Security

Lecture 5

Issues of Database Security (1/6)

- **Legal and ethical issues** regarding the right to access certain information
- **Policy issues** at governmental, institutional, or corporate level as to what kinds of information should not be made publicly available
- **System-related issues** such as system levels at which various security functions should be enforced

Issues of Database Security (2/6)

- DBMS includes a database security and authorization subsystem that is responsible for ensuring the security of portions of a database against unauthorized access

- Two types of database security mechanisms
  - **Discretionary security mechanisms**
    - Used to grant privileges to users, including capability to access specific data files, records, or fields in a specified mode (read, insert, delete, or update)

Issues of Database Security (3/6)

- **Mandatory security mechanisms**
  - Used to enforce multilevel security by classifying data and users into various security classes (or levels) and then implementing the appropriate security policy of the organization
  - Eg. Permit users at a certain classification level to see only the data items classified at the user's own (or lower) classification level

Issues of Database Security (4/6)

- Security mechanism of a DBMS must include provisions for restricting access to the database system as a whole
- This function is called **access control** and handled by creating user accounts and passwords to control login process by DBMS
- Need to **control access to statistical database** which is used to provide statistical information or summaries of values based on age groups, income levels, education levels, and other criteria

Issues of Database Security (5/6)

- Statistical database users like government statisticians are allowed to access the database to retrieve statistical information about a population but not to access detailed confidential info on specific individuals

- This is **statistical database security**

Issues of Database Security (6/6)

- Another security issue is **data encryption**
- Protect sensitive data that is being transmitted via some type of communications network
- Data is encoded
- An unauthorized user who accesses the encoded data will have difficulty deciphering it, but authorized users are given decoding algorithm (keys) to decipher the data

Database security and the DBA (1/2)

- Granting privileges to users who need to use the system and classifying users and data in accordance with the policy of the organization
- DBA has DBA account in DBMS, called system or **superuser** account, which provides powerful capabilities that are not made available to regular database accounts and users

Database security and the DBA (2/2)

- DBA perform the following types of actions
  1. **Account creation** : creates a new account and password for user or group of users to enable them to access DBMS
  2. **Privilege granting** : permits the DBA to grant certain privileges to certain accounts
  3. **Privilege revocation** : permits DBA to revoke (cancel) certain privileges that were previously given to certain accounts
  4. **Security level assignments** : assigning user accounts to the appropriate security classification level

Access protection, user accounts, and DB audits (1/3)

- Person or group of persons need to apply for a user account
- DBA will create a new account number and password
- User must log in using these two wherever database access is needed
- DBMS checks account no and password
- Hence, keep track of database users and their accounts and passwords by creating an **encrypted table** or file with two fields **AccountNo and Password**
- Table can be maintained by DBMS
- Whenever a new account is created, a record is inserted to table
- Whenever an account is cancelled, corresponding record must be deleted from table

Access protection, user accounts, and DB audits (2/3)

- Database system must keep track of all operations on database that are applied by a certain user throughout each login session, which consists of sequence of database interactions that a user performs from time of logging in till logging off
- Important to keep track of update operations that are applied to database so that, if the database is tampered with, DBA can find out which user did the tampering
- For keeping records of all updates applied to database and of particular user who applied each update, we can modify system log

Access protection, user accounts, and DB audits (3/3)

- **System log** includes an entry for each operation applied to database that may be required for recovery from a transaction failure or system crash
- If any tampering is suspected, a **database audit** is performed
- This **consists of reviewing the log to examine all accesses and operations applied to database during a certain time period**
- Database audits are important esp. for sensitive database that are updated by many transactions and users, like banking database updated by many tellers
- **A database log that is used mainly for security purposes is sometimes** called **audit trail**

Types of Discretionary Privileges (1/5)

- Authorization identifier is used
- It refers to a user account (or group of accounts)

- Two levels for assigning privileges to use the database system
  - **Account level** : DBA specifies the particular privileges that each account holds independently of the relations in database

  - **The relation (table) level** : Can control the privilege to access each individual relation or view in database

Types of Discretionary Privileges (2/5)

- **Privileges at account level** apply to capabilities provided to the account itself
- It include **CREATE SCHEMA** or **CREATE TABLE** privilege, **CREATE VIEW** privilege, **ALTER** privilege, **DROP** privilege, **MODIFY** privilege, **SELECT** privilege
- If a certain account does not have CREATE TABLE privilege, no relations can be created from that account

Types of Discretionary Privileges (3/5)

- In **relation level**, a relation may refer to base relation or view
- Privileges at this level specify for each user the individual relations on which type of command can be applied
- **Granting and revoking of privileges** follow an authorization model for discretionary privileges known as **access matrix model**
- Rows of matrix M represent **subjects** (users, accounts, programs)
- Columns represent **objects** (relations, records, columns, views, operations)
- Each position M (i, j) in the matrix represents types of privileges (read, write, update) that subject i holds on object j

