INFS1200/7900
Introduction to Information Systems

Database Security

Hassan Khosravi

Learning Outcomes

Description	Tag
Differentiate security and privacy	Database Security
Explain at a high-level the four database control measures: access control, inference control, flow control and data encryption.	
Describe at a high level how the Discretionary access control mechanism works.	
Given a set of commands for granting and revoking privileges, determine which users would have what level of access to which resources.	
Describe at a high level how the Mandatory access control mechanism works.	
Given a set of users and resources with their classification rankings, apply the Bell-LaPadula model to determine which users would have what level of access to which resources.	
Describe at a high level how the Role-based access control mechanism works.	
Compare and contrast different access control mechanisms.	
Explain SQL injection and the risks associated with it	

Intro to Database Security Issues

Access Control Mechanisms

SQL Injection

Other Database Control Measures

Sensitive Data Types

information that is protected against unwarranted disclosure

1. Inherently sensitive
2. From a sensitive source
3. Declared sensitive
4. A sensitive attribute or sensitive record
5. Sensitivity in relation to previously disclosed data

Sensitive Data

--> privacy is important

Patient data is private

Patient data has insights for scientific research on biomedicine, drug innovation, public health …

How can access to patient’s data be (mis)used?

CCTV cameras (can) record private conversations from general public

Audio data can contain critical information on criminal, and terrorist activity

How can access to data on people’s movements, behaviours and social habits be (mis)used?

Security vs. Privacy

- **Privacy**: Ability of individuals to control the terms under which their sensitive data (personal information) is acquired and used

- **Security**: A required building block for privacy, which includes
  - Preventing storage of sensitive data
  - Ensuring appropriate/authorized use of sensitive data

Why Database Security

- Legal or policy reasons
  - E.g. Privacy Act of Australia intends to protect privacy of individuals' data (medical, financial rating, etc)
- Ethical reasons
  - E.g. accessing employee salary packages, student grades, …
- Technical reasons
  - E.g. Protect from malware, performance overload, …

Threats to Database Security

- Loss of confidentiality CIA
  - Unauthorized disclosure of confidential information
- Loss of integrity
  - Improper modification of information
- Loss of availability
  - Legitimate user cannot access data objects

Database Control Measures

1. Access control
   – Handled by creating user accounts and passwords

2. Inference control
   – Must ensure information about individuals cannot be accessed

3. Flow control
   – Prevents information from flowing to unauthorized users

4. Data encryption
   – Used to protect sensitive transmitted data

Basic DBMS Security Functions

- **User Accounts**: 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

Username	Password	SessionStart	SessionEnd	SessionID
Jake	J15a	01.03.06.11.03	01.03.06.11.12	78
Nelly	Mb67	21.07.09.13.34	21.07.09.13.49	209
Victor	Y87g	…		

SessionID	Object	BV	AV
78	CDB.ORDER.Amt	2590	2700
209	CDB.CUST.cname	A. Kern	Anika Kern
…			

Intro to Database Security Issues

Access Control Mechanisms

SQL Injection

Other Database Control Measures

Access Control Mechanisms

- Discretionary Access Control
  - Used to grant privileges to users
- Mandatory Access Control
  - Classify data and users into various security classes
  - Implement security policy
- Role-based Access Control
  - Privileges are associated based on organizational roles rather than individual users.

Discretionary Access Control

- Two levels for assigning privileges to use a database system
  - Account level (higher level)
    - Example: CREATE SCHEMA or CREATE TABLE privilege
  - Relation (or table) level
    - Access matrix model

Relation-level Access

- Each relation R assigned an owner account
- Owner can grant (select, modification and references) privileges to other users on any owned relation

	Jake	Aiden	Nelly	Sham
CUST	Read	Read	Modify	X
CUSTORDER	X	X	Read	X
CUSTORDER.Amt	X	Read	Read	X
SUPP.Status	X	Read	Modify	Reference
SUPP.Address	X	Read	Modify	Modify

