NULL	Tên người dùng được gán quyền
OWNER	VARCHAR2(30)	NOT NULL	Chủ sở hữu của đối tượng
TAPBLE_NAME	VARCHAR2(30)	NOT NULL	Tên đối tượng
GRANTOR	VARCHAR2(30)	NOT NULL	Người thực hiện gán quyền
PRILVILEGE	VARCHAR2(40)	NOT NULL	Quyền trên đối tượng
GRANTABLE	VARCHAR2(3)		Quyền này có GRANT OPTION (YES) hay không (NO)
HIERARCHY	VARCHAR2(3)		Quyền này có HIERARCHY OPTION (YES) hay không (NO)

QUYỀN TRONG SYSTEM – R...

- Ví dụ cụ thể trong Oracle 11g.
- Bảng dùng cho userE

OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRA	HIE
USERA	SINHVIEN	USERC	UPDATE	YES	NO
USERA	SINHVIEN	USERB	SELECT	YES	NO
USERA	SINHVIEN	USERC	SELECT	YES	NO
USERA	SINHVIEN	USERB	INSERT	YES	NO

MÔ HÌNH CẤP QUYỀN SYSTEM R

1. Giới thiệu
2. Quyền trong System R
3. Gán/thu hồi quyền trong System R

GÁN/THU HỒI QUYỀN SYSTEM R

❖ *Gán quyền (Grant prilvileges):*

- Nếu một user được gán quyền trên một table với GRANT OPTION, anh ta có thể gán và thu hồi quyền cho các user khác với các quyền anh ta có.

❖ *Thu hồi quyền (Revoke prilvileges):*

- Mô hình quyền System R sử dụng cơ chế ***thu hồi đệ quy.***
- Nếu x thu hồi quyền của y, trong khi đó x không gán quyền gì cho y trước đó, thì việc thu hồi quyền này bị loại bỏ.

GÁN / THU HỒI QUYỀN SYSTEM R...

GRANT privileges **ON** object **TO** users **[WITH GRANT OPTION]**

REVOKE privileges **ON** object **FROM** users **{CASCADE}**

Chu y: Nếu trong câu lênh Grant không có GRANT OPTION thì câu lệnh REVOKE với tùy chọn CASCADE sẽ bị lỗi.

GÁN/THU HỒI QUYỀN SYSTEM R...

- Người dùng (người trao đặc quyền trên một bảng) cũng có thể ghi rõ từ khoá PUBLIC, thay cho (users). Khi đó, tất cả những người dùng của CSDL đều được trao đặc quyền trên bảng.

EMPLOYEE

EMPID	NAME	BDATE	ADDRESS	SEX	SALARY	DEPTNO

Scott: **GRANT** SELECT **ON** EMPLOYEE **TO** user1;

GRANT SELECT **ON** EMPLOYEE **TO** user2 **WITH GRANT OPTION;**

GRANT INSERT **ON** EMPLOYEE(NAME,BDATE) **TO** user3;

GRANT UPDATE **ON** EMPLOYEE(SALARY) **TO** user4 **WITH GRANT OPTION;**

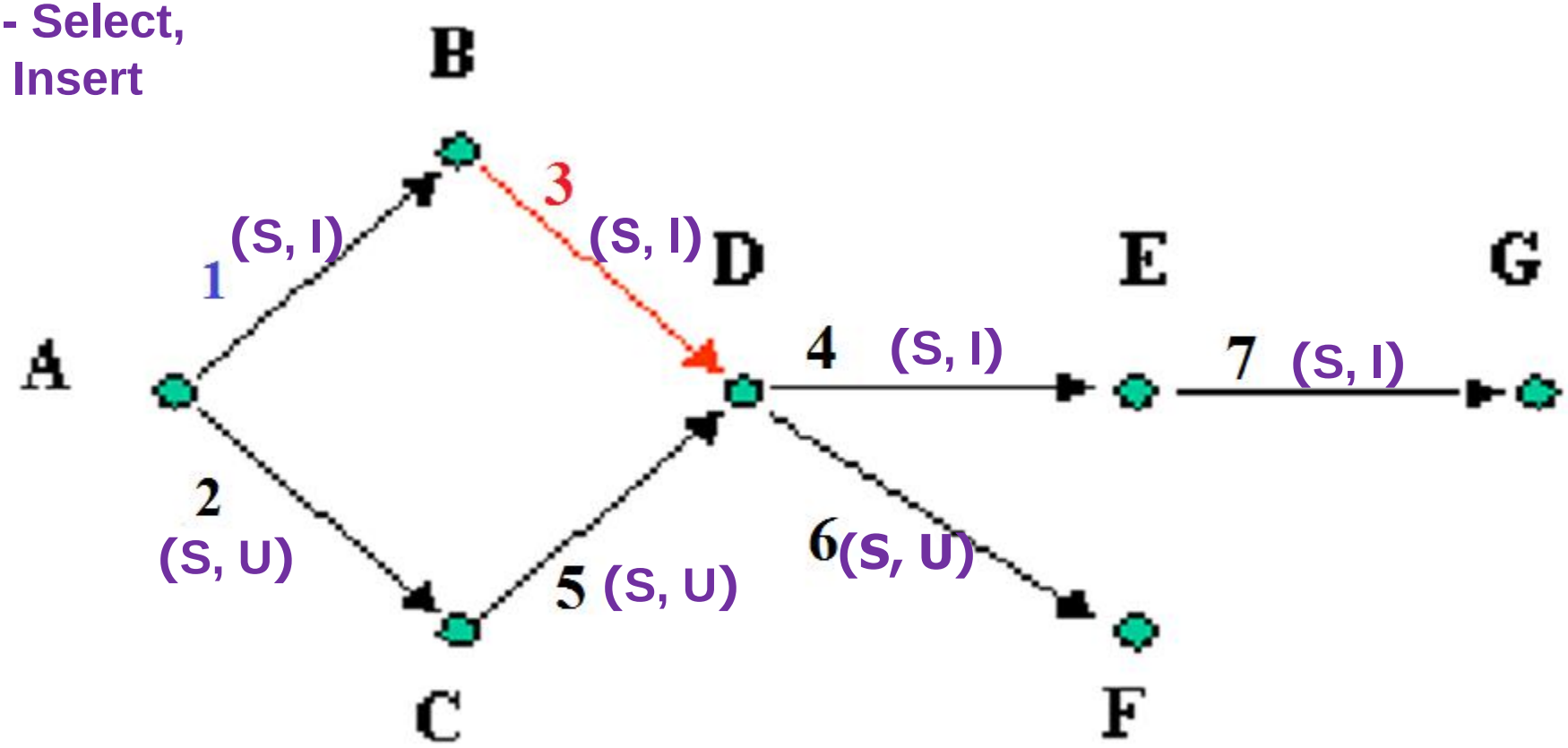
REVOKE SELECT **ON** EMPLOYEE **FROM** user1 **CASCADE?**

REVOKE SELECT **ON** EMPLOYEE **FROM** user2 **CASCADE?**

GÁN/THU HỒI QUYỀN SYSTEM R...

