Bài 2.2. Mô hình an toàn MAC

LOGO

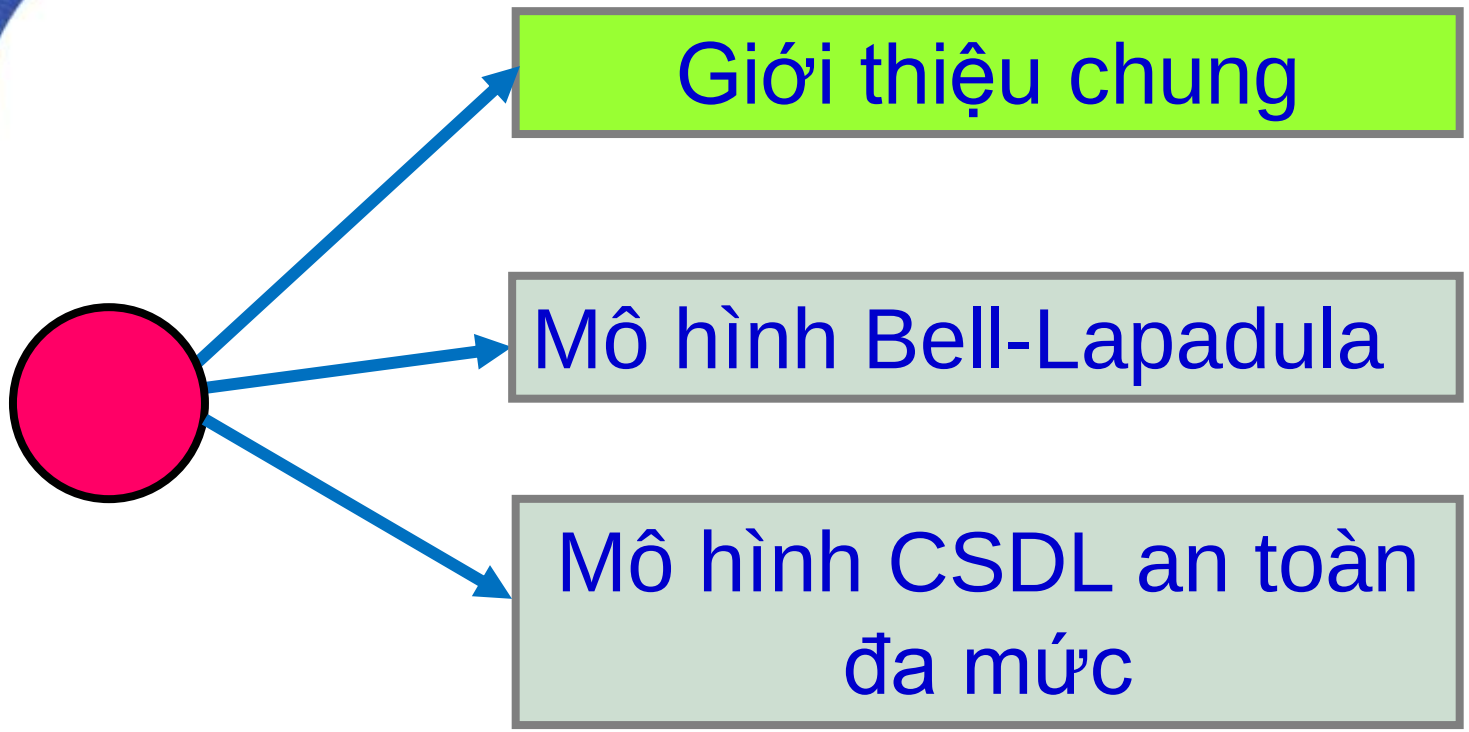
CHƯƠNG 2
CÁC MÔ HÌNH VÀ CHÍNH SÁCH AN TOÀN

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

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 MÔ HÌNH, CHÍNH SÁCH AN TOÀN BẮT BUỘC (MAC)



GIỚI THIỆU CHUNG

- Chính sách an toàn bắt buộc sẽ đảm bảo an toàn cho hệ thống ở mức độ cao hơn so với chính sách an toàn tùy ý, bởi vì ngoài việc kiểm soát quyền truy nhập vào dữ liệu thì chính sách an toàn bắt buộc còn kiểm soát luồng dữ liệu.
- ***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),…

GIỚI THIỆU CHUNG

❖ *MAC:*

- Được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt
- Hạn chế truy nhập của các chủ thể vào các đối tượng bằng cách sử dụng các nhãn an toàn (label).

