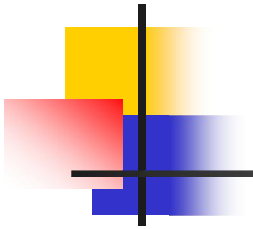
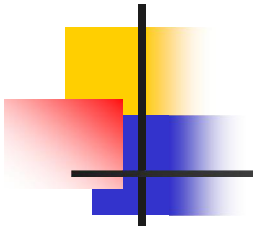
Chương 1
Tổng quan về an toàn thông tin trong cơ sở dữ liệu

Giảng viên: Trần Thị Lượng



Mục tiêu

- Chương này trình bày những ***hiểm họa*** tiềm ẩn có thể xảy ra đối với CSDL, đồng thời trình bày những ***giải pháp*** có thể sử dụng để bảo vệ CSDL đối với những hiểm họa đó.



Nội dung

1.1 Giới thiệu
1.2 Một số khái niệm trong CSDL
1.3 Các vấn đề an toàn trong CSDL
    1.3.1 Các hiểm họa đối với an toàn CSDL
    1.3.2 Các yêu cầu bảo vệ CSDL
1.4 Kiểm soát an toàn
    1.4.1 Kiểm soát luồng
    1.4.2 Kiểm soát suy diễn
    1.4.3 Kiểm soát truy nhập
1.5 Thiết kế CSDL an toàn

Nội dung

1.1 Giới thiệu
1.2 Một số khái niệm trong CSDL
1.3 Các vấn đề an toàn trong CSDL
    1.3.1 Các hiểm họa đối với an toàn CSDL
    1.3.2 Các yêu cầu bảo vệ CSDL
1.4 Kiểm soát an toàn
    1.4.1 Kiểm soát luồng
    1.4.2 Kiểm soát suy diễn
    1.4.3 Kiểm soát truy nhập
1.5 Thiết kế CSDL an toàn

1.1 Giới thiệu

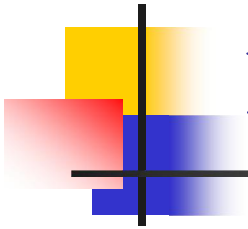
- Sự phát triển lớn mạnh của công nghệ thông tin trong những năm qua đã dẫn đến việc sử dụng rộng rãi các hệ thống máy tính trong hầu hết các tổ chức cá nhân và công cộng, chẳng hạn như: ngân hàng, trường học, tổ chức dịch vụ và sản xuất, bệnh viện, thư viện, quản lý phân tán và tập trung..vv.
- Độ tin cậy của phần cứng, phần mềm ngày càng được nâng cao cùng với việc liên tục giảm giá, tăng kỹ năng chuyên môn của các chuyên viên thông tin đã góp phần khuyến khích việc sử dụng các dịch vụ máy tính một cách rộng rãi.

1.1 Giới thiệu

- Một đặc điểm cơ bản của DBMS là khả năng quản lý đồng thời nhiều giao diện ứng dụng. Mỗi ứng dụng có một cái nhìn thuần nhất về CSDL, có nghĩa là có cảm giác chỉ mình nó đang khai thác CSDL.
- Việc sử dụng rộng rãi các ***CSDL phân tán*** và tập trung đã đặt ra nhiều yêu cầu nhằm đảm bảo các chức năng thương mại và an toàn dữ liệu

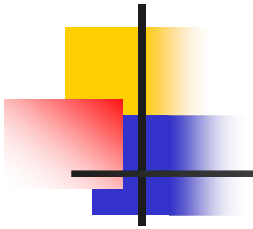
1.1 Giới thiệu

- Độ phức tạp trong thiết kế và thực thi của các hệ thống an toàn dựa vào nhiều yếu tố, như:
  - Tính không đồng nhất của người sử dụng
  - Phạm vi sử dụng: sự phân nhỏ hoặc mở rộng khu vực của các hệ thống thông tin (cả ở cấp quốc gia và quốc tế)
  - Các hậu quả khó lường do mất mát thông tin,
  - Những khó khăn trong việc xây dựng mô hình, đánh giá và kiểm tra độ an toàn của dữ liệu.



1.1 Giới thiệu

- *An toàn thông tin trong CSDL*
  - *Tính bí mật*
  - *Tính toàn vẹn*
  - *Tính sẵn sàng*



Nội dung

1.1 Giới thiệu

1.2 Một số khái niệm trong CSDL

1.3 Các vấn đề an toàn trong CSDL

- 1.3.1 Các hiểm họa đối với an toàn CSDL
- 1.3.2 Các yêu cầu bảo vệ CSDL

1.4 Kiểm soát an toàn

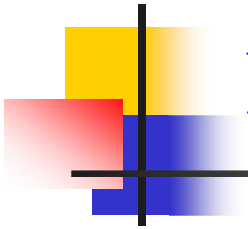
- 1.4.1 Kiểm soát luồng
- 1.4.2 Kiểm soát suy diễn
- 1.4.3 Kiểm soát truy nhập

1.5 Thiết kế CSDL an toàn

1.2 Một số khái niệm trong CSDL

- ***CSDL:*** là một tập hợp dữ liệu và một tập các quy tắc tổ chức dữ liệu chỉ ra các mối quan hệ giữa chúng.
- ***DBMS:*** Hệ thống phần mềm cho phép quản lý, thao tác trên CSDL, tạo ra sự trong suốt phân tán với người dùng gọi là hệ quản trị CSDL.
- ***Mô hình logic:*** phụ thuộc vào DBMS (ví dụ mô hình quan hệ, mô hình phân cấp, mô hình mạng)
- ***Mô hình khái niệm:*** độc lập với DBMS.

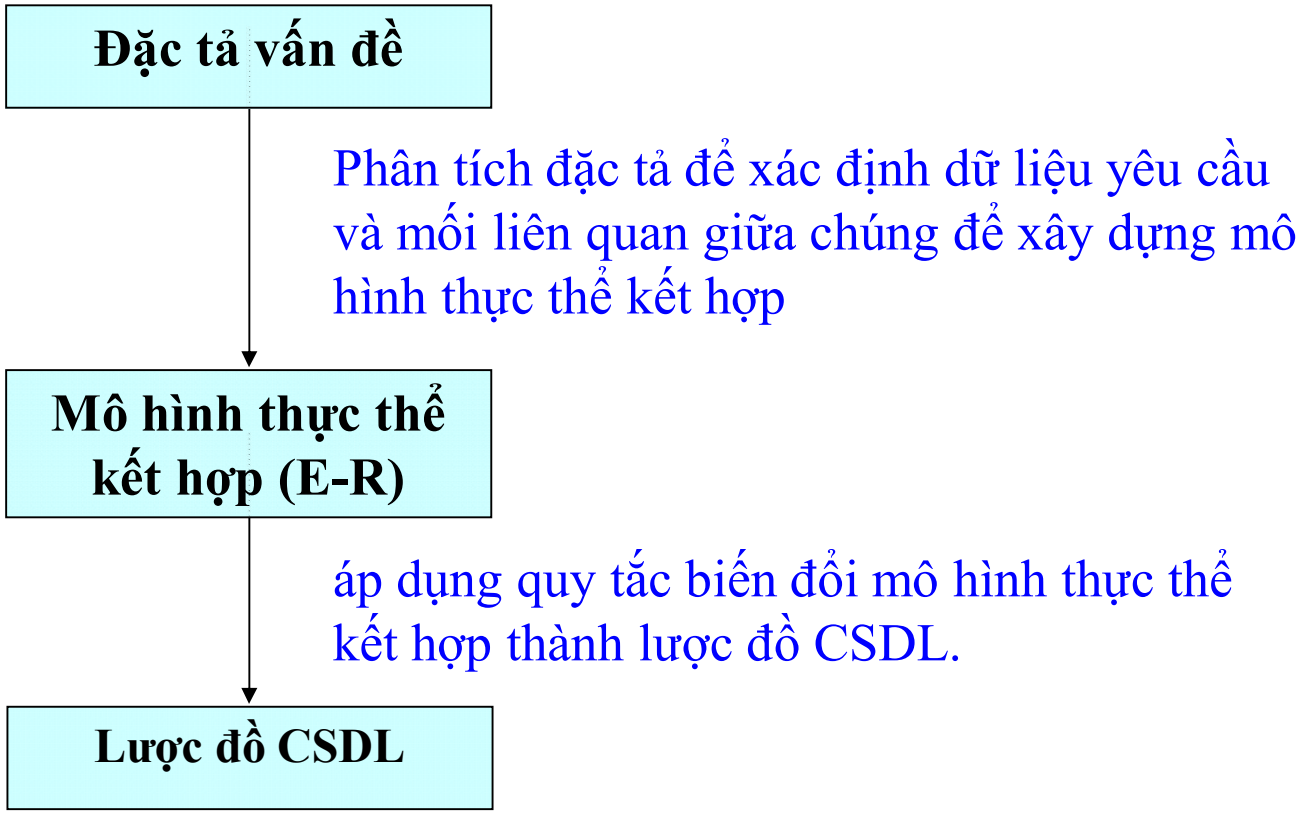
  Ví dụ: mô hình quan hệ thực thể (E-R) là một trong các mô hình khái niệm phổ biến nhất, được xây dựng dựa trên khái niệm thực thể.



1.2 Một số khái niệm trong CSDL

- Các bước thiết kế một CSDL?

1.2 Một số khái niệm trong CSDL

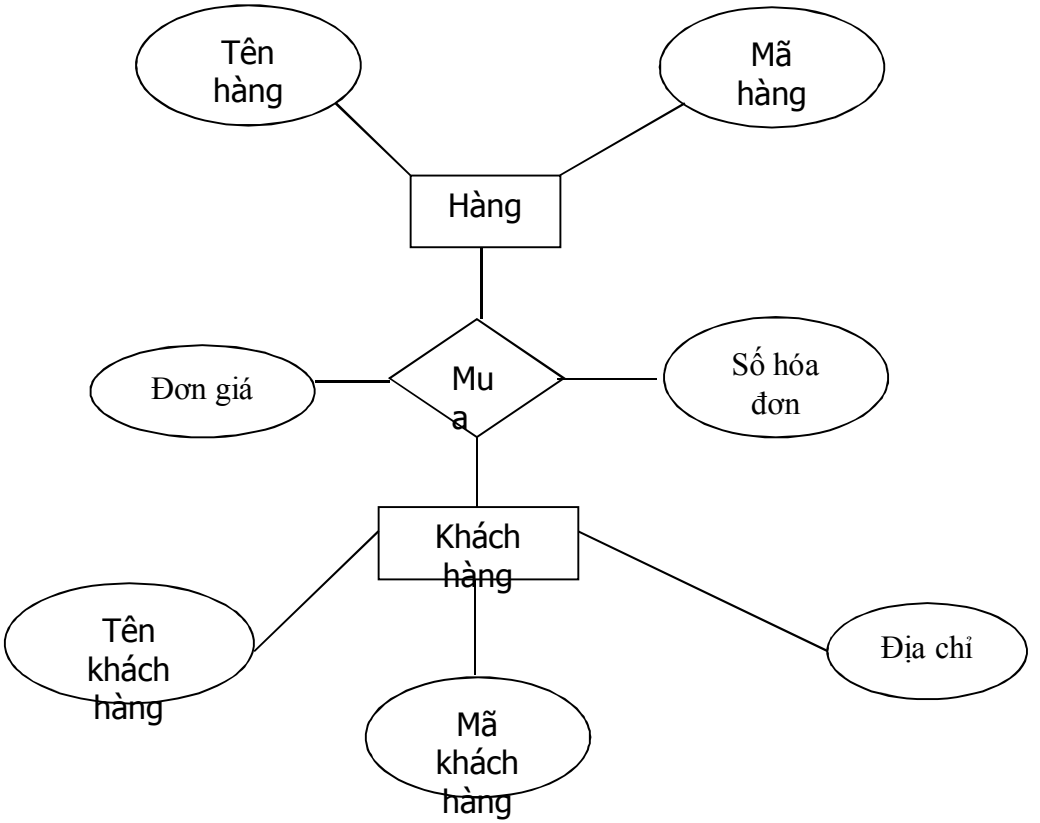


Lược đồ CSDL xây dựng theo hướng phân tích thiết kế

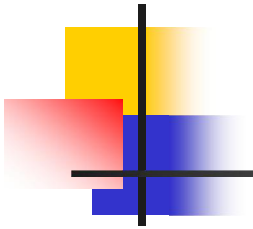
1.2 Một số khái niệm trong CSDL

- Ví dụ: Từ việc đặc tả các yêu cầu của các đối tượng khách hàng trong việc mua hàng, ta có mô hình quan hệ thực thể giữa hai thực thể: Khách hàng – Hàng như sau: Khách hàng *mua* Các mặt Hàng, mỗi lần mua thể hiện qua một *Số hoá đơn*.

1.2 Một số khái niệm trong CSDL



Hình 1.2. Mô hình thực thể quan hệ giữa Hàng và Khách hàng



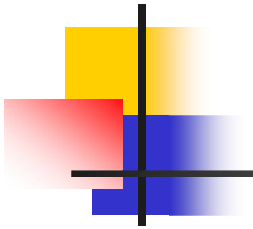
- KH(MaKH, HoTen, DiaChi)
- HD(SoHD, NgayLap, MaKH)
- CTHD(SoHD,MaHang, SoLuong)
- Hang(MaHang, TenHang, DonGia, MaLoai)
- LoaiHang(MaLoai, TenLoai)

1.2 Một số khái niệm trong CSDL

- ***Các ngôn ngữ trong DBMS:***
  - Ngôn ngữ định nghĩa dữ liệu (DDL)
  - Ngôn ngữ thao tác dữ liệu (DML)
  - Ngôn ngữ hỏi (QL).

Giới thiệu về SQL

- * SQL là viết tắt của Structured Query Language - Ngôn ngữ truy vấn cấu trúc.
  * SQL cho phép bạn truy cập vào CSDL.
  * SQL là một chuẩn ngôn ngữ của ANSI.
  * SQL có thể thực thi các câu truy vấn trên CSDL.
  * SQL có thể lấy dữ liệu từ CSDL.
  * SQL có thể chèn dữ liệu mới vào CSDL.
  * SQL có thể xoá dữ liệu trong CSDL.
  * SQL có thể sửa đổi dữ liệu hiện có trong CSDL.