❖ Thu hồi quyền đệ quy*: (Revoke with cascade option)*

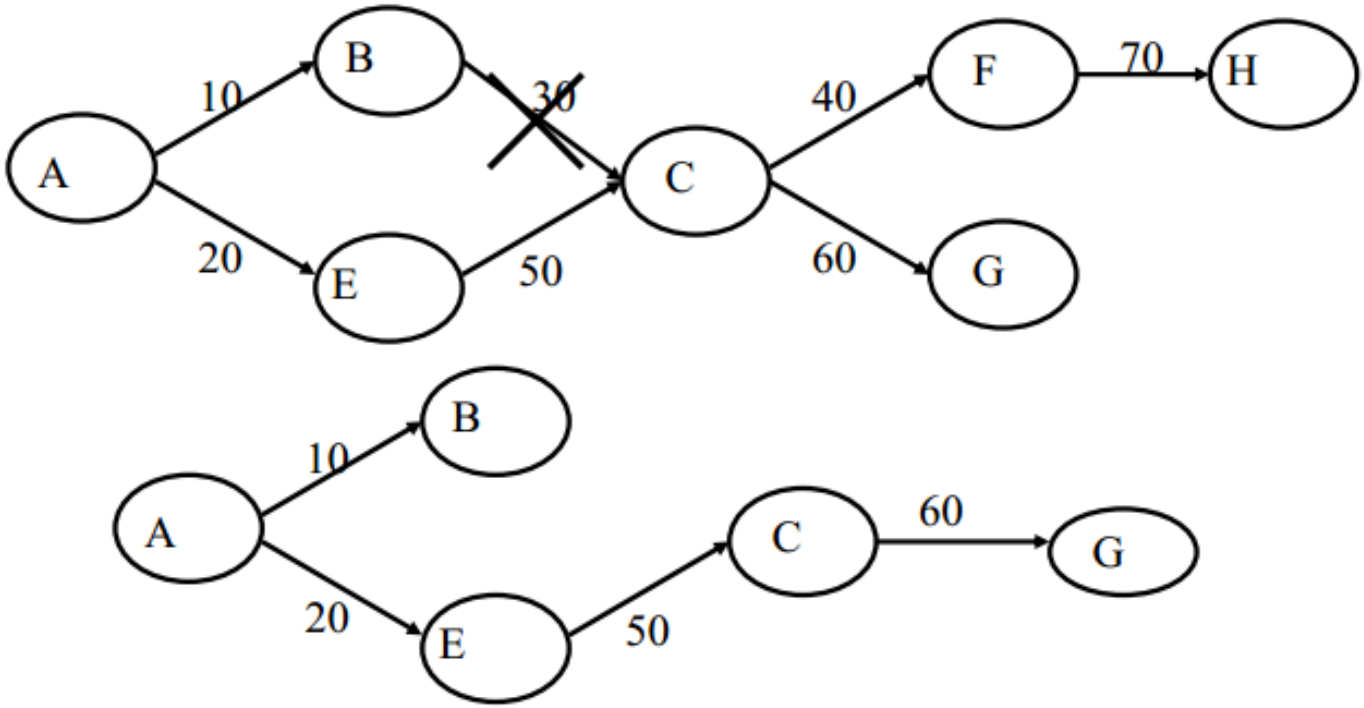
S - Select,
I - Insert



Bước cuối cùng: B thu hồi quyền của D đệ quy (CASCADE), **vậy E và G, F còn quyền gì?**

GÁN/THU HỒI QUYỀN SYSTEM R...

- Thu hồi quyền đệ quy: trong System R dựa vào nhãn thời gian mỗi lần cấp quyền truy nhập cho người dùng.



GÁN/THU HỒI QUYỀN SYSTEM R...

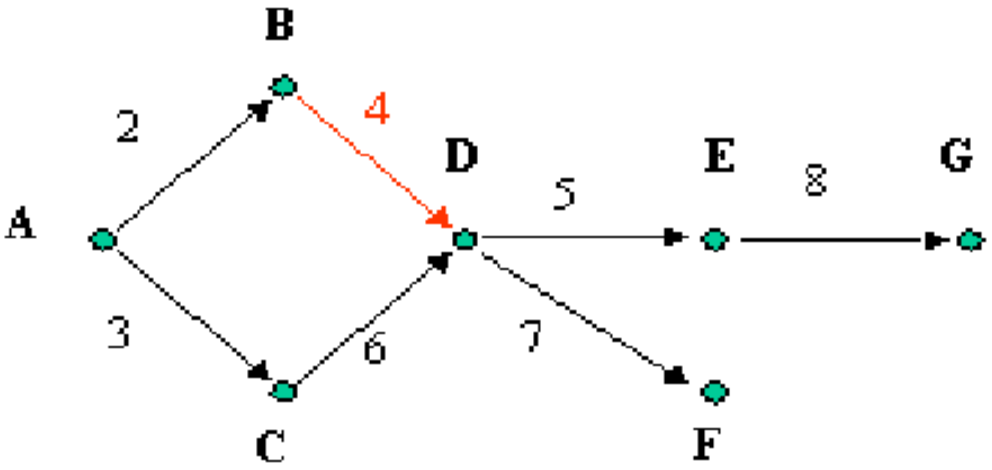
❖ Thu hồi quyền không đệ quy *(Revoke non-cascading):*

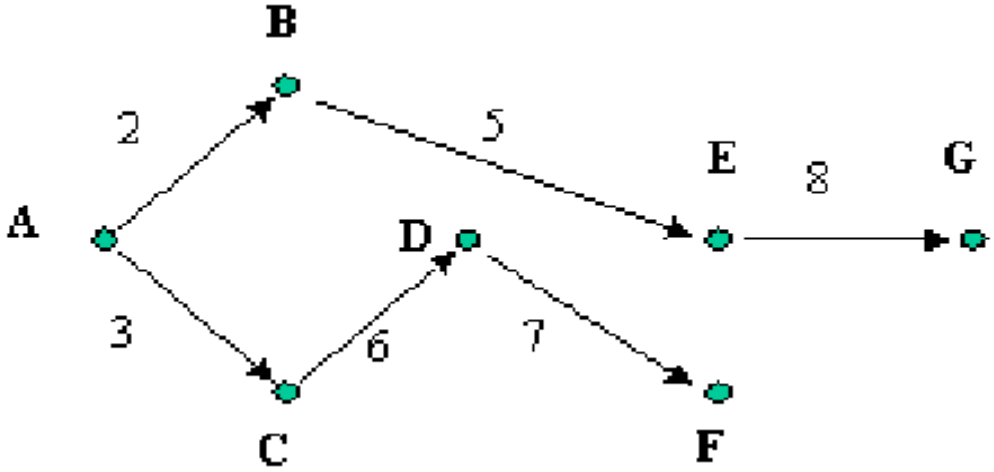
- Thực tế khi một người dùng A thay đổi công việc hay vị trí thì đôi khi tổ chức chỉ muốn lấy lại quyền truy nhập của A mà không muốn lấy lại các quyền truy nhập mà A đã cấp => áp dụng thu hồi quyền không đệ quy.
- Vẫn dựa vào nhãn thời gian.

MỞ RỘNG CHO MÔ HÌNH CẤP QUYỀN SYSTEM R…

❖Thu hồi quyền không đệ quy:

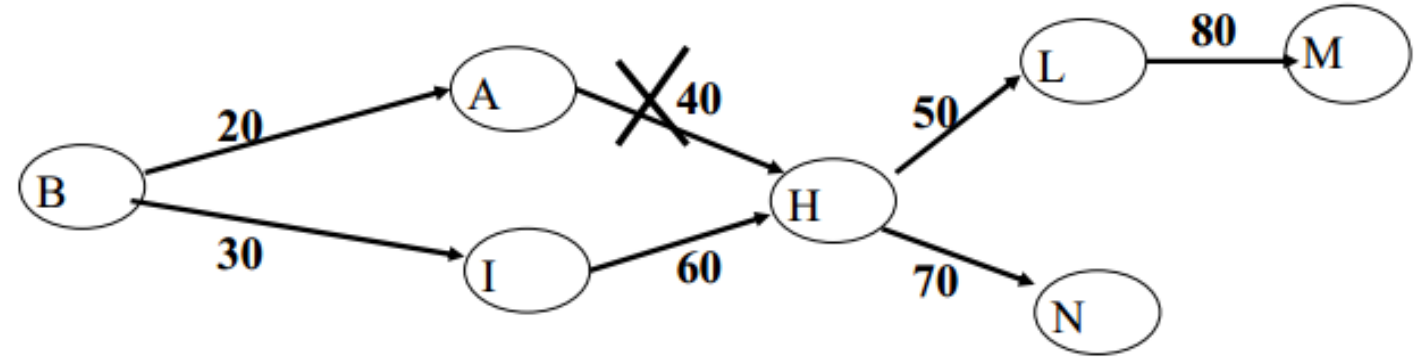
- Khi A thu hồi quyền truy nhập trên B thì tất cả quyền truy nhập mà B đã cấp cho chủ thể khác được thay bằng A đã cấp cho những chủ thể này.
- Cần lưu ý đến nhãn thời gian nữa!!!