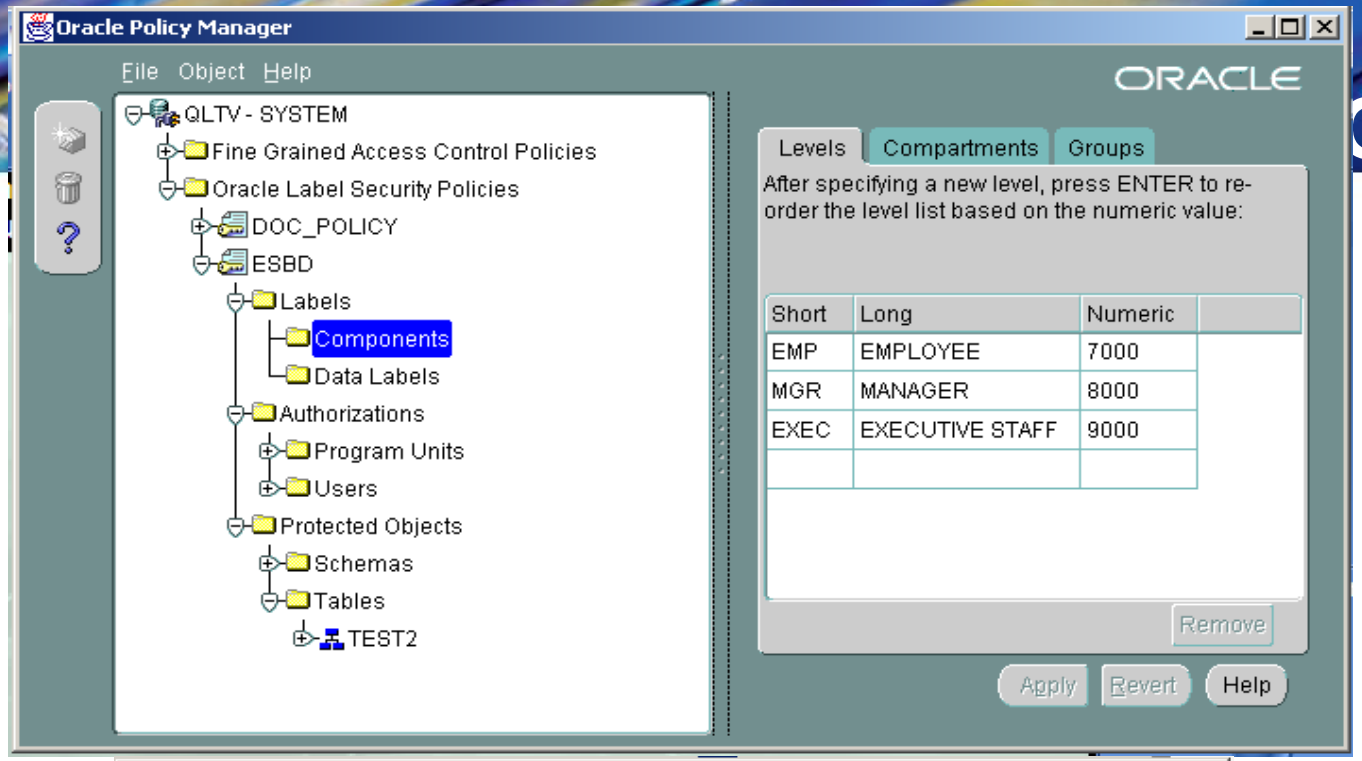
MAC (Mandatory Access Control)

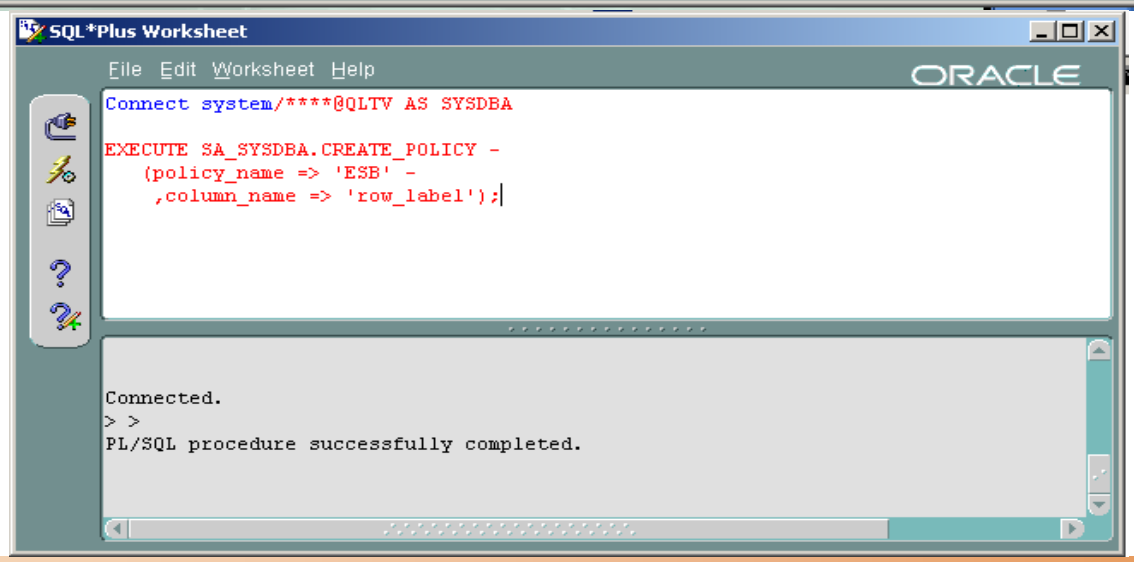
- Mọi chủ thể và đối tượng trong hệ thống đều được gắn với một ***lớp an toàn.***
- *Lớp an toàn của User KH: Classification*
  - ***Vd: Class(S)***
- *Lớp an toàn của đối tượng KH: Clearance*
  - ***Vd: Clear(O)***

