Database Security

MBI301-Database Management & Data Security

Mamta Sagar
Department of Bioinformatics
University Institute of Engineering & Technology, CSJM University, Kanpur

Goals of DB Security

- **Integrity:**

  Only authorized users should be allowed to modify data.

- **Availability:**

  Making data available to the authorized users and application programs.

- **Secrecy (or Confidentiality):**

  Protection of data from unauthorized disclosure.

1 Introduction to Database Security Issues

- Types of Security
  - Legal and ethical issues
  - Policy issues
  - System-related issues
  - The need to identify multiple security levels

Introduction to Database Security Issues (2)

- Threats to databases
  - Loss of **integrity**
  - Loss of **availability**
  - Loss of **confidentiality**

- To protect databases against these types of threats four kinds of countermeasures can be implemented:
  - **Access control**
  - **Inference control**
  - **Flow control**
  - **Encryption**

Introduction to Database Security Issues (3)

- A DBMS typically includes a database security and authorization subsystem that is responsible for ensuring the security portions of a database against unauthorized access.
- Two types of database security mechanisms:
  - **Discretionary** security mechanisms
  - **Mandatory** security mechanisms

Introduction to Database Security Issues (4)

- The security mechanism of a DBMS must include provisions for restricting access to the database as a whole
  - This function is called **access control** and is handled by creating user accounts and passwords to control login process by the DBMS.

1.2 Database Security and the DBA

- The database administrator (**DBA**) is the central authority for managing a database system.
  - The DBA's responsibilities include
    - granting privileges to users who need to use the system
    - classifying users and data in accordance with the policy of the organization
- The DBA is responsible for the overall security of the database system.

1.2 Database Security and the DBA (2)

- The DBA has a DBA account in the DBMS
  - Sometimes these are called a system or superuser account
  - These accounts provide powerful capabilities such as:
    - 1. Account creation
    - 2. Privilege granting
    - 3. Privilege revocation
    - 4. Security level assignment
  - Action 1 is access control, whereas 2 and 3 are discretionarym and 4 is used to control mandatory authorization

1.3 Access Protection, User Accounts, and Database Audits

- Whenever a person or group of person s need to access a database system, the individual or group must first apply for a user account.
  - The DBA will then create a new **account id** and **password** for the user if he/she deems there is a legitimate need to access the database
- The user must log in to the DBMS by entering account id and password whenever database access is needed.

1.3 Access Protection, User Accounts, and Database Audits

- The database system must also keep **track of all operations** on the database that are applied by a certain user throughout **each login session**.
  - To keep a record of all updates applied to the database and of the particular user who applied each update, we can modify **system log**, which includes an entry for each operation applied to the database that may be required for recovery from a transaction failure or system crash.

1.3 Access Protection, User Accounts, and Database Audits

- If any tampering with the database is suspected, a **database audit** is performed
  - A database audit consists of reviewing the log to examine all accesses and operations applied to the database during a certain time period.
- A database log that is used mainly for security purposes is sometimes called an **audit trail**.

Discretionary Access Control Based on Granting and Revoking Privileges

- The typical method of enforcing **discretionary access control** in a database system is based on the **granting** and **revoking privileges**.

DB Security Mechanisms

- Access control
- Flow control
- Inference control
- Encryption

Access Control Methods

- **Discretionary Access Control**

  grants privileges to users, including the capability to access specific data files, records, or fields in a specific mode (such as read, insert, delete, or update).

- **Mandatory Access Control**

  classifies users and data into multiple levels of security, and then enforces appropriate rules.

Discretionary Access Control

GRANT SCHEMA DB-schema-name **AUTHORIZATION** users;

GRANT privileges **ON** object **TO** users **[WITH GRANT OPTION]**

REVOKE [GRANT OPTION FOR] privileges **ON** object **FROM** users **{CASCADE | RESTRICT}**

Privileges:

SELECT,INSERT,DELETE,UPDATE,REFERENCES

EMPLOYEE

NAME	EMP-ID	BDATE	ADDRESS	SEX	SALARY	DEPTNO

```
GRANT SELECT ON EMPLOYEE TO user3;

GRANT SELECT ON EMPLOYEE TO user3  WITH
   GRANT OPTION;

GRANT INSERT ON EMPLOYEE(NAME,SSN)  TO user3;

GRANT UPDATE ON EMPLOYEE(SALARY) TO user3;

REVOKE SELECT ON EMPLOYEE FROM user3
   CASCADE;
```

