BUỔI 5

Các yêu cầu bảo vệ CSDL

* Bảo vệ nhiều mức (Multilevel Security):
* Dữ liệu được phân loại thành nhiều mức nhạy cảm
* Mục đích: 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
* 

Chương 2

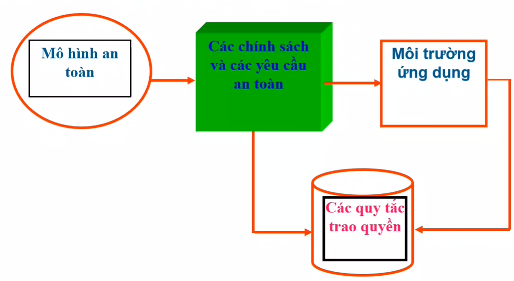
CÁC MÔ HÌNH VÀ CHÍNH SÁCH AN TOÀN

1. Các khái niệm cơ bản

Câu hỏi:

* Mô hình an toàn (Security model) là gì?
  + 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 (Security policy) là gì?
  + Là những phát biểu mức tổng quát về ATTT từ phía nhà quản lý

Quy tắc trao quyền trong tổ chức:



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)

Hai loại mô hình an toàn là:

* Mô hình an toàn tuỳ ý (Discretionary security models) - DAC
  + Mô hình ma trận truy nhập, mô hình Take - Grant
* Mô hình an toàn bắt buộc (Mandatory security models) - MAC
  + Mô hình Bell - Lapadula, mô hình Biba

2. Các mô hình và chính sách an toàn tuỳ ý (DAC)

2.1 Một số khái niệm

Mô hình an toàn tuỳ ý đã được nghiên cứu trong một thời gian dài và là nền tảng cho các hệ điều hành và các DBMS

***Chính sách tuỳ ý (DAC):*** chỉ rõ những đặc quyền mà mỗi chủ thể có thể có được trên các đối tượng và trên hệ thống (object privilege - DML, system privilege - DDL)

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

***Được định nghĩa trên một tập:***

* Các đối tượng an toàn (security objects)
* Các chủ thể an toàn (secutiry subjects)
* Và các đặc quyền truy nhập (access privilege)

(Quyền truy nhậ gồm: objects privilege, system privilege)

***Đặc điểm:***

* Người dùng có thể bảo vệ dữ iệu mà họ sở hữu…
* Người chủ sở hữu của CSDL sẽ có quyền cao nhất với CSDL đó
* Người chủ sở hữu (owner) có thể gán quyền truy nhập (read, write, excecute… ) tới các user khác
* Việc gán và thu hồi quyền truy nhập là “tuỳ ý” do những người dùng này

Case study 1 :

Linh (owner): SV(MaSV, Hoten, quequan, sdt, email)

Linh 🡪 Nam: **Grant Select, insert on SV to Nam (with grant option);** tuỳ chọn giúp quản lý việc phân quyền của user được phân quyền

Linh 🡨 Nam: **Revoke Select, Insert on SV from Nam (CASCADE constraint);** tuỳ chọn thu hồi quyền đệ quy

Linh (admin):

Linh 🡪 Nam: **Grant Drop table, create database, alter table to Nam (with admin option);**   
Linh 🡨 Nam: **Grant Drop table, create database, alter table from Nam (CASCADE constraint);**

**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, 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

**Tuỳ ý** : có nghĩa rằng người sử dụng có khả năng cấp phát hoặc thu hồi quyền truy nhập trên một số đối tượng

**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

2.2 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

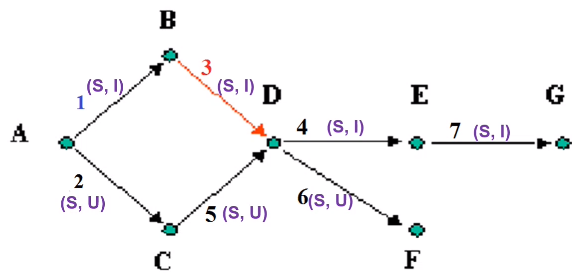
Giới thiệu:

* System R là một hệ quản trị CSDL quan hệ đầu tiên của IBM được bắt đầu năm 1074 thuộc phòng thí nghiệm nghiên cứ 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
* 5 chế độ truy nhập vào 1 table:
  + Select
  + Insert
  + Delete
  + Update
  + Drop
* 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

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, insert, update,…)
* T: tên bảng, trên đó truy nhập được gán
* Ts: thời điểm quyền được gán
* G: người gán quyền (grantor)
* Go {yes, no}: grant option

Gán/thu hồi quyền trong System R

* Gán quyền (Grant privilege):
  + Nếu 1 user được gán quyền trên 1 table với GRANT OPTION, anh ta có thể gán và thu hồi quyền cho các user khác với quyền anh ta có
* Thu hồi quyền (Revoke privilege):
  + Mô hình quyền System R sử dụng cơ chế thu hồi quyền đệ quy
  + Nếu x thu hồi quyền của y, trong đó x không gán quyền gì cho y trước đó. Thì việc thu hồi quyền này bị loại bỏ
* 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
* Thu hồi quyền đệ quy: (Revoke with cascade option)
  + 
  + Sau khi B thu hồi quyền đệ quy của D S, I thì E,G mất hết, F vẫn còn quyền S, U của C
* 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
  + 