MAC (Mandatory Access Control)

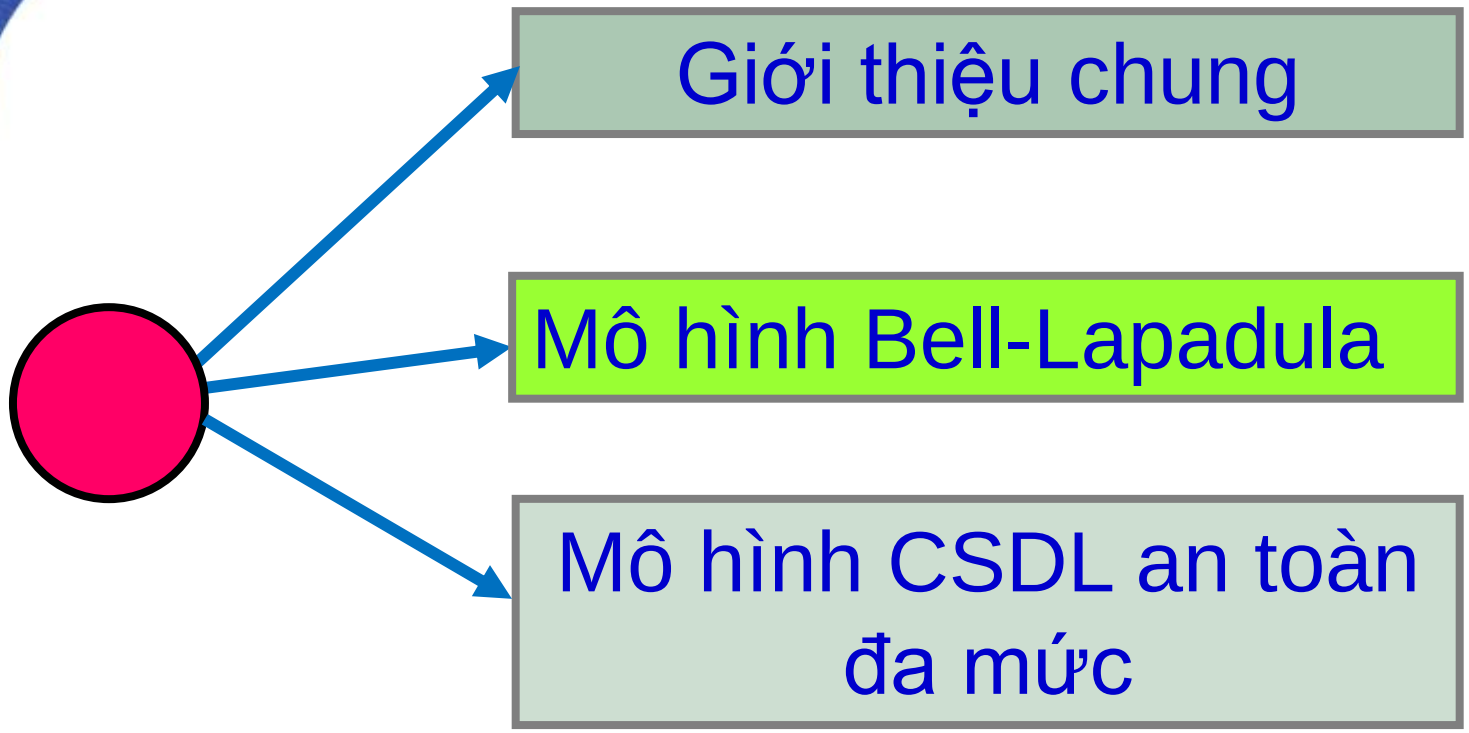
KIỂM SOÁT MAC TRONG ORACLE

- Mỗi lớp an toàn được xác định bởi một ***nhãn – Label.***
- *Lớp an toàn = (Mức nhạy cảm, Vùng ứng dụng)*
- *Label = (Level, Compartment, Group)*
  - **Level** (thành phần bắt buộc): là thành phần phân cấp, thể hiện mức nhạy cảm
  - **Compartment** (tuỳ chọn): là các thành phần không phân cấp, sử dụng để phân loại dữ liệu.
  - **Group** (tuỳ chọn): là thành phần phân cấp, được dùng để hỗ trợ phân loại người dùng.


