
Data Security
and
Integrity

Contents

- Introduction
- Database Security In General
  - Information System
  - Information / Data Security
- Information Security Triangle
- Information Security Architecture
- Database Security
  - Security Levels
  - Dangers for Databases
  - Security Methods

Contents

- Database Security Methodology
- Security Layers in DBMS
  - Authentication
  - Authorization
  - Views and Data Security
  - Virtual Private Database
- Data Auditing

Introduction

- In the modern era of information security violation and attacks increased on each day.
- For data security we need to implement more strict policies in a way our business operations not blocked and execute smoothly.

Security Measures:

- Prevent the physical access to the servers where data reside.
- Implement operating system operations in more secure way.
- Implement security models that enforce security measures.
- DBA should implement the security polices to protect the data.

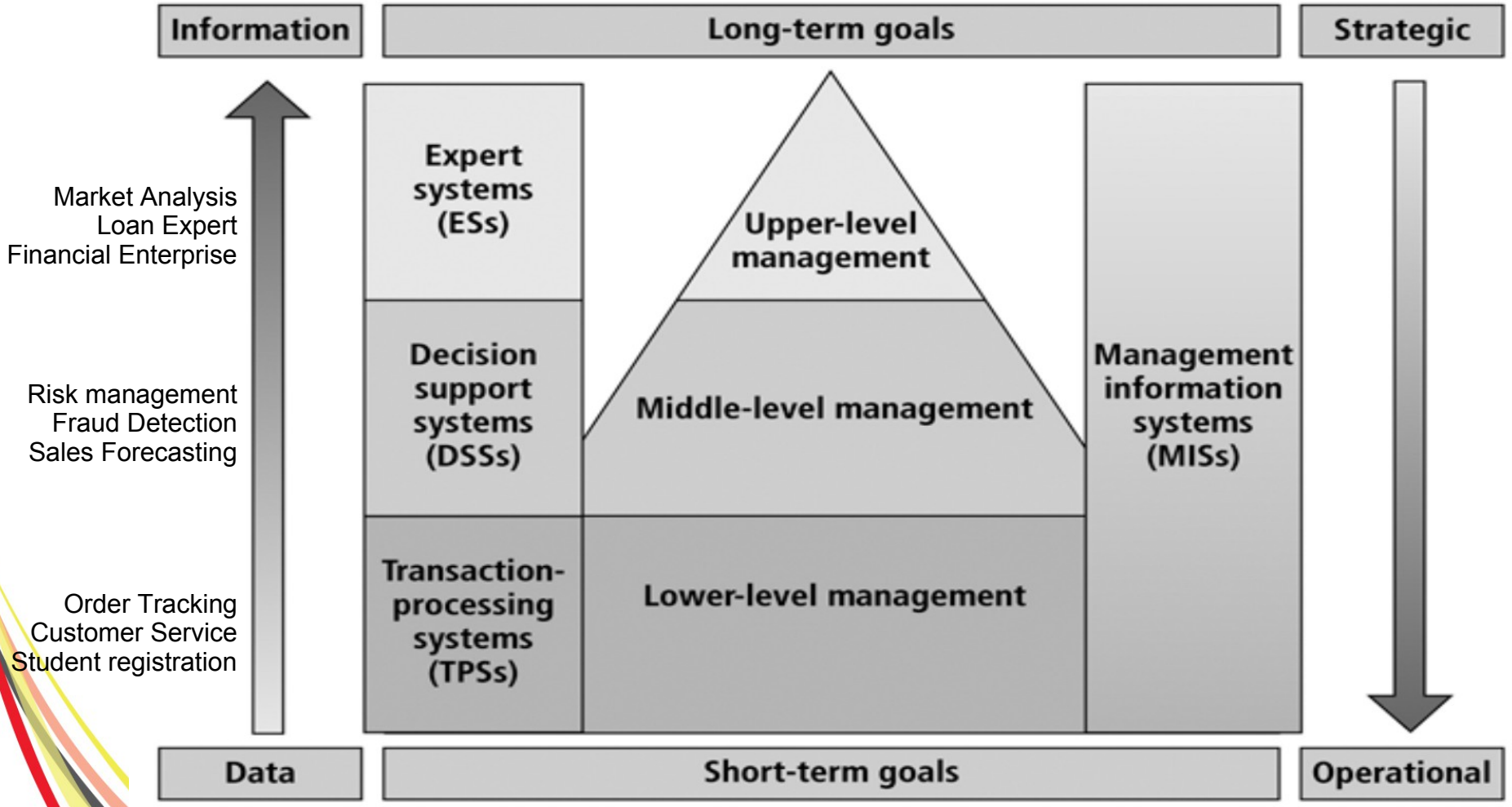
Database Security In General

- Degree to which data is fully protected from tampering or unauthorized acts.
- Comprises **information system** and **information security** concepts.

