Contents

Database Security

- Ensuring security for large DBs is an important and difficult task
- Many different issues involved
  - legal
  - social
  - ethical
  - etc
- Most countries have Data Protection Legislation
  - Requires holders of personal information to take reasonable precautions to ensure that there is no unauthorised access to the data

Access Control

- Prevent unauthorised persons from accessing the system
  - To obtain information
  - To make malicious changes
- DBMS can restrict access to the DB
  - User Accounts
  - Privileges
  - Security Levels
- Database Administrator (DBA) is responsible for
  - User Account Creation
    - Encrytion table maintained by the DBMS
  - Privilege Granting and Revocation
    - Discretionary Access Control
  - Security Level Assignment
    - Mandatory Access Control
  - Role Based Access

Privileges

- Access privileges can be specified at two levels
  - Account level
    - DBA can specify the privileges that each account holds independently of the relations in the database
  - Relation Level
    - DBA can control the privilege to access each individual relation or view in the database

Account Level Privileges

- These privileges apply to the capabilities provided to an account
- Example of privileges include:
  - CREATE SCHEMA
  - CREATE TABLE
  - CREATE VIEW
  - ALTER
  - DROP

Relation Level Privileges

- Can be specified on entire relations or on specific attributes
    - Determine what operations can be performed
- Each relation has an "owner"
    - Typically the account which created the table
    - This account then controls the granting and revoking of privileges to other accounts for that table
- Privilege types are
    - Read privilege
        - Give an account the ability to use SELECT to retrieve rows from this relation
    - Modification Privileges
        - Gives an account the ability to use INSERT, UPDATE and DELETE to modify rows in this relation
    - Reference Privilege
        - Gives an account the ability to refer to this relation when specifying integrity constraints

Views

- Views are an important *discretionary authorisation mechanism*
- Allow the owner of a relation to grant partial access to the information contained in that relation
    - Access to a restricted set of attributes
    - Access to a restricted set of rows
- A view acts as a new relation in the DB

Granting Privileges

- Privileges are allocated to users using the GRANT command in SQL
    - GRANT privilege TO user;
    - GRANT privilege ON relation TO user;
- The owner of a relation
    - Automatically has all the relation privileges granted to theme
    - Can use the GRANT command to specify user privileges for that relation

Revoking Privileges

- It is often desirable to remove a privilege from a particular user
  - Temproary access
  - Abuse of privilege
- In SQL the REVOKE command is used to cancel privileges
  - REVOKE privilege FROM user;
  - REVOKE privilege ON relation FROM user;

Propogation of Privileges

- Whenever the owner A of a relation R grant privileges on R to another user B, the privilege can be given with or without the GRANT OPTION
  - If the GRANT OPTION is given, then B can also grant that privilege on R to other users
- Command syntax
  - GRANT privilege ON relation TO user WITH GRANT OPTION;

Dangers of Propagation

Example 1

- A is the owner of relation R
- A grants B the DELETE privilege on R, with GRANT OPTION
- B grants C the DELETE privilege on R, also with GRANT OPTION
- In this way, privileges can propagate without the knowledge of the relation owner
- If A revokes the privilege granted to B, all the privileges that B propagated should automatically be revoked by the DBMS

Example 2

- A is the owner of relation R
- A grants B the DELETE privilege on R, with GRANT OPTION
- B grants C the DELETE privilege on R, also with GRANT OPTION
- B and C both grant the DELETE privilege on R
- B later revokes the DELETE privilege from D
- However, D continues to have the DELETE privilege, as it was also granted from C

Mandatory Access Control

- Mandatory Access Control classifies data and users based upon *security levels*
    - Can be combined with discretionary access control
    - Desirable in government, military and intelligence
- Not commonly available in Commercial DBMS
    - Some companies, for instance Oracle, have released special versions of DBMS for government which include MAC
- Most simple example of security levels are:
    - Top secret, secret, confidential, unclassified
    - TS $\geq$ S $\geq$ C $\geq$ U
- Each *subject* and *object* are given a security level
    - Subject (User account, application program…)
    - Object (Relation, tuple, attribute, view, operation…)
- The security level of the subject is compared with that of the object
    - For the DBMS to decide if the action is permitted

Access Control Comparison

- Discretionary Access Control
    - Flexible
    - Complex to manage
    - Can be vulnerable to malicious attacks
- Mandatory Access Control
    - Rigid
    - Very secure
- Trade off between security and applicability

Role-Based Access Control

- Privileges and other permissions are associated with organisational roles rather than individual user accounts
- Users are then assigned to appropriate roles
- Roles can be created in SQL using

  - CREATE ROLE
  - DESTROY ROLE
- GRANT and REVOKE are then used to allocate privileges to the created roles
- Users are allocated to roles
  - GRANT role TO user1
  - Multiple individuals can be assigned to each role
  - Any individual assigned to a role automatically has the privileges associated with that role
- An individual can be assigned to multiple roles