Oracle Policy Manager
File Object Help
ORACLE
QLTV - SYSTEM
Fine Grained Access Control Policies
Oracle Label Security Policies
DOC_POLICY
ESBD
Labels
Components
Data Labels
Authorizations
Program Units
Users
Protected Objects
Schemas
Tables
TEST2
Levels
Compartments
Groups
After specifying a new level, press ENTER to re-order the level list based on the numeric value:
Short
Long
Numeric
EMP
EMPLOYEE
7000
MGR
MANAGER
8000
EXEC
EXECUTIVE STAFF
9000
Remove
Apply
Revert
Help


SQL*Plus Worksheet
File Edit Worksheet Help
ORACLE
Connect system/****@QLTV AS SYSDBA
EXECUTE SA_SYSDBA.CREATE_POLICY -
(policy_name => 'ESB' -
,column_name => 'row_label');
Connected.
> >
PL/SQL procedure successfully completed.

CÁC MÔ HÌNH, CHÍNH SÁCH AN TOÀN BẮT BUỘC (MAC)



MÔ HÌNH
BELL – LAPADULA (BLP)

TỔNG QUAN VỀ MÔ HÌNH BLP

- Xuất hiện năm 1975, do quân đội Mỹ
- Phù hợp sử dụng trong các hệ thống của quân đội và chính phủ
- ***Mục đích:*** đảm bảo tính bí mật
- Đây là mô hình chính tắc đầu tiên về điều khiển luồng thông tin
- Là một mô hình tĩnh: mức an toàn (nhãn an toàn) không thay đổi

MÔ HÌNH BLP

Người dùng được phân mức độ an toàn, KH: ***Clear(S)***

Đối tượng được phân mức độ nhạy cảm, KH: ***Class(O)***

Top Secret

Secret

Confidential

Unclassified

Mức an toàn quân sự	Mức an toàn thương mại
Tuyệt mật	Hạn chế
Tối mật	Sở hữu
Mật	Nhạy cảm
Không phân loại	Công cộng

