Mansoura University
Faculty of Computers and Information
Department of Information System
First Semester- 2020-2021

[IS313P] Database System II

Grade: 3 rd. IS & IT

Dr. Amira Rezk

DATABASE SECURITY AND AUTHORIZATION

AGENDA

- Introduction
- Discretionary Access Control Based on Granting Revoking Privileges
- Mandatory Access Control
- Role-Based Access Control

INTRODUCTION

- Database security means protecting the database from unauthorized access, modification or destruction.
- Database security pillars
  - Authentication and Authorization
  - Confidentiality
  - Integrity
  - Availability

DATABASE SECURITY PILLARS
AUTHENTICATION AND AUTHORIZATION

- Authentication refers to the process of identifying a user.
  - It occurs during both initial login and each time a user attempts to use a database for the first time during a session.
- Authorization refers to the process of determining what a user can do.
  - It occurs every time a user attempts to perform any operation within a database

DATABASE SECURITY PILLARS, CONT… CONFIDENTIALITY/ INTEGRITY / AVAILABILITY

- Confidentiality refers to the need to maintain secrecy over data, (critical to the organization), whereas Privacy refers to the need to protect data about individuals.
  - Generally it means that protection of information against unauthorized disclosure
- Integrity means prevention of unauthorized or improper modification of data.
- Availability means that users can access the database in general and all the data for which they are authorized. Also, it ensures that data is accessible to the right person when it is needed.

SECURITY POLICIES

- A Security policy is the statement of the security that the system is expected to enforce. Every organization should have a publication that prescribes the security policies and procedures that must be followed. It should define:
  - The specific rules,
  - Who is responsible for enforcing them, and
  - What procedures should be followed when requesting exceptions to policy or when reporting and responding to expected security breaches.

SECURITY CONTROL

- There are three types of security controls that need to be implemented for a successful security policy to be put into action.
- Administrative controls consist of policies that determine how the organization will function.
- Technical controls use software and hardware resources to control access to information and computing systems, to help mitigate the potential for errors and blatant security policy violations.
- Physical controls monitor and protect the physical environment of the workplace and computing facilities.

