Buổi 6

MÔ HÌNH, CHÍNH SÁCH AN TOÀN TUỲ Ý

**Kiểm soát truy nhập phụ thuộc dữ liệu**

Kiểm soát truy cập cơ sở dữ liệu thường phụ thuộc vào dữ liệu. Ví dụ, một sô người dùng có thể bị giới hạn chỉ nhìn thấy các giá trị lương nhỏ hơn 30000$. Một người trưởng phòng chỉ nhìn thấy các giá trị lương của các nhân viên trong phòng mình quản lý

**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)* là 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 tại 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
* 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 chiế trực tiếp vào các bảng này
* 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;**

**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 (Vitual Private Database)

**Kiểm soát truy nhập dựa vào vai trò**

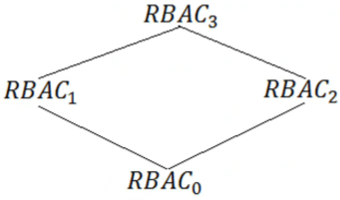
Hầu hết các DBMS đều hỗ trợ RBAC. RBAC có thể dùng kết hợp với DAC hoặc MAC hoặc được dùng độc lập

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 1 cách dễ dàng hơn

Vai trò (ROLE) là một tập các quyền

Mô hình RBAC gồm 4 mô hình con là RBAC0, RBAC1, RBAC2. RBAC3



Mô hình nền tảng RBAC0 ở dưới cùng, là yêu cầu tối thiếu 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 đến nhau

RBAC3 là mô hình tổng hợp của 3 mô hình RBAC0, RBAC1, RBAC2

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

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 lits (columns)*

Mô hình, chính sách an toàn DAC

Ưu điểm:

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 Sever, Oracle,…

Nhược điểm:

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 Troạn Horse: DAC cho phép đọc thông tin từ một đối tượng và chuyển đến một đối tượng khác