High sensitive

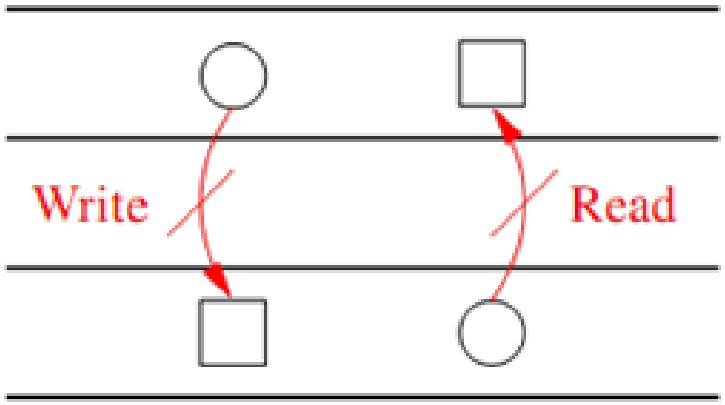
Sensitive

Confidential

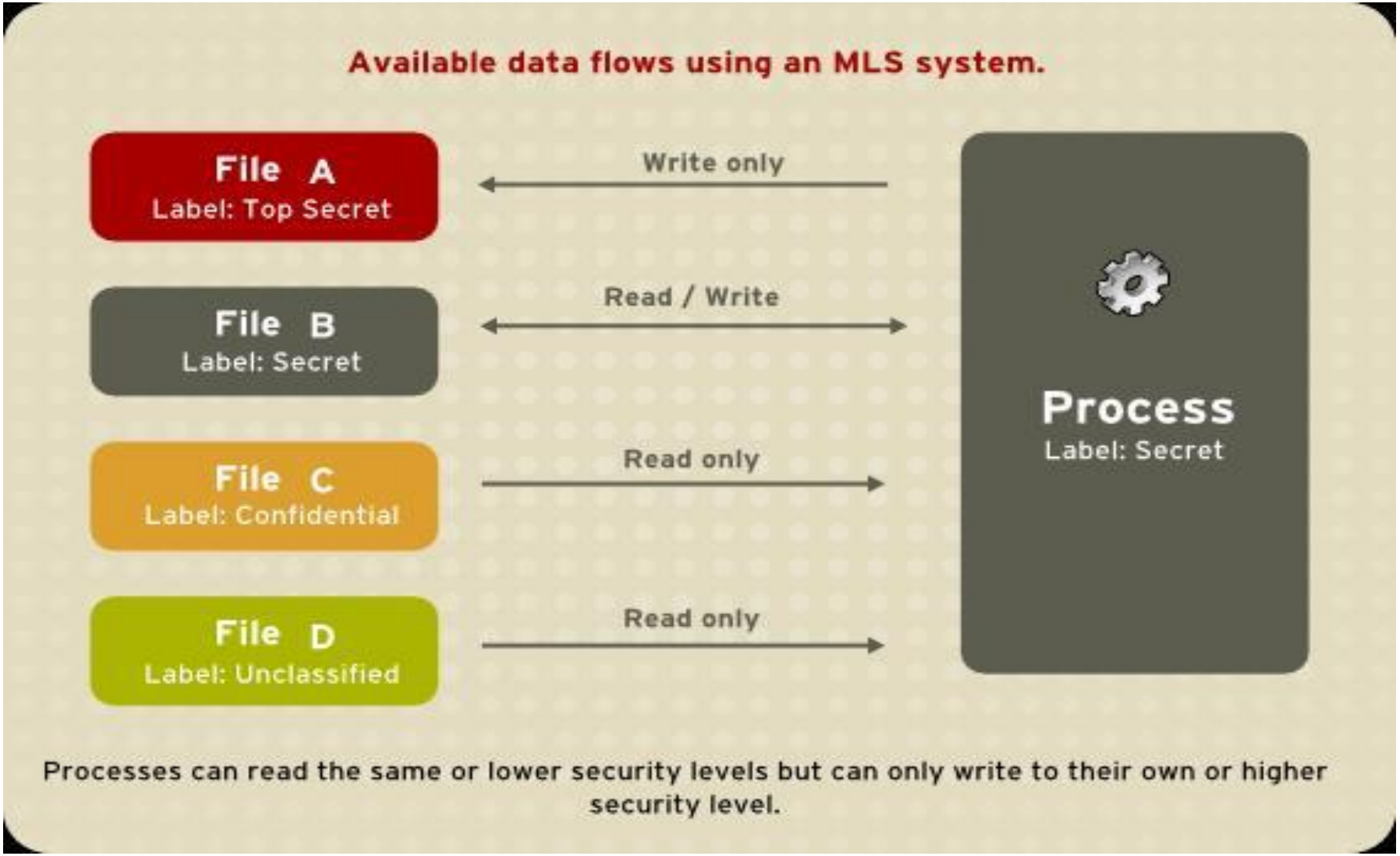
Public

CÁC THUỘC TÍNH CỦA BLP

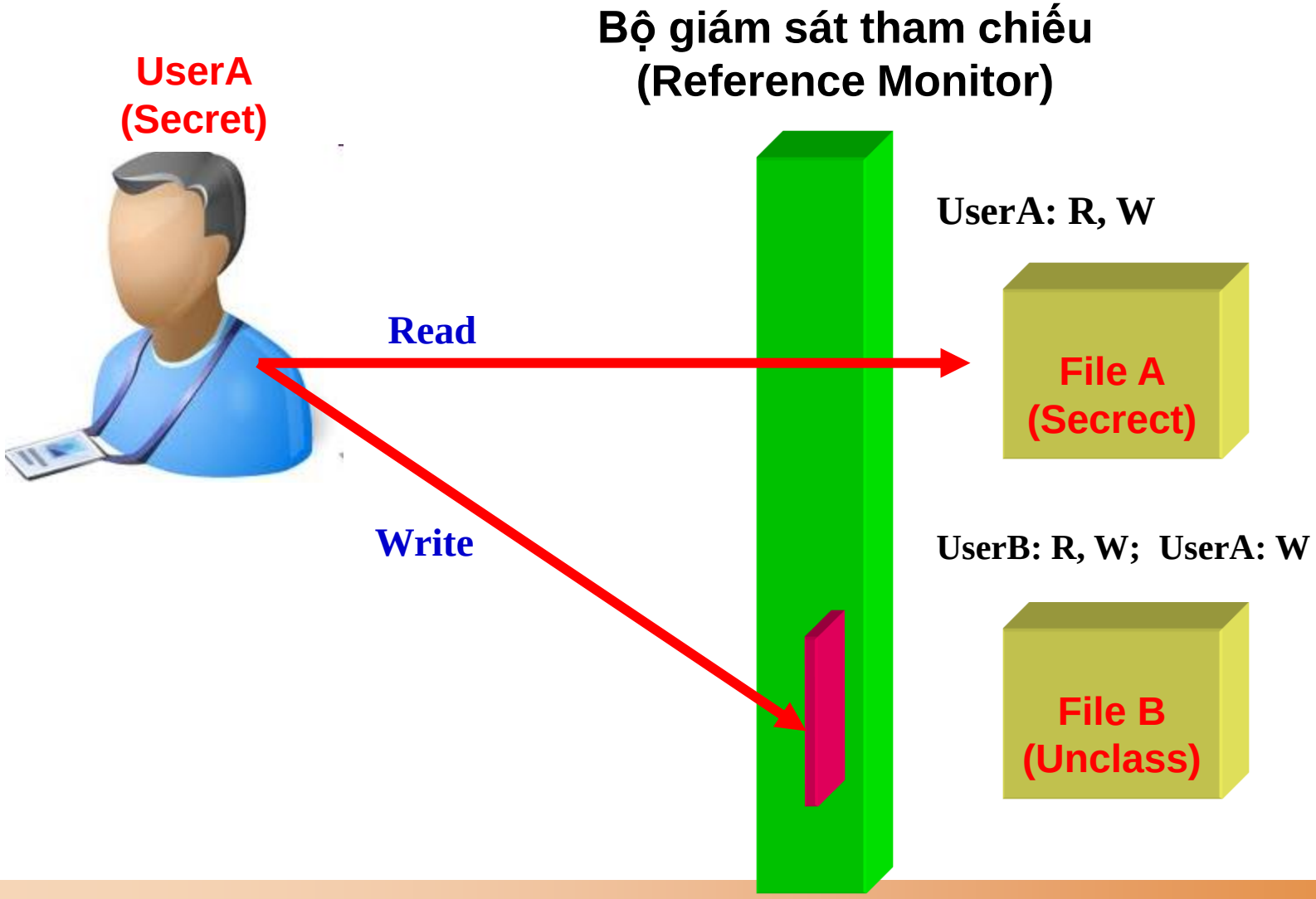
- *Thuộc tính an toàn đơn giản (Not Read up):*
  - Một chủ thể S được phép truy nhập đọc đến một đối tượng O chỉ khi Clear (S)≥class(O)
- *Thuộc tính * (Not Write down):*
  - Một chủ thể S được phép truy nhập ghi lên một đối tượng O chỉ khi Clear (S) ≤ class(O)