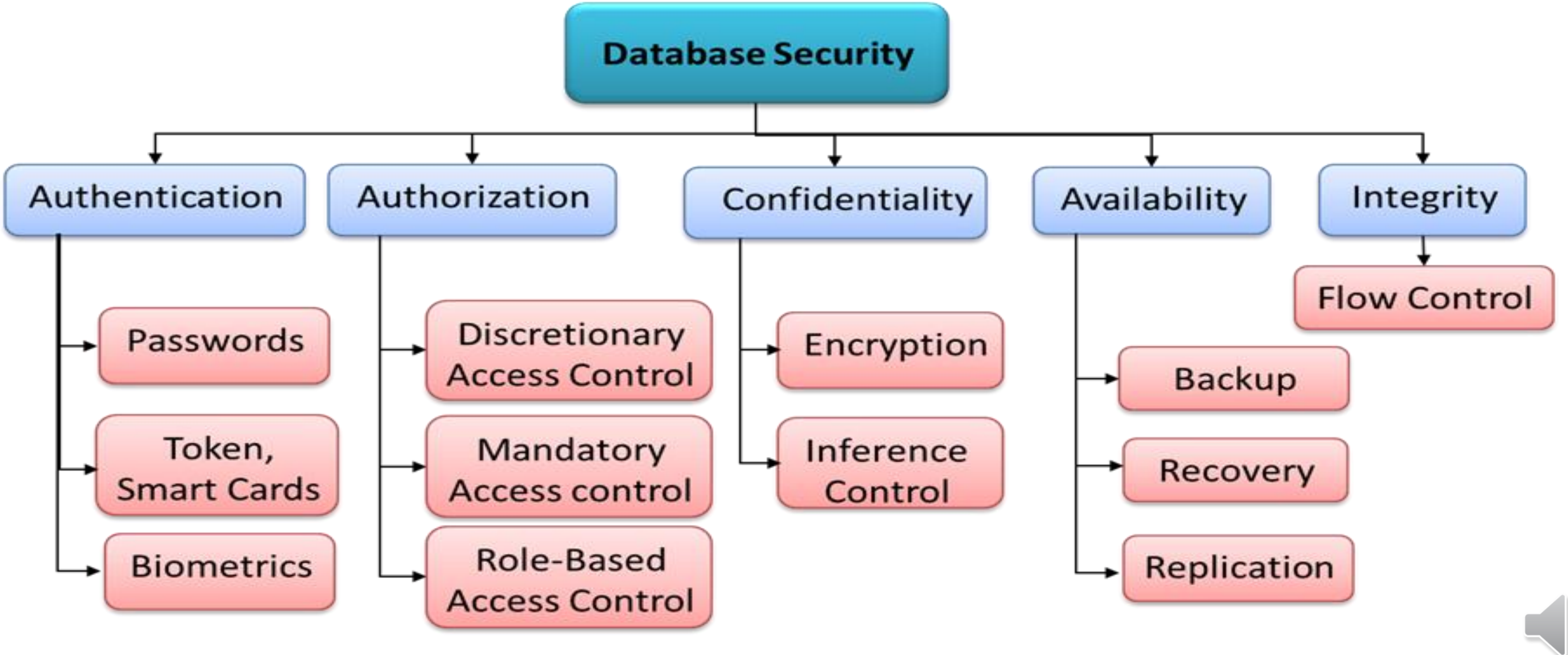
DATABASE SECURITY AND THE DBA

- 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 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.
  - Account creation
  - Privilege granting
  - Privilege revocation
  - Security level assignment

ACCESS PROTECTION, USER ACCOUNTS, AND DATABASE AUDITS

- Whenever a person or group of persons 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 number and password for the user if there is a legitimate need to access the database.
- The database system must also keep track of all operations on the database that are applied by a certain user throughout each login session. (log file)
- A database log that is used mainly for security purposes is sometimes called an audit trail.

DATABASE SECURITY MECHANISMS



ACCESS CONTROL

- Access Control is the most important technique or mechanism for implementing the authorization.
- The basic principle in all access control models is that a subject is or is not permitted to perform a certain operation on an object.
- The subject can be characterized by its identity, its roles in an organization, its tasks, and so on
- The default approach adopted by most access control policies is that any request which is not authorized by the access control policies is denied.
- The most common models are:
  - Discretionary Access Control—DAC
  - Mandatory Access Control—MAC
  - Role-Based Access Control—RBAC

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.
- Types of Discretionary Privileges
- The account level: At this level, the DBA specifies the particular privileges that each account holds independently of the relations in the database.
- The relation (or table level): At this level, the DBA can control the privilege to access each individual relation or view in the database.

DISCRETIONARY ACCESS CONTROL
TYPES OF DISCRETIONARY PRIVILEGES

- The privileges at the account level apply to the capabilities provided to the account itself and can include:
  - the CREATE SCHEMA or CREATE TABLE privilege, to create a schema or base relation;
  - the CREATE VIEW privilege;
  - the ALTER privilege, to apply schema changes such adding or removing attributes from relations;
  - the DROP privilege, to delete relations or views;
  - the MODIFY privilege, to insert, delete, or update tuples;
  - and the SELECT privilege, to retrieve information from the database by using a SELECT query.

DISCRETIONARY ACCESS CONTROL

TYPES OF DISCRETIONARY PRIVILEGES

- The second level of privileges applies to the relation level, whether they are base relations or virtual (view) relations.
- 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 represents subjects (users, accounts, programs) and the columns represent objects (relations, records, columns, views, operations). Each position M(i,j) in the matrix represents the types of privileges (read, write, update) that subject i holds on object j.

DISCRETIONARY ACCESS CONTROL
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.
- The owner account holder can pass privileges on any of the owned relation to other users by granting privileges to their accounts.