Information System

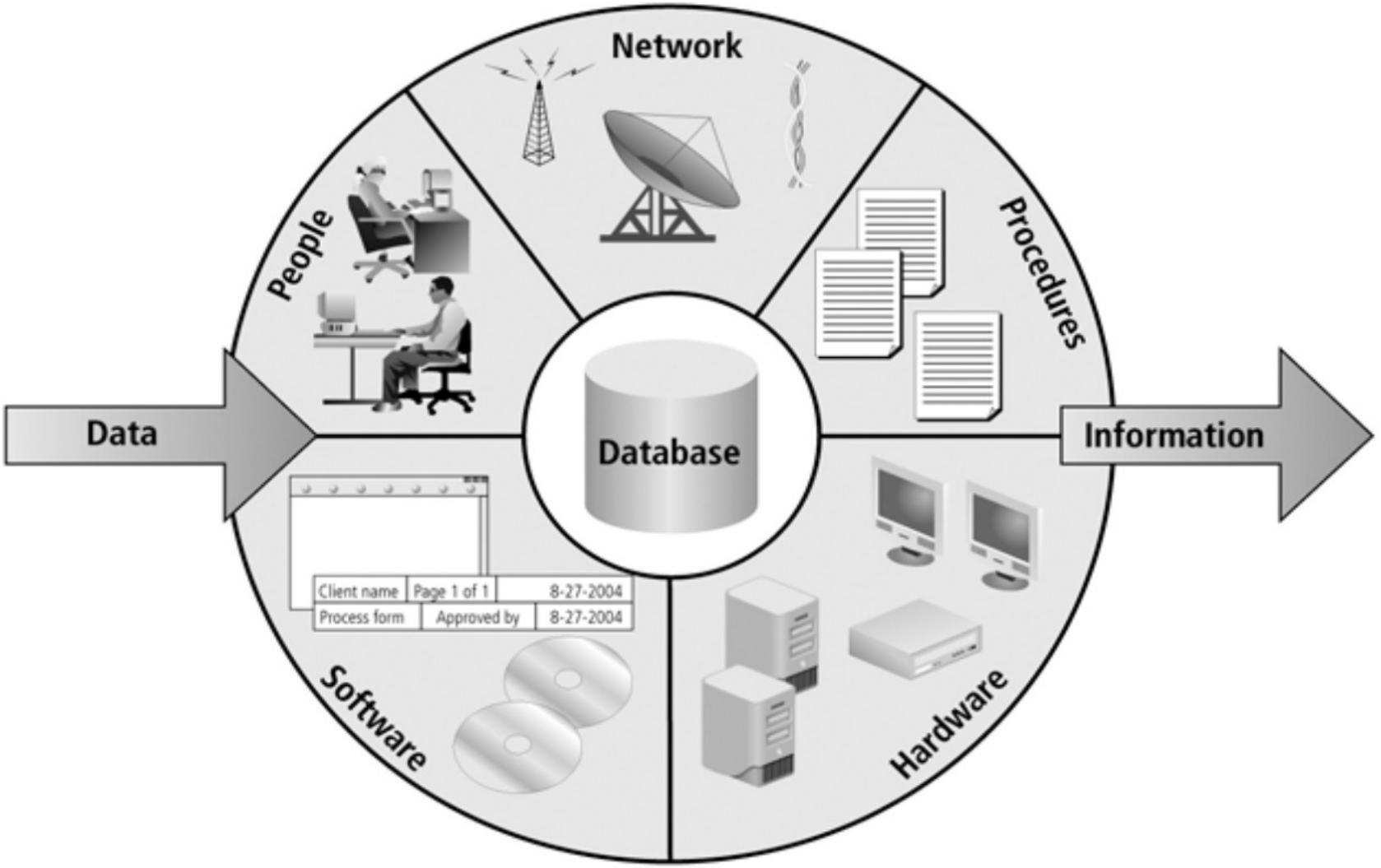
- Information system (IS) comprised of components working together to produce and generate accurate information.
- In IS wise decisions require
  - Accurate and timely information
  - Information integrity
- IS categorized based on usage as
  - Low-level
  - Mid-level
  - High-level

Information System ...



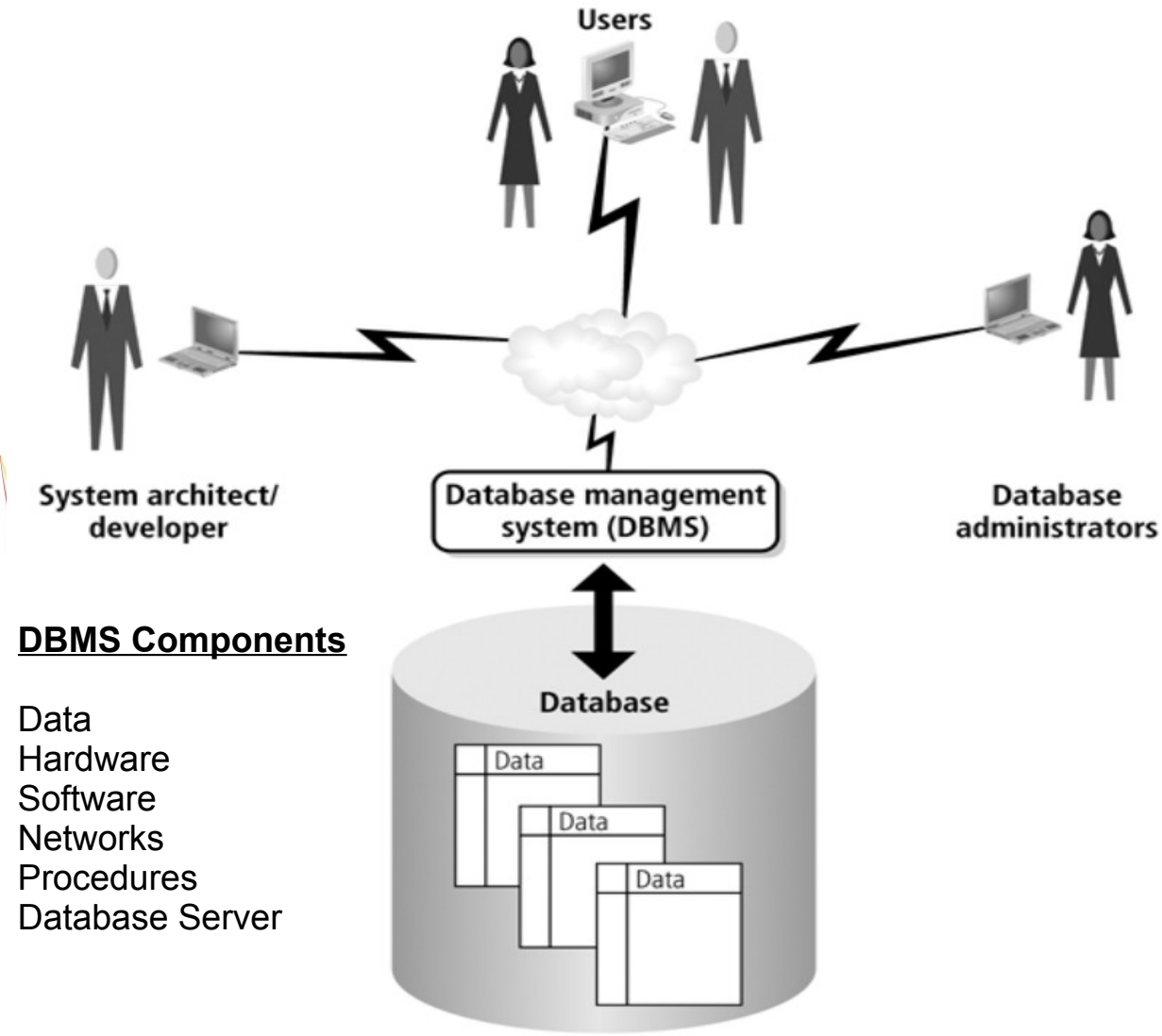
Typical use of system applications at various management level

Information System ...



Information System Components

Database and DBMS Environment



DBMS Components

Data
Hardware
Software
Networks
Procedures
Database Server

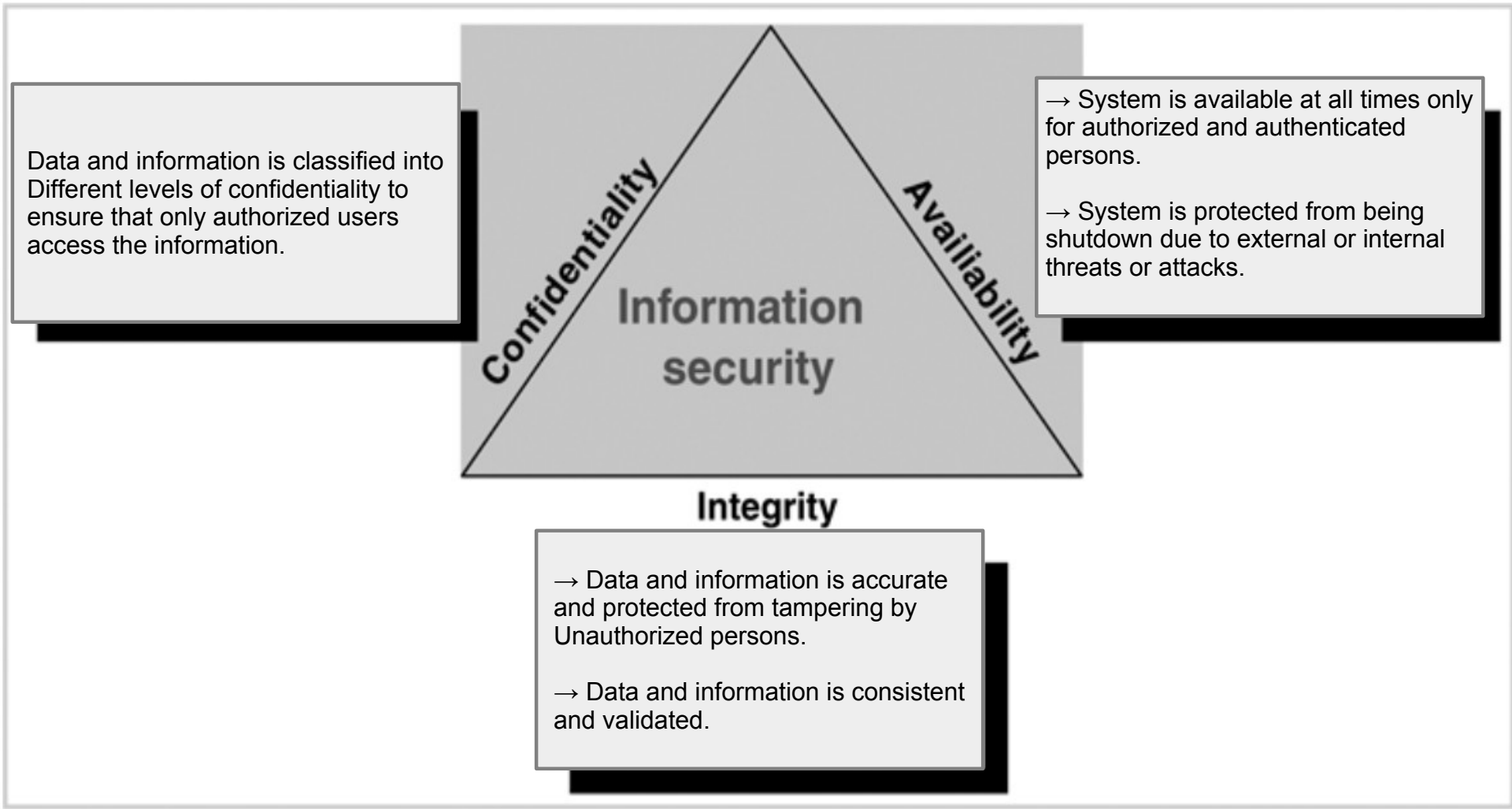
DBMS Functions

Organize data
Store and retrieve data efficiently
Manipulate data (update and delete
Enforce referential integrity and consistency
Enforce and implement data security policies and procedures
Back up, recover, and restore data
Data security …..

Information / Data Security

