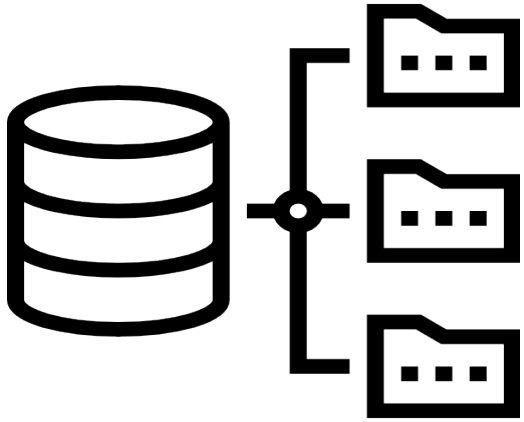
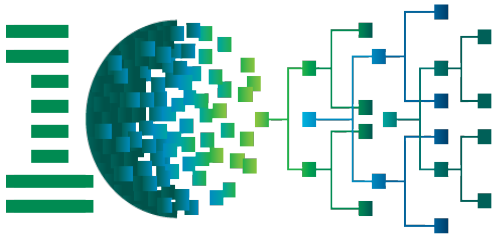
Advanced Database- IS411





Introduced by

Dr. Ebtsam Adel

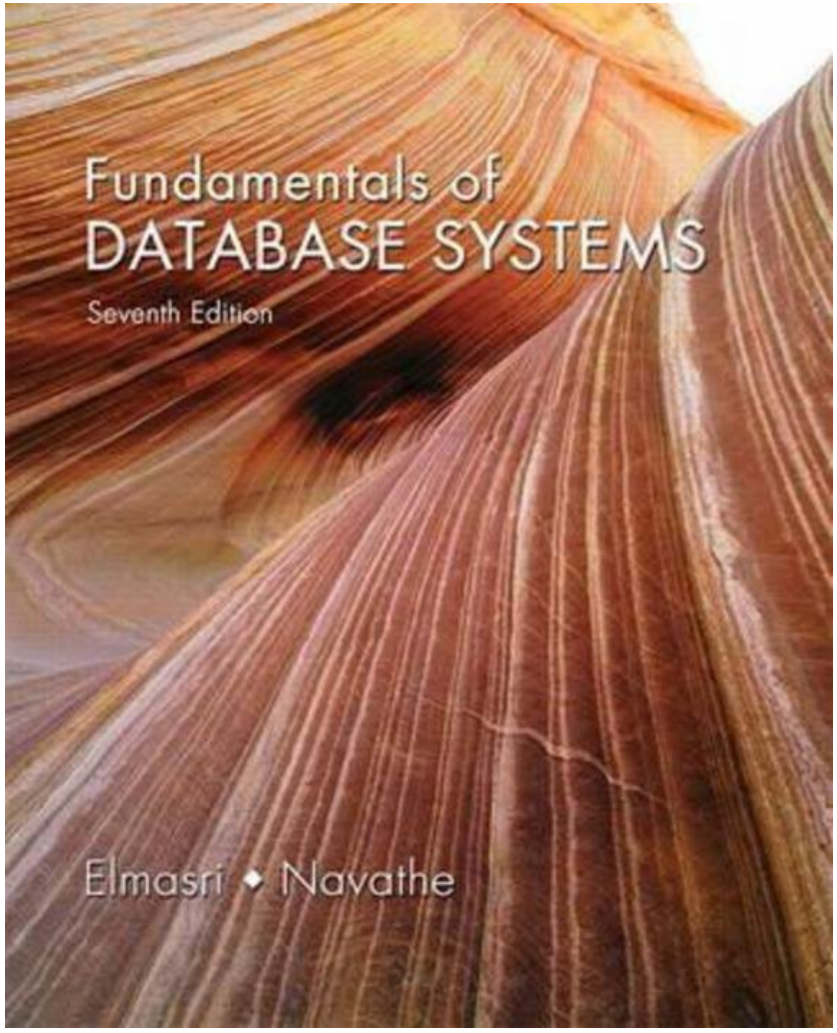
Lecturer of Information Systems,
Information Systems department,
Faculty of computers and information,
Damanhour university


QUIZ!

- Discuss the different types of failures. What is meant by catastrophic failure?

- Discuss the actions taken by the read_item and write_item operations on a database.