DISCRETIONARY ACCESS CONTROL
TYPES OF DISCRETIONARY PRIVILEGES

- In SQL the following types of privileges can be granted on each individual relation R:
- SELECT (retrieval or read) privilege on R: Gives the account retrieval privilege.
  - In SQL this gives the account the privilege to use the SELECT statement to retrieve tuples from R.
- MODIFY privileges on R: This gives the account the capability to modify tuples of R.
  - In SQL this privilege is further divided into UPDATE, DELETE, and INSERT privileges to apply the corresponding SQL command to R. In addition, both the INSERT and UPDATE privileges can specify that only certain attributes can be updated by the account.

DISCRETIONARY ACCESS CONTROL
TYPES OF DISCRETIONARY PRIVILEGES

- REFERENCES privilege on R: This gives the account the capability to reference relation R when specifying integrity constraints. The privilege can also be restricted to specific attributes of R.

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

DISCRETIONARY ACCESS CONTROL
SPECIFYING PRIVILEGES USING 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.

DISCRETIONARY ACCESS CONTROL
REVOKING PRIVILEGES

- In some cases it is desirable to grant a privilege to a user temporarily.
- For example, the owner of a relation may want to grant the SELECT privilege to a user for a specific task and then revoke that privilege once the task is completed. Hence, a mechanism for revoking privileges is needed.
- In SQL, a REVOKE command is included for the purpose of canceling privileges.

DISCRETIONARY ACCESS CONTROL
PROPAGATION OF PRIVILEGES USING THE GRANT OPTION

- Whenever the owner A of a relation R grants a privilege on R to another account B, 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 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

- Suppose that the DBA creates four accounts (A1, A2, A3, and A4) and wants only A1 to be able to create base relations; then the DBA must issue the following GRANT command in SQL:
- GRANT CREATETAB TO A1;
- In SQL2 the same effect can be accomplished by having the DBA issue a CREATE SCHEMA command as follows:
- CREATE SCHAMA EXAMPLE AUTHORIZATION A1;

AN EXAMPLE(2)

- User account A1 can create tables under the schema called EXAMPLE.
- Suppose that A1 creates the two base relations EMPLOYEE and DEPARTMENT; A1 is then owner of these two relations and hence all the relation privileges on each of them.
- Suppose that A1 wants to grant A2 the privilege to insert and delete tuples in both of these relations, but A1 does not want A2 to be able to propagate these privileges to additional accounts:
- GRANT INSERT, DELETE ON EMPLOYEE, DEPARTMENT TO A2;

P

R

u

EMPLOYEE

Name	Ssn	Bdate	Address	Sex	Salary	Dno

DEPARTMENT

Dnumber	Dname	Mgr_ssn

AN EXAMPLE(4)

- Suppose that A1 wants to allow A3 to retrieve information from either of the two tables and also to 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;
- A3 can grant the SELECT privilege on the EMPLOYEE relation to A4 by issuing:
  - GRANT SELECT ON EMPLOYEE TO A4;
- (Notice that A4 can not propagate the SELECT privilege because GRANT OPTION was not given to A4.)

AN EXAMPLE(5)

- Suppose that A1 decides to revoke the SELECT privilege on the EMPLOYEE relation from A3; A1 can issue:
  - REVOKE SELECT ON EMPLOYEE FROM A3;
- (The DBMS must now automatically revoke the SELECT privilege on EMPLOYEE from A4, too, because A3 granted that privilege to A4 and A3 does not have the privilege anymore.)

AN EXAMPLE(6)

- Suppose that A1 wants to give back to A3 a limited capability to SELECT from the EMPLOYEE relation and wants to allow A3 to be able to propagate the privilege. The limitation is to retrieve only the NAME, BDATE, and ADDRESS attributes and only for the tuples with DNO=5.
- A1 then create the 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 as follows:
  - GRANT SELECT ON A3EMPLOYEE TO A3 WITH GRANT OPTION;

AN EXAMPLE(7)

- Finally, suppose that A1 wants to allow A4 to update only the SALARY attribute of EMPLOYEE;
- A1 can issue:
  - GRANT UPDATE ON EMPLOYEE (SALARY) TO A4;
- (The UPDATE or INSERT privilege can specify particular attributes that may be updated or inserted in a relation. Other privileges (SELECT, DELETE) are not attribute specific.)