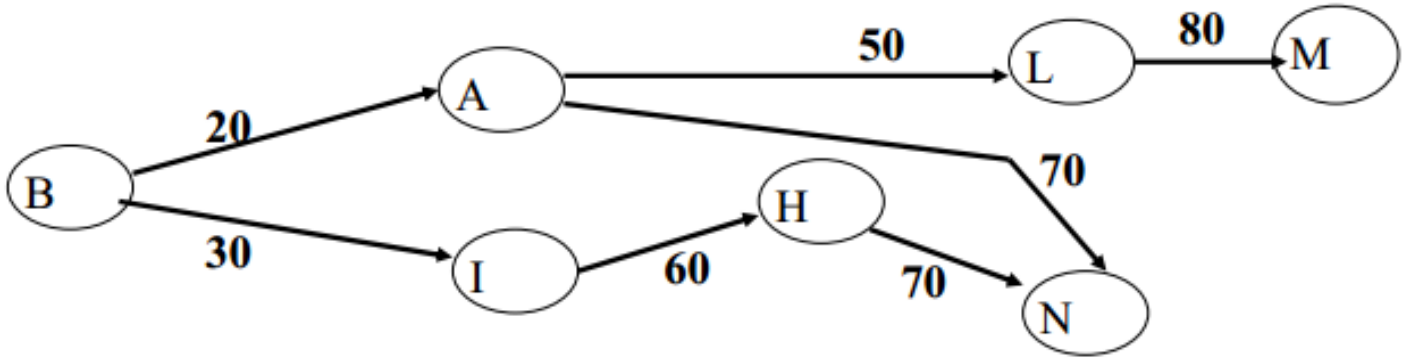




MỞ RỘNG CHO MÔ HÌNH CẤP QUYỀN SYSTEM R…

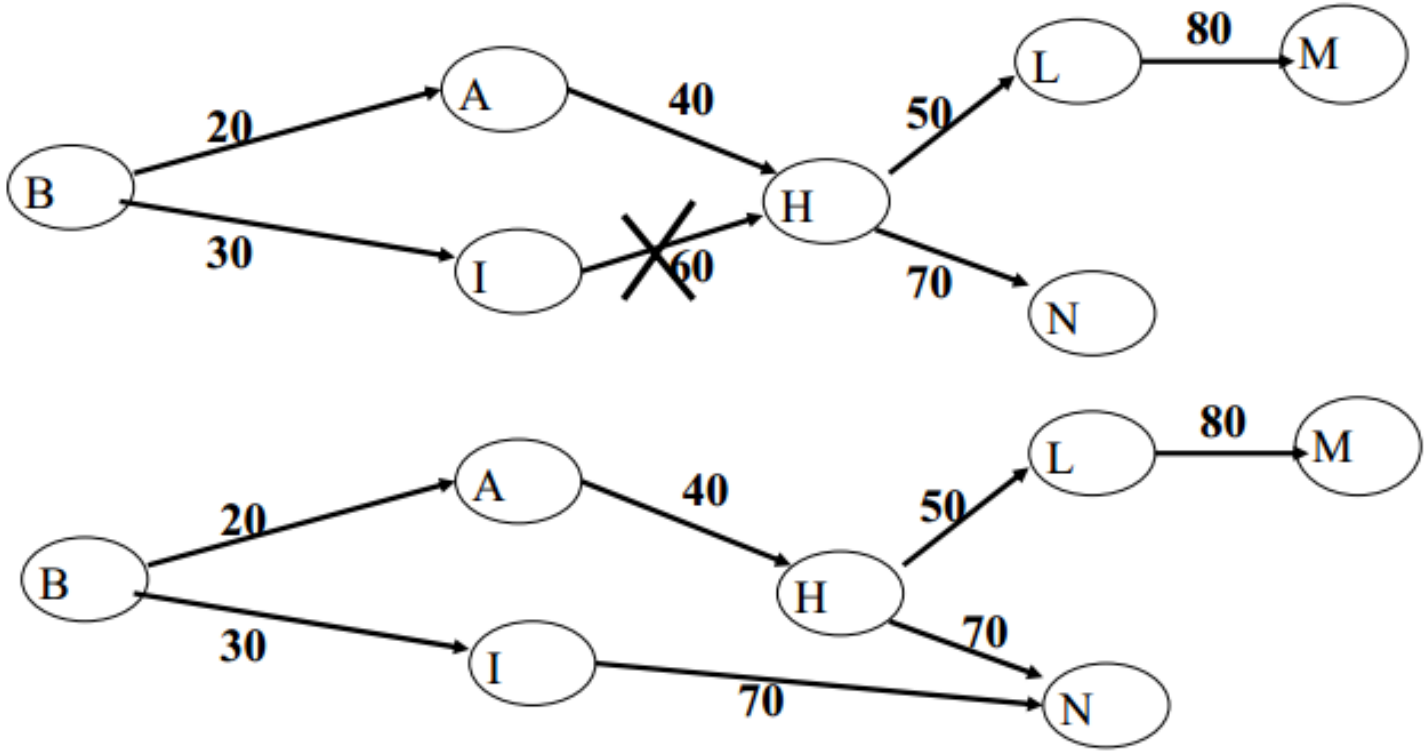
❖ Thu hồi quyền không đệ quy (Ví dụ 1):





MỞ RỘNG CHO MÔ HÌNH CẤP QUYỀN SYSTEM R…

❖ Thu hồi quyền không đệ quy (Ví dụ 2):