Giới thiệu về SQL

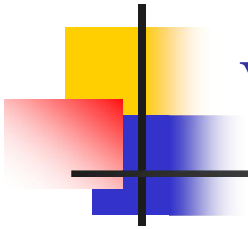
- SQL là một chuẩn của ANSI (American National Standards Institute - Viện tiêu chuẩn quốc gia Hoa kỳ) về truy xuất các hệ thống CSDL. Các câu lệnh SQL được sử dụng để truy xuất và cập nhật dữ liệu trong một CSDL.
- SQL hoạt động với hầu hết các chương trình CSDL như MS Access, DB2, Informix, MS SQL Server, Oracle, Sybase v.v...

1.2 Một số khái niệm trong CSDL

- ***DDL(Data Definition Language):*** là ngôn ngữ máy tính để định nghĩa lược đồ CSDL logic.

  Cỏc lệnh DDL quan trọng nhất của SQL là:

  - * CREATE TABLE - tạo ra một bảng mới.
    * ALTER TABLE - thay đổi cấu trỳc của bảng.
    * DROP TABLE - xoỏ một bảng.
    * CREATE INDEX - tạo chỉ mục (khoỏ để tỡm kiếm - search key).
    * DROP INDEX - xoỏ chỉ mục đó được tạo.



Ví dụ

- Lệnh **Create** sau sẽ tạo ra một table tên ***Employees***

```
CREATE TABLE Employees(
    EmpID   int NOT NULL,
    Name    varchar(30) NOT NULL,
    Salary  numeric(10),
    Contact  varchar(40) NOT NULL
    )
```

Ví dụ:

- Lệnh **Alter:**

  ALTER TABLE *Employees*

  ADD *email* varchar(40) NULL

- Lệnh **Drop** sau đây sẽ hoàn toàn xóa table khỏi database nghĩa là cả định nghĩa của table và data bên trong table đều biến mất (khác với lệnh Delete chỉ xóa data nhưng table vẫn tồn tại).

  DROP TABLE *Employees*

1.2 Một số khái niệm trong CSDL

- ***DML(Data Manipulation Language):*** là họ các ngôn ngữ máy tính được người dùng sử dụng để tìm kiếm, chèn, xóa và cập nhật dữ liệu trong một CSDL. Ví dụ về DML như các câu lệnh của SQL: SELECT, INSERT, UPDATE, DELETE

Ví dụ:

- **Select**

```
SELECT EmpID, Name
FROM Employees WHERE (EmpID = 10)
```

- **Insert**

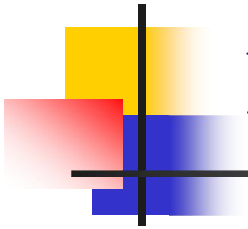
```
INSERT INTO Employees
VALUES (101, ‘Lan', ‘HN’,’lan@yahoo.com’)
```

- **Update**

```
UPDATE Employees SET  Name = ‘Minh'
WHERE  EmpID = 101
```

- **Delete**

```
DELETE FROM  Employees
WHERE EmpID = 101
```



1.2 Một số khái niệm trong CSDL

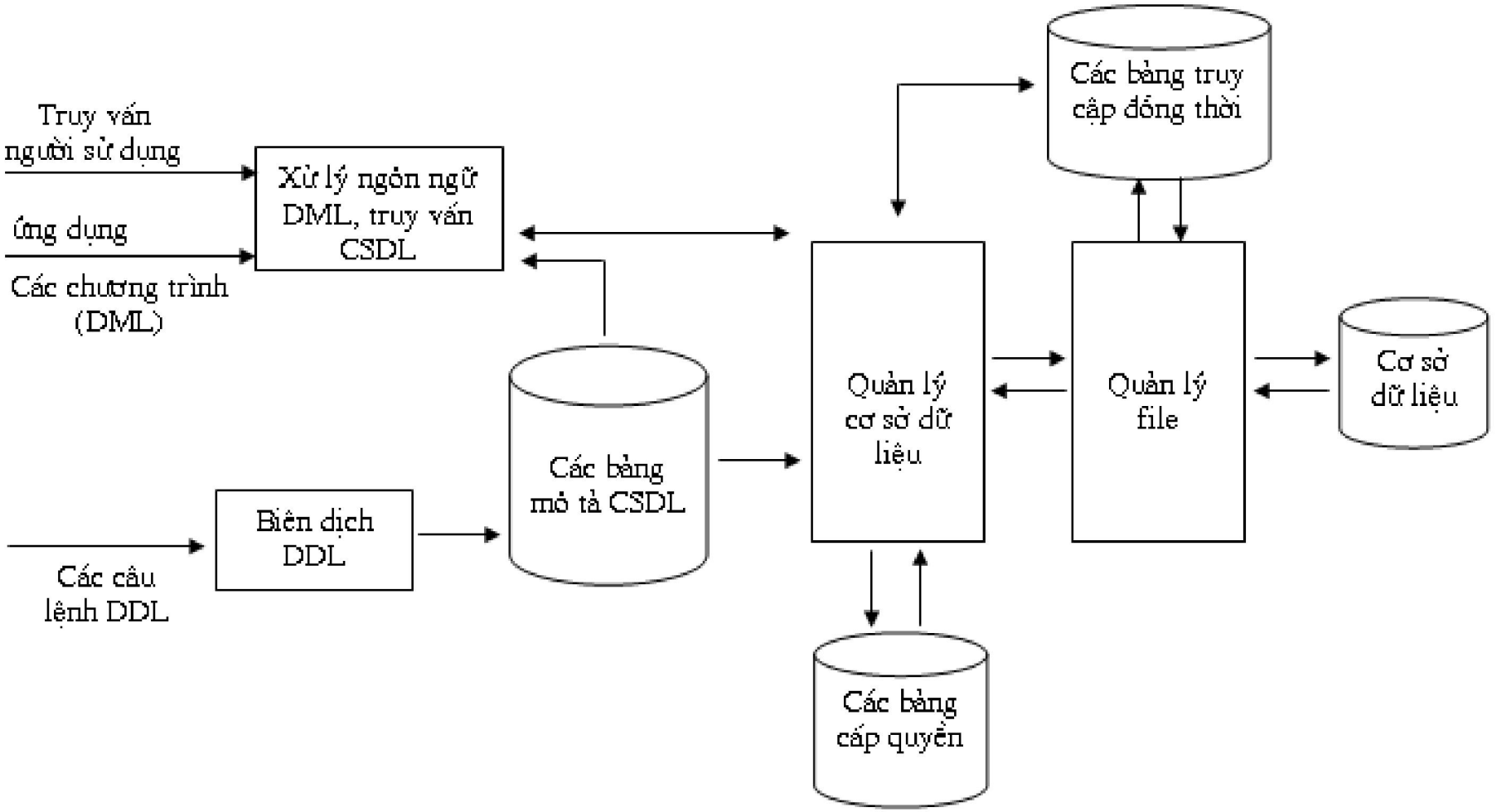
1.2.1 Các thành phần của một DBMS

1.2.2 Các mức mô tả dữ liệu

1.2.1 Các thành phần của một DBMS

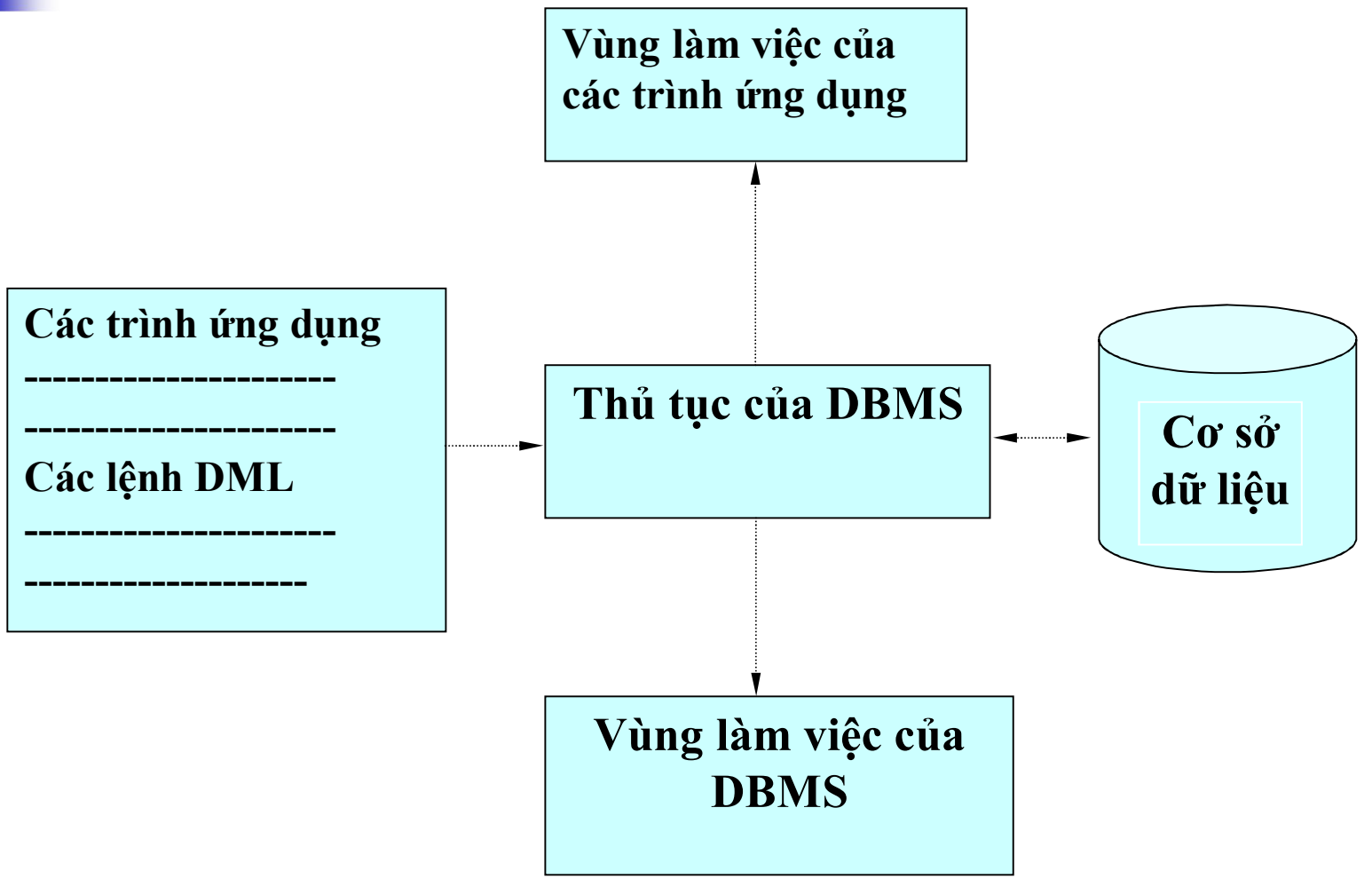
- Một DBMS thông thường bao gồm nhiều modul tương ứng với các chức năng sau:
  - Trõnh biên dịch DDL (DDL Compilation)
  - Trình biên dịch ngôn ngữ DML(DML Compiler)
  - Bộ xử lý truy vấn (Querying Language)
  - Bộ quản lý CSDL - DBMS
  - Bộ quản trị file
- Tập hợp dữ liệu hỗ trợ các modul này là:
  - Các bảng mô tả CSDL
  - Các bảng cấp quyền
  - Các bảng truy nhập đồng thời

