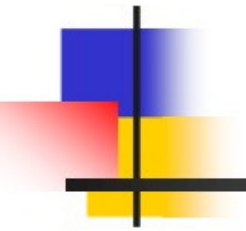
- Introduction

- Security Issues
  - Legal and Ethical
  - Policy
  - System-related
  - Security levels and categories
- Security Threats
  - Loss of integrity
  - Loss of Confidentiality
  - Loss of Availability



Database Security and Authorization

Chapter 23

- 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  '%Bahrain%' ;
```

Note: What if only one or few employees are from Bahrain?

--- Access Control

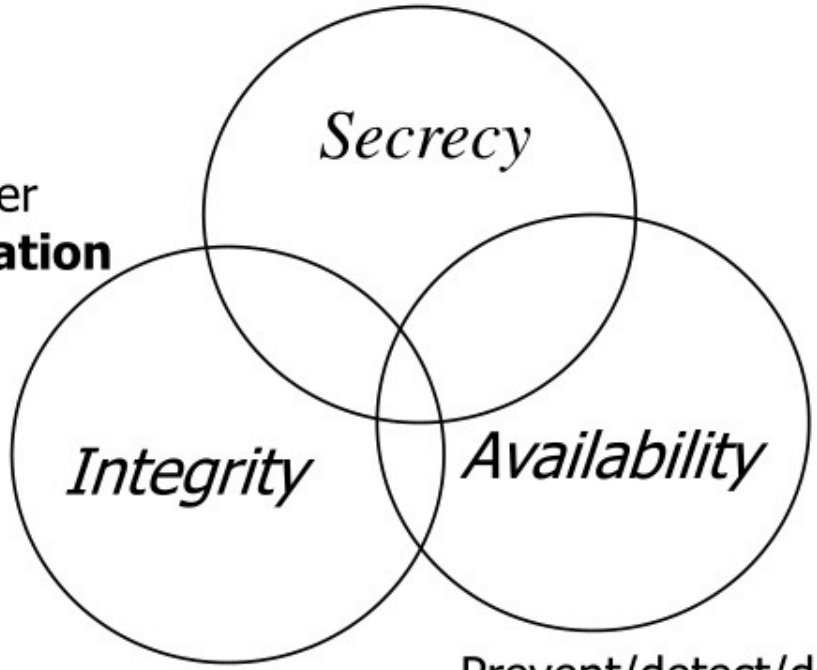
- Subject: active entity that requests access to an object
  - e.g., user or program
- Object: passive entity accessed by a subject
  - e.g., record, relation, file
- Access right (privileges): how a subject is allowed to access an object
  - e.g., subject s can read object o

- DAC ...

- The typical method of enforcing **discretionary access control** in a database system is based on the granting and revoking **privileges**
- Has two levels:
  - **Account level**
    - Create objects (table, view, index, Triggers, Procedures, etc)
    - Alter objects
    - Drop objects
  - **Table level**
    - MODIFY privilege, to insert, delete, or update tuples; and the
    - SELECT privilege
    - REFERENCES privilege

-- Security Objectives

Prevent/detect/deter improper **Disclosure** of information



Prevent/detect/deter Improper **modification** of information

Prevent/detect/deter improper **Denial of access** to services

-- Database Security and DBA

- The DBA is a person who has a **DBA account** in the DBMS, sometimes called a **system** or **superuser account**, which provides powerful capabilities
- The DBA is responsible for the overall security of the database system.
  1. Account creation
  2. Privilege granting
  3. Privilege revocation
  4. Security level assignment
- Action 1 is access control, whereas 2 and 3 are discretionary and 4 is used to control mandatory authorization

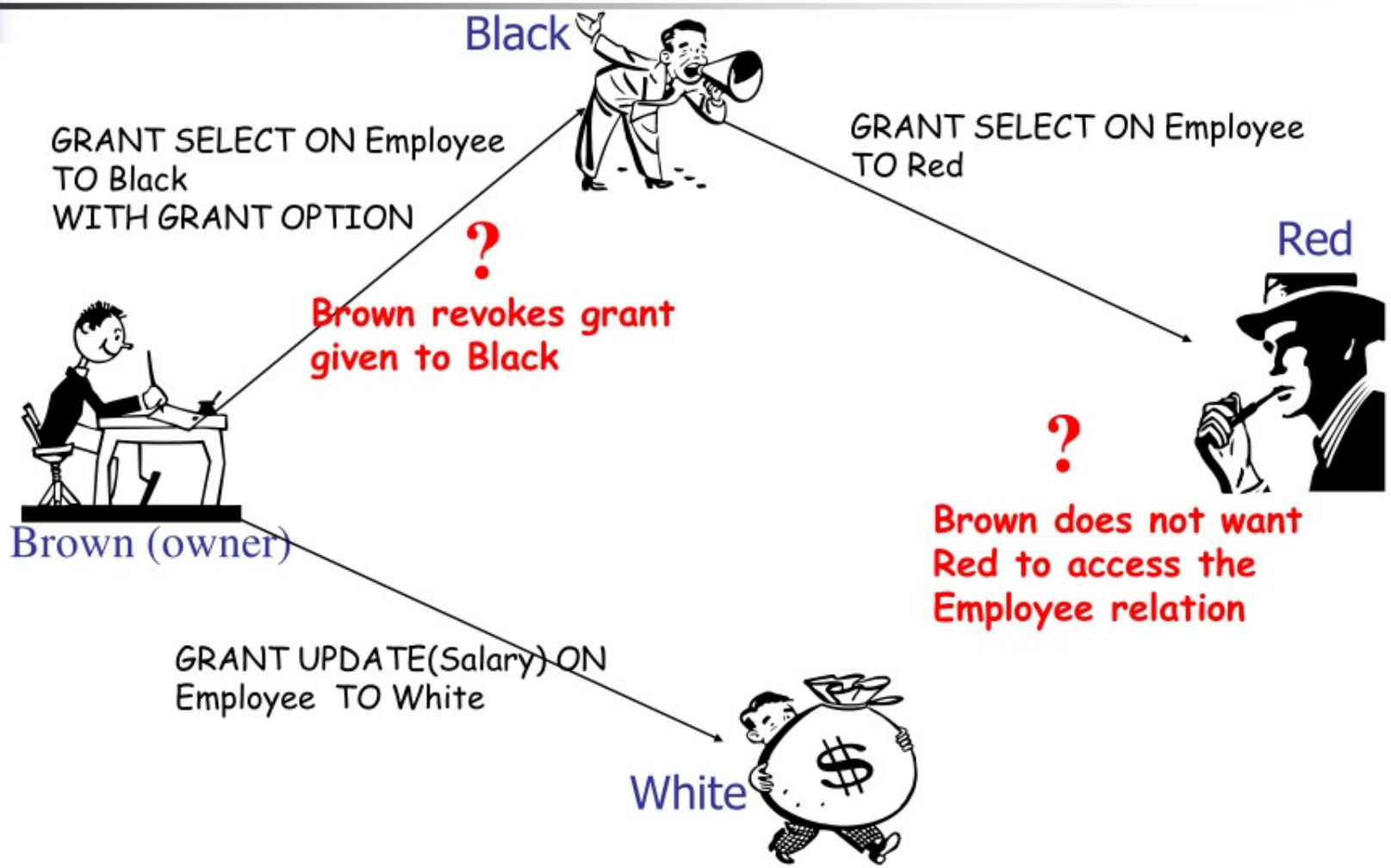
… --- Access Protection, User Accounts, and Database Audits

- 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.
- If any tampering with the database is suspected, a **database audit** is performed, which 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**.

… --- Access Protection, User Accounts, and Database Audits

- 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.
- If any tampering with the database is suspected, a **database audit** is performed, which 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**.

-- Problems with DAC



- 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.

-- Security Control Mechanisms

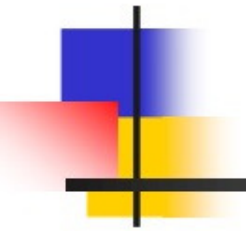
- Access control
  - creating user accounts and passwords to control login process by the DBMS
- Inference control
