



# **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 of information
  - Loss of availability
    - Legitimate user cannot access data objects
  - Loss of confidentiality
    - Unauthorized disclosure of confidential information

# 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
  - Privilege granting
  - Privilege revocation
  - 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



# Sensitive Data and Types of Disclosures

- Sensitivity of data
  - Inherently sensitive
  - From a sensitive source
  - Declared sensitive
  - A sensitive attribute or sensitive record
  - Sensitivity in relation to previously disclosed data

# 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
  - 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
- 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
    - Example: CREATE SCHEMA or CREATE TABLE privilege
    - Not defined for SQL2
  - Relation (or table) level
    - Defined for SQL2
    - Access matrix model

# 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



# Revocation and Propagation of Privileges (cont'd.)

- Horizontal and vertical propagation limits
  - Limiting horizontal propagation to an integer number  $i$ 
    - Account  $B$  given the GRANT OPTION can grant the privilege to at most  $i$  other accounts
  - Vertical propagation limits the depth of the granting of privileges
  - Not available currently in SQL or other relational systems

## 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

# 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
  - Users are assigned to appropriate roles
- Can be used with traditional discretionary and mandatory access control
- Mutual exclusion of roles
  - Authorization time exclusion
  - Runtime exclusion
- Identity management

# 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

# XML Access Control

- Digital signatures for XML
  - XML Signature Syntax and Processing specification
    - Defines mechanisms for countersigning and transformations
- XML encryption
  - XML Encryption Syntax and Processing specification
    - Defines XML vocabulary and processing rules



# Access Control Policies for the Web and Mobile Applications

- E-commerce environments require elaborate access control policies
  - Go beyond traditional DBMSs
- Legal and financial consequences for unauthorized data breach
- Content-based access control
  - Takes protection object content into account
- Credentials

# 30.4 SQL Injection

- SQL injection
  - Most common threat to database system
- Other common threats
  - Unauthorized privilege escalation
  - Privilege abuse
  - Denial of service
  - Weak authentication

# 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

# 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

# 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

# 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



# 30.6 Introduction to 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 nonconfidential

# Introduction to Flow Control (cont'd.)

## ■ Covert channels

- Allows information to pass from a higher classification level to a lower classification level through improper means
- Timing channel requires temporal synchronization
- Storage channel does not require temporal synchronization

# 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

- 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
- 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
- Information included in the certificate
  - Owner information
  - Public key of the owner
  - Date of certificate issue and validity period
  - Issuer identification
  - Digital signature

## 30.8 Privacy Issues and Preservation

- Growing challenge for database security
- Limit performing large-scale mining and analysis
- Central warehouses for vital information
  - Violating security could expose all data
- Distributed data mining algorithms
- Remove identity information in released data
- Inject noise into the data
  - Must be able to estimate errors introduced
- Mobile device privacy



# 30.9 Challenges to Maintaining Database Security

- Data quality
  - Quality stamps
  - Application-level recovery techniques to automatically repair incorrect data
- Intellectual property rights
  - Digital watermarking techniques

# Challenges to Maintaining Database Security (cont'd.)

- Database survivability
  - Confinement
  - Damage assessment
  - Reconfiguration
  - Repair
  - Fault treatment

# 30.10 Oracle Label-Based Security

- Oracle label security
  - Enables row-level access control
  - Every table or view has an associated security policy
- Virtual private database (VPD) technology
  - Feature that adds predicates to user statements to limit their access in a transparent manner to the user and the application
  - Based on policies

