



# **CHAPTER 30**

## **Database Security**

# 30.1 Introduction to Database Security Issues

- Database security a broad area
  - Legal, ethical, policy, and system-related issues
- Threats to databases
  - Loss of integrity
    - Improper modification (insert, delete, etc.) of information
    - Lost of integrity, authorized changes (accidentally or intentional. It could result in more **inaccuracies, errors**.
  - Loss of availability
    - Legitimate user cannot access data objects
  - Loss of confidentiality
    - Unauthorized disclosure of confidential information
    - Violation of data protection acts, loss of public confidence

# Introduction to Database Security Issues (cont'd.)

- Database works as part of a network of services
  - Applications, Web servers, firewalls, SSL terminators, and security monitoring systems
- Types of database control measures
  - Access control
  - Inference control
  - Flow control
  - Encryption

# Introduction to Database Security Issues (cont'd.)

- Discretionary security mechanisms
  - Used to grant privileges to users
- Mandatory security mechanisms
  - Classify data and users into various security classes
  - Implement security policy
- Role-based security

# Introduction to Database Security Issues (cont'd.)

- 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
  - Data encryption
    - Used to protect sensitive transmitted data

# Database Security and the DBA

- Database administrator (DBA)
  - Central authority for administering database system
  - Superuser or system account
- DBA-privileged commands
  - Account creation
    - New accounts and passwords for a (group) users
  - Privilege granting: grant access to accounts
  - Privilege revocation: cancel such priviliages
  - 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
  - DBA can show who made changes. Especially for sensitive data



# Sensitive Data and Types of Disclosures

- Sensitivity of data
  - Inherently sensitive
    - E.g. salary, or a patient has HIV
  - From a sensitive source
    - E.g. an informer whose ID must be kept secret
  - Declared sensitive
    - The owner may have declared it as sensitive
  - A sensitive attribute or sensitive record
    - Eg. A particular attribute
  - Sensitivity in relation to previously disclosed data
    - E.g. a location associated with a crime event

# Sensitive Data and Types of Disclosures (cont'd.)

- Factors in deciding whether it is safe to reveal the data
  - Data availability
    - Not available when being updated by other users (concurrency control)
  - Access acceptability
    - Authorized users
  - Authenticity assurance
    - External characteristics of the user
    - Example: access only allowed during working hours

# Sensitive Data and Types of Disclosures (cont'd.)

- Typically a tradeoff between precision and security
- Ideal combination: maximize precision with perfect security
- Precision
  - Protect all sensitive data while making available as much nonsensitive data as possible
- Security
  - Ensuring data kept safe from corruption and access suitably controlled

# Relationship Between Information Security and Information Privacy

- Concept of privacy goes beyond security
  - Ability of individuals to control the terms under which their personal information is acquired and used
  - Security a required building block for privacy
- Preventing storage of personal information
- Ensuring appropriate use of personal information
- Trust relates to both security and privacy

# 30.2 Discretionary Access Control Based on Granting and Revoking Privileges

- Two levels for assigning privileges to use a database system
  - **Account level**
    - DBA specifies privileges for each account
    - Example: CREATE SCHEMA or CREATE TABLE privilege
    - Not defined for SQL2

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

- **Relation (or table) level**
  - DBA specifies privileges for each relation (view)
  - Defined for SQL2

	File 1	File 2	File 3	Program 1
Ann	own read write	read write		execute
Bob	read		read write	
Carl		read		execute read

# Discretionary Access Control (cont'd.)

- 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
    - SELECT (retrieval or read) privilege on R
    - Modification privilege on R
    - References privilege on R

# Specifying Privileges Through the Use of Views

- Consider owner A of relation R and other party B
  - A can create view V of R that includes only attributes A wants B to access
    - Grant SELECT on V to B
- Can define the view with a query that selects only those tuples from R that A wants 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

## 30.3 Mandatory Access Control and Role-Based Access Control for Multilevel Security

- Mandatory access control
  - Additional security policy that classifies data and users based on security classes
  - Typical security classes
    - Top secret
    - Secret
    - Confidential
    - Unclassified
  - Bell-LaPadula model
    - Subject and object classifications

