Computer Security

Tuan M. Nguyen & Van K. Nguyen

Database Security

Content

- Introduction to Databases
- Security Requirements
- Database Security Levels
- Reliability and Integrity
- Attacks against database

Introduction to Databases

- Database – collection of *data* and set of *rules* that organize the data by specifying certain relationships among the data.
- Database administrator (DBA)
- Database management system (DBMS) – database manager

Introduction to Databases

- Records – contain related group of data
- Fields – elementary data items
- Schema – logical structure of database
- Subschema – view into database

Name	First	Address	City	State	Zip	Airport
ADAMS	Charles	212 Market St.	Columbus	OH	43210	CMH
BENCHLY	Zeke	501 Union St.	Chicago	IL	60603	ORD
CARTER	Marlene	411 Elm St.	Columbus	OH	43210	CMH

Introduction to Databases

- **Queries**
  - Commands that retrieve, modify, add, or delete fields and records of the database
  - Most query languages are based on SQL, a structured query language.
  - SELECT NAME = ‘ADAMS’
  - SELECT (ZIP = ‘43210’) ^ (NAME = ‘ADAMS’)

Introduction to Databases

- Advantages of Using Databases
  - Shared access
  - Minimal redundancy
  - Data consistency
  - Data integrity
  - Controlled access

Security Requirements

- Physical database integrity
- Logical database integrity
- Element integrity
- Auditability
- Access control
- User authentication
- Availability

Security Requirements

- Integrity of the Database
  - Users must be able to trust the accuracy of the data values
  - Updates are performed by authorized individuals
  - Integrity is the responsibility of the DBMS, the OS, and the computing system manager
  - Must be able to reconstruct the database at the point of a failure

Security Requirements

- Element Integrity
  - Correctness or accuracy of elements
  - Field checks
  - Access control
  - Maintain a change log – list every change made to the database

Security Requirements

- Auditability & Access Control
  - Desirable to generate an audit record of all access to the database (reads/writes)
  - **Pass-through problem** – accessing a record or element without transferring the data received to the user (no reads/writes)
  - Databases separated logically by user access privileges