Specifying Privileges Through Views

- Consider owner A of relation R and other party B
  - A can create view V of R that includes only **attributes** and **tuples** that A wants B to access

```
GRANT SELECT ON V TO B;
```

```
SELECT uid, name
      FROM EMP, DEP
      WHERE DEP = 'Research' AND
      EMP.Dname=DEP.Dname
```

B is only allowed to see id and names of employees in research department

Revocation and Propagation of Privileges

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

```
REVOKE SELECT ON V FROM B;
```

- Propagation of privileges using the GRANT OPTION
  - If GRANT OPTION is given, B can grant privilege to other accounts

```
GRANT SELECT ON V TO B WITH GRANT OPTION;
```

  - If privileges granted to B are revoked, then all privileges granted by B should automatically be revoked.

Active Learning Question

- Which of the following statement is used to remove the privilege from a user?

A. Remove update on department from Amir

B. Revoke update on employee from Amir

C. Delete select on department from Raj

D. Grant update on employee from Amir

Active Learning Question

- if u1 provides authorization to u2 which in turn u2 gives to u3 which of the following is correct ?

u1 --> u2 --> u3

A. If u1 revokes authorization from u3 then u2's authorization is revoked

B. If u1revokes authorization from u2 then u3's authorization is also revoked

C. If u2's authorization is revoked then then u1's authorization is also automatically revoked.

Mandatory Access Control

- Additional security policy that classifies data and users based on security classes

- Typical security classes
    - Top secret (TS)
    - Secret (S)
    - Confidential (C)
    - Unclassified (U)

- Bell-LaPadula model is commonly used
    - Subject and object classifications

Subject and Object Classifications

- Simple security property intuitive
  - Subject S not allowed read access to object O unless class(S) ≥ class(O)

    subject s1 with TS clearance can read object o1 with classification S
    subject s2 with C clearance cannot read object o1 with classification S
- Star property
  - Subject not allowed to write an object unless

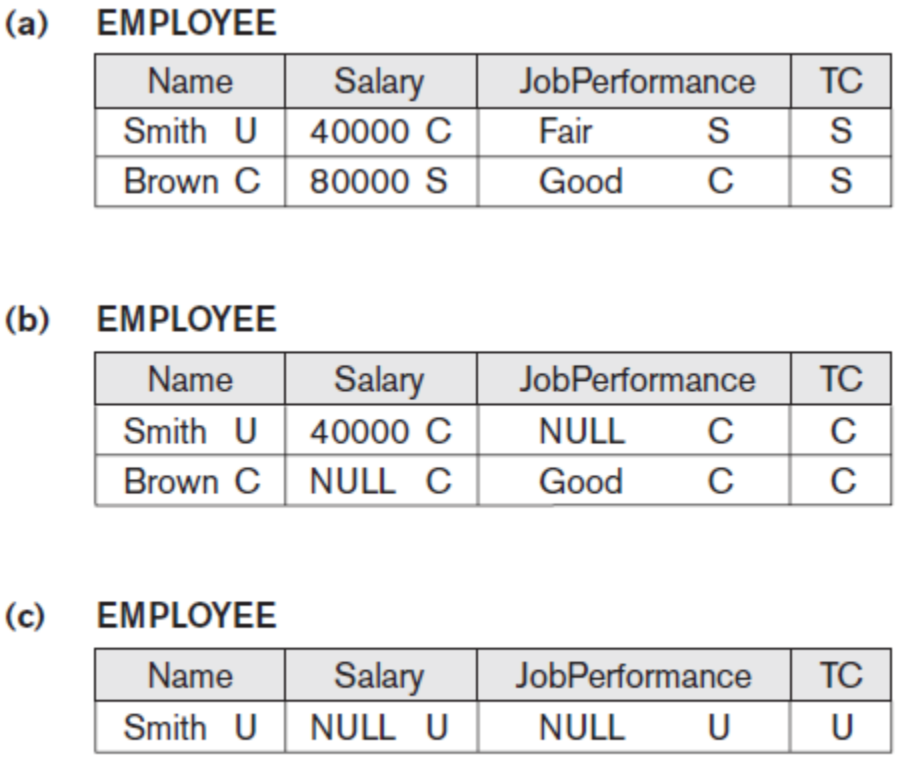
    class(S) ≤ class(O)
  - Prevent information from flowing from higher to lower classifications
  - For example user with TS clearance cannot make a copy of an object with classification TS and then write it back as an object with classification U.