MANDATORY ACCESS CONTROL

- The discretionary access control techniques of granting and revoking privileges on relations has traditionally been the main security mechanism for relational database systems.
- This is an all-or-nothing method: A user either has or does not have a certain privilege.
- In many applications, and additional security policy is needed that classifies data and users based on security classes. This approach as mandatory access control, would typically be combined with the discretionary access control mechanisms.

MANDATORY ACCESS CONTROL

- Typical security classes are top secret (TS), secret (S), confidential (C), and unclassified (U), where TS is the highest level and U the lowest:
  - TS ≥ S ≥ C ≥ U
- The commonly used model for multilevel security, known as the Bell-LaPadula model, classifies each subject (user, account, program) and object (relation, tuple, column, view, operation) into one of the security classifications, T, S, C, or U:
  - clearance (classification) of a subject S as class(S) and to the classification of an object O as class(O).

MANDATORY ACCESS CONTROL

- Two restrictions are enforced on data access based on the subject/object classifications:
- A subject S is not allowed read access to an object O unless class(S) ≥ class(O). This is known as the simple security property.
- A subject S is not allowed to write an object O unless class(S) ≤ class(O). This known as the star property (or * property).

MANDATORY ACCESS CONTROL

- To incorporate multilevel security notions into the relational database model, it is common to consider attribute values and tuples as data objects.
- Hence, each attribute A is associated with a classification attribute C in the schema, and each attribute value in a tuple is associated with a corresponding security classification.
- In addition, in some models, a tuple classification attribute TC is added to the relation attributes to provide a classification for each tuple as a whole. Hence, a multilevel relation schema R with n attributes would be represented as
- R(A1,C1,A2,C2, …,An,Cn,TC)
  - where each Ci represents the classification attribute associated with attribute Ai.

MANDATORY ACCESS CONTROL

- The value of the TC attribute in each tuple t – which is the highest of all attribute classification values within t – provides a general classification for the tuple itself, whereas each Ci provides a finer security classification for each attribute value within the tuple.

- The apparent key of a multilevel relation is the set of attributes that would have formed the primary key in a regular (single-level) relation.

COMPARING DISCRETIONARY ACCESS CONTROL AND MANDATORY ACCESS CONTROL

- Discretionary Access Control (DAC) policies are characterized by a high degree of flexibility, which makes them suitable for a large variety of application domains.
- The main drawback of DAC models is their vulnerability to malicious attacks, such as Trojan horses embedded in application programs.

COMPARING DISCRETIONARY ACCESS CONTROL AND MANDATORY ACCESS CONTROL

- By contrast, mandatory policies ensure a high degree of protection in a way, they prevent any illegal flow of information.
- Mandatory policies have the drawback of being too rigid and they are only applicable in limited environments.
- In many practical situations, discretionary policies are preferred because they offer a better trade-off between security and applicability.

ROLE-BASED ACCESS CONTROL

- Role-based access control (RBAC) emerged rapidly in the 1990s as a proven technology for managing and enforcing security in large-scale enterprise-wide systems.
- Its basic notion is that permissions are associated with roles, and users are assigned to appropriate roles.
- Roles can be created using the CREATE ROLE and DESTROY ROLE commands.
- The GRANT and REVOKE commands discussed under DAC can then be used to assign and revoke privileges from roles.

ROLE-BASED ACCESS CONTROL

- RBAC appears to be a viable alternative to traditional discretionary and mandatory access controls; it ensures that only authorized users are given access to certain data or resources.
- Many DBMSs have allowed the concept of roles, where privileges can be assigned to roles.
- Role hierarchy in RBAC is a natural way of organizing roles to reflect the organization's lines of authority and responsibility.

ROLE-BASED ACCESS CONTROL

- Another important consideration in RBAC systems is the possible temporal constraints that may exist on roles, such as time and duration of role activations, and timed triggering of a role by an activation of another role.
- Using an RBAC model is highly desirable goal for addressing the key security requirements of Web-based applications.
- In contrast, discretionary access control (DAC) and mandatory access control (MAC) models lack capabilities needed to support the security requirements emerging enterprises and Web-based applications.

Questions?