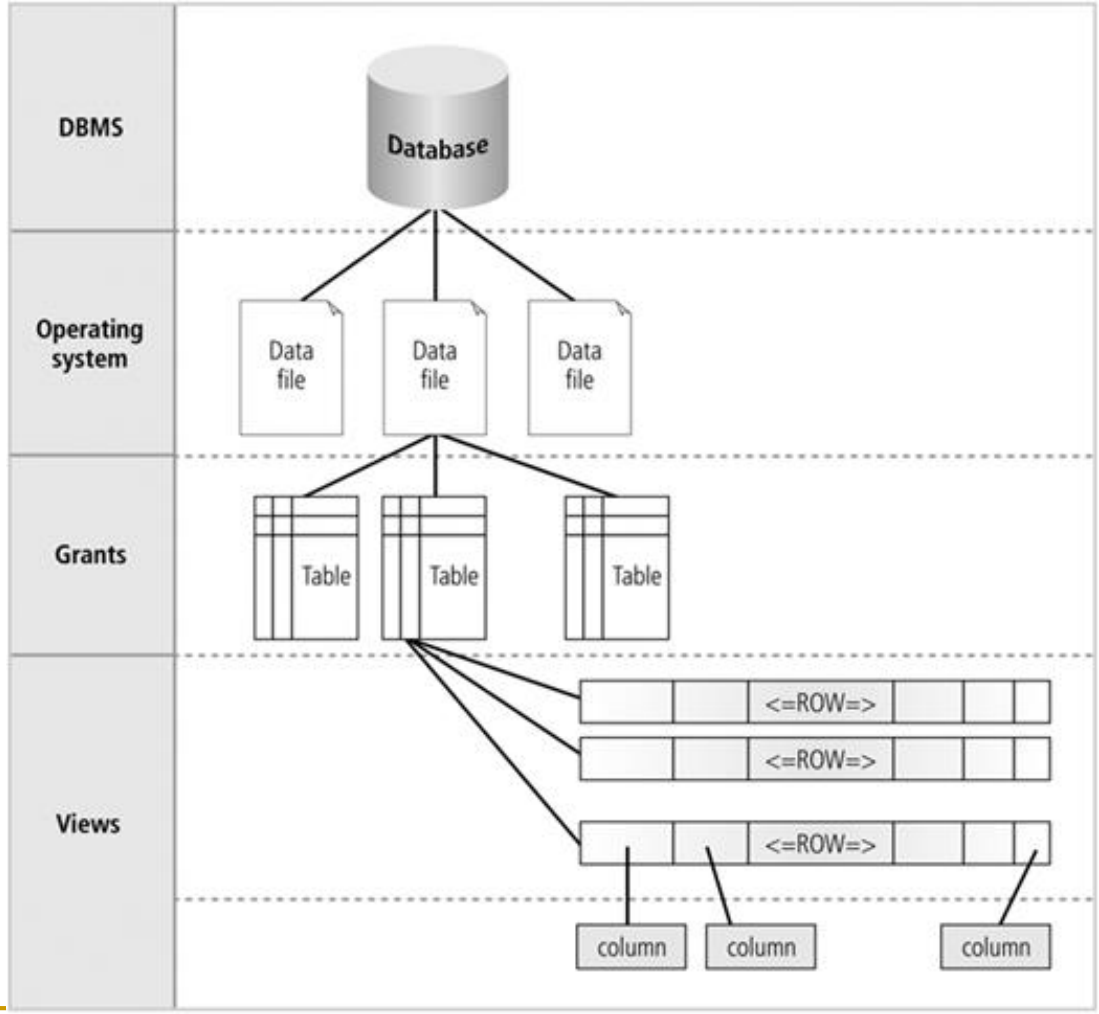
Security Requirements

- Other Security Requirements
  - User Authentication
  - Confidentiality
  - Availability

Database Security Levels

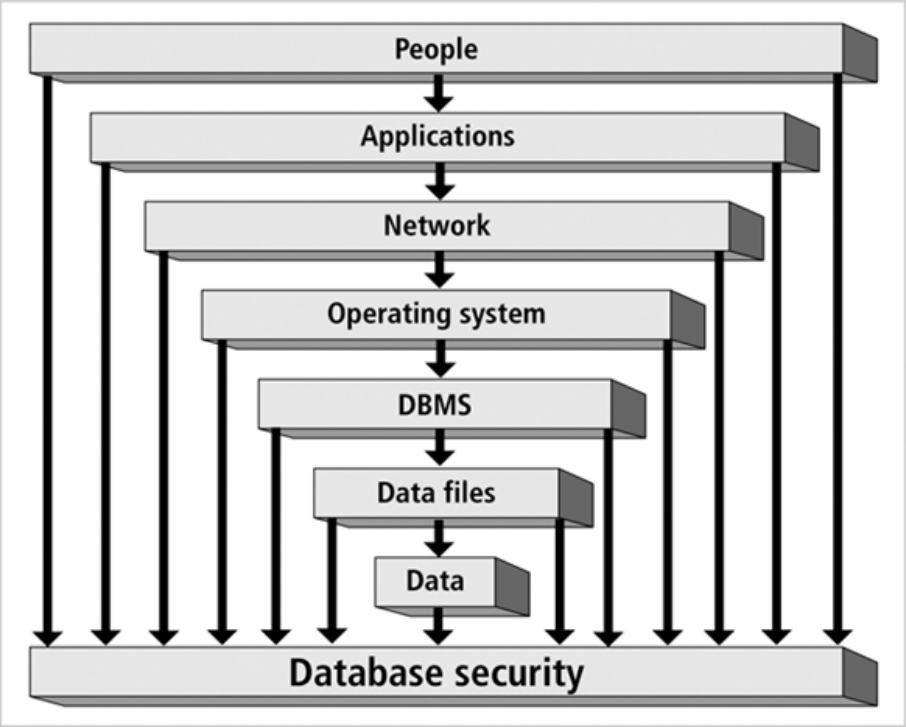
- Relational database: collection of related data files
- Data file: collection of related tables
- Table: collection of related rows (records)
- Row: collection of related columns (fields)