Types of Discretionary Privileges (4/5)

- To control granting and revoking of relation privileges, each relation R in a database is assigned an **owner account**
- **Owner of a relation is given all privileges on that relation**
- DBA can assign an owner to a whole schema by creating the schema and associating the appropriate authorization identifier with that schema using CREATE SCHEMA command
- **Owner account holder can pass privileges on any of the owned relations to other users by granting privileges to their accounts**

Types of Discretionary Privileges (5/5)

- Types of privileges can be granted on each individual relation R
  - **SELECT**
    - retrieval privilege
    - Give the account the privilege to use the SELECT statement to retrieve tuples from R
  - **MODIFY**
    - Modify tuples of R
    - Further divided into UPDATE, DELETE, INSERT
  - **REFERENCES**
    - Reference relation R when specifying integrity constraints
- To create a view, account must have SELECT privilege on all relations involved in the view definition

Specifying privileges using views

- If an owner A of a relation R wants another account B to be able to retrieve only some fields of R, then A creates a view V of R that includes only those attributes and then grant SELECT on V to B
- Same applies to limiting B to retrieving only certain tuples of R
- A view V' can be created by defining the view by means of a query that selects only those tuples from R that A wants to allow B to access

Revoking privileges

- In SQL, a REVOKE command is included for the purpose of canceling privileges

Propagation of privileges using the GRANT OPTION (1/2)

- Whenever owner A of a relation R grants a privilege on R to another account B, the privilege can be given to B with or without the **GRANT OPTION**
- **If GRANT OPTION is given, B can also grant privilege on R to other accounts**
- Suppose that B is given the GRANT OPTION by A and that B then grants the privilege on R to a third account C, also with GRANT OPTION
- Hence, **privileges on R can propagate to other accounts without the knowledge of owner of R**

Propagation of privileges using the GRANT OPTION (2/2)

- **If owner A now revokes the privilege granted to B, all the privileges that B propagated will automatically be revoked by the system**
- It is **possible for a user to receive a certain privilege from two or more sources**
- Eg. A4 may receive a certain UPDATE R privilege from both A2 and A3
- In such a case, if A2 revokes this privilege from A4, A4 will still continue to have the privilege by virtue of having been granted from A3
- If A3 later revokes privilege from A4, A4 totally loses privilege

Propagation of privileges – Example (1/6)

- Suppose DBA creates four accounts – A1, A2, A3, A4 and wants only A1 to be able to create base relations

CREATE SCHEMA EXAMPLE AUTHORIZATION A1;

- User A1 can create tables under schema EXAMPLE
- Suppose A1 creates two base relations EMPLOYEE and DEPARTMENT
- A1 is the owner of these two relations and has all the relation privileges on each of them
- Next, suppose A1 wants to grant to A2 the privilege to insert and delete tuples in both these relations

Propagation of privileges – Example (2/6)

- However, A1 does not want A2 to be able to propagate these privileges to other accounts
- A1 can issue the command

  GRANT INSERT, DELETE ON EMPLOYEE, DEPARTMENT TO A2;

- Suppose A1 wants to allow A3 to retrieve information from either of the two tables and also be able to propagate the SELECT privilege to other accounts

- A1 can issue the command

  GRANT SELECT ON EMPLOYEE, DEPARTMENT TO A3 WITH GRANT OPTION;

Propagation of privileges – Example (3/6)

- A3 can now grant the SELECT privilege on EMPLOYEE relation to A4 by issuing the command

  GRANT SELECT ON EMPLOYEE TO A4;

- A4 cannot propagate the SELECT privilege to other accounts since GRANT OPTION is not given to A4
- Now suppose A1 decided to revoke the SELECT privilege on EMPLOYEE relation from A3

  REVOKE SELECT ON EMPLOYEE FROM A3;

- The SELECT privilege on EMPLOYEE from A4 is also revoked

Propagation of privileges – Example (4/6)

- Suppose A1 wants to allow A3 a limited capability to SELECT from EMPLOYEE relation and wants to allow A3 to be able to propagate the privilege

- Limitation is to retrieve only the NAME, BDATE, and ADDRESS attributes and only for the tuples with DNO=5

Propagation of privileges – Example (5/6)

- A1 then create the following view

```
CREATE VIEW A3EMPLOYEE AS
        SELECT NAME, BDATE, ADDRESS
        FROM EMPLOYEE
        WHERE DNO=5;
```

- After the view is created, A1 can grant SELECT on the view A3EMPLOYEE to A3

```
GRANT SELECT ON A3EMPLOYEE TO A3 WITH GRANT OPTION;
```

Propagation of privileges – Example (6/6)

- Finally, suppose A1 wants to allow A4 to update only SALARY attribute of EMPLOYEE

  GRANT UPDATE ON EMPLOYEE (SALARY) TO A4;