Kiến trúc của một DBMS



Kiến trúc của DBMS

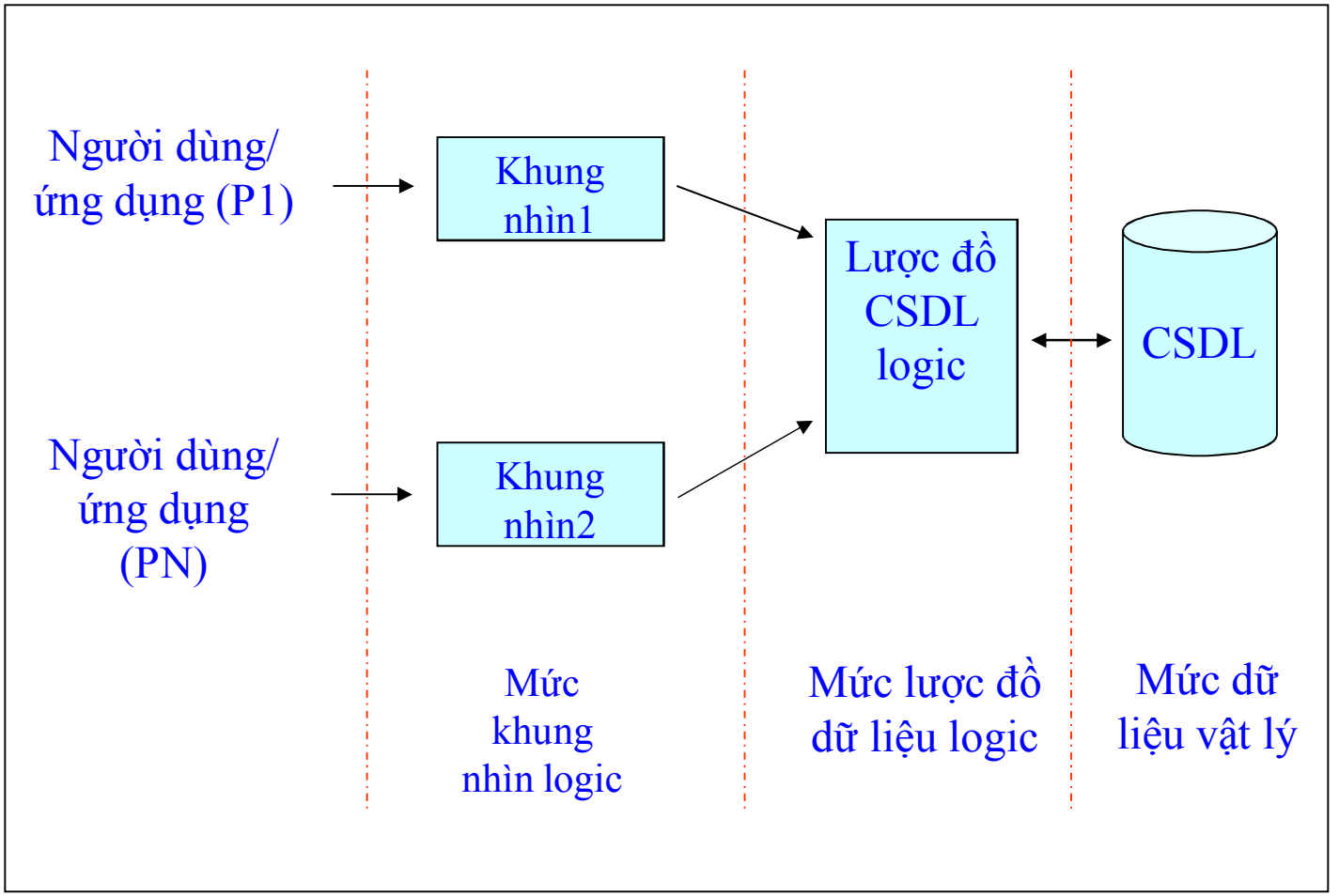
Tương tác giữa trình ứng dụng và CSDL



1.2.2 Các mức mô tả dữ liệu

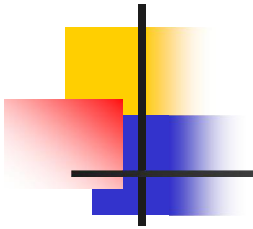
- ***Lược đồ dữ liệu vật lý***: Mức này mô tả cấu trúc lưu trữ dữ liệu trong các file trên bộ nhớ ngoài. Dữ liệu được lưu trữ dưới dạng các bản ghi và các con trỏ trỏ tới bản ghi.
- ***Lược đồ dữ liệu logic:*** ở mức này, mọi dữ liệu trong CSDL được mô tả bằng mô hình lôgíc của DBMS. Các dữ liệu và quan hệ của chúng được mô tả thông qua DDL của DBMS.
- ***Khung nhìn logic:*** phụ thuộc các yêu cầu của mô hình logic và các mục đích của ứng dụng. Khung nhìn logic mô tả một phần lược đồ CSDL logic. Sử dụng DDL để định nghĩa các khung nhìn logic, DML để thao tác trên các khung nhìn này.

1.2.2 Các mức mô tả dữ liệu



1.2.2 Các mức mô tả dữ liệu

- DBMS cho phép các mức khác nhau hỗ trợ độc lập logic và độc lập vật lý.
  - ***Độc lập dữ liệu vật lý:*** là khả năng sửa đổi lược đồ vật lý mà không phải viết lại các chương trình ứng dụng.
  - ***Độc lập dữ liệu logic:*** là khả năng sửa đổi lược đồ logic mà không phải viết lại các chương trình ứng dụng. Những thay đổi ở lược đồ logic cần thiết phải sửa đổi ở khung nhìn logic tương ứng.



Nội dung

1.1 Giới thiệu

1.2 Một số khái niệm trong CSDL

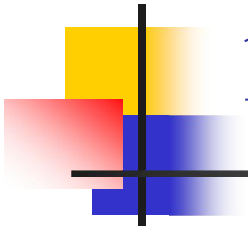
1.3 Các vấn đề an toàn trong CSDL

- 1.3.1 Các hiểm họa đối với an toàn CSDL
- 1.3.2 Các yêu cầu bảo vệ CSDL

1.4 Kiểm soát an toàn

- 1.4.1 Kiểm soát luồng
- 1.4.2 Kiểm soát suy diễn
- 1.4.3 Kiểm soát truy nhập

1.5 Thiết kế CSDL an toàn



1.3 Các vấn đề an toàn trong CSDL

1.3.1 Các hiểm họa đối với an toàn CSDL

1.3.2 Các yêu cầu bảo vệ CSDL

1.3.1 Các hiểm hoạ đối với an toàn CSDL

- ***Một hiểm hoạ*** xảy ra một số người dùng hoặc nhóm người người dùng sử dụng các kỹ thuật đặc biệt để tiếp cận nhằm khám phá, sửa đổi trái phép thông tin quan trọng trong hệ thống.
- ***Các xâm phạm*** tính an toàn CSDL bao gồm: ***đọc, sửa, xoá dữ liệu trái phép.*** Có ba loại xâm phạm:
  - Khai thác dữ liệu trái phép thông qua suy diễn thông tin được phép.
  - Sửa đổi dữ liệu trái phép.
  - Từ chối dịch vụ hợp pháp

1.3.1 Các hiểm hoạ đối với an toàn CSDL

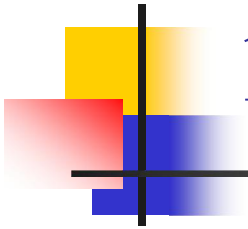
- ***Các hiểm hoạ*** an toàn: *có chủ ý* và *ngẫu nhiên*.
  - ***Các hiểm họa ngẫu nhiên:***
    - Các thảm hoạ trong thiên nhiên, chẳng hạn như động đất, hoả hoạn, lụt lội...
    - Các lỗi phần cứng hay phần mềm có thể dẫn đến việc áp dụng các chính sách an toàn không đúng.
    - Các sai phạm vô ý do con người gây ra, chẳng hạn như nhập dữ liệu đầu vào không chính xác, hay sử dụng các ứng dụng không đúng

1.3.1 Các hiểm hoạ đối với an toàn CSDL

- ***Hiểm họa cố ý:*** liên quan đến hai lớp người dùng sau:
  - ***Người dùng hợp pháp:*** là người có thể lạm dụng quyền, sử dụng vượt quá quyền hạn được phép của họ.
  - ***Người dùng truy nhập thông tin trái phép:*** có thể là những người nằm ngoài tổ chức hay bên trong tổ chức. Họ tiến hành các hành vi phá hoại phần mềm CSDL hay phần cứng của hệ thống, hoặc đọc ghi dữ liệu trái phép.

1.3.1 Các hiểm hoạ đối với an toàn CSDL

- ***Nhận xét:*** Từ những xâm phạm an toàn và các hiểm họa cố ý và vô ý có thể xảy ra, dẫn đến yêu cầu phải bảo vệ CSDL chống lại những xâm phạm đó.



1.3 Các vấn đề an toàn trong CSDL

1.3.1 Các hiểm họa đối với an toàn CSDL

1.3.2 Các yêu cầu bảo vệ CSDL

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Các yêu cầu bảo vệ CSDL bao gồm:***
  - Bảo vệ chống truy nhập trái phép
  - Bảo vệ chống suy diễn
  - Bảo vệ toàn vẹn CSDL
  - Toàn vẹn dữ liệu thao tác
  - Toàn vẹn ngữ nghĩa của dữ liệu
  - Khả năng lưu vết và kiểm tra
  - Xác thực người dùng
  - Bảo vệ dữ liệu nhạy cảm
  - Bảo vệ nhiều mức

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Bảo vệ chống truy nhập trái phép***
  - Chỉ trao quyền cho những người dùng hợp pháp.
  - Việc kiểm soát truy nhập cần tiến hành trên các đối tượng dữ liệu mức thấp hơn file: bản ghi, thuộc tính.
  - Kiểm soát truy nhập CSDL phức tạp hơn kiểm soát file.

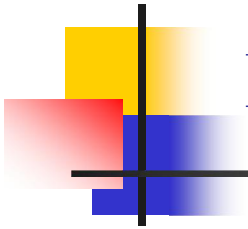
1.3.2 Các yêu cầu bảo vệ CSDL

- ***Bảo vệ chống suy diễn:***
  - Suy diễn là khả năng cú được cỏc thụng tin bớ mật từ những thụng tin khụng bớ mật.
  - Suy diễn trong CSDL quan hệ bình thường.
  - Suy diễn trong cỏc CSDL thống kờ (Quan trọng)

(Vớ dụ)

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Bảo vệ toàn vẹn CSDL***
  - Bảo vệ CSDL khỏi những người dùng không hợp pháp, tránh sửa đổi nội dung dữ liệu trái phép.
  - DBMS đưa ra các kiểm soát bằng các ràng buộc DL, thủ tục sao lưu, phục hồi và các thủ tục an toàn đặc biệt.
  - Hệ thống phục hồi của DBMS sử dụng các ***file nhật ký***, ghi lại tất cả các phép toán được thực hiện trên dữ liệu: đọc, ghi, xóa, chèn.



Một số phương phỏp đảm bảo toàn vẹn dữ liệu

- Kiểu dữ liệu (Data Type)
- Không có định nghĩa Null (Not Null Definitions)
- Định nghĩa mặc định (Default Definitions)
- Các thuộc tính định danh (Identity Properties)
- Các ràng buộc (Constraints)
- Các quy tắc (Rules)
- Triggers
- Các chỉ mục (Indexes)

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Toàn vẹn dữ liệu thao tác***
  - Yêu cầu này đảm bảo tính tương thích logic của dữ liệu khi có nhiều giao tác thực hiện đồng thời.
  - Một giao tác là một loạt các hoạt động xảy ra được xem như một đơn vị công việc (unit of work) nghĩa là hoặc thành công toàn bộ hoặc không làm gì cả (all or nothing).
  - Sử dụng kỹ thuật khúa để đảm bảo truy nhập đồng thời vào cựng một thực thể dữ liệu.

Ví dụ về giao tác

- Chúng ta muốn chuyển một số tiền $1000 từ account1 sang account2 như vậy công việc này cần làm các bước sau:

1. Trừ $1000 từ account1
2. Cộng $1000 vào account2

Tuy nhiên việc chuyển tiền trên phải được thực hiện dưới dạng một transaction nghĩa là giao tác chỉ được xem là hoàn tất (commited) khi cả hai bước trên đều thực hiện thành công. Nếu vì một lý do nào đó ta chỉ có thể thực hiện được bước 1 (chẳng hạn như vừa xong bước 1 thì điện cúp hay máy bị treo) thì xem như giao tác không hoàn tất và cần phải được phục hồi lại trạng thái ban đầu (roll back).

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Toàn vẹn ngữ nghĩa của dữ liệu:***
  - Yêu cầu này đảm bảo tính tương thích logic của các dữ liệu bị thay đổi, bằng cách kiểm tra các giá trị dữ liệu có nằm trong khoảng cho phép hay không (đó là các ràng buộc toàn vẹn).
  - ***Ràng buộc*** (Constraints) là những thuộc tớnh mà ta ỏp đặt lờn một bảng hay một cột để trỏnh việc lưu dữ liệu khụng chớnh xỏc vào CSDL

Một số ràng buộc dữ liệu

- ***Ràng buộc khóa chính (Primary Key Constraint)***

  Một bảng thường cú một hay nhiều cột cú giỏ trị mang tớnh duy nhất để xỏc định một hàng bất kỳ trong bảng. Ta thường gọi là khúa chớnh (Primary Key) ví dụ:

```
CREATE TABLE Table1
        (Col1   INT   PRIMARY KEY,
         Col2   VARCHAR(30)
        )
```

Một số ràng buộc dữ liệu

- ***Ràng buộc khóa ngoại (Foreign Key Constraint)***

Khúa ngoại (Foreign Key) là một cột hay một sự kết hợp của nhiều cột được sử dụng để ỏp đặt mối liờn kết dữ liệu giữa hai bảng. Khúa ngoại của một bảng sẽ giữ giỏ trị của khúa chớnh của một bảng khỏc để kiểm soỏt DL của bảng này.

```
CREATE TABLE SinhVien
    (MaSV  INT   PRIMARY  KEY, HoTen Varchar(30),
     MaLop varchar(10) REFERENCES  Lop(MaLop)
    )
```

Một số ràng buộc dữ liệu

- ***Ràng buộc kiểm tra (Check Constraint)***

Ràng buộc kiểm tra dựng để giới hạn hay kiểm soỏt giỏ trị được phộp insert vào một cột. Ràng buộc kiểm tra dựa trờn một biểu thức logic để kiểm tra xem một giỏ trị cú hợp lệ khụng.

```
CREATE TABLE Table1
        (Col1   INT   PRIMARY  KEY,
         Col2   INT
         CONSTRAINT  limit_amount  CHECK
        (Col2   BETWEEN   0   AND  1000),
         Col3 VARCHAR(30)
         )
```

1.3.2 Các yêu cầu bảo vệ CSDL

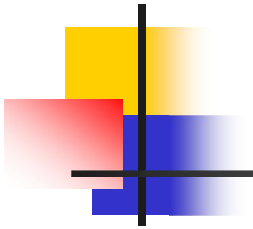
- ***Khả năng lưu vết và kiểm tra***
  - Là khả năng ghi lại mọi truy nhập tới dữ liệu (với các phép toán *read* và *write)*. Khả năng kiểm tra và lưu vết đảm bảo tính toàn vẹn dữ liệu vật lý và trợ giúp cho việc phân tích dãy truy nhập vào CSDL

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Xác thực người dùng***
  - Yêu cầu này thực sự cần thiết để xác định tính duy nhất của người dùng. Định danh người dùng làm cơ sở cho việc trao quyền. Người dùng được phép truy nhập dữ liệu, khi hệ thống xác định được người dùng này là hợp pháp.
- ***Quản lý và bảo vệ dữ liệu nhạy cảm***
  - Dữ liệu nhạy cảm là dữ liệu không được để công khai
  - Dữ liệu nhạy cảm chỉ được cấp cho người dùng hợp pháp

1.3.2 Các yêu cầu bảo vệ CSDL

- ***Bảo vệ nhiều mức***
  - Bao gồm một tập các yêu cầu bảo vệ: dữ liệu được phân loại thành nhiều mức nhạy cảm.
  - Mục đích của bảo vệ nhiều mức là phân loại các mục thông tin khác nhau, đồng thời phân quyền cho các mức truy nhập khác nhau vào các mục riêng biệt. Một yêu cầu nữa đối với bảo vệ nhiều mức là khả năng gán mức cho các thông tin.