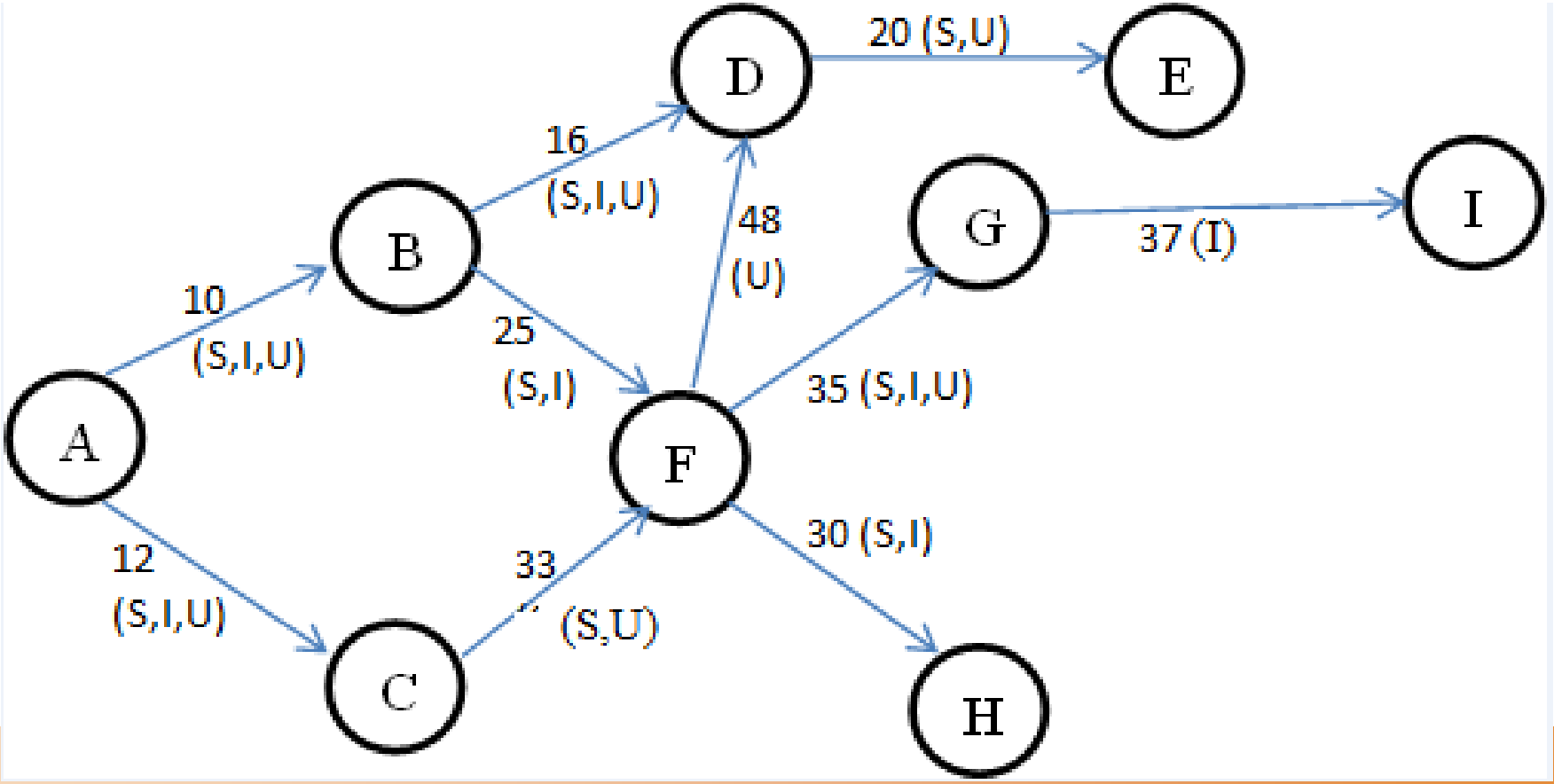
BÀI TẬP VỀ NHÀ

a) Vẽ sơ đồ cho dãy các câu lệnh gán quyền trong bảng dưới đây.
b) Vẽ lại sơ đồ và giải thích khi E thu hồi không đệ quy cả ba quyền Select (S), Insert (I), Update (U) đã gán cho C.

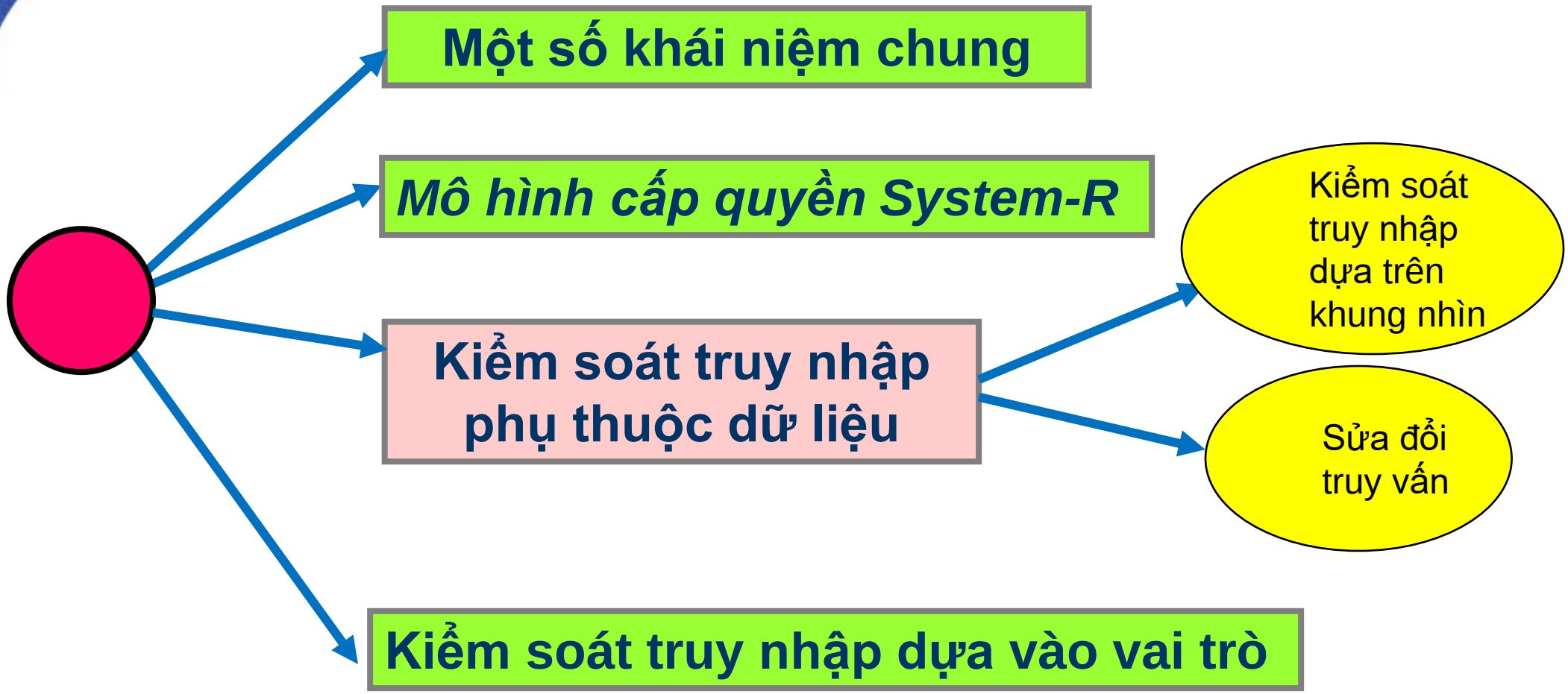
Người dùng	Câu lệnh	Nhãn thời gian
B	Grant Select, Insert, Update to A with grant option	10
B	Grant Select, Insert, Delete to C with grant option	17
A	Grant Select, Insert, Update to E with grant option	12
E	Grant Select, Insert, Update to C with grant option	15
C	Grant Select, Update to D with grant option	16
C	Grant Select, Delete, Update to G with grant option	22
D	Grant Update to H without grant option	20

BÀI TẬP VỀ NHÀ

Vẽ lại sơ đồ và giải thích khi B thu hồi quyền đệ quy của D cả ba quyền Select (S), Insert (I), Update (U) và B thu hồi quyền đệ quy của F cả hai quyền S và I.