Database Security Levels



Menaces to Databases

- Security access point: place where database security must be protected and applied

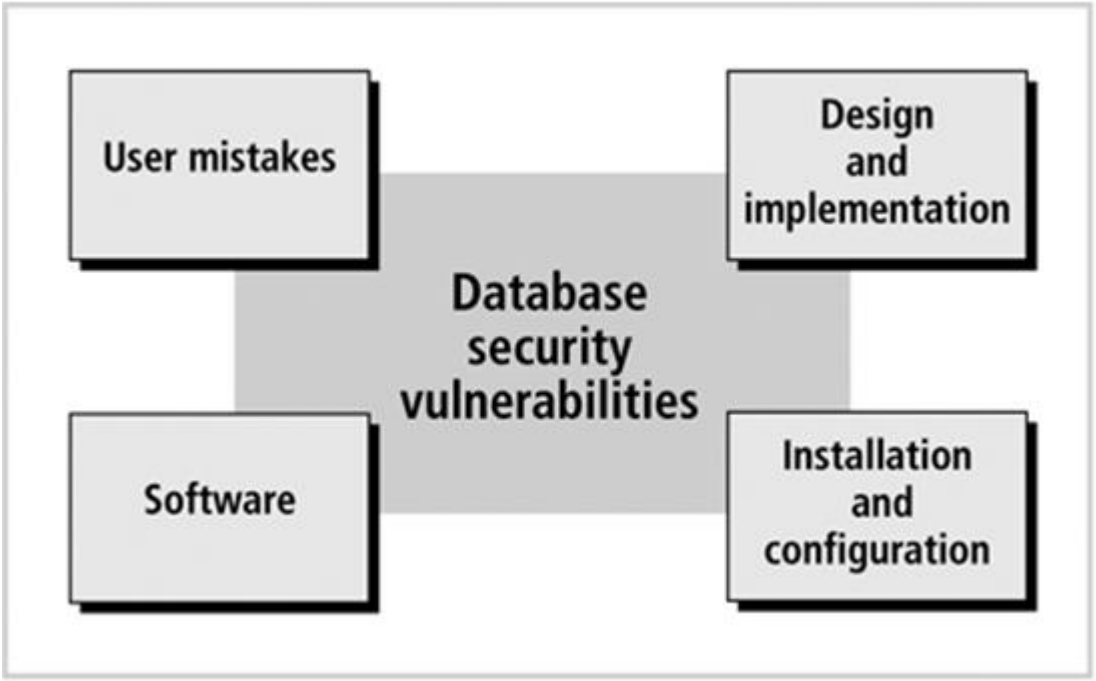


Menaces to Databases

- Security gaps: points at which security is missing
- Vulnerabilities: kinks in the system that can become threats
- Threat: security risk that can become a system breach