Materials



CHAPTER 30
Database Security

Outlines

- ✓ Introduction to Database Security Issues
- ✓ Discretionary Access Control Based on Granting and Revoking Privileges
- ✓ Mandatory Access Control and Role-Based Access Control for Multilevel Security

Introduction to Database Security Issues

Introduction to Database Security Issues

Types of security:-

- legal and ethical issues
- Policy issues at the governmental
- System-related issues
- The need to identify multiple security levels

Introduction to Database Security Issues

Database security is a broad area that addresses many issues, including the following:

- Various **legal and ethical issues** regarding the right to access certain information. for example, some information may be deemed to be private and cannot be accessed legally by unauthorized organizations or persons.

- **Policy issues at the governmental**, institutional, or corporate level regarding what kinds of information should not be made publicly available—for example, credit ratings and personal medical records.

Introduction to Database Security Issues

- **System-related issues** such as the system levels at which various security functions should be enforced—for example, whether a security function should be handled at the physical hardware level, the operating system level, or the DBMS level.

- The need in some organizations to identify **multiple security levels** and to categorize the data and users based on these classifications—for example, top secret, secret, confidential, and unclassified.

Introduction to Database Security Issues

- **Threats to databases**
  - Loss of integrity
    - Improper modification of information (*for example change code of student*)
  - Loss of availability
    - Legitimate user **cannot access** data objects
  - Loss of confidentiality
    - **Unauthorized** disclosure of confidential information.

Control Measures

Introduction to Database Security Issues

- To protect databases against the threats, it is common to implement four kinds of control measures:
  - Access control (grant, revoke)
  - Inference control (concurrency control)
  - Flow control (transfer data between tables)
  - Encryption

Introduction to Database Security Issues

Control measures

- Access control
  - Handled by creating user accounts and passwords
- Inference control
  - Must ensure information about individuals cannot be accessed
- Flow control
  - Prevents information from flowing to unauthorized users.

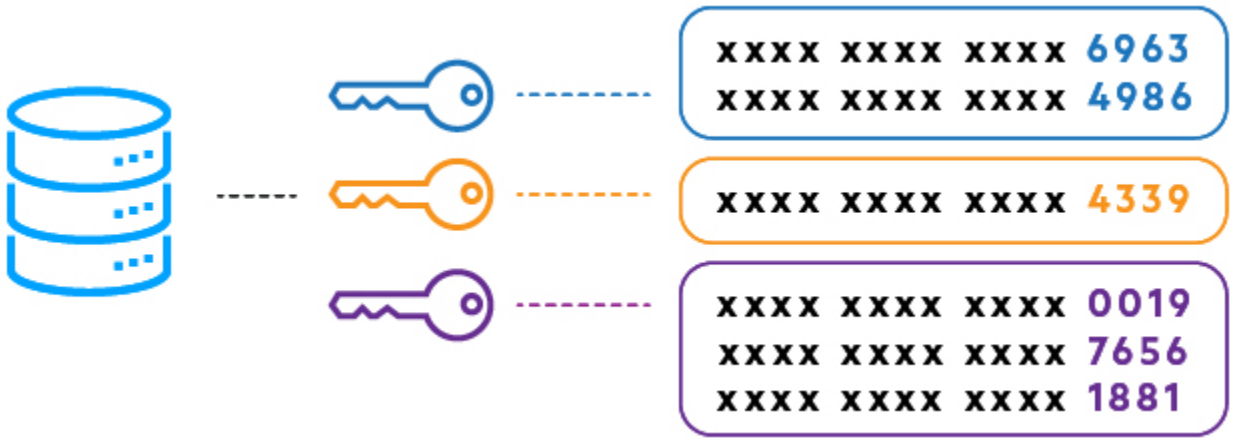
- **Covert channels** are pathways on which information flows implicitly in ways that violate the security policy of an organization.

Introduction to Database Security Issues

- **Data encryption**: Used to protect sensitive transmitted data. that is transmitted via some type of communications network.

- **Encryption** can be used to provide additional protection for sensitive portions of a database as well.

- The data is encoded using some coding algorithm.



Introduction to Database Security Issues

- DBMS typically 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 "تقديري"
  – Used to grant privileges to users.

➢ **Mandatory** security mechanisms
  – Classify data and users into various security classes
  – Implement security policy

Introduction to Database Security Issues

- **Statistical databases** are used to provide **statistical information** or summaries of values based on various criteria.
- For example, a database for population statistics may provide statistics based on age groups, income levels, household size, education levels, and other criteria.
- Statistical database users such as government statisticians or market research firms are allowed to access the database to retrieve statistical information about a population but not to access the detailed confidential information about **specific individuals**.