Nội dung

1.1 Giới thiệu

1.2 Một số khái niệm trong CSDL

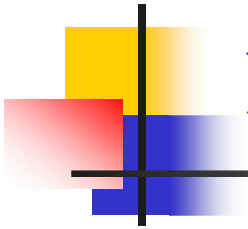
1.3 Các vấn đề an toàn trong CSDL

- 1.3.1 Các hiểm họa đối với an toàn CSDL
- 1.3.2 Các yêu cầu bảo vệ CSDL

1.4 Kiểm soát an toàn

- 1.4.1 Kiểm soát luồng
- 1.4.2 Kiểm soát suy diễn
- 1.4.3 Kiểm soát truy nhập

1.5 Thiết kế CSDL an toàn



1.4 Kiểm soát an toàn

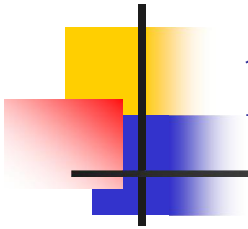
1.4.1 Kiểm soát luồng

1.4.2 Kiểm soát suy diễn

1.4.3 Kiểm soát truy nhập

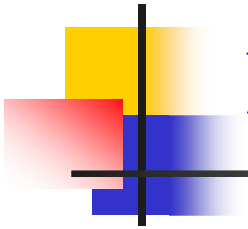
1.4.1 Kiểm soát luồng

- ***Một luồng*** giữa đối tượng X và đối tượng Y xuất hiện khi có một lệnh đọc (*read*) giá trị từ X và ghi (*write*) giá trị vào Y
- ***Kiểm soát luồng*** *là kiểm tra xem thông tin trong một số đối tượng có đi vào các đối tượng có mức bảo vệ thấp hơn hay không*
- Nếu điều này xảy ra thì rõ ràng thông tin ở đối tượng có mức nhạy cảm cao đã bị tiết lộ xuống đối tượng có mức thấp hơn.



1.4.1 Kiểm soát luồng

- ***Nhận xét:*** Kiểm soát luồng thông tin trong CSDL thương áp dụng với các CSDL nhiều mức.



1.4 Kiểm soát an toàn

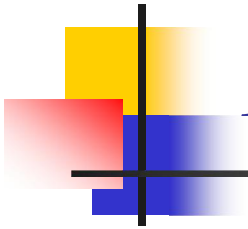
1.4.1 Kiểm soát luồng

1.4.2 Kiểm soát suy diễn

1.4.3 Kiểm soát truy nhập

1.4.2 Kiểm soát suy diễn

- ***Kiểm soát suy diễn:*** nhằm mục đích bảo vệ dữ liệu không bị khám phá gián tiếp.
- Mục dữ liệu Y là bí mật, X công khai. Suy diễn có nghĩa là: X =>Y với Y = f(X).
- Hai loại suy diễn:
  - ***Suy diễn dữ liệu bình thường***
  - ***Suy diễn dữ liệu thống kê***



1.4.2 Kiểm soát suy diễn

- ***Suy diễn dữ liệu thông thường:***

  Các kênh suy diễn chính gồm:

  - ***Truy nhập gián tiếp***
  - ***Dữ liệu tương quan***
  - ***Dữ liệu vắng mặt***

1.4.2 Kiểm soát suy diễn

- ***Truy nhập gián tiếp*:** xảy ra khi người dùng không hợp pháp khám phá ra bộ dữ liệu Y thông qua các câu hỏi truy vấn được phép trên dữ liệu X, cùng với các điều kiện trên Y.

  SELECT X FROM R WHERE Y = value

  SELECT Name FROM NhanSu WHERE Luong=5000

1.4.2 Kiểm soát suy diễn

- ***Dữ liệu tương quan:*** là một kênh suy diễn tiêu biểu, xảy ra khi dữ liệu có thể nhìn thấy được X và dữ liệu không thể nhìn thấy được Y kết nối với nhau về mặt ngữ nghĩa. Kết quả là có thể khám phá được thông tin về Y nhờ đọc X.

  Ví dụ: Bảng **Nhân sự**

SUM(Lương, (ChucVu='Nhanvien', Lương>1000)) = 1500

COUNT(Lương, (ChucVu='Nhanvien', Lương>1000)) = 1

=> Tìm ra lương của người này

1.4.2 Kiểm soát suy diễn

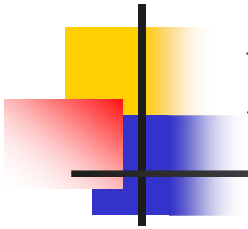
- ***Dữ liệu vắng mặt:*** người dùng chỉ biết được sự tồn tại của một tập giá trị X, còn một số ô trống. Từ đó, người dùng có thể tìm được tên của đối tượng, mặc dù họ không được phép truy nhập vào thông tin chứa trong đó.

	Nhắc nhở	Cảnh cáo	Đuổi học
M	1⊗	3	1⊗
F	2	1⊗	3
Tổng cộng	3	4	4

Đếm các số lượng sinh viên theo giới tính và hình thức kỷ luật

1.4.2 Kiểm soát suy diễn

- ***Suy diễn thống kê:*** là một khía cạnh khác của suy diễn dữ liệu. Trong các CSDL thống kê, người dùng không được phép truy nhập vào các dữ liệu đơn lẻ, chỉ được phép truy nhập vào dữ liệu thông qua các hàm thống kê. Tuy nhiên với một người có kinh nghiệm, anh ta vẫn có thể khám phá được dữ liệu thông qua các thống kê đó.
- Có hai loại kiểm soát đối với các tấn công thống kê:
  - **Xáo trộn dữ liệu**
  - **Kiểm soát câu truy vấn**



1.4 Kiểm soát an toàn

1.4.1 Kiểm soát luồng

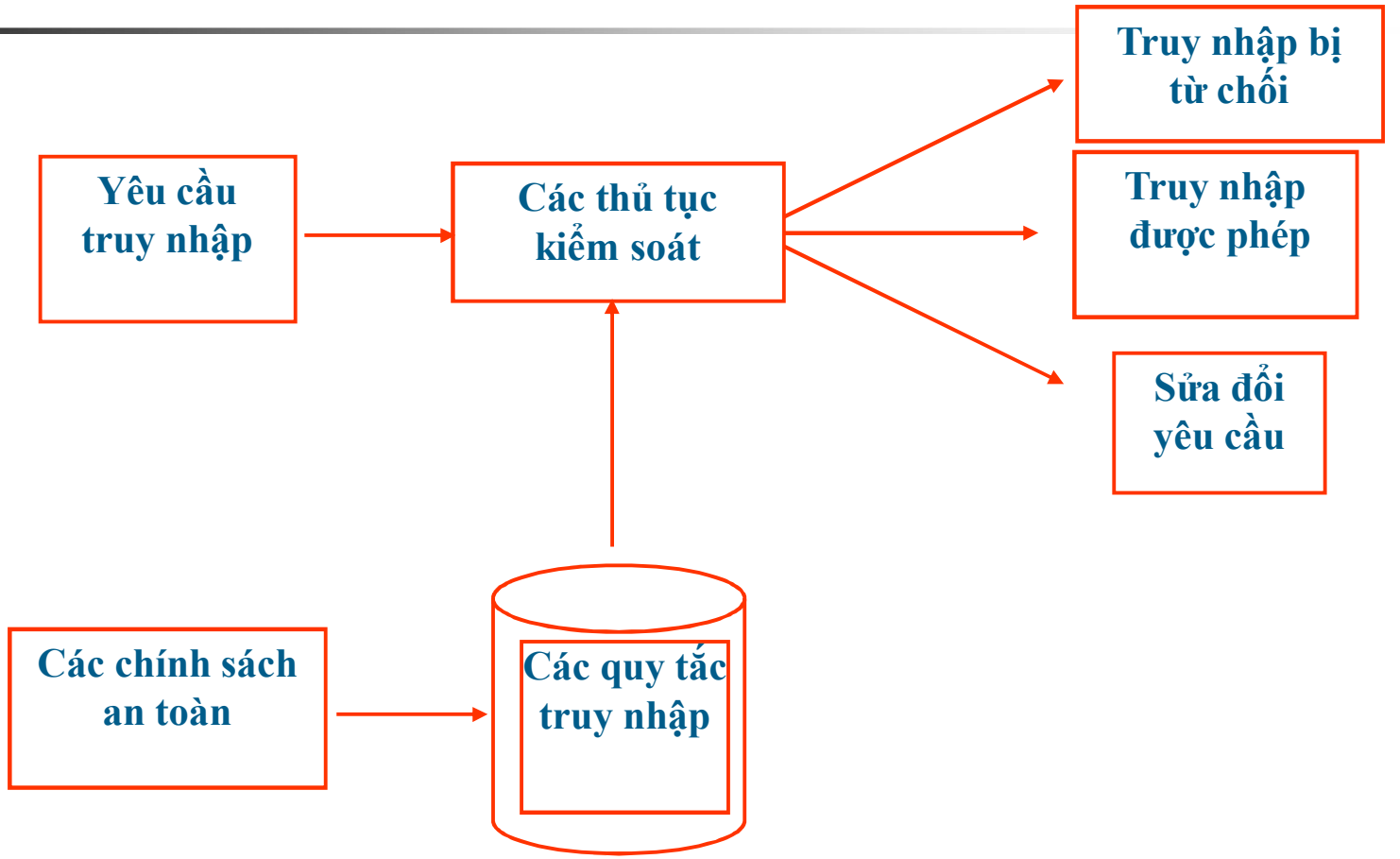
1.4.2 Kiểm soát suy diễn

1.4.3 Kiểm soát truy nhập

1.4.3 Kiểm soát truy nhập

- ***Kiểm soát truy nhập:*** trong các hệ thống thông tin là đảm bảo mọi truy nhập trực tiếp vào các đối tượng của hệ thống phải tuân theo các quy tắc trong chính sách bảo vệ.
- Một hệ thống kiểm soát truy nhập bao gồm các ***chủ thể*** (người dùng, tiến trình) truy nhập vào ***đối tượng*** (dữ liệu, chương trình) thông qua các phép toán *read, write, run*.

1.4.3 Kiểm soát truy nhập



Hệ thống kiểm soát truy nhập

1.4.3 Kiểm soát truy nhập

- ***Câu hỏi:***

"Mỗi chủ thể được phép truy nhập bao nhiêu thông tin"?

1.4.3 Kiểm soát truy nhập

- ***Chính sách đặc quyền tối thiểu*:** còn được gọi là chính sách (***need-to-know***). Theo chính sách này, các chủ thể của hệ thống chỉ được sử dụng một lượng thông tin tối thiểu cần cho hoạt động của họ.
  Nhược điểm:
  - Việc ước tính lượng thông tin tối thiểu này là rất khó.
  - Những hạn chế truy nhập thông tin có thể vô ích đối với các chủ thể vô hại.

1.4.3 Kiểm soát truy nhập

***Chính sách đặc quyền tối thiểu*:**

- Mỗi đối tượng an toàn -object sẽ được gắn một compartment (chứa nội dung của nó).
- Mỗi chủ thể -subject được phép truy nhập vào một đối tượng nếu ***nhu cầu tối thiểu (NTK)*** của anh ta phải vượt quá nội dung của đối tượng đó
- Ví dụ:

Compartment ={ medical data, financial data, private data}

Comp(O) = {medical data, financial data}

Chủ thể S được truy nhập vào O nếu Comp(O) $\subseteq$NTK(S)

1.4.3 Kiểm soát truy nhập

- ***Mở rộng Chính sách đặc quyền tối thiểu thành kiểm soát luồng thông tin:***
  - ***Read:*** S được quyền đọc O nếu Comp(O) $\subseteq$ NTK(S)
  - ***Write***: S được quyền ghi O nếu Comp(O) $\supseteq$ NTK(S)
  - ***Ví dụ:***

Compartments = {medical data(M), financial data(F), private data(P) }

Comp(O) = {M, F}

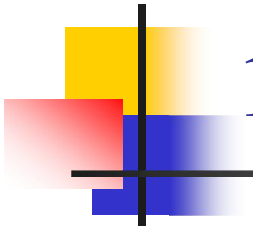
NTK(S1) = {F}, NTK(S2) = P, NTK(S3)= {P,M}

NTK (S4) = {F, M, P}

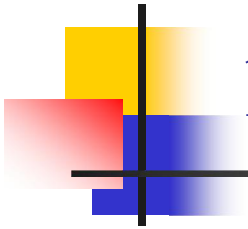
- ***Hỏi S1, S2, S3, S4 được quyền truy nhập gì vào O?***

1.4.3 Kiểm soát truy nhập

- ***Chính sách đặc quyền tối đa:***
  - Dựa vào nguyên tắc ***"khả năng sẵn sàng tối đa"*** của dữ liệu, để có thể chia sẻ dữ liệu đến mức tối đa.
  - Chính sách này phù hợp với các môi trường như: trường đại học, trung tâm nghiên cứu, là những nơi cần trao đổi dữ liệu, không cần bảo vệ nghiêm ngặt.