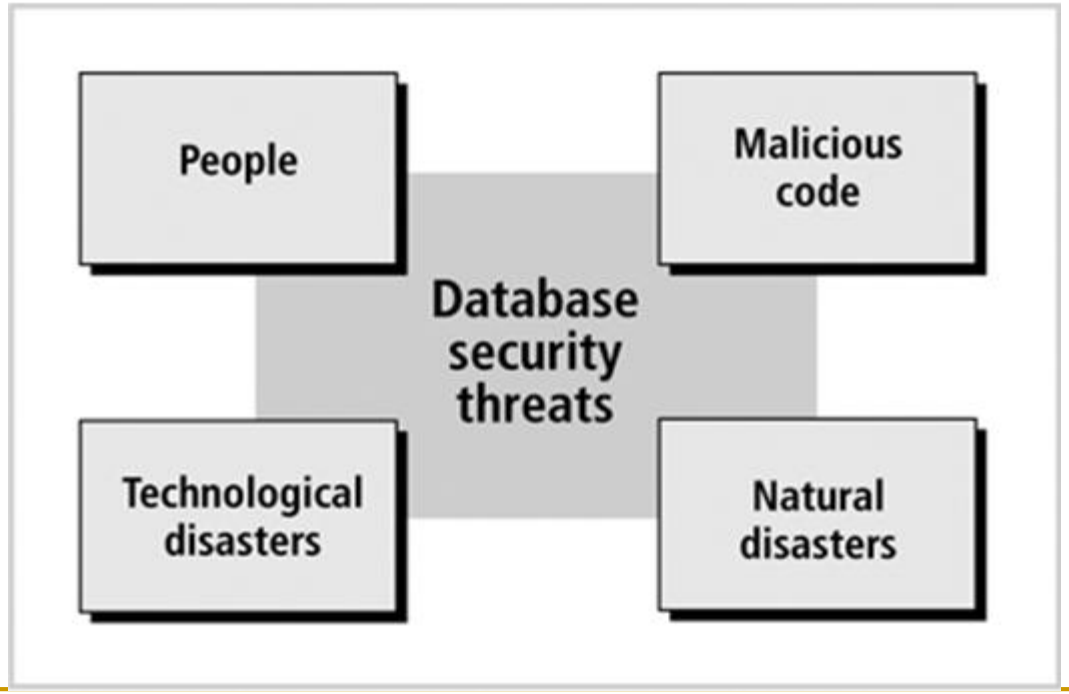
Menaces to Databases

- Security vulnerability: a weakness in any information system component



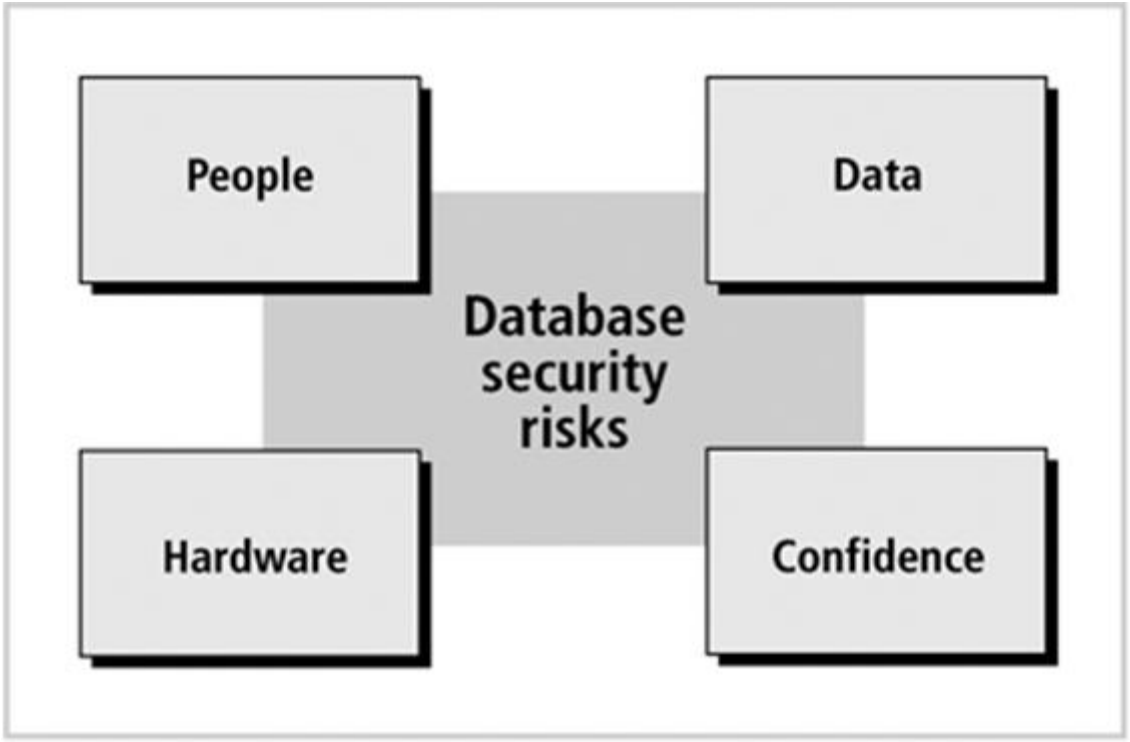
Menaces to Databases

- Security threat: a security violation or attack that can happen any time because of a security vulnerability



Menaces to Databases

- Security risk: a known security gap intentionally left open



Reliability and Integrity

- Database concerns
  - Database integrity
  - Element integrity
  - Element accuracy
- Some protection from OS
  - File access
  - Data integrity checks

Reliability and Integrity

- Two-Phase Update
  - Failure of computing system in middle of modifying data
  - Intent Phase – gather resources needed for update; write **commit flag** to the database
  - Update Phase – make permanent changes

Reliability and Integrity

- Redundancy / Internal Consistency
  - Error detection / Correction codes (parity bits, Hamming codes, CRCs)
  - Shadow fields
  - Log of user accesses and changes

Reliability and Integrity

- Concurrency/Consistency
  - Access by two users sharing the same database must be constrained (lock)
  - Monitors –check entered values to ensure consistency with rest of DB
  - State Constraints – describes condition of database (unique employee #)
  - Transition Constraints – conditions before changes are applied to DB

Reliability and Integrity

- Access control
  - Physical access
  - Access control techniques
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)
    - Role Based Access Control (RBAC)
- Identification and authentication
- Authorization
- Accountability

Attacks against database

- **Inference Attack**
  - Data mining technique performed by analyzing data in order to illegitimately gain knowledge about a subject or database Identification and authentication