MÔ HÌNH BLP


Available data flows using an MLS system.
File A
Label: Top Secret
Write only
File B
Label: Secret
Read / Write
File C
Label: Confidential
Read only
File D
Label: Unclassified
Read only
Process
Label: Secret
Processes can read the same or lower security levels but can only write to their own or higher security level.

MÔ HÌNH BLP


Bộ giám sát tham chiếu
(Reference Monitor)
UserA
(Secret)
Read
Write
UserA: R, W
File A
(Secrect)
UserB: R, W; UserA: W
File B
(Unclass)

NHẬN XÉT _BLP

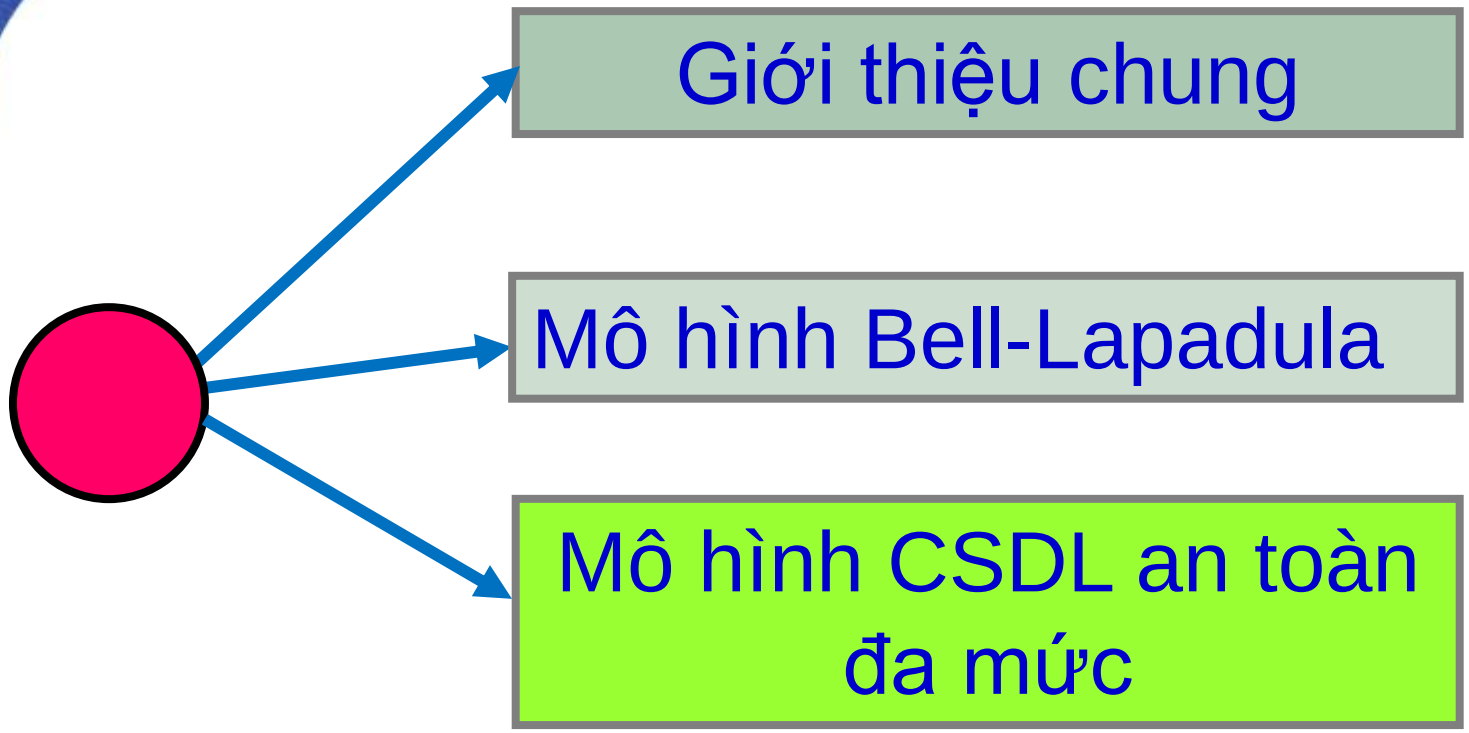
❖ *Ưu điểm:*

- Các nhãn an toàn của các chủ thể và các đối tượng không bao giờ được thay đổi trong suốt thời gian hệ thống hoạt động.