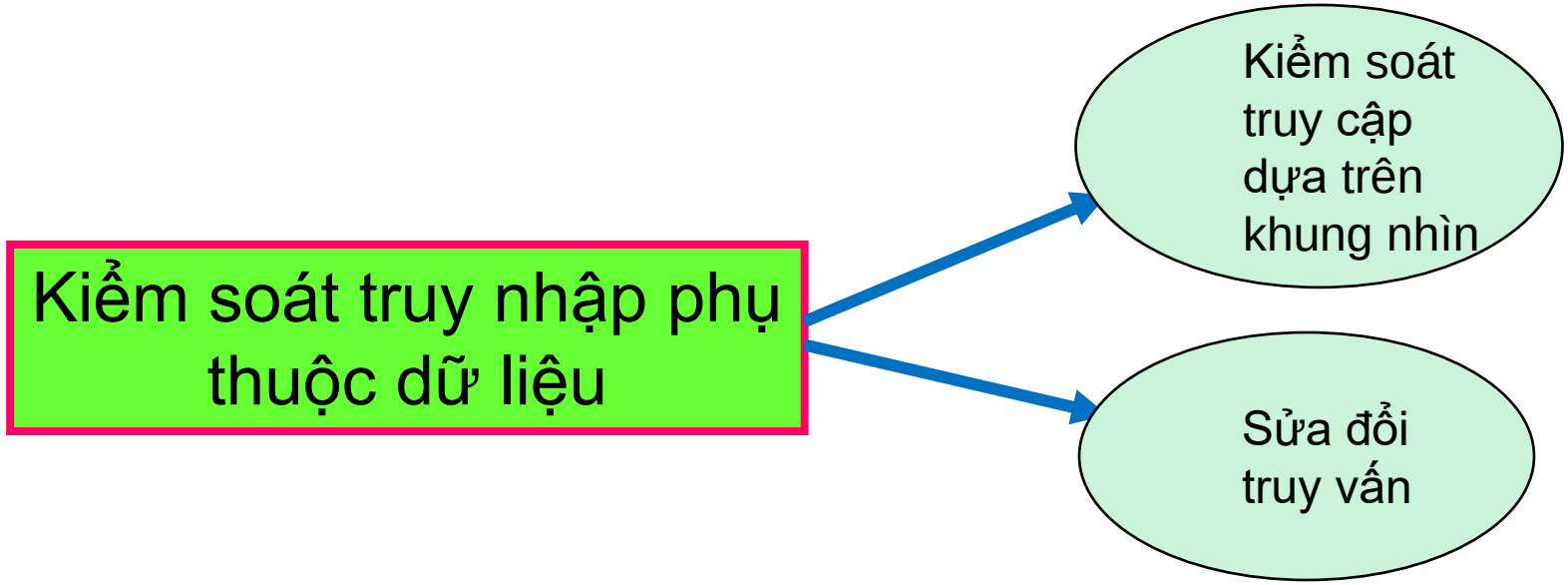
MÔ HÌNH, CHÍNH SÁCH AN TOÀN TÙY Ý



Kiểm soát truy nhập phụ thuộc dữ liệu

KIỂM SOÁT TRUY CẬP PHỤ THUỘC DỮ LIỆU

- Kiểm soát truy cập cơ sở dữ liệu thường *phụ thuộc vào dữ liệu.* Ví dụ, một số người dùng có thể bị giới hạn chỉ nhìn thấy các giá trị lương nhỏ hơn $30,000. một người trưởng phòng chỉ nhìn thấy các giá trị lương của các nhân viên trong phòng mình quản lý.



KIỂM SOÁT TRUY CẬP DỰA TRÊN KHUNG NHÌN

- **Cơ chế kiểm soát dựa trên khung nhìn:**
  - Là cơ chế bảo vệ bên dưới của các DBMS dựa trên System R
  - Thay vì truy nhập trực tiếp vào bảng quan hệ cơ sở, người dùng chỉ được truy nhập vào các bảng khung nhìn ảo.
- Một *bảng cơ sở (table)* một bảng "thực" trong cơ sở dữ liệu
- Một *khung nhìn (View)* là một bảng "ảo" được đưa ra từ các bảng cơ sở và các khung nhìn khác

Views:

- Một user muốn tạo các view trên các table cơ sở, anh ta phải được:
  - Admin trao quyền *create View.*
  - Anh ta ít nhất phải có quyền read (select) trên các bảng cơ sở này, mới có quyền tạo các view.

KIỂM SOÁT TRUY CẬP DỰA TRÊN KHUNG NHÌN

- Người dùng (*người định nghĩa một khung nhìn*) là chủ sở hữu của khung nhìn. Tuy nhiên, chưa chắc anh ta đã được phép thực hiện tất cả các đặc quyền trên khung nhìn.
- *Phụ thuộc vào các quyền mà người dùng* có được trên các *bảng có khung nhìn tham chiếu* trực tiếp vào các bảng này.

KIỂM SOÁT TRUY CẬP DỰA TRÊN KHUNG NHÌN

- Nếu user (người định nghĩa khung nhìn) được phép thực hiện một đặc quyền (ví dụ: SELECT) trên tất cả các bảng cơ sở với GRANT OPTION, thì anh ta cũng có đặc quyền đó với GRANT OPTION trên khung nhìn.
- Sau khi có một khung nhìn đã được định nghĩa, nếu người sở hữu khung nhìn nhận thêm hoặc bị thu hồi các đặc quyền trên các bảng cơ sở, thì các đặc quyền này **sẽ được áp dụng trên khung nhìn**, có nghĩa là người dùng sẽ được thêm hoặc bị thu hồi chúng trên khung nhìn.

❖ *Views:*

- Một view có thể được tạo từ một hoặc nhiều table cơ sở (Join).
- Cú pháp tạo View:

```
create view view_name
as query_definition;
```

***Ví dụ*:**

```
CREATE VIEW  View_EMPLOYEE1 AS
SELECT  EMPID, NAME, DEPTNO
FROM  EMPLOYEE
```

```
Create View  View_LopSV  as
    Select SV.*, Lop.TenLop From SV, Lop
    Where SV.MaLop = Lop.MaLop;
```

KIỂM SOÁT TRUY CẬP DỰA TRÊN KHUNG NHÌN

Smith

Carol

Điểm yếu

	Column Name	Data Type	Length	Allow Nulls
🔑	EmpID	int	4	
	EmpName	varchar	50	✓
	Birthday	char	10	✓
	DeptNo	numeric	9	✓
	Salary	numeric	9	✓

Table

	EmpID	EmpName	Birthday	DeptNo	Salary
	1	Selina	20 /06/1984	2	2000
	2	John	10/11/1989	3	3000
	3	Kathy	04/03/1988	2	4000
	4	Bruce	05/11/1985	3	2000
▶					

View

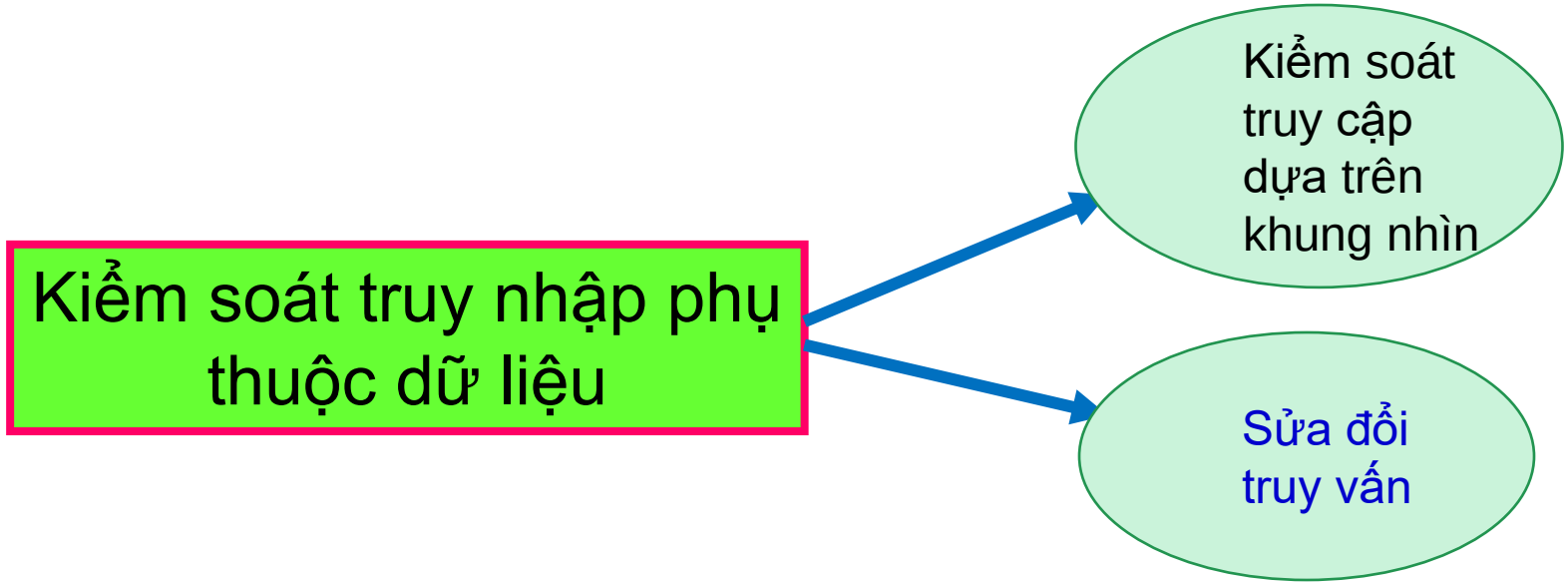
Denied!