# Mandatory Access Control and Role-Based Access Control for Multilevel Security (cont'd.)

- Simple security property
  - Subject  $S$  not allowed read access to object  $O$  unless  $\text{class}(S) \geq \text{class}(O)$
- Star property
  - Subject not allowed to write an object unless  $\text{class}(S) \leq \text{class}(O)$
  - Prevent information from flowing from higher to lower classifications
- Attribute values and tuples considered as data objects

(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

(d) EMPLOYEE

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

Figure 30.2 A multilevel relation to illustrate multilevel security (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 (d) Polyinstantiation of the Smith tuple

Top secret  
Secret  
Confidential  
Unclassified

# Comparing Discretionary Access Control and Mandatory Access Control

- DAC policies have a high degree of flexibility
  - Do not impose control on how information is propagated
- Mandatory policies ensure high degree of protection
  - Rigid
  - Prevent illegal information flow

# Role-Based Access Control

- Permissions associated with organizational roles
  - E.g. Roles: manager, purchase agent.
  - Multiple users may assigned to a role.
  - Privileges are associated to a role
- Can be used with traditional discretionary and mandatory access control
- Mutual exclusion of roles
  - Authorization time exclusion
  - Runtime exclusion
- Identity management (a unique name for a user)

# Role-Based Access Control

		File 1	File 2	File 3	Program 1
manager	Ann	own read write	read write		execute
	Bob	read		read write	
secretary	Carl		read		execute read

# Label-Based Security and Row-Level Access Control

- Sophisticated access control rules implemented by considering the data row by row
- Each row given a label
  - Used to prevent unauthorized users from viewing or altering certain data
- Provides finer granularity of data security
- Label security policy
  - Defined by an administrator



# 30.4 SQL Injection

- SQL injection
  - Most common threat to database system
- Other common threats
  - Unauthorized privilege escalation
    - A user attempts to attack vulnerable points using his existing privileges
  - Privilege abuse
    - E.g. A DBA abuses his privileges to add money in customer's account
  - Denial of service by making resources unavailable
  - Weak authentication:
    - an attacker impersonates someone else

# SQL Injection Methods

- Attacker injects a string input through the application
  - Changes or manipulates SQL statement to attacker's advantage
- Unauthorized data manipulation or execution of system-level commands
- SQL manipulation
  - Changes an SQL command in the application
  - Example: adding conditions to the WHERE clause

```
SELECT * FROM users WHERE username = 'jake' and PASSWORD =  
'jakespasswd' ;
```

The attacker can try to change (or manipulate) the SQL statement by changing it as follows:

```
SELECT * FROM users WHERE username = 'jake' and (PASSWORD =  
'jakespasswd' or 'x' = 'x') ;
```

# SQL Injection Methods (cont'd.)

- SQL manipulation (cont'd.)
  - 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

# Risks Associated with SQL Injection

- Database fingerprinting
- Denial of service
- Bypassing authentication
- Identifying injectable parameters
- Executing remote commands
- Performing privilege escalation

# 30.5 Introduction to Statistical Database Security

- Statistical databases 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

PERSON

Name	<u>Ssn</u>	Income	Address	City	State	Zip	Sex	Last_degree
------	------------	--------	---------	------	-------	-----	-----	-------------

Figure 30.3 The PERSON relation schema for illustrating statistical database security

# Introduction to Statistical Database Security (cont'd.)

- 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
- Prohibit sequences of queries that refer to the same population of tuples
- Introduce slight noise or inaccuracy
- Partition the database
  - Store records in groups of minimum size

# Classification of Attributes(Cont'd)

## Hospital Patient Data

DOB	Sex	Zipcode	Disease
1/21/76	Male	53715	Heart Disease
4/13/86	Female	53715	Hepatitis
2/28/76	Male	53703	Brochitis
1/21/76	Male	53703	Broken Arm
4/13/86	Female	53706	Flu
2/28/76	Female	53706	Hang Nail

# Classification of Attributes(Cont'd)

Hospital Patient Data

DOB	Sex	Zipcode	Disease
1/21/76	Male	53715	Heart Disease
4/13/86	Female	53715	Hepatitis
2/28/76	Male	53703	Brochitis
1/21/76	Male	53703	Broken Arm
4/13/86	Female	53706	Flu
2/28/76	Female	53706	Hang Nail