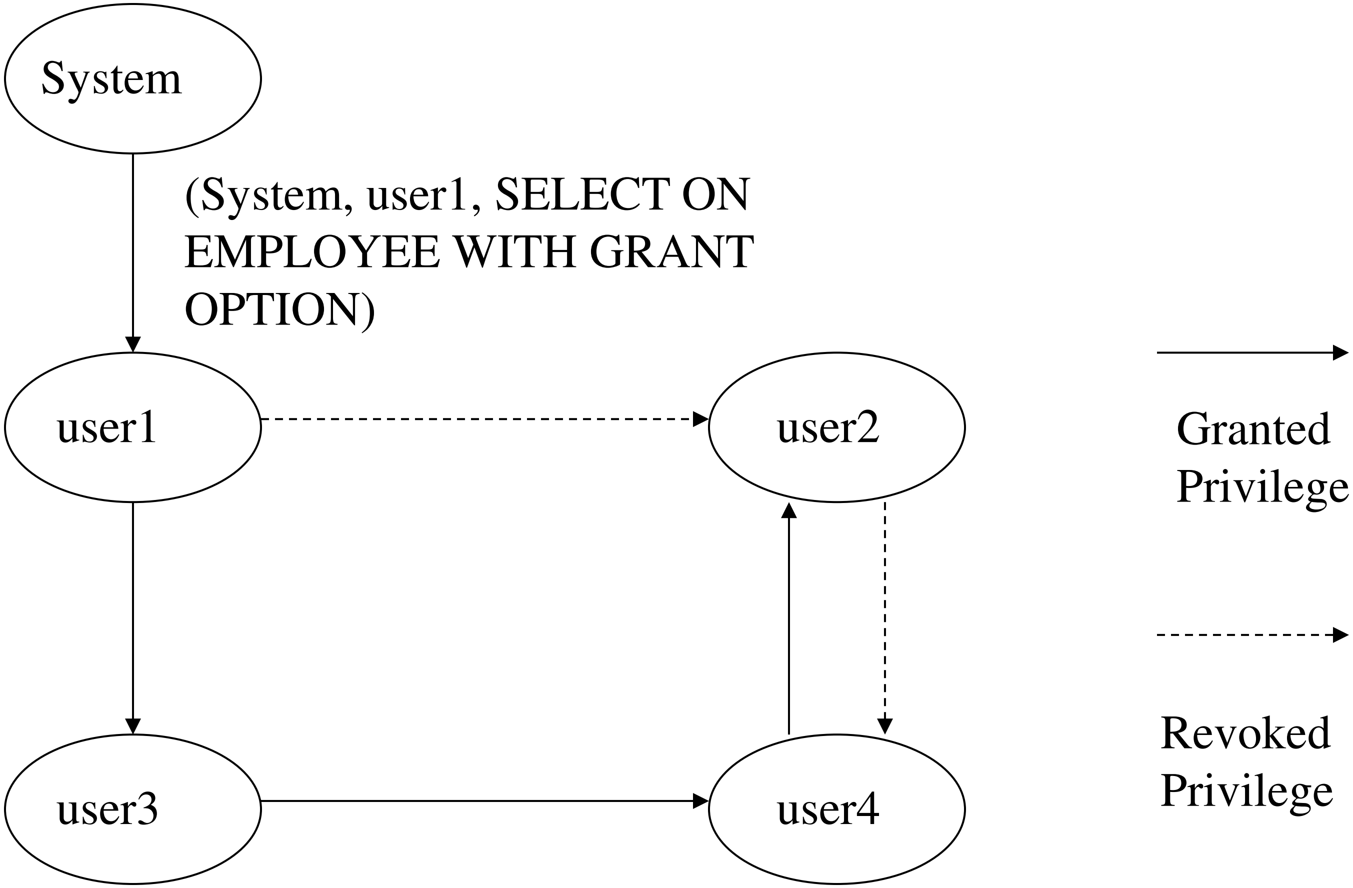
Access Control Using Views

The owner of a relation can create a view containing only limited columns and/or tuples, then grants the view to other users.

Example:

```
CREATE VIEW User3-EMPLOYEE AS
SELECT EMP-ID, NAME, DEPTNO
FROM EMPLOYEE
```

Weakness of Discretionary Access Control



Authorization Graph

Mandatory Access Control

- Each data object is assigned a **security class**.
- Each subject (user or program) is assigned a **clearance** for a security class.
- Security classes could be:

  Top Secret (TS)

  Secret (S)

  Confidential (C)

  Unclassified (U)

Restrictions on Read/Write

- Simple Security Property:

  Subject *S* is allowed to read object *O* only if *class(S)* ≥ *class(O)*.