Sam

	EmpName	Salary
▶	Selina	2000
	John	3000
	Kathy	4000
	Bruce	2000
*		

KIỂM SOÁT TRUY CẬP PHỤ THUỘC DỮ LIỆU

- Kiểm soát truy cập cơ sở dữ liệu thường *phụ thuộc vào dữ liệu.* Ví dụ, một số người dùng có thể bị giới hạn chỉ nhìn thấy các giá trị lương nhỏ hơn $30,000. một người trưởng phòng chỉ nhìn thấy các giá trị lương của các nhân viên trong phòng mình quản lý.



SỬA ĐỔI TRUY VẤN

- Là một kỹ thuật khác phục vụ cho việc thực thi kiểm soát truy cập phụ thuộc dữ liệu.
- Đối mỗi một truy vấn mà người dùng thực hiện sẽ được sửa đổi lại để hạn chế thêm người dùng sao cho phù hợp với quyền của người đó.
- Kỹ thuật này đã được ứng dụng trong Oracle và gọi là cơ chế VPD (Virtual Private Database).

SỬA ĐỔI TRUY VẤN

- Ví dụ: có bảng EMPLOYEE
- Thomas được cấp quyền sau:

```
GRANT SELECT ON
EMPLOYEE  TO Thomas
WHERE  DEPT = 'Toy'
```

- Bây giờ g/s Thomas thực hiện:

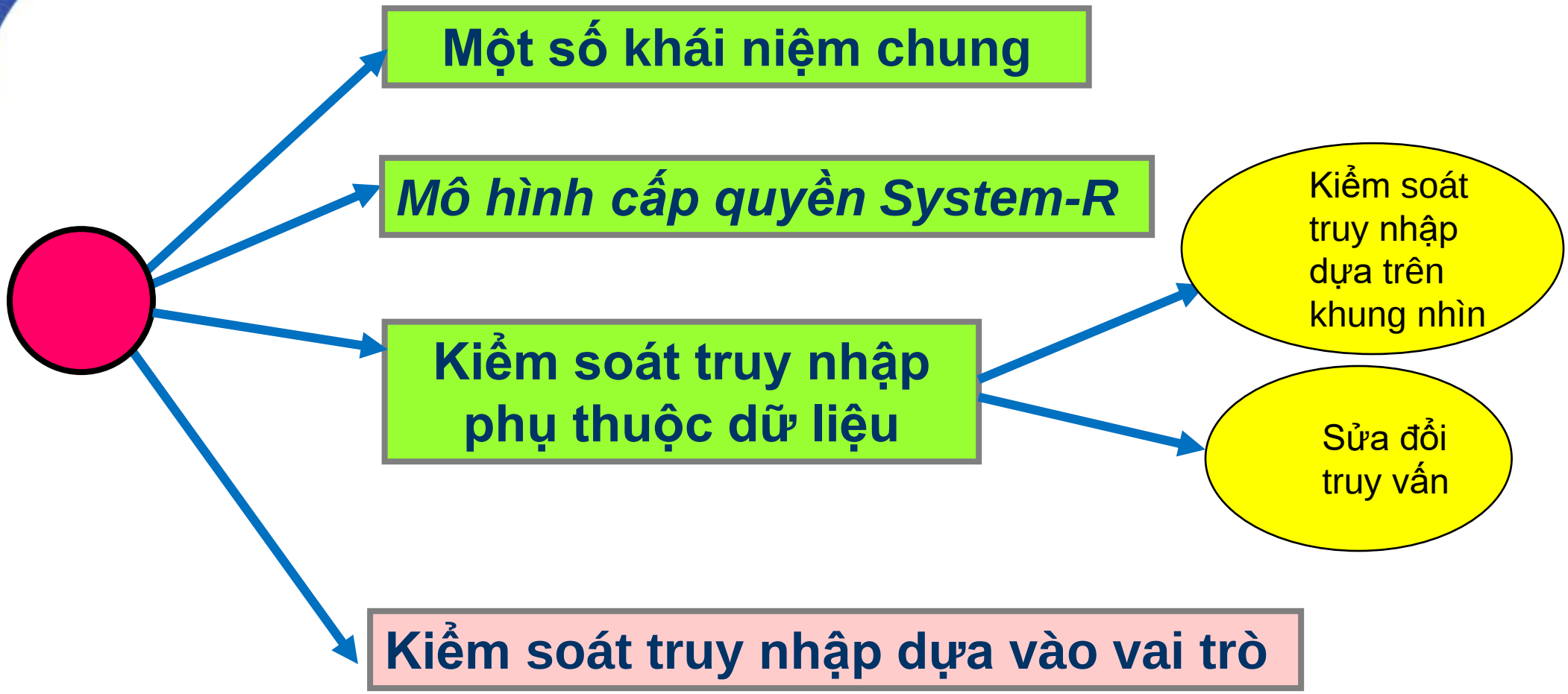
```
SELECT NAME, DEPT, SALARY,
MANAGER FROM EMPLOYEE
```

- DBMS sẽ tự động sửa đổi truy vấn này:

```
SELECT NAME, DEPT, SALARY,
MANAGER FROM EMPLOYEE
WHERE DEPT = 'Toy'
```

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	NULL

MÔ HÌNH, CHÍNH SÁCH AN TOÀN TÙY Ý



KIỂM SOÁT TRUY CẬP DỰA VÀO VAI TRÒ (RBAC)

- Hầu hết các DBMS đều hỗ trợ RBAC. RBAC có thể dùng kết hợp với DAC hoặc MAC hoặc được dùng độc lập.
- RBAC được áp dụng vào đầu những năm 1970. Khái niệm chính của RBAC là những quyền hạn được liên kết với những vai trò (role).
- Mục đích chính của RBAC là giúp cho việc quản trị an toàn một cách dễ dàng hơn.