❖ *Hạn chế:*

- Mới chỉ quan tâm tới tính bí mật
- Chưa chỉ ra cách thay đổi các quyền truy nhập cũng như cách tạo và xóa các chủ thể cũng như các đối tượng

CÁC MÔ HÌNH, CHÍNH SÁCH AN TOÀN BẮT BUỘC (MAC)



MÔ HÌNH CSDL ĐA MỨC (MULTILEVEL SECURITY – MLS)

- Hệ thống Multi-level Security (MLS) là hệ thống an toàn nhiều mức, mỗi chủ thể và đối tượng trong đó đều được gắn nhãn an toàn thể hiện mức độ nhạy cảm của các chủ thể và các đối tượng đó.

MÔ HÌNH CSDL ĐA MỨC (MULTILEVEL SECURITY – MLS)

- Mục đích: đảm bảo tính bí mật.
- Thường được áp dụng cho lĩnh vực quân sự.
- *CSDL đa mức:* là CSDL mà người dùng và dữ liệu được phân thành các mức an toàn khác nhau (chẳng hạn như không phân lớp - U, mật - C, tuyệt mật - S, tối mật - TS).
- Chủ thể khi truy nhập bị giới hạn bởi những điều khiển truy nhập bắt buộc là "Not read up, Not write down", theo mô hình của Bell - LaPadula.

MÔ HÌNH CSDL ĐA MỨC (MULTILEVEL SECURITY – MLS)

❖Đa thể hiện (polyinstantiation):

- Là một kỹ thuật trong CSDL cho phép CSDL có thể chứa nhiều thể hiện của cùng một dữ liệu với các mức nhạy cảm khác nhau.
- Trong các DBMS quan hệ, có thể có nhiều bản ghi khác nhau nhưng có cùng một khóa chính với các mức nhạy cảm khác nhau.
- Các bản ghi đa thể hiện là các bản ghi với cùng khóa chính nhưng có các lớp user truy nhập khác nhau gắn với các khóa chính đó.

VÍ DỤ, XÉT BA THỂ HIỆN CỦA BẢNG QUAN HỆ PROJECT

LOGO

Title	Subject	Client	TC
Alpha, S	Development, S	A,S	S
Beta, U	Research, S	B,S	S
Celsius, U	Production, U	C,U	U

Hình a) Project$_S$

Title	Subject	Client	TC
Beta, U	-,U	-,U	U
Celsius, U	Production, U	C,U	U

Hình b) Project$_S$

Hình c)
tổng hợp đa thể hiện

Title	Subject	Client	TC
Alpha, S	Development, S	A,S	S
Beta, U	Research, S	B,S	S
Celsius, U	Production, U	C,U	U
Alpha, U	Production, U	D, U	U

ĐA THỂ HIỆN (POLYINSTANTIATION)

- Vấn đề đa thể hiện xuất hiện nhằm tránh kênh ngầm.
- Kênh ngầm (convert channel): Lampson (1973) đã định nghĩa một kênh ngầm như một cách để đi vào luồng thông tin.
  - Ví dụ trên, khi một người dùng mức *S* muốn chèn (insert) một bản ghi có mức nhạy cảm *U* vào cơ sở dữ liệu, nếu hoạt động này bị từ chối (vì đã tồn tại một bản ghi như thế ở mức cao hơn) thì người dùng có thể suy diễn ra sự tồn tại của bản ghi này, kết quả là có một kênh ngầm xảy ra.

BÀI TẬP VỀ MÔ HÌNH BLP VÀ MLS
VÍ DỤ : MỘT BẢNG VỀ SINH VIÊN

MaSV	Hoten	Diem	SoLanKyLuat	ChucVu
MS01	Lan	9	0	Lớp trưởng
MS02	Nam	4	02	Sinh viên
MS03	Huệ	8	0	Lớp phó
MS04	Hải	3	02	Sinh viên
….	….	….	…	…

Yêu cầu:

- Xây dựng hệ thống Multilevel Security trên hệ thống CSDL chứa bảng này
- Phân quyền cho 3 lớp user dựa vào mô hình Bell-Lapadula

VD: MỘT BẢNG VỀ SINH VIÊN

C	C	S	TS	C
MaSV	**Hoten**	**Diem**	**SoLanKyLuat**	**ChucVu**
MS01	Lan	9	0	Lớp trưởng
MS02	Nam	4	02	Sinh viên
MS03	Huệ	8	0	Lớp phó
MS04	Hải	3	02	Sinh viên
….	….	….	…	…