Multilevel Security Example

(a) The original EMPLOYEE tuples

(b) Appearance of EMPLOYEE after filtering for classification C users

(c) Appearance of EMPLOYEE after filtering for classification U users. Second row is removed since attributes related to the key were NULL



(a) EMPLOYEE

Name	Salary	JobPerformance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

(b) EMPLOYEE

Name	Salary	JobPerformance	TC
Smith U	40000 C	NULL C	C
Brown C	NULL C	Good C	C

(c) EMPLOYEE

Name	Salary	JobPerformance	TC
Smith U	NULL U	NULL U	U

Mandatory Access Control ensure a high degree of protection and prevents illegal flow of information. However they are too rigid in that they require a strict classification of objects and subjects.

Role-Based Access Control

- Permissions associated with organizational roles
  - Users are assigned to appropriate roles

```
GRANT ROLE full-time TO emp_typ1;
GRANT ROLE intern TO emp_typ2;
```

- Can be used with traditional discretionary and mandatory access control.

This model has several desirable features, such as flexibility and better support for administration making it an attractive candidate for web-based applications.

Example

- Assume that there are 4 users: A1, A2, A3, A4
  1. DBA issues GRANT CREATETAB TO A1 (where CREATETAB gives Create Table privilege)
  2. A1 creates two base relations: EMPLOYEE and DEPARTMENT
  3. A1 gives the following privileges:
     GRANT INSERT, DELETE ON EMPLOYEE, DEPARTMENT TO A2
     GRANT SELECT ON EMPLOYEE, DEPARTMENT TO A3 WITH GRANT OPTIONS

Q1: Can A3 issue GRANT SELECT ON EMPLOYEE TO A4? can

Q2: If A1 issues REVOKE SELECT ON EMPLOYEE FROM A3, does A4 still have SELECT privilege on EMPLOYEE? No

Q3: What type if Access Control is being used: Discretionary, Mandatory or Role Based? discretionary

Intro to Database Security Issues

Access Control Mechanisms

SQL Injection

Other Database Control Measures

SQL Injection

- SQL injection
  - Most common threat to database system

Attacker injects a string input through the (often web) application which changes or manipulates SQL statement to attacker's advantage

- Other common threats
  - Unauthorized privilege escalation
  - Privilege abuse
  - Denial of service
  - Weak authentication

SQL Injection Methods

- SQL manipulation
  - Changes an SQL command in the application
  - Example: adding conditions to the WHERE clause Typical manipulation attack occurs during database login

- Code injection
  - Add additional SQL statements or commands that are then processed

- Function call injection
  - Database or operating system function call inserted into vulnerable SQL statement to manipulate data or make a privileged system call

SQL Manipulation Example

A simple query to check if query returns any result:

SELECT * FROM users WHERE username = ‘jake’ AND password = ‘jakespassword’

Attacker’s manipulation:

SELECT * FROM users WHERE username = ‘jake’ AND (password = ‘jakespassword’ OR ‘x’=‘x’)

this part is always true

Now the attacker can login as ’jake’ and perform everything that ‘jake’ is authorized to do in the database system

Example

Given two tables:

- CUST (id, cname, address)
- SUPP (sno, sname, contactemail)

Access is restricted to CUST (customer data). How can an attacker use SQL injection to destroy SUPP (supplier data)

```
SELECT * FROM CUST; DROP TABLE SUPP
```

Risks Associated with SQL Injection

- **Database fingerprinting**: Attacker determines the type of database being used.
- **Denial of service**: Attacker denies service to valid users.
- **Bypassing authentication**: attacker gains access to database without valid authorization.
- **Identifying injectable parameters**: attacker determines information about backend structure
- **Executing remote commands**: attacker executes harmful commands remotely.
- **Performing privilege escalation**: attacker upgrades their access level