KIỂM SOÁT TRUY CẬP DỰA VÀO VAI TRÒ (RBAC)

rights

Privilege

access

Role

Group: AT4

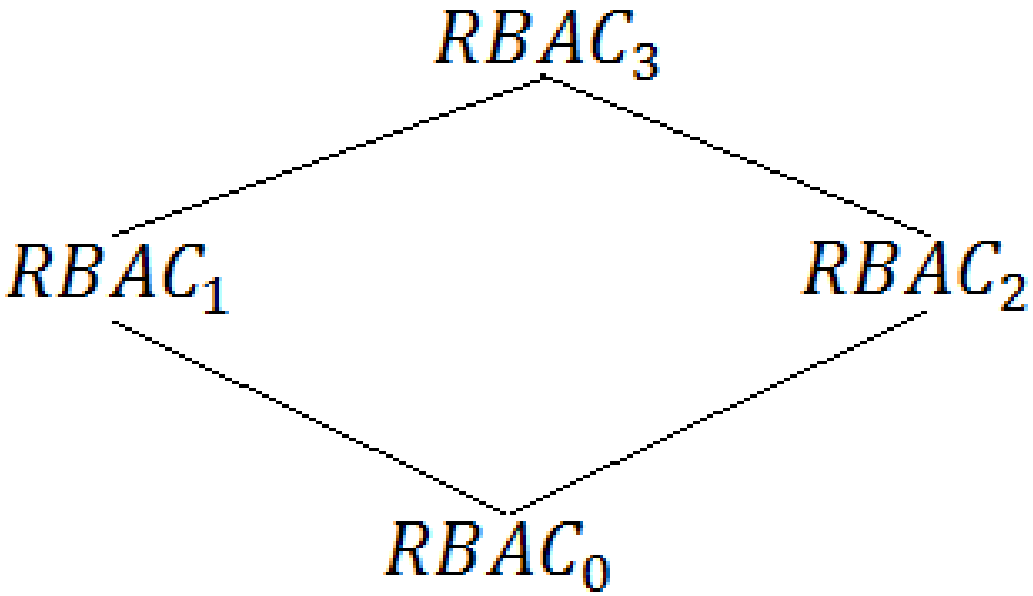
AT4A

AT4B

AT4C

KIỂM SOÁT TRUY CẬP DỰA VÀO VAI TRÒ (RBAC)

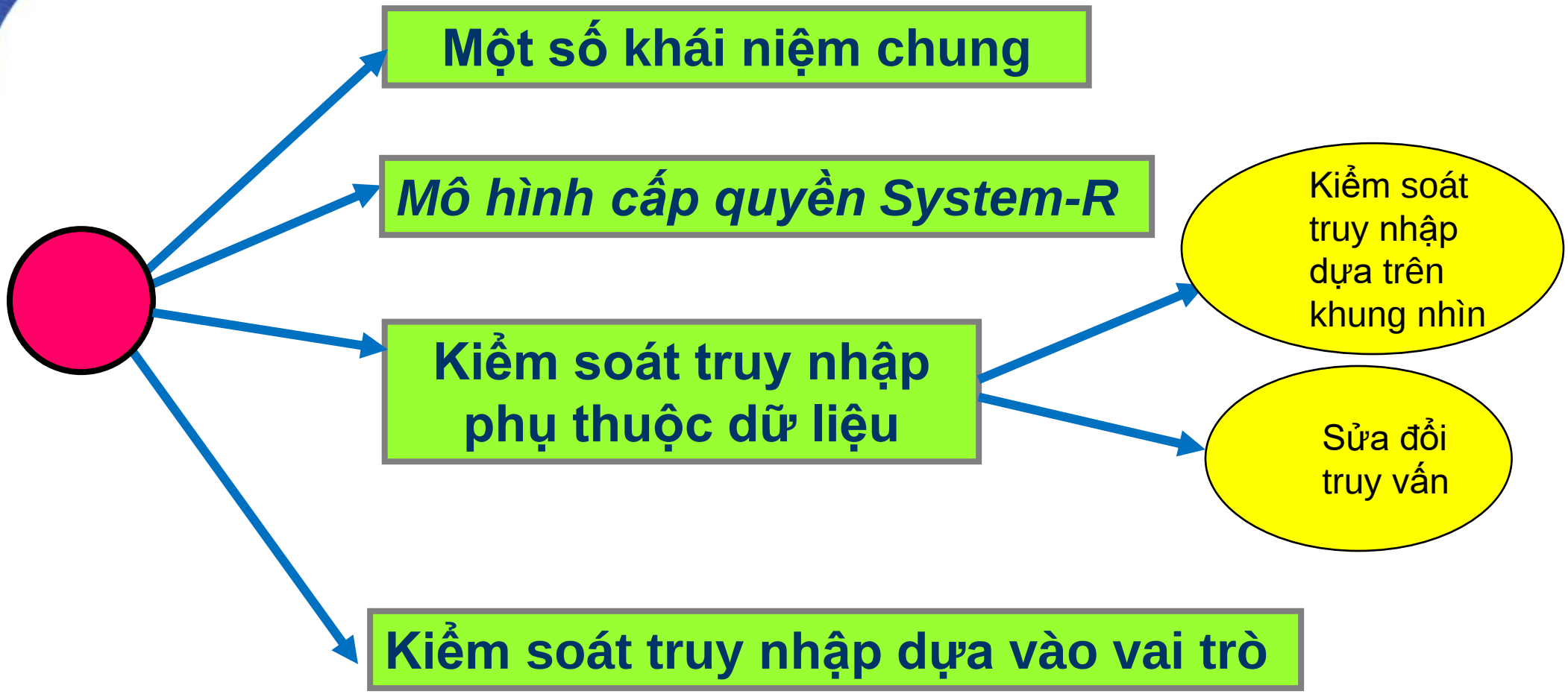
- Mô hình RBAC gồm bốn mô hình con là: RBAC0, RBAC1, RBAC2, RBAC3.



KIỂM SOÁT TRUY CẬP DỰA VÀO VAI TRÒ (RBAC)

- 4 mô hình con RBAC0, RBAC1, RBAC2, RBAC3.
  - Mô hình nền tảng RBAC0 ở dưới cùng, là yêu cầu tối thiểu cho bất kì hệ thống nào có hỗ trợ RBAC.
  - Mô hình RBAC1, RBAC2 được phát triển từ mô hình RBAC0 nhưng có thêm các điểm đặc trưng cho từng mô hình: mô hình RBAC1 thêm vào khái niệm của hệ thống phân cấp vai trò, RBAC2 thêm vào các ràng buộc. RBAC1, RBAC2 không liên quan nhau.
  - RBAC3 là mô hình tổng hợp của ba mô hình RBAC0, RBAC1 và RBAC2.

MÔ HÌNH, CHÍNH SÁCH AN TOÀN TÙY Ý



VÍ DỤ VỀ MÔ HÌNH DAC ĐIỂN HÌNH
MÔ HÌNH MA TRẬN TRUY NHẬP

- Là một mô hình trừu tượng, mô tả trạng thái bảo vệ của một hệ thống
- Được giới thiệu đầu tiên bởi Butler W. Lampson in 1971.
- Mỗi phần tử trong ma trận thể hiện các quyền truy nhập của các chủ thể trên các đối tượng

Objects

Subjects

	File 1	File 2	File 3	…	File n
User 1	read	write	-	-	read
User 2	write	execute	write	-	-
User 3	-	-	-	read	read
…		Read/ write	execute	write	
User m	read	write	read	write	Read/ Write

VÍ DỤ VỀ MÔ HÌNH DAC ĐIỂN HÌNH
MÔ HÌNH MA TRẬN TRUY NHẬP

- Ứng dụng ma trận truy nhập: trong HĐH, trong các ứng dụng web, …
- Thực hiện dựa trên hai khái niệm:
  - *Capabilities (rows)*
  - *ACL-Access control lists (columns)*