Vote Registration Data

Name	DOB	Sex	Zipcode
Andre	1/21/76	Male	53715
Beth	1/10/81	Female	55410
Carol	10/1/44	Female	90210
Dan	2/21/84	Male	02174
Ellen	4/19/72	Female	02237



# Classification of Attributes(Cont'd)

Hospital Patient Data

DOB	Sex	Zipcode	Disease
1/21/76	Male	53715	Heart Disease
4/13/86	Female	53715	Hepatitis
2/28/76	Male	53703	Brochitis
1/21/76	Male	53703	Broken Arm
4/13/86	Female	53706	Flu
2/28/76	Female	53706	Hang Nail

Vote Registration Data

Name	DOB	Sex	Zipcode
Andre	1/21/76	Male	53715
Beth	1/10/81	Female	55410
Carol	10/1/44	Female	90210
Dan	2/21/84	Male	02174
Ellen	4/19/72	Female	02237

□ Andre has heart disease!

# Classification of Attributes(Cont'd)

Hospital Patient Data

DOB	Sex	Zipcode	Disease
1/21/76	Male	53715	Heart Disease
4/13/86	Female	53715	Hepatitis
2/28/76	Male	53703	Brochitis
1/21/76	Male	53703	Broken Arm
4/13/86	Female	53706	Flu
2/28/76	Female	53706	Hang Nail

Vote Registration Data

Name	DOB	Sex	Zipcode
Andre	1/21/76	Male	53715
Beth	1/10/81	Female	55410
Carol	10/1/44	Female	90210
Dan	2/21/84	Male	02174
Ellen	4/19/72	Female	02237

Zipcode	Age	Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
4790*	≥40	Flu
4790*	≥40	Heart Disease
4790*	≥40	Cancer
476**	3*	Heart Disease
476**	3*	Heart Disease

# Classification of Attributes(Cont'd)

Hospital Patient Data

DOB	Sex	Zipcode	Disease
1/21/76	Male	53715	Heart Disease
4/13/86	Female	53715	Heart Disease
2/28/76	Male	53703	Heart Disease
1/21/76	Male	53703	Heart Disease
4/13/86	Female	53706	Heart Disease
2/28/76	Female	53706	Hang Nail

Vote Registration Data

Name	DOB	Sex	Zipcode
Andre	1/21/76	Male	53715
Beth	1/1/81	Female	55410
Carol	10/1/44	Female	90210
Dan	2/21/84	Male	02174
Ellen	4/19/72	Female	02237

I know already that the last record has a Hang Nail.  
A statistical query about the amount of patients having  
Heart disease (i.e. 5 patients) will also show that  
**5 first patients have heart disease**

# 30.7 Encryption and Public Key Infrastructures

- Encryption converts data into cyphertext
  - Performed by applying an encryption algorithm to data using a prespecified 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

# Encryption and Public Key Infrastructures (cont'd.)

- Symmetric key algorithms
  - Also called secret key algorithms
  - Need for sharing the secret key
    - Can apply some function to a user-supplied password string at both sender and receiver
- Public (asymmetric) key encryption
  - Involves public key and private key
  - Private key is not transmitted
  - Two keys related mathematically
    - Very difficult to derive private key from public key

# Encryption and Public Key Infrastructures (cont'd.)

- Public (asymmetric) key encryption steps
  - Each user generates a pair of keys to be used for encryption and decryption of messages
  - Each user places public key in a public register or other accessible file
    - Keeps companion key private
  - Sender encrypts message using receiver's public key
  - Receiver decrypts message using receiver's private key
- RSA public key encryption algorithm

# Digital Signatures

- Using encryption techniques to provide authentication in applications
- Like signatures, Associates a text with a person
- Consist of string of symbols
- Each is unique
  - Function of the message it is signing, along with a timestamp
  - Depends on secret number unique to the signer
  - Associates a text with a person
- Public key techniques used to create digital signatures

# Digital Certificates

- Combines value of a public key with the identity of the person or service that holds the corresponding private key into a digitally signed statement
- E.g. Verisign: verifies the identity of Easyjet
- Information included in the certificate
  - Owner information
  - Public key of the owner
  - Date of certificate issue and validity period
  - Issuer identification
  - Digital signature