Protection Techniques

- Blind variables (using parameterized statements)
  - Protects against injection attacks
  - Improves performance
- Filtering input (input validation)
  - Remove escape characters from input strings
  - Escape characters can be used to inject manipulation attacks
- Function security
  - Standard and custom functions should be restricted

Intro to Database Security Issues

Access Control Mechanisms

SQL Injection

Other Database Control Measures

Database Control Measures

1. Access control
   - Handled by creating user accounts and passwords

2. Inference control
   - Must ensure information about individuals cannot be accessed

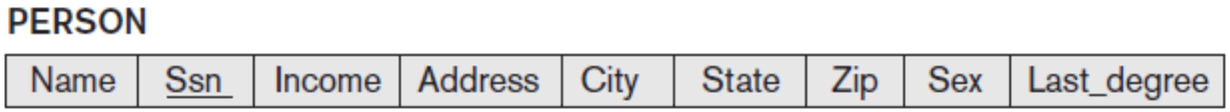
3. Flow control
   - Prevents information from flowing to unauthorized users

4. Data encryption
   - Used to protect sensitive transmitted data

Inference Control

- Statistical databases are used to provide statistics about various populations
  - Users permitted to retrieve statistical information
  - Must prohibit retrieval of individual data

- **Population**: set of tuples of a relation (table) that satisfy some selection condition
  - e.g. Sex = 'Female' and Last-Degree = 'PhD'

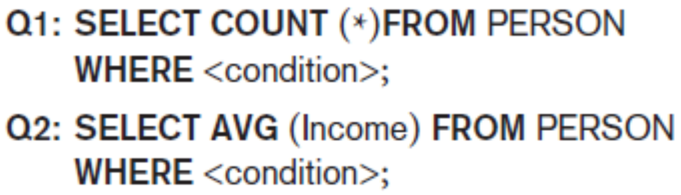


PERSON

Name	Ssn	Income	Address	City	State	Zip	Sex	Last_degree

Inference Control

- Only statistical queries are allowed



```
Q1: SELECT COUNT (*)FROM PERSON
    WHERE <condition>;
Q2: SELECT AVG (Income) FROM PERSON
    WHERE <condition>;
```

- Preventing the inference of individual information
  - Provide minimum threshold on number of tuples

    e.g. minimum threshold is 5 --> if return less than 5 tuples --> don't show the information

```
SELELCT *
FROM PERSON
WHERE Last_Degree = ‘PhD’ AND Sex = ‘Female’
AND City = ‘Ballarat’ and STATE = ‘VIC’
```

  - Prohibit sequences of queries that refer to the same population of tuples

    try to have multiple queries, when the multiple queries combine to give the information
    --> try not to narrow the data?

  - Introduce slight noise or inaccuracy

    noise data into database

  - Partition the database

    group by

    - Store records in groups of minimum size

Flow Control

- Flow control
  - Regulates the distribution or flow of information among accessible objects
  - Verifies information contained in some objects does not flow explicitly or implicitly into less protected objects
- Flow policy
  - Specifies channels along which information is allowed to move (Simple form: confidential and non confidential)

Data Encryption

- Encryption converts data into cyphertext
  - Performed by applying an encryption algorithm to data using a pre-specified encryption key
  - Resulting data must be decrypted using a decryption key to recover original data
- Data Encryption Standard (DES)
  - Developed by the U.S. Government for use by the general public
- Advanced Encryption Standard (AES)
  - More difficult to crack

Learning Outcomes Revisited

Description	Tag
Differentiate security and privacy	Database Security
Explain at a high-level the four database control measures: access control, inference control, flow control and data encryption.	
Describe at a high level how the Discretionary access control mechanism works.	
Given a set of commands for granting and revoking privileges, determine which users would have what level of access to which resources.	
Describe at a high level how the Mandatory access control mechanism works.	
Given a set of users and resources with their classification rankings, apply the Bell-LaPadula model to determine which users would have what level of access to which resources.	
Describe at a high level how the Role-based access control mechanism works.	
Compare and contrast different access control mechanisms.	
Explain SQL injection and the risks associated with it	