MÔ HÌNH MA TRẬN TRUY NHẬP

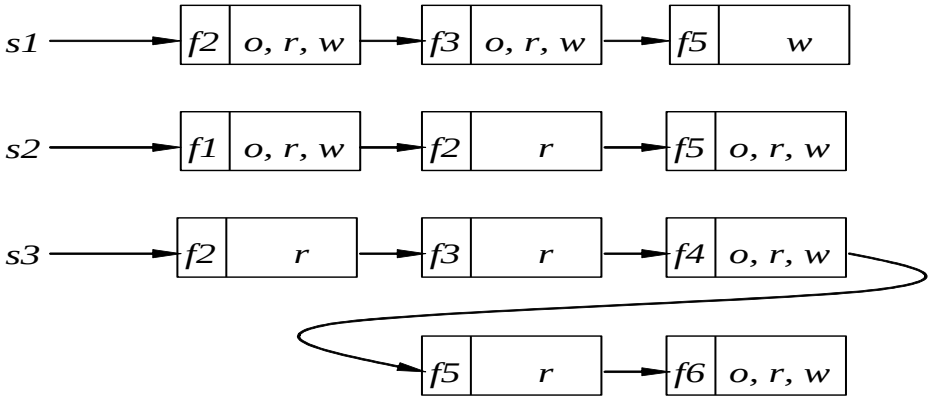
o: own
r: read
w:write

	f1	f2	f3	f4	f5	f6
s1		o, r, w	o, r, w		w	
s2	o, r, w	r			o, r, w	
s3		r	r	o, r, w	r	o, r, w

Access Matrix

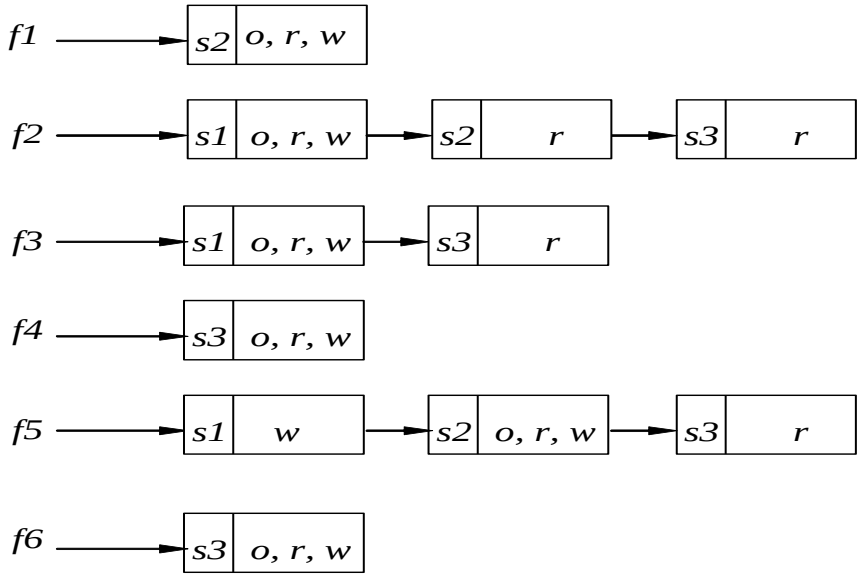
Capabilities

Capabilities



Access Control List (ACLs)

Access Control List



ƯU NHƯỢC ĐIỂM CỦA MÔ HÌNH/CHÍNH SÁCH DAC

MÔ HÌNH, CHÍNH SÁCH AN TOÀN DAC

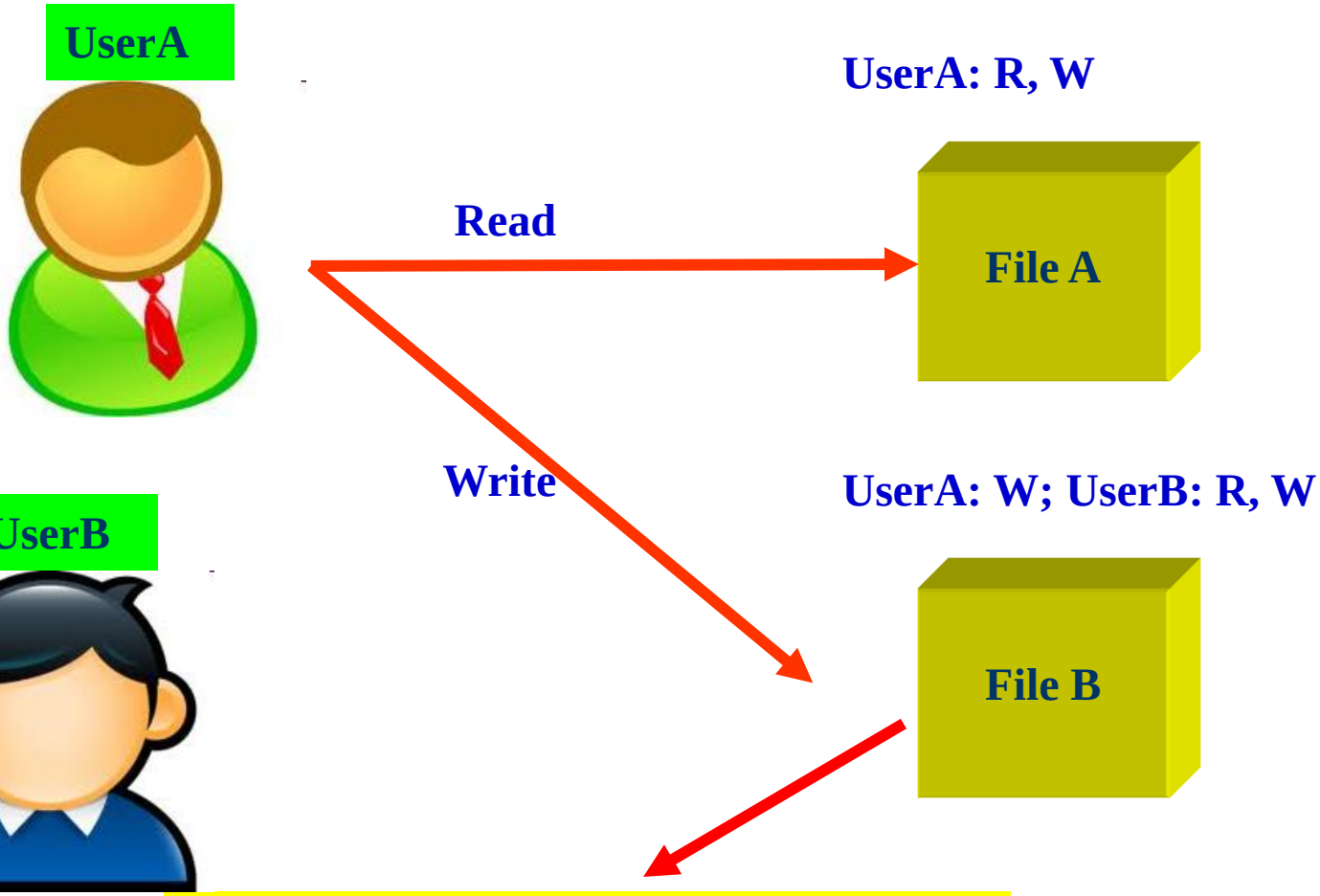
- Đây là một kỹ thuật phổ biến, chỉ có một vài vấn đề nghiên cứu mở
- Hầu hết các hệ quản trị (DBMS) thương mại đều hỗ trợ nó như: Access, SQL Server, Oracle,…

MÔ HÌNH, CHÍNH SÁCH AN TOÀN DAC

- Việc gán và thu hồi quyền DAC cũng khá phức tạp, nếu không được quản lý tốt thì rất dễ bị lộ thông tin bí mật.
- *Tấn công Trojan Horse:* DAC cho phép đọc thông tin từ một đối tượng và chuyển đến một đối tượng khác.

MÔ HÌNH, CHÍNH SÁCH AN TOÀN DAC

Ví dụ về Trojan Horse



Nội DUNG

1. Các khái niệm cơ bản
2. Các mô hình và chính sách an toàn tùy ý
3. *Các mô hình và chính sách an toàn bắt buộc*
4. Các mô hình an toàn khác

Thank You!

Question?