Database Security and the DBA

Database Security and the DBA

- **Database administrator (DBA)**: is the Central authority for administering database system.

- The DBA's responsibilities include granting privileges to users who need to use the system and classifying users and data in accordance with the policy of the organization.

- The DBA has a DBA account in the DBMS, sometimes called a system or superuser account, which provides powerful capabilities that are not made available to regular database accounts and users.

Database Security and the DBA

- **DBA-privileged commands**
  1. Account creation
  2. Privilege granting
  3. Privilege revocation "cancellation"
  4. Security level assignment

Access Control, User Accounts, and Database Audits

- User must log in using assigned username and password.

- Login session
  - Sequence of database operations by a certain user.
  - Recorded in **system log.**

- Database audit
  - Reviewing **log** to examine all accesses and operations applied during a certain time period.

Discretionary Access Control Based on Granting and Revoking Privileges

Types of Discretionary Privileges

- Two levels for **assigning privileges** to use a database system.

➢ **Account level:** At this level, the DBA specifies the particular privileges that each account holds independently of the relations in the database.

- CREATE SCHEMA or CREATE TABLE privilege,
- CREATE VIEW privilege;
- the ALTER privilege, to apply schema changes such as adding or removing attributes from relations;
- the DROP privilege, to delete relations or views;
- the MODIFY privilege, to insert, delete, or update tuples;
- and SELECT privilege, to retrieve information from the database by using a SELECT query.

Types of Discretionary Privileges

- **Relation (or table) level:** which includes base relations and virtual (view) **relations**.

- These privileges are defined for SQL2.

- The granting and revoking of privileges generally follow an authorization model for discretionary privileges known as the **access matrix model**, where the **rows** of a matrix M represent **subjects** (users, accounts, programs) and the **columns** represent **objects** (relations, records, columns, views, operations).

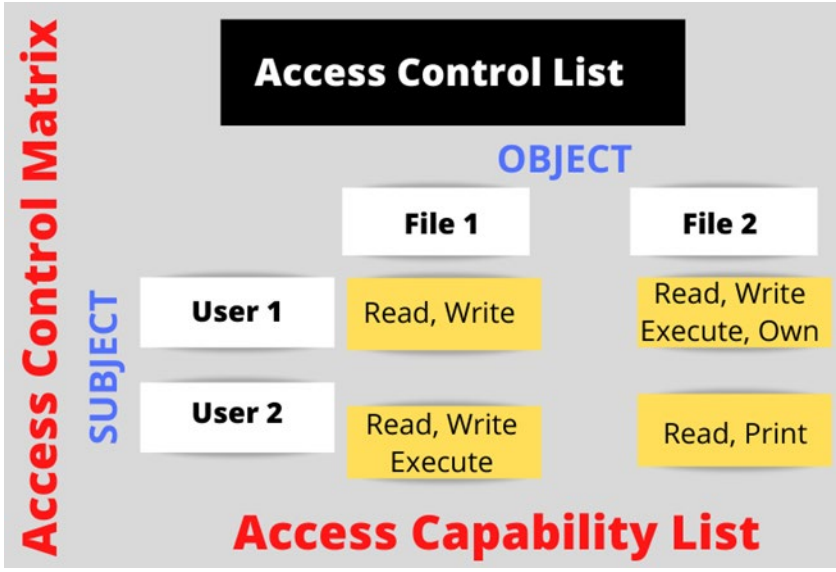
Types of Discretionary Privileges

Each position $M(i, j)$ in the matrix represents the types of **privileges** (read, write, update) that **subject** i holds on object j.

Access Matrix

Domain	Object			
	File 1	File 2	File 3	File 4
D1	Read Write	Read	Read	Read
D2	Read	Write	-	Execute
D3	Write	-	Write	Execute

access matrix model



Types of Discretionary Privileges

- To control the granting and revoking of relation privileges, each relation *R* in a database is assigned an **owner account**, which is typically the account that was used when the relation was created in the first place.
- The **owner** of a relation is given **all privileges** on that relation.
- In SQL2, the DBA can assign an owner to a whole schema by creating the schema and associating the appropriate authorization identifier with that schema, using the **CREATE SCHEMA** command.
- The 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

- **Relation or table level (cont'd.)**
  - Each relation R assigned an owner account.
  - Owner of a relation given all privileges on that relation.
  - Owner can grant privileges to other users on any owned relation.