- **SQL injection**
  - Code injection technique that exploits a security vulnerability occurring in the database layer of an application.

Attacks against database

- Inference Attack
  - Direct Attack: tries to determine values of sensitive fields by seeking them directly with queries that yield few records
    - List NAME where SEX=M ^ DRUGS=1
    - List NAME where (SEX=M ^ DRUGS=1) v (SEX#M ^ SEX#F) v (DORM=AYRES)

Attacks against database

- Inference Attack
  - Sum
    - Show STUDENT-AID WHERE SEX=F ^ DORM=Grey
  - Count
    - Show Count, STUDENT-AID WHERE SEX=M ^ DORM=Holmes
    - List NAME where (SEX=M ^ DORM=Holmes)
  - Median
  - Tracker Attacks – using additional queries that produce small results

Attacks against database

- Inference Attack - Controls
  - Suppression – don't provide sensitive data
  - Concealing – don't provide actual values
  - Limited Response Suppression
  - Combined Results
    - Sums
    - Ranges
    - Rounding
  - Query Analysis – "should the result be provided"

Attacks against database

- SQL Injection
  - Incorrectly filtered escape characters
    - SELECT * FROM users WHERE name = 'a' OR 't'='t';
  - Incorrect type handling
    - statement := "SELECT * FROM data WHERE id = " + **a_variable** + ";"
    - SELECT * FROM DATA WHERE id=**1;DROP TABLE users**;
  - Vulnerabilities inside the database server

Attacks against database

- SQL Injection - preventing
  - Parameterized statements
    - Enforcement at the database level
    - Enforcement at the coding level
  - *escape* dangerous characters
    - Check user's inputs

Sumary

- Database security: degree to which data is fully protected from tampering or unauthorized acts
- Enforce security at all database levels
- Data requires highest level of protection: data access point must be small


Thank you