# Label Security Architecture

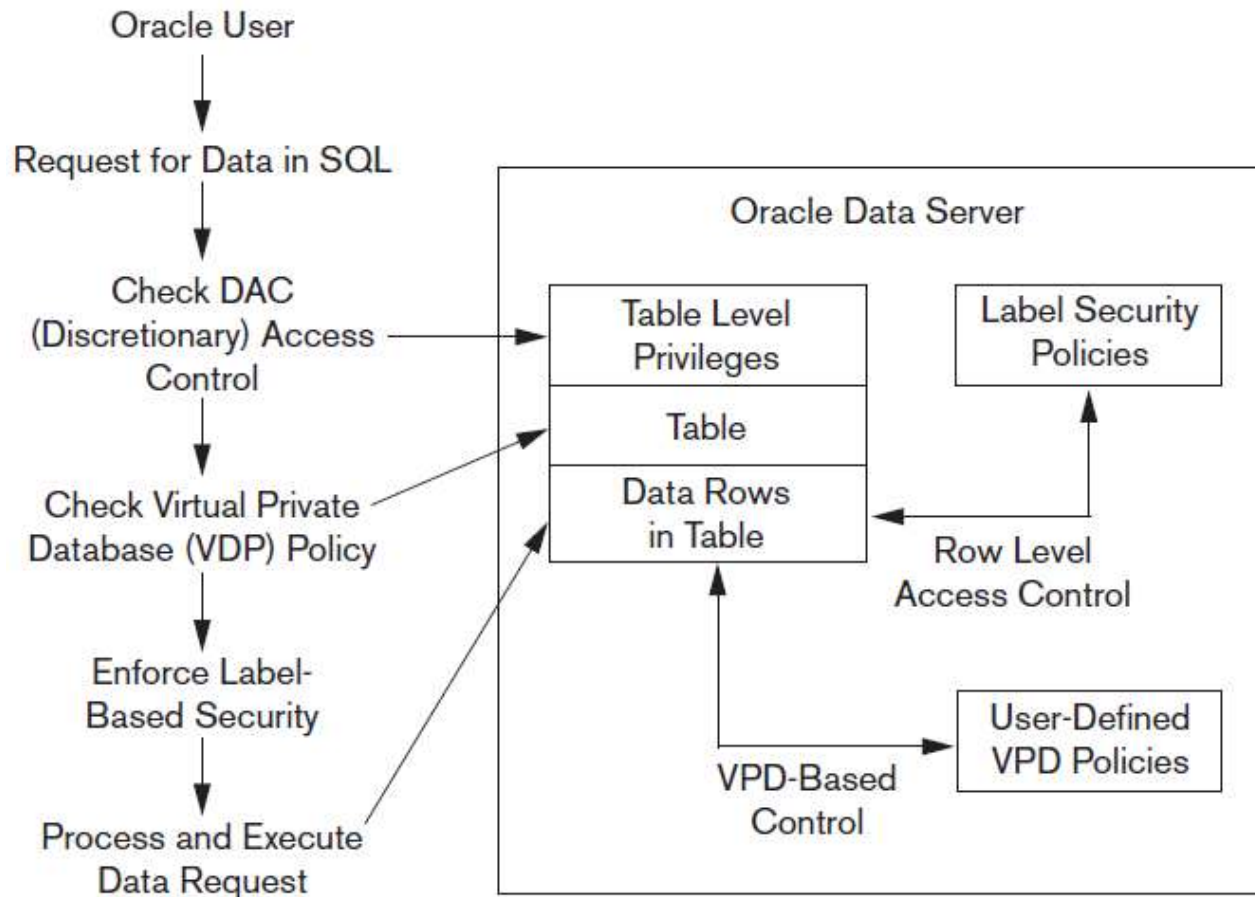


Figure 30.4 Oracle label security architecture. Data from: Oracle (2007)

# How Data Labels and User Labels Work Together

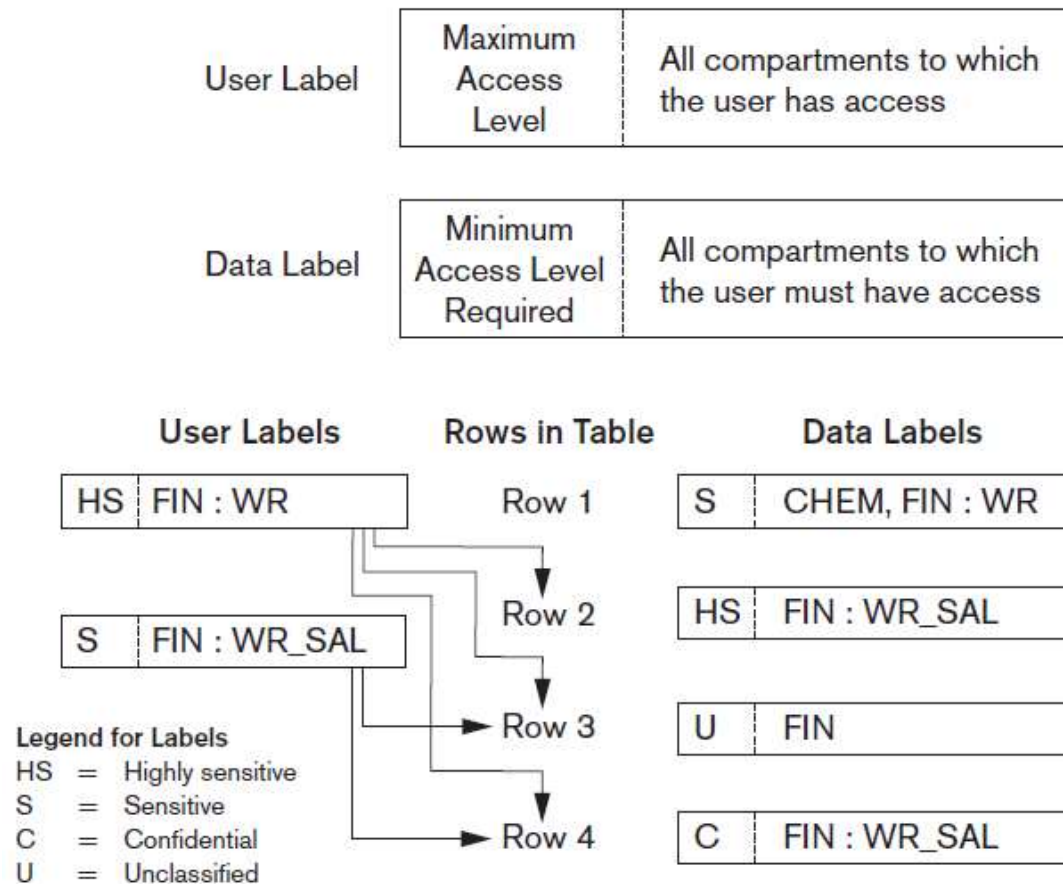


Figure 30.5 Data labels and user labels in Oracle. Data from: Oracle (2007)

# 30.11 Summary

- Threats to databases
- Types of control measures
  - Access control
  - Inference control
  - Flow control
  - Encryption
- Mandatory access control
- SQL injection
- Key-based infrastructures