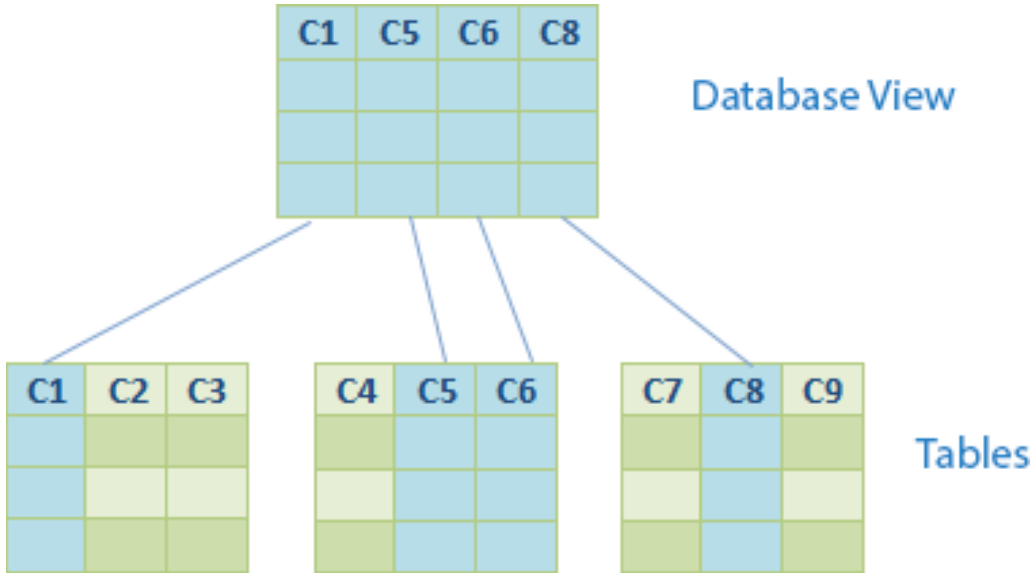
1. **SELECT** (retrieval or read) privilege on R.

2. **Modification** privilege on R: In SQL, this includes three privileges: UPDATE, DELETE, and INSERT.

3. **References** privilege on R: This gives the account the capability to reference (or refer to) a relation R when specifying **integrity constraints**.

Types of Discretionary Privileges

- Notice that to create a **view**, the account must have the SELECT privilege on all **relations** involved in the view definition in order to specify the query that corresponds to the view.



Specifying Privileges through the Use of Views

Specifying Privileges through Views

- The mechanism of **views** is an important discretionary authorization mechanism in its own right. For example,

- if the owner A of a relation R wants another account B to be able to retrieve only **some fields** of R, then A can create a view V of R that includes **only those attributes** and then **grant** SELECT on V to B.

- The 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.

Revocation and Propagation of Privileges

- **Revoking of Privileges**
  - Useful for granting a privilege **temporarily**
  - **REVOKE** command used to cancel a privilege.

- Propagation of privileges using the **GRANT OPTION**
  - If GRANT OPTION is given, B can grant privilege to other accounts.
  - **DBMS** must **keep track** of how privileges were granted if DBMS allows propagation.

Propagation of Privileges

- Whenever the 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 the GRANT OPTION is given, this means that B can also grant that 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 the GRANT OPTION. In this way, privileges on R can **propagate** to other accounts without the knowledge of the owner of R.
- If the owner account A now revokes the privilege granted to B, all the privileges that B propagated based on that privilege should **automatically** be revoked by the system.

An Example to Illustrate Granting and Revoking of Privileges

Suppose that the **DBA** creates four accounts—A1, A2, A3, and A4—and wants only A1 to be able to create base relations. To do this, the **DBA** must issue the following **GRANT** command in SQL:

GRANT CREATETAB **TO** A1;

GRANT INSERT, DELETE **ON** EMPLOYEE, DEPARTMENT **TO** A2;

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

GRANT SELECT **ON** EMPLOYEE **TO** A4;

REVOKE SELECT **ON** EMPLOYEE **FROM** A3;

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

30.2.6 Specifying Limits on Propagation of Privileges

- Techniques to limit the propagation of privileges have been developed, although they have not yet been implemented in most DBMSs and *are not a part* of SQL.

- Limiting **horizontal propagation** to an integer **number *i*** means that an account *B* given the GRANT OPTION can grant the privilege to **at most *i*** other accounts.

- **Vertical propagation** is more complicated; it **limits the depth** of the granting of privileges.


Thank You!
Any questions?