1.4.3 Kiểm soát truy nhập



1.4.3 Kiểm soát truy nhập

1.4.3.1 Hệ thống khép kín và hệ thống mở

1.4.3.2 Các chính sách quản lý quyền

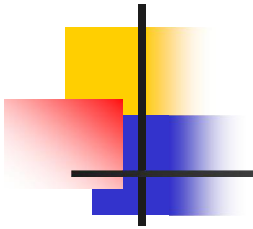
1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

1.4.3.4 Các quy tắc trao quyền

1.4.3.5 Cơ chế an toàn (trong thủ tục kiểm soát truy nhập)

1.4.3.1 Hệ thống khép kín và hệ thống mở

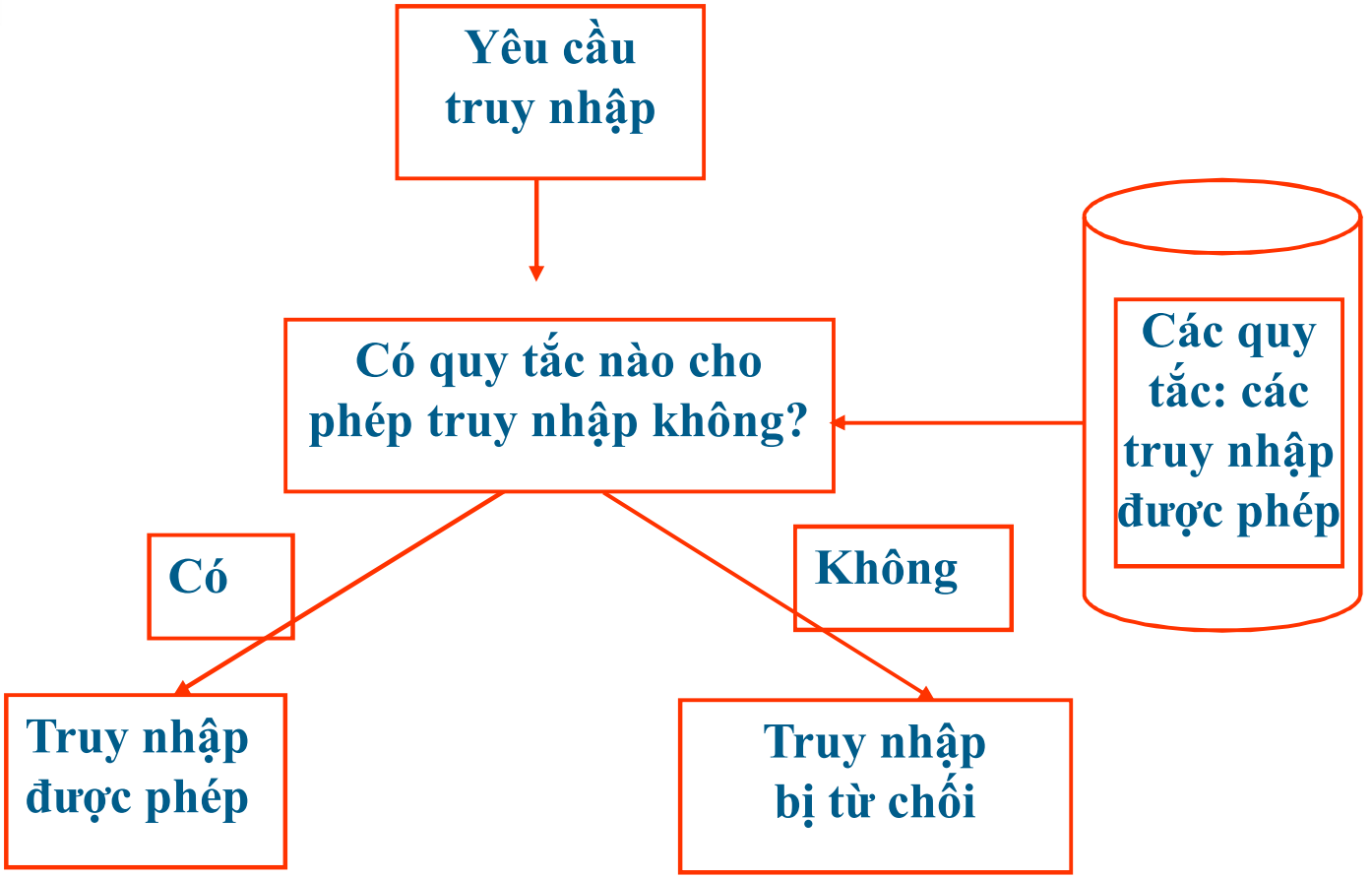
- ***Hệ thống khép kín*** là hệ thống chỉ cho phép các truy nhập hợp pháp, còn ***hệ thống mở*** là hệ thống cho phép các truy nhập không bị cấm.



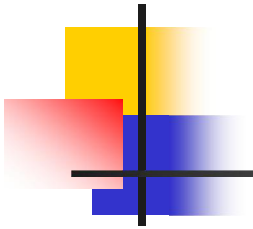
Hệ thống khép kín

- Chỉ rõ mỗi chủ thể có những quyền truy nhập nào trên các đối tượng của hệ thống nhờ các quy tắc trao quyền.
- Tuân theo chính sách đặc quyền tối thiểu.
- Quản lý quyền tốt.
- Mức độ bảo vệ tốt.

Hệ thống khép kín



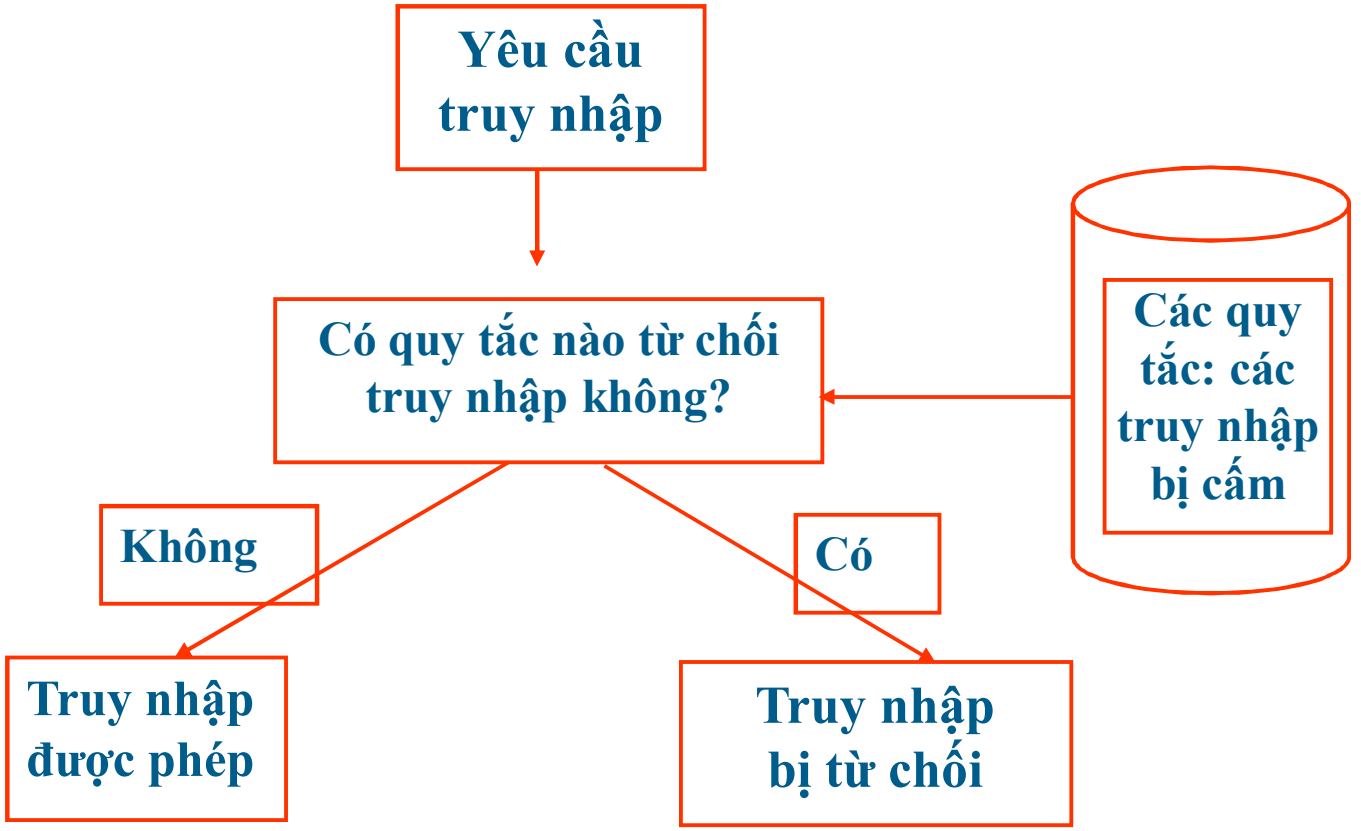
Kiểm soát truy nhập trong các hệ thống khép kín



Hệ thống mở

- Chỉ rõ mỗi chủ thể có các đặc quyền nào không được phép trên các đối tượng của hệ thống. Đây là những quyền mà chủ thể bị từ chối, thông qua cơ chế kiểm soát (user được phép làm những việc mà hệ thống không cấm=>mở).
- Tuân theo chính sách đặc quyền tối đa.
- Mức độ bảo vệ không tốt bằng hệ thống khép kín: người dùng có thể lợi dụng để trao các đặc quyền cho user khác một cách trái phép.
- Quản lý quyền không tốt.

Hệ thống mở



Kiểm soát truy nhập trong các hệ thống mở

1.4.3 Kiểm soát truy nhập

1.4.3.1 Hệ thống khép kín và hệ thống mở

1.4.3.2 Các chính sách quản lý quyền

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

1.4.3.4 Các quy tắc trao quyền

1.4.3.5 Cơ chế an toàn (trong thủ tục kiểm soát truy nhập)

1.4.3.2 Các chính sách quản lý quyền

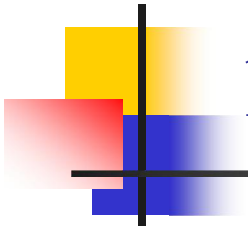
- ***Chính sách quản lý quyền:*** nhằm xác định "ai" có thể trao quyền hoặc huỷ bỏ quyền truy nhập:
  - ***Chính sách quản lý quyền tập trung:*** là chính sách trong đó việc trao quyền và hủy bỏ quyền chỉ do một người quản trị trung tâm thực hiện.
  - ***Chính sách quản lý quyền phi tập trung:*** là chính sách quản lý quyền mà việc trao và hủy bỏ quyền do nhiều người, và mỗi người có một quyền quản lý tự trị không ảnh hưởng bởi những người khác. Ví dụ: hệ thống phân tán.

1.4.3.2 Các chính sách quản lý quyền

- Một số chính sách quản lý quyền trung gian:
  - ***Chính sách trao quyền phi tập trung phân cấp*:** trong đó, người trao quyền trung tâm có trách nhiệm chia nhỏ trách nhiệm quản trị CSDL cho những người quản trị cấp dưới (Ví dụ SQL Server).
  - ***Chính sách dựa vào quyền sở hữu*:** người tạo ra đối tượng (ví dụ: table, View) là người sở hữu đối tượng đó, sẽ là người có quyền trao hoặc huỷ bỏ quyền truy nhập tới đối tượng này, đôi khi cần có sự đồng ý của người quản trị trung tâm. Ví dụ: hệ quản trị Oracle.

1.4.3.2 Các chính sách quản lý quyền

- Một số chính sách quản lý quyền trung gian:
  - ***Chính sách trao quyền hợp tác***: Việc trao các quyền đặc biệt trên một số tài nguyên nào đó không thể chỉ do một người quyết định mà phải có sự đồng ý của một nhóm người dùng cụ thể (Chính sách này giống với kiểu tập trung nhưng khác là người quản trị cao nhất là một nhóm người).



1.4.3 Kiểm soát truy nhập

1.4.3.1 Hệ thống khép kín và hệ thống mở

1.4.3.2 Các chính sách quản lý quyền

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

1.4.3.4 Các quy tắc trao quyền

1.4.3.5 Cơ chế an toàn (trong thủ tục kiểm soát truy nhập)

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

- ***Hệ thống nhiều mức:*** là hệ thống an toàn mà các chủ thể và các đối tượng trong đó đều được phân cấp mức độ nhạy cảm.
- Bao gồm hai chính sách truy nhập:
  - ***Kiểm soát truy nhập bắt buộc (MAC – Mandatory Access Controls):*** hạn chế truy nhập của các chủ thể vào các đối tượng bằng cách sử dụng các ***nhãn an toàn.***
  - ***Kiểm soát truy nhập tuỳ ý (DAC – Discretionary Access Controls):*** cho phép lan truyền các quyền truy nhập từ chủ thể này đến chủ thể khác.

Chính sách KS truy nhập bắt buộc (MAC)

- ***MAC*** được áp dụng cho các thông tin có yêu cầu bảo vệ nghiêm ngặt, trong các môi trường mà ở đó dữ liệu hệ thống và người dùng đều được phân loại rõ ràng.
- Mọi chủ thể và đối tượng trong hệ thống đều được gắn với một ***lớp an toàn.***
- ***Lớp an toàn = (Mức nhạy cảm, Vùng ứng dụng)***
  - Thành phần: *Mức nhạy cảm* là thành phần phân cấp.
  - Thành phần: *Vùng ứng dụng* là thành phần không phân cấp

Kiểm soát MAC trong quân sự

- ***Lớp an toàn = (Mức nhạy cảm, Vùng ứng dụng)***
  - ***Mức nhạy cảm***:

    0 = Không phân loại (U - Unclassified)

    1 = Mật (C – Confidential)

    2 = Tuyệt mật (S – Secret)

    3 = Tối mật (TS – Top Secret)
  - ***Vùng ứng dụng:*** Hạt nhân – Nato – Cơ quan tình báo

Mũi tên thể hiện chiều dữ liệu được phép di chuyển

Chính sách KS truy nhập bắt buộc (MAC)

- ***Ví dụ trong thương mại:***
- ***Lớp an toàn = (Mức nhạy cảm, Vùng ứng dụng)***
  - ***Mức nhạy cảm:***

    0 = Không phân loại (U - Unclassified)