- *-Property:

  Subject *S* is allowed to write object *O* only if *class(S)* ≤ *class(O)*.

Multilevel Relation and Polyinstantiation

EMP-ID	NAME	SALARY	DEPTNO	SECURITY CLASS
1	smith	100000	5	S
2	brown	80000	4	C
1	smith	null	5	C

Flow Control

- Flow control checks that information contained in some data objects does not flow (explicitly or implicitly) into less protected objects.
- A clearance for a security class can be assigned to each application program.
- Like a DB user, each application program is subjected to the same read/write restrictions.

Security Issues

- Another security is that of **flow control**, which prevents information from flowing in such a way that it reaches unauthorized users.

- Channels that are pathways for information to flow implicitly in ways that violate the security policy of an organization are called **covert channels**.

Covert Channels

A covert channel allows information to pass from a higher classification level to a lower classification level through improper means.

Example:

A distributed DB system has to sites, one with S (secret) level and the other with U (unclassified) level. During the repeated execution of a transaction, the U site agrees to commit all the time while the S site agrees to commit if the bit value is ‘1’ and does not agree to commit if the bit value is ‘0’.

Role-Based Access Control

- Mandatory access control is rigid because the security class should be assigned to each subject and data object.
- In the real world, access privileges are associated with the role of the person in the organization. (example: bank teller)
- Each role is created and is granted/revoked privileges.
- Each user is granted/revoked roles.

Introduction to Database Security Issues (5)

- The security problem associated with databases is that of controlling the access to a **statistical database**, which is used to provide statistical information or summaries of values based on various criteria.
  - The countermeasures to **statistical database security** problem is called **inference control measures**.

Inference Control

Must prohibit the retrieval of individual data through statistical (aggregate) operations on the database.

Example:

```
SELECT  MAX(Salary)
FROM    EMPLOYEE
WHERE   Dept = ‘CSE’ AND
        Address LIKE ‘%Cincinnati%’;
```

Note: What if only few employees live in Cincinnati?

Solutions for Inference Control

- No statistical queries are permitted whenever the number of tuples in the selected population is smaller than a certain number.
- Prohibit a sequence of queries that refer to the same population of tuples repeatedly.
- Partition the database into groups larger than certain size, and queries can refer to any complete group or set of groups, but never to a subset of a group.

Introduction to Database Security Issues

- A final security issue is **data encryption**, which is used to protect sensitive data (such as credit card numbers) that is being transmitted via some type communication network.
- The data is **encoded** using some **encoding algorithm**.
  - An unauthorized user who access encoded data will have difficulty deciphering it, but authorized users are given decoding or decrypting algorithms (or keys) to decipher data.

Encryption and PKI (Public Key Infrastructure)

- Each user generates a pair of keys: a *public key* and a *private key* for encryption and decryption of messages.
- Public key and private key are interchangeable: a message encrypted using one key can be decrypted by the other key.
- The public key of the pair is made public for others to use, whereas the private key is kept by the owner.
- Since the keys are generated by using exponentiation and modulo functions, it is hard to crack them.

PKI (Continued)

- If a sender wishes to send a private message to a receiver, the sender encrypts the message using the receiver’s public key.
- When the receiver receives the message, he or she decrypts it using the receiver’s private key. No other recipient can decrypt the message because only the receiver knows his or her private key.

Digital Signatures

- Like a handwritten signature, a digital signature is a means of associating a mark unique to a person with a body of text.
- The message sender generates the digital signature by hashing the message.
- The sender encrypts the digital signature using his/her private key first, then encrypts it using the public key of the receiver.
- The receiver decrypts the digital signature using his/her private key first, then decrypts it using the public key of the sender.
- To validate the message itself, the receiver hashes the message and compare the hash value with the decrypted digital signature.

Secure Electronic Transaction

- A buyer encrypts the non-credit card information using the public key of the seller, and encrypts the credit card information using the public key of the credit card company. Then, both are sent to the seller.
- The seller decrypts the non-credit card information using his/her private key, and forwards the credit card information (which he/she cannot decrypt) to the credit card company.
- The credit card company decrypts the card information using its private key. If the credit card company approves the card information, the transaction goes through.

References: Lecture was prepared using following Notes

- Soon M. Chung, Department of Computer Science , and Engineering. Wright State University. schung@cs.wright.edu 937-775-5119
- 5th Edition, Fundamentals Database Systems, Elmasri & Nawathe

Question?

What is covert channel ?