TS
C
S
C

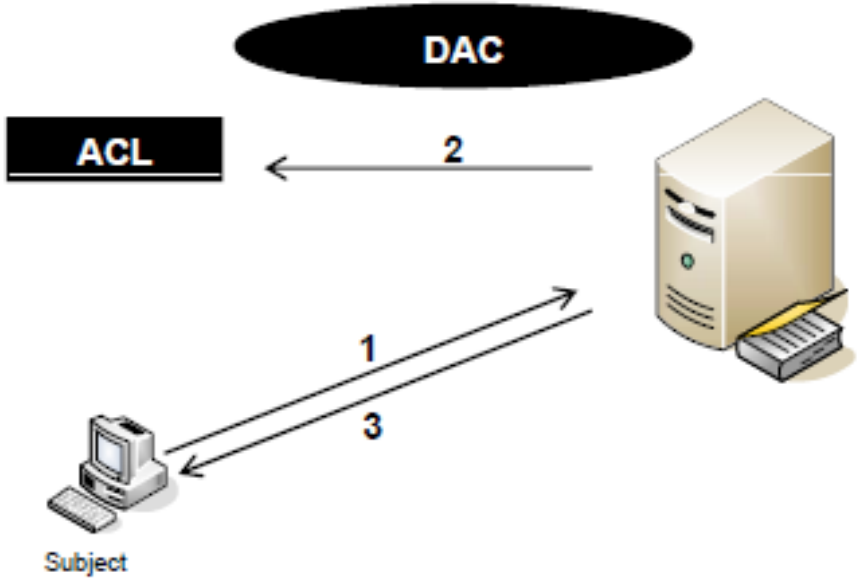
MÔ HÌNH, CHÍNH SÁCH MAC

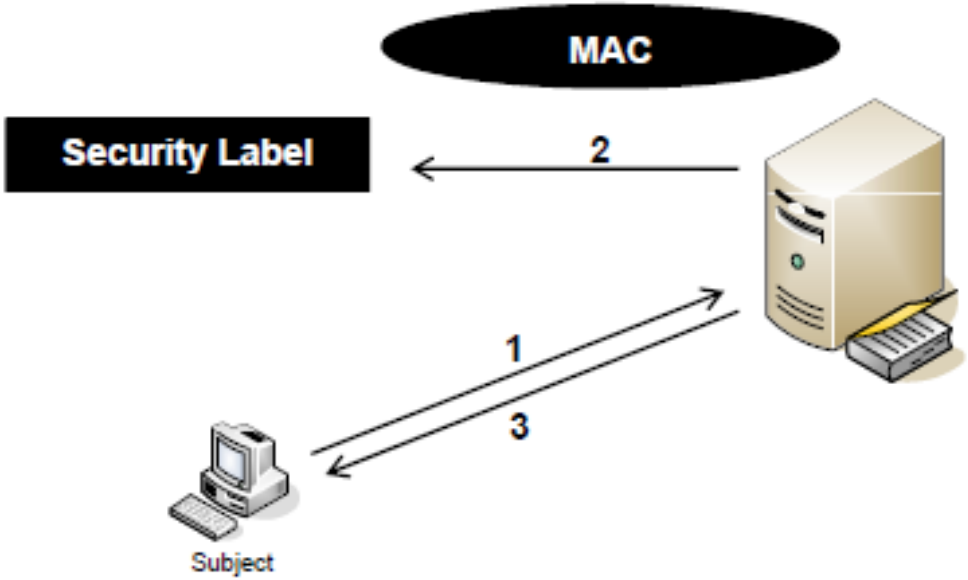
- Độ an toàn cao vì sử dụng các nhãn an toàn, phù hợp với các môi trường đòi hỏi độ an toàn nghiêm ngặt như quân sự, quốc phòng.
- Khắc phục được hạn chế của DAC trong vấn đề trao quyền.

MÔ HÌNH, CHÍNH SÁCH MAC

- Phức tạp: việc gắn nhãn không tốt có thể dẫn đến việc gán nhãn không đầy đủ hoặc không nhất quán.
- Thiếu kỹ thuật gán nhãn an toàn tự động: tốn công sức.
- Kênh ngầm: không giải quyết được hoàn toàn tấn công Trojan Horse.

XEM LẠI : DAC VÀ MAC





BÀI TẬP VỀ NHÀ

- Sự khác nhau giữa MAC và DAC?
- Việc áp dụng MAC, DAC trong các DBMS?

GIỚI THIỆU MỘT SỐ MÔ HÌNH AN TOÀN KHÁC

- **Mô hình Biba:** là một biến thể của mô hình Bell – Lapadula mà tập trung chính vào việc đảm bảo tính toàn vẹn thông tin trong một hệ thống.
- **Mô hình Clark-Wilson**: nhằm ngăn chặn các người dùng có quyền thực hiện các sửa đổi không được phép trên dữ liệu. Mô hình này thực hiện một hệ thống với bộ ba – một chủ thể, một chương trình và một đối tượng.
- **Mô hình bức tường Trung Hoa (Chinese Wall model):** là sự kết hợp giữa thương mại tự do với các điều khiển bắt buộc theo luật. Nó được ứng dụng trong hoạt động của nhiều tổ chức tài chính.
- **Mô hình mắt lưới (Lattice model)**: liên quan đến các thông tin quân sự. Các mô hình điều khiển truy nhập dựa trên lưới được phát triển vào đầu những năm 1970 để giải quyết vấn đề đảm bảo tính bí mật của thông tin quân sự.

Thank You!

Question?