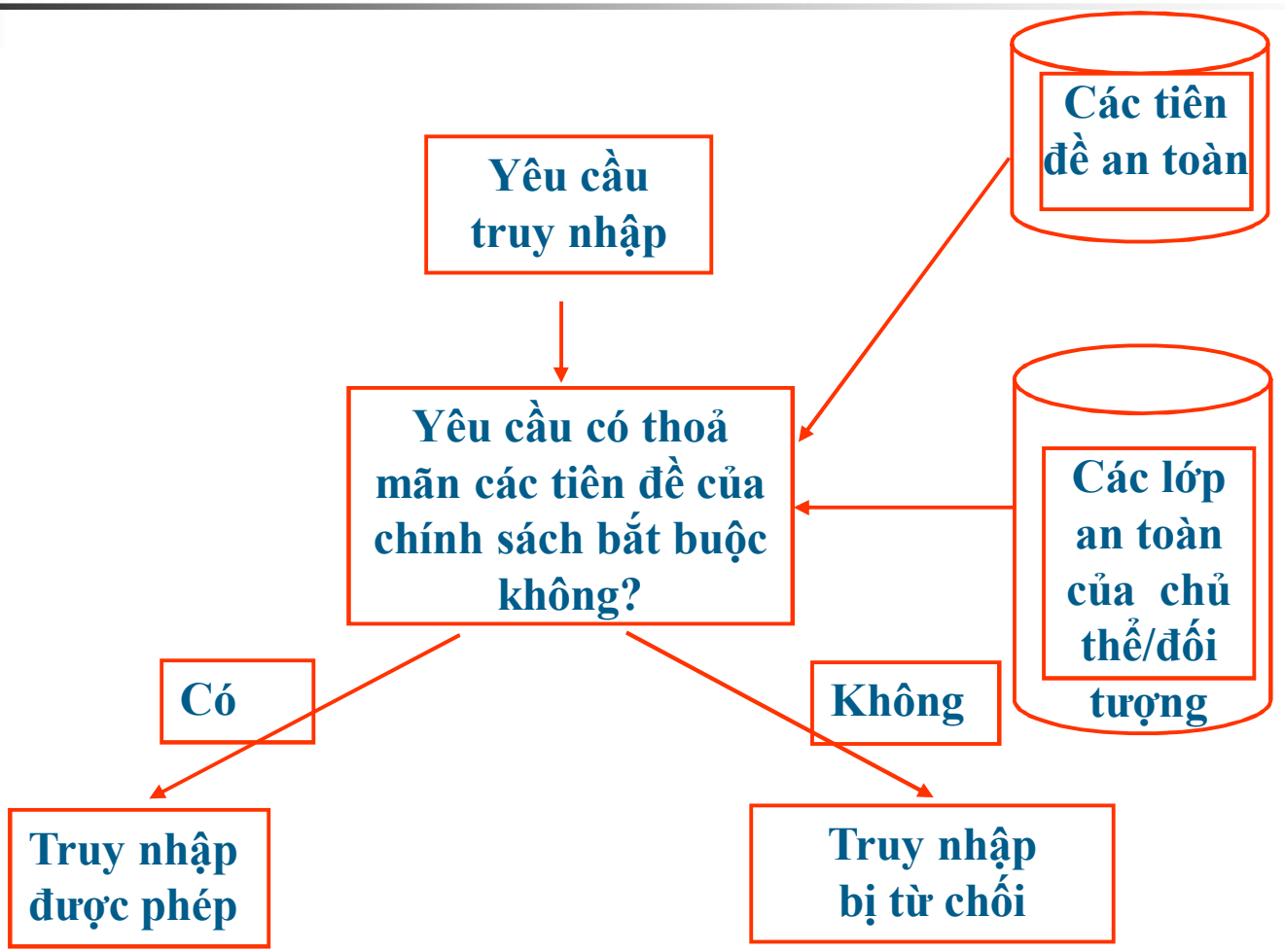
    1 = Nhạy cảm (S – Sensitive)

    2 = Rất nhạy cảm (HS – High Sensitive)
  - ***Vùng ứng dụng:*** Phòng làm việc – Vùng, miền.

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.

Chính sách KS truy nhập bắt buộc (MAC)



Chính sách KS truy nhập bắt buộc (MAC)

- ***Ưu điểm***: kiểm soát an toàn cao
- ***Nhược điểm:***
  - Phức tạp
  - Làm giảm tính linh hoạt của hệ thống (ảnh hưởng đến hiệu năng).
  - Người dùng không được phép thay đổi quyền (phải có sự đồng ý của nhà quản trị trung tâm).

Mô hình kiểm soát truy nhập tùy ý (DAC)

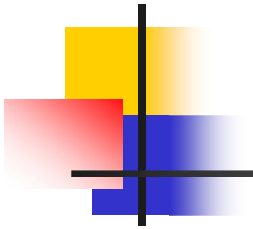
- Được định nghĩa trên một tập
  - Các đối tượng an toàn (security objects)
  - Các chủ thể an toàn (security subjects)
  - Và các đặc quyền truy nhập (access prilvilege)
- Đặc điểm:
  - Người dùng có thể bảo vệ dữ liệu mà họ sở hữu
  - Người chủ sở hữu (owner) có thể gán quyền truy nhập (read, write, execute…) tới các user khác.
  - Việc gán và thu hồi quyền truy nhập là "tùy ý" do những người dùng này.
- Thuận lợi:
  - 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: SQL Server, Oracle,…

Mô hình kiểm soát truy nhập tùy ý (DAC)

- Giả sử O là một tập các đối tượng an toàn, S là một tập các chủ thể an toàn, T là một tập các đặc quyền truy nhập.
- Để biểu diễn các quy tắc truy nhập dựa vào nội dung, giả sử P là tập các tân từ.
- Khi đó, bộ <*o,s,t,p*> (o in O, s in S, t in T, p in P) là một *quy tắc truy nhập*.
- f là hàm xác định xem quyền *f(o,s,t,p)* có hợp lệ hay không?

$$f: O \times S \times T \times P \rightarrow \{True, False\}$$

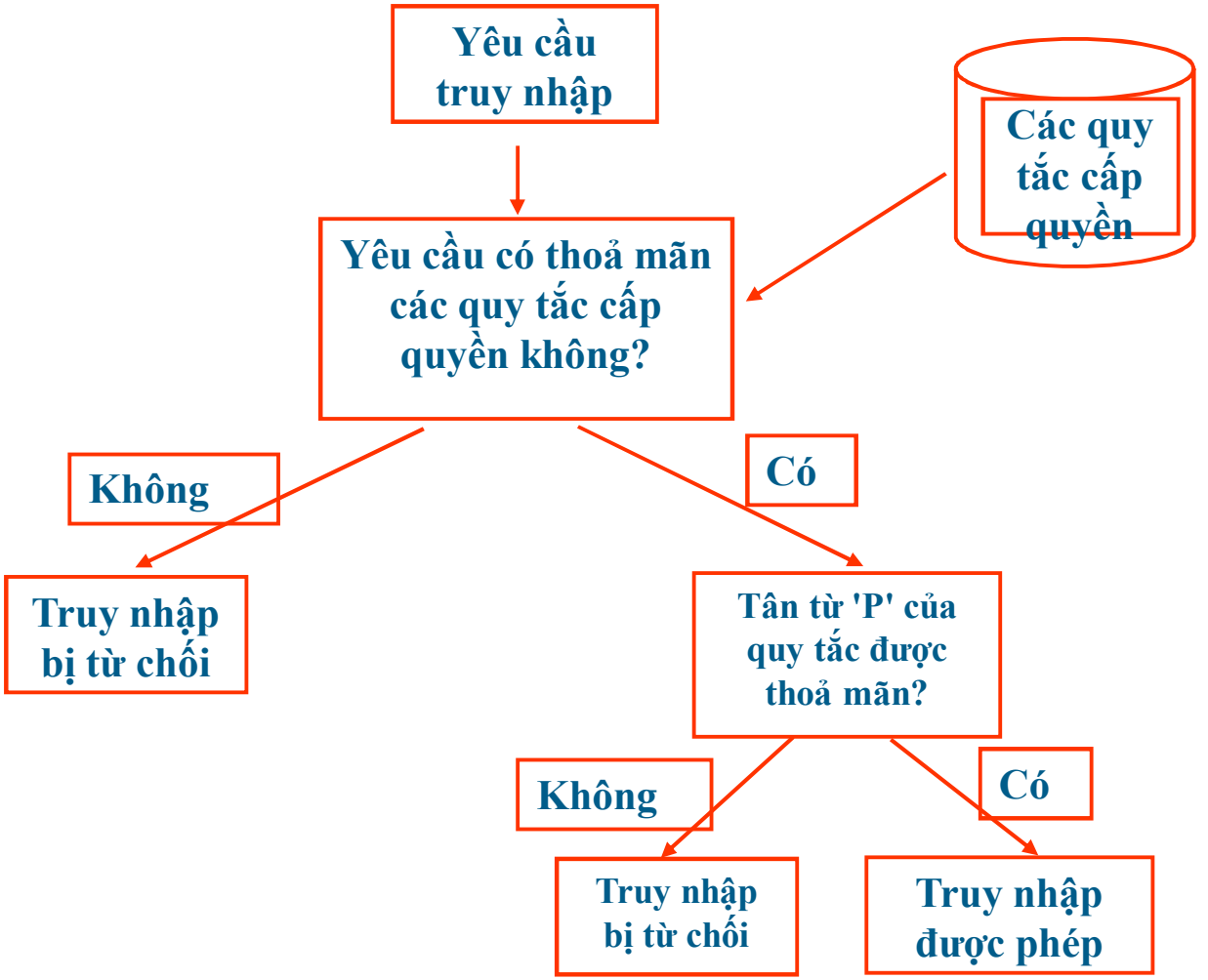
- Nếu *f(o,s,t,p) = True* thì chủ thể s có quyền truy nhập t vào đối tượng o, trong phạm vi được định nghĩa bởi tân từ p
- *Nguyên tắc ủy quyền*: một chủ thể s_i có quyền truy nhập (o,t,p) thì được phép ủy quyền đó cho một chủ thể s_j khác (i!=j).



Chính sách KS truy nhập tuỳ ý (DAC)

- ***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).
- 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.

Chính sách KS truy nhập tuỳ ý (DAC)



Chính sách KS truy nhập tuỳ ý (DAC)

- ***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. Điều này ngầm định rằng, việc phân quyền kiểm soát dựa vào ***quyền sở hữu*** (*kiểu chính sách cấp quyền dựa vào quyền sở hữu*)

Chính sách KS truy nhập tuỳ ý (DAC)

- ***Trao quyền:*** *V*iệc 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, anh ta có thể thu hồi quyền đã truyền cho người khác.

Chính sách KS truy nhập tuỳ ý (DAC)

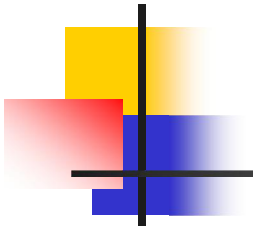
- ***Nhận xét:*** DAC cho phép đọc thông tin từ một đối tượng và chuyển đến một đối tượng khác (đối tượng này có thể được ghi bởi một chủ thể)

  => Tạo ra sơ hở để cho tấn công con ngựa thành Toroa sao chép thông tin từ một đối tượng đến một đối tượng khác.

- ***Ví dụ***: UserA là chủ sở hữu tableA, anh ta tạo ra khung nhìn ViewA từ bảng này (sao chép thông tin). UserA không cho phép UserB được đọc tableA nhưng lại vô tình gán quyền Write cho UserB trên ViewA.

  Như vậy, UserB có thể đọc thông tin tableA dù không được quyền trên bảng này.

Ví dụ về Trojan Horse



R: UserA, W: UserA

UserA

File A

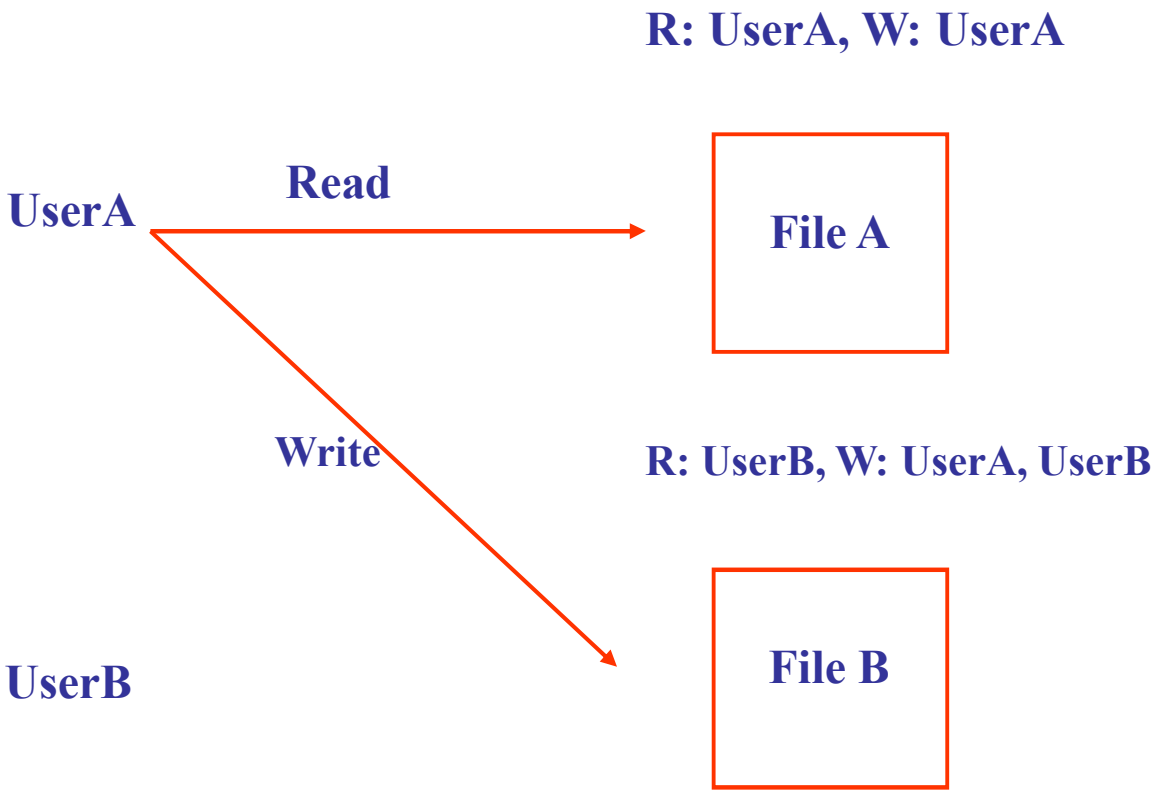
R: UserB, W: UserA, UserB

UserB

File B

UserB không thể đọc file A

Ví dụ về Trojan Horse



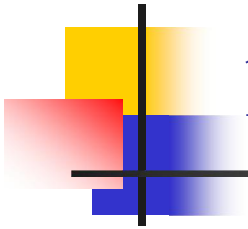
UserB có thể đọc nội dung
file A (được copy sang file B)

Chính sách KS truy nhập tuỳ ý (DAC)

- ***Ưu điểm:***
  - Dễ dàng thực hiện, hệ thống linh hoạt
- ***Nhược điểm:***
  - Khó quản lý việc gán/thu hồi quyền
  - Dễ bị lộ thông tin
  - Kiểm soát an toàn không tốt.

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

- So sánh sự khác nhau giữa MAC và DAC?