  - The countermeasures to **statistical database security** problem
- Flow control
  - Prevents information from flowing in such a way that it reaches unauthorized users
- Encryption
  - protect sensitive data that is being transmitted via some type communication network.

- Mandatory Access Control (MAC) …

- **Security label**
  - Top-Secret, Secret, Public
- **Objects:** security classification
  - File 1 is Secret, File 2 is Public
- **Subjects:** security clearances
  - Ali is cleared to Secret, Mustafa is cleared to Public
- **Dominance (□)**
  - Top-Secret □ Secret □ Public

- Access Control Methods

- Discretionary Access Control (DAC)
  - 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 (MAC)
  - classifies users and data into multiple levels of security, and then enforces appropriate rules
- Role-Based Access Control (RBAC)



END

Chapter Outline

- Introduction
- Access Control Methods
- Discretionary Access Control
- Mandatory Access Control
- Role Based Access Control
- Introduction to Statistical Database Security

... -- Example

- 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.)

... -- Example

- 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.)

... -- Example

- 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.)

... -- Example

- 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.)

... -- Example

- 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.)

... -- Example

- 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.)

... -- Example

- 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.)

Chapter Objectives

- To discuss the techniques used for protecting the database against persons who are not authorized to access either certain parts of the database or the whole database

-- Techniques to limit the propagation of privileges

- Limiting **horizontal propagation** to an integer number *k:* means that an account B given the GRANT OPTION can grant the privilege to at most *k* other accounts.
- **Vertical propagation** is more complicated; it limits the depth of the granting of privileges
- They have not yet been implemented in most DBMSs and are not a part of SQL.

-- 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.

… - DAC …

- 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

… - MAC

- **Access rights**: defined by comparing the security classification of the requested objects with the security clearance of the subject
  - If *access control rules* are satisfied, access is permitted Otherwise access is rejected
- Two restrictions are enforced on data access based on subject/object classification
  1. Simple property: A subject S is not allowed read access an object O unless class(S) >= Class(O)
  2. Star property: A subject S is not allowed to write an object O unless class(S) <= class(0)