1.4.3 Kiểm soát truy nhập

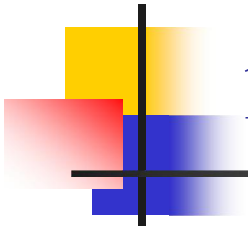
1.4.3.1 Hệ thống khép kín và hệ thống mở

1.4.3.2 Các chính sách quản lý quyền

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

1.4.3.4 Các quy tắc trao quyền

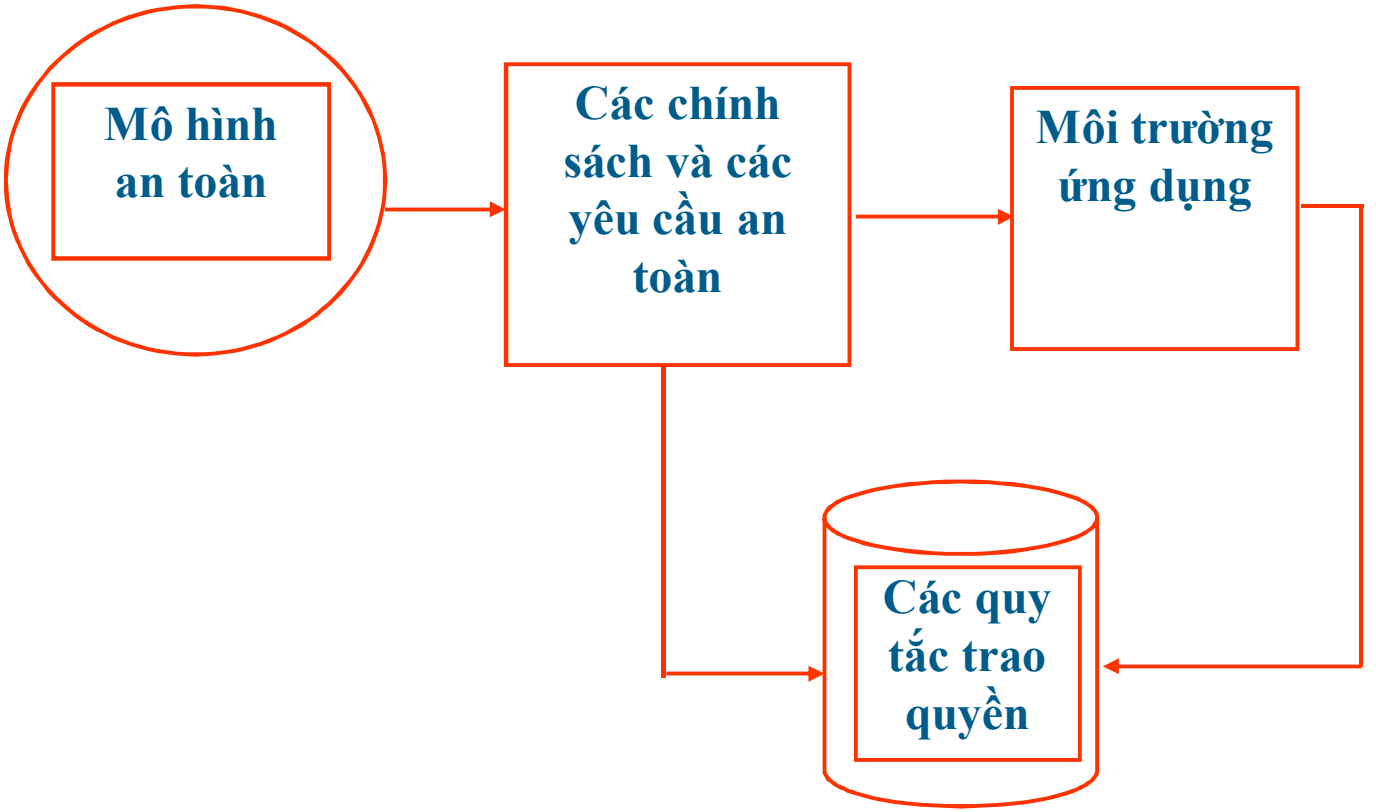
1.4.3.5 Cơ chế an toàn (trong thủ tục kiểm soát truy nhập)



1.4.3.4 Các quy tắc trao quyền

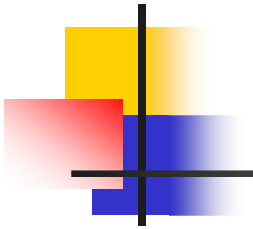
- Các yêu cầu và chính sách an toàn do tổ chức đưa ra, người trao quyền có nhiệm vụ chuyển các yêu cầu này thành các quy tắc trao quyền.
- ***Quy tắc trao quyền*** biểu diễn đúng với môi trường phần mềm/phần cứng bảo vệ.

1.4.3.4 Các quy tắc trao quyền



Thiết kế các quy tắc trao quyền

Các mô hình an toàn (Security Model)



- Mô hình an toàn (security model) là một khái niệm trừu tượng để biểu diễn một chính sách an toàn (security policy) của một tổ chức
- ***Đối tượng an toàn (Security Object):*** là một thực thể thụ động chứa thông tin như: CSDL, một bảng, khung nhìn, một bản ghi, hoặc có thể là một segment, một printer,…
- ***Chủ thể an toàn (Security Subject):***
  - Là một thực thể chủ động, là một user hoặc một tiến trình hoạt động dưới điều khiển của một user.
  - Các chủ thể an toàn có thể thay đổi trạng thái CSDL và di chuyển thông tin giữa các đối tượng và chủ thể khác nhau

1.4.3.4 Các quy tắc trao quyền

- ***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.
- Hai loại mô hình an toàn là:
  - ***Mô hình an toàn tùy ý*** *(Discretionary security models)*
  - ***Mô hình an toàn bắt buộc*** *(Mandatory security models).*

1.4.3.4 Các quy tắc trao quyền

- ***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),…

Mô hình an toàn trong quân sự

- Các đối tượng và chủ thể an toàn được gán cho các nhãn an toàn

  Đối tượng: Confidential<classified<secret<Top_secret

  Chủ thể: Public<Confidential< High_Security
- Ký hiệu mức an toàn của một đối tượng O là class(O), của một chủ thể S là clear(S)
- Một chủ thể an toàn được truy nhập vào một đối tượng an toàn nếu mức an toàn của anh ta ít nhất cũng bằng mức an toàn của đối tượng này:

  Clear(S)>= Class(O)

1.4.3.4 Các quy tắc trao quyền

- ***Ví dụ mô hình an toàn ma trận truy nhập:*** trong đó tập các ***quy tắc trao quyền*** của một hệ thống được thể hiện như một ma trận A, gọi là *ma trận truy nhập* hay *ma trận cấp quyền:*
  - Các hàng thể hiện các chủ thể của hệ thống
  - Các cột thể hiện các đối tượng của hệ thống.
  - Một ô A[i, j] sẽ thể hiện chủ thể si được phép truy nhập tới đối tượng Oj với các quyền gì.

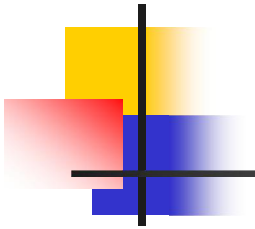
Ma trận truy nhập

- Ví dụ: Ma trận quyền với ***kiểm soát phụ thuộc tên***

	Đ?i tư?ng		
Ch? th?	**File F1**	**File F2**	**File F3**
Ngư?i dùng 1	R,W	EXEC	EXEC
Ngư?i dùng 2	-	-	CR, DEL
Chương trình P1	R,W	R	-

Ma trận truy nhập

- Một ***quy tắc trao quyền*** được thể hiện qua một bộ bốn *(s, o , t, p).*
- Với:
  - *s = chủ thể*
  - *o = đối tượng*
  - *t = kiểu quyền truy nhập*
  - *p = tân từ.*



Ma trận truy nhập

- Một số dạng kiểm soát trong ma trận truy nhập:
  - ***Kiểm soát phụ thuộc tên (Name)***
  - ***Kiểm soát dựa vào nội dung dữ liệu (Data)***
  - ***Kiểm soát dựa vào thời gian (Time)***
  - ***Kiểm soát dựa vào ngữ cảnh (Context)***
  - ***Kiểm soát dựa vào lược sử (History)*:**

Ma trận truy nhập

- ***Một số dạng kiểm soát trong ma trận truy nhập:***
  - ***Kiểm soát phụ thuộc tên (Name)***
  - ***Kiểm soát dựa vào nội dung dữ liệu (Data):*** là kiểm soát dựa vào giá trị của dữ liệu được truy nhập. Ví dụ, một chủ thể có thể được cấp quyền đọc bảng EMPLOYEE chỉ với các bản ghi công nhân có trường salary<=100.
  - ***Kiểm soát dựa vào thời gian (Time)*:** là các điều kiện ràng buộc về thời gian của truy nhập. Ví dụ: một chủ thể chỉ có thể đọc bảng EMPLOYEE trong khoảng thời gian từ 8h sáng đến 5h chiều.

Ma trận truy nhập

- ***Kiểm soát dựa vào ngữ cảnh (Context)***: là các điều kiện ràng buộc về các kết nối dữ liệu truy nhập. Ví dụ, một chủ thể có thể được quyền đọc tên và lương của các công nhân nhưng không thể đọc được cả hai trường cùng lúc.
- ***Kiểm soát dựa vào lược sử (History)*:** là các điều kiện ràng buộc phụ thuộc vào các truy nhập được thực hiện trước đó. Ví dụ, một chủ thể có thể có quyền đọc lương của các công nhân nếu trước đó anh ta không đọc trường tên của bảng EMPLOYEE.

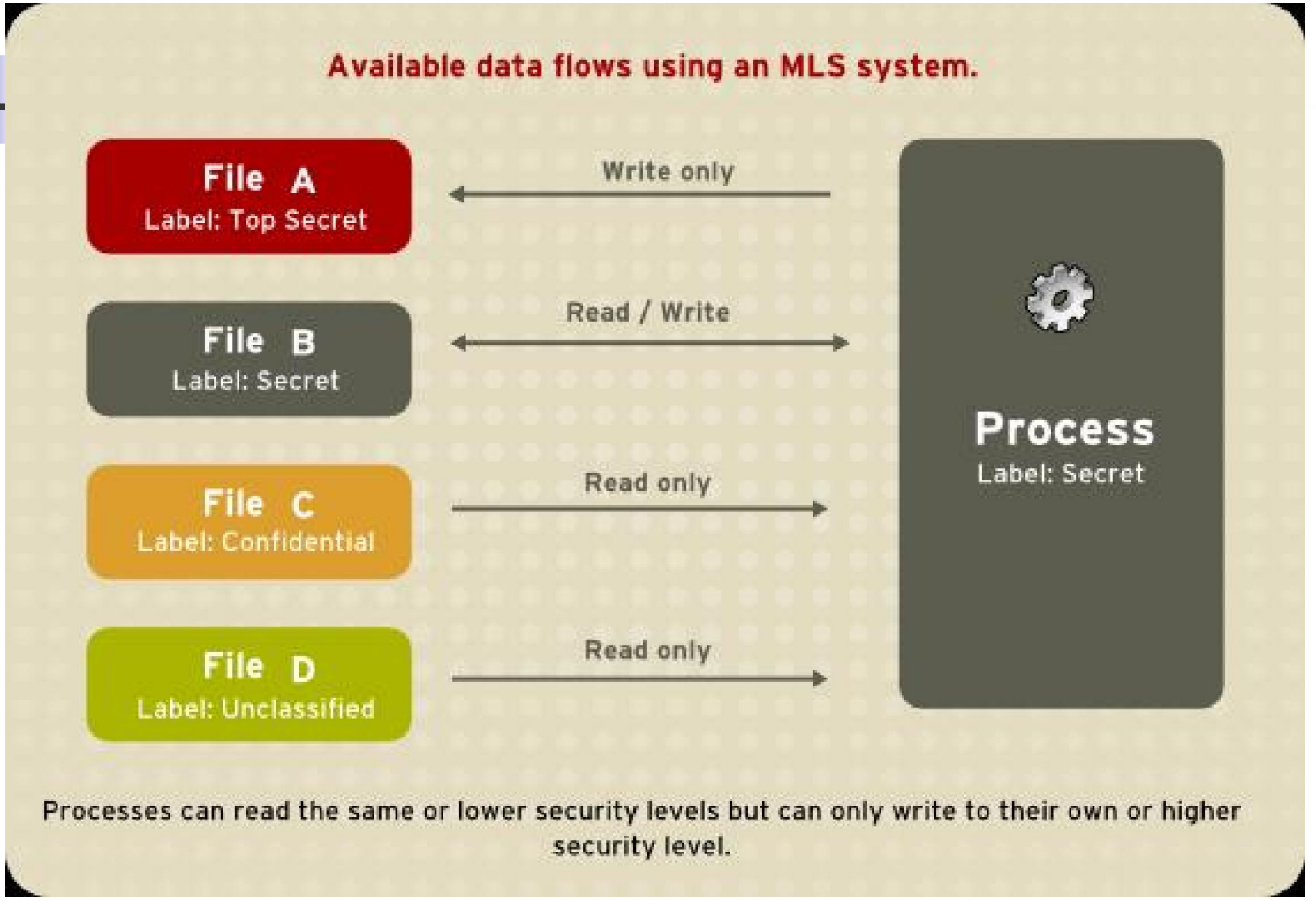
Mô hình Bell- LaPadula (BLP):

- ***Mục tiêu:*** đảm bảo tính bí mật
- ***Thuộc tính an toàn đơn giản:***
  - Một chủ thể S được phép truy nhập đọc đến một đối tượng O chỉ khi Clear (S)>=class(O)
- ***Thuộc tính *:***
  - Một chủ thể S được phép truy nhập ghi lên một đối tượng O chỉ khi Clear (S) <= class(O)
- Hai thuộc tính này đảm bảo rằng không có luồng thông tin trực tiếp nào từ các đối tượng mức cao xuống các đối tượng mức thấp.

Mô hình Bell- LaPadula (BLP):

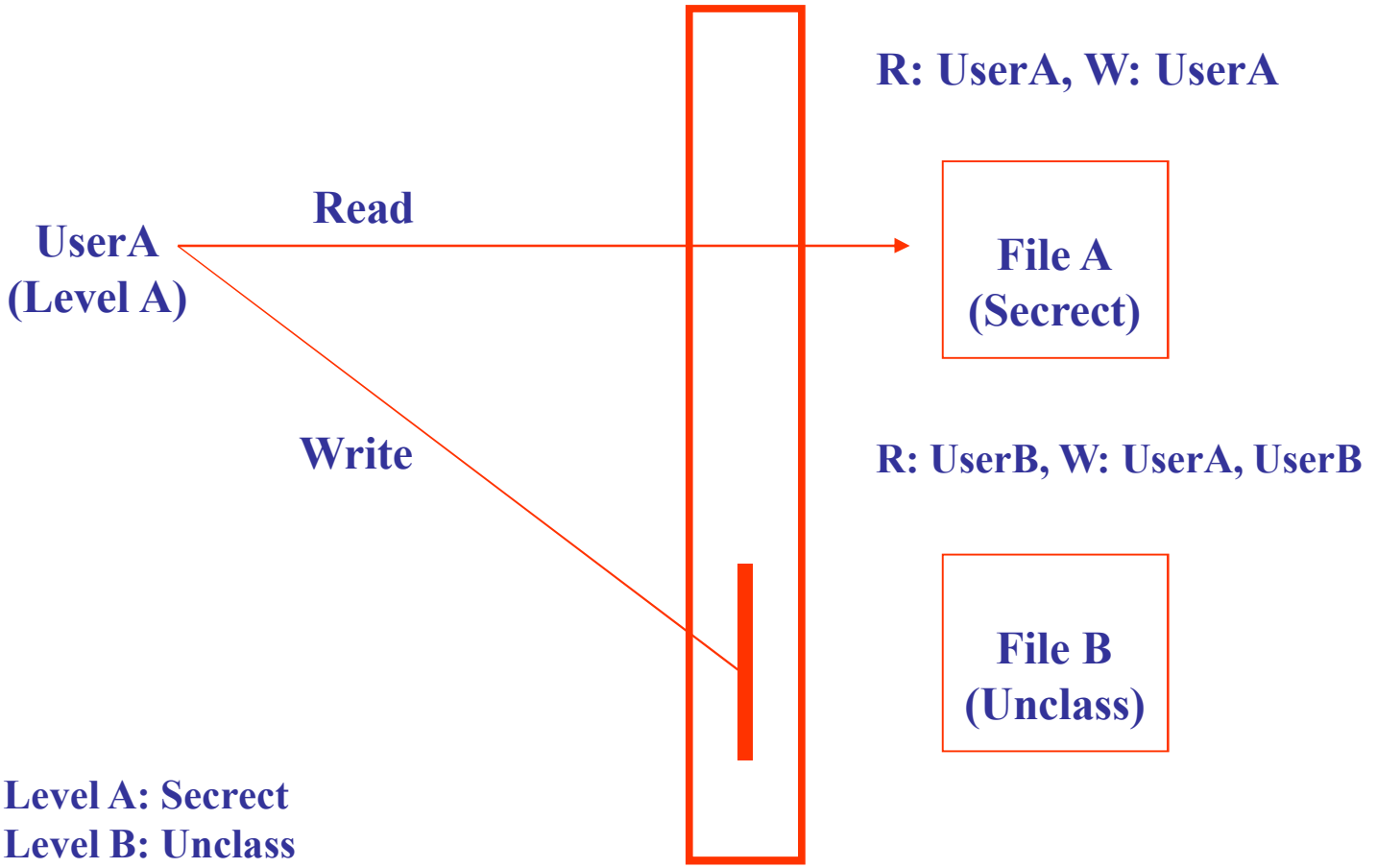
- ***Quy tắc không đọc lên: (not Read up)***
  - Các chủ thể chỉ có thể đọc thông tin có mức nhạy cảm ngang hoặc thấp hơn mức an toàn mà nó được gán().
  - Điều này giúp không bị lô thông tin cho những người dùng không được quyền truy xuất đến dữ liệu đó.
- ***Quy tắc không ghi xuống (not Write down):***
  - Chủ thể ở mức cao chỉ được ghi dữ liệu lên mức gán nhãn ngang nó hoặc cao hơn().
  - Điều này ngăn người dùng vô tình ghi dữ liệu từ mức cao xuống mức thấp làm lộ thông tin cần bảo vệ.

LAPADULA (BLP)



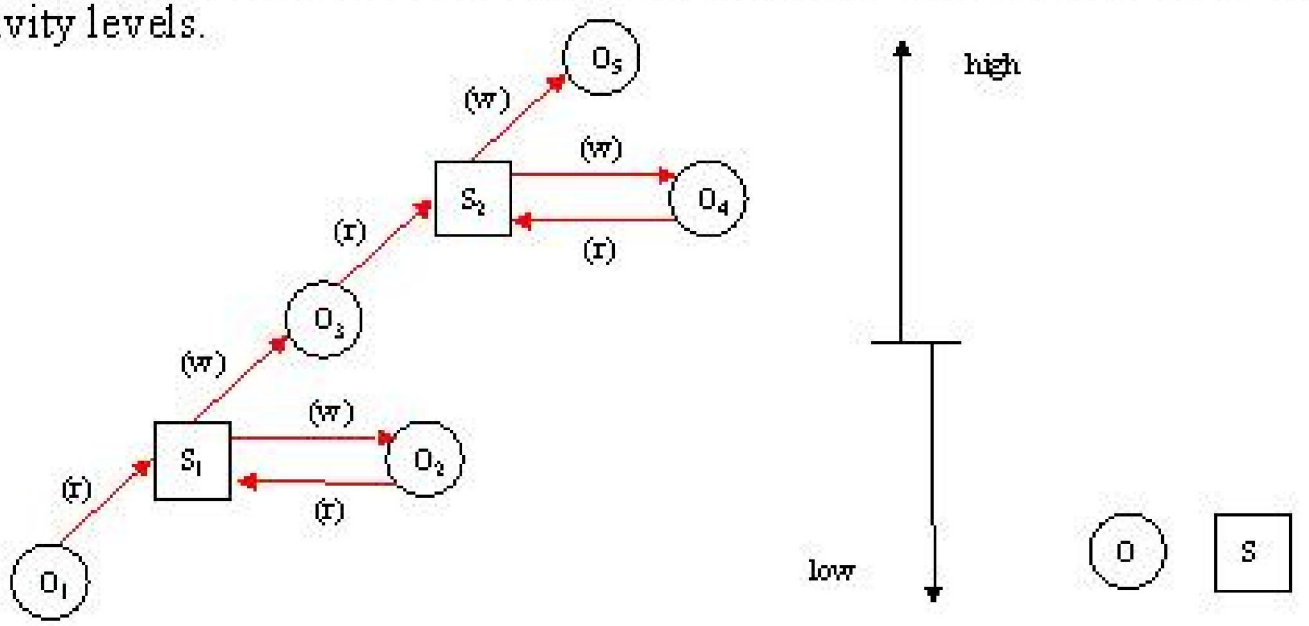
Mô hình Bell- LaPadula (BLP):

Bộ giám sát tham chiếu
(Reference Monitor)

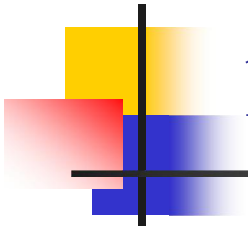


Mô hình Bell-Lapadula (BLP)

The *-property protects information from being ‚written-down' along the hierarchy of sensitivity levels.



‚Write' if no ‚read' to higher classified data!



1.4.3 Kiểm soát truy nhập

1.4.3.1 Hệ thống khép kín và hệ thống mở

1.4.3.2 Các chính sách quản lý quyền

1.4.3.3 Kiểm soát truy nhập trong hệ thống nhiều mức

1.4.3.4 Các quy tắc trao quyền

1.4.3.5 Các cơ chế an toàn

1.4.3.5 Các cơ chế an toàn

- ***Các cơ chế an toàn:*** trong một hệ thống kiểm soát truy nhập có nhiệm vụ thực hiện các chính sách an toàn và các quy tắc trao quyền. Các cơ chế an toàn bao gồm:
  - Cơ chế kiểm soát truy nhập: phát hiện và ngăn chặn các truy nhập trái phép.
  - Cơ chế kiểm toán và phát hiện xâm nhập.

1.4.3.5 Các cơ chế an toàn

- ***Các cơ chế bên ngoài:***
  - Là các biện pháp kiểm soát quản lý và kiểm soát vật lý, có thể ngăn ngừa truy nhập trái phép vào tài nguyên vật lý (phòng, thiết bị đầu cuối, các thiết bị khác)
  - Chống lại các hiểm hoạ ngẫu nhiên như chập điện, hỏa hoạn, động đất, hay ảnh hưởng của các điều kiện môi trường.
  - Cơ chế này không bảo vệ đầy đủ do các tấn công ngẫu nhiên không thể đoán trước được.

1.4.3.5 Các cơ chế an toàn

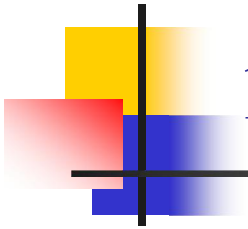
- ***Các cơ chế bên trong:***
  - Hoạt động bằng cách: xác thực danh tính của người dùng và kiểm tra tính hợp pháp của các hành động mà người dùng yêu cầu theo quyền của người dùng.
  - Gao gồm 3 cơ chế cơ bản
    - *Xác thực* (*authentication*)
    - *Các kiểm soát truy nhập* (*access controls*)
    - *Các cơ chế kiểm toán* (*auditing mechanisms*)

1.4.3.5 Các cơ chế an toàn

- ***Cơ chế xác thực***: Cơ chế này ngăn chặn người dùng trái phép sử dụng hệ thống bằng cách kiểm tra định danh người dùng.
- ***Cơ chế kiểm soát truy nhập*:** Sau khi xác thực thành công, các câu truy vấn của người dùng có được đáp lại hay không, tuỳ thuộc vào các quyền mà người dùng hiện có.

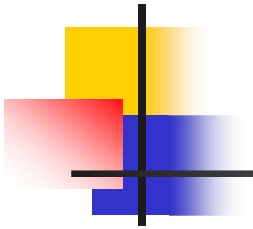
1.4.3.5 Các cơ chế an toàn

- ***Các cơ chế kiểm toán*:** giám sát việc sử dụng tài nguyên hệ thống của người dùng. Các cơ chế này bao gồm hai giai đoạn:
  - ***Giai đoạn ghi vào nhật ký*:** tất cả các câu hỏi truy nhập và câu trả lời liên quan đều được ghi lại (dù được trả lời hay bị từ chối).
  - ***Giai đoạn báo cáo:*** các báo cáo của giai đoạn trước được kiểm tra, nhằm phát hiện các xâm phạm hoặc tấn công có thể xảy ra.



1.4.3.5 Các cơ chế an toàn

- ***Nhận xét:*** Cơ chế kiểm toán của một số hệ thống còn phải làm thủ công, tốn công sức, nên cần có các công cụ kiểm toán tự động, hỗ trợ nhà quản trị.



Nội dung

1.1 Giới thiệu

1.2 Một số khái niệm trong CSDL

1.3 Các vấn đề an toàn trong CSDL

- 1.3.1 Các hiểm họa đối với an toàn CSDL
- 1.3.2 Các yêu cầu bảo vệ CSDL

1.4 Kiểm soát an toàn

- 1.4.1 Kiểm soát luồng
- 1.4.2 Kiểm soát suy diễn
- 1.4.3 Kiểm soát truy nhập

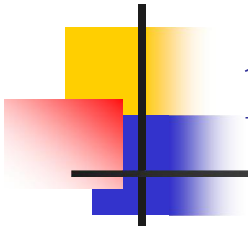
1.5 Thiết kế CSDL an toàn

1.5 Thiết kế CSDL an toàn

- ***An toàn vật lý:*** kiểm soát truy nhập vật lý vào hệ thống xử lý, bảo vệ hệ thống xử lý khỏi các thảm hoạ tự nhiên, thảm họa do con người hoặc máy móc gây ra.
- ***An toàn logic****:* chống lại các tấn công có thể xảy ra đối với hệ thống, xuất phát từ sự không trung thực, gây lỗi hoặc thiếu tinh thần trách nhiệm của những người bên trong hoặc bên ngoài hệ thống.
- Các biện pháp an toàn vật lý không bảo vệ một cách đầy đủ.

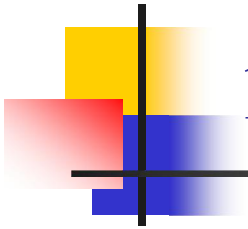
1.5 Thiết kế CSDL an toàn

- Việc thiết kế một hệ thống an toàn phụ thuộc vào:
  - Môi trường ứng dụng: vì Các đặc tính an toàn làm tăng chi phí và giảm hiệu năng, tăng độ phức tạp của hệ thống, làm giảm tính mềm dẻo, đòi hỏi nguồn nhân lực cho việc thiết kế, quản lý và duy trì, tăng yêu cầu đối với phần mềm và phần cứng.
  - Tình trạng kinh tế



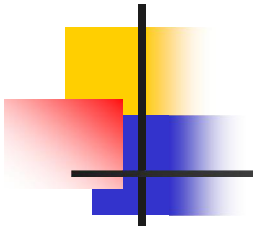
1.5.1 CSDL trong các cơ quan chính phủ

- Ví dụ: CSDL năng lượng của một xí nghiệp, điều tra dân số, xã hội, tài chính, các thông tin tội phạm.



1.5.2 Các CSDL thương mại

- Ví dụ: CSDL độ đo kinh tế, ngân hàng, dự báo và kế hoạch phát triển công ty, công nghiệp, tài chính, bảo hiểm thân thể



Tóm lại

- Khi phát triển một hệ thống an toàn, chúng ta cần quan tâm đến một số khía cạnh thiết yếu sau:
  - Các đặc điểm của môi trường cần bảo vệ.
  - Các yêu cầu bảo vệ bên ngoài và bên trong.
  - Tổ chức vật lý của các thông tin được lưu giữ.
  - Các đặc tính an toàn do hệ điều hành và phần cứng cung cấp.
  - Độ tin cậy của phần mềm và phần cứng.
  - Các khía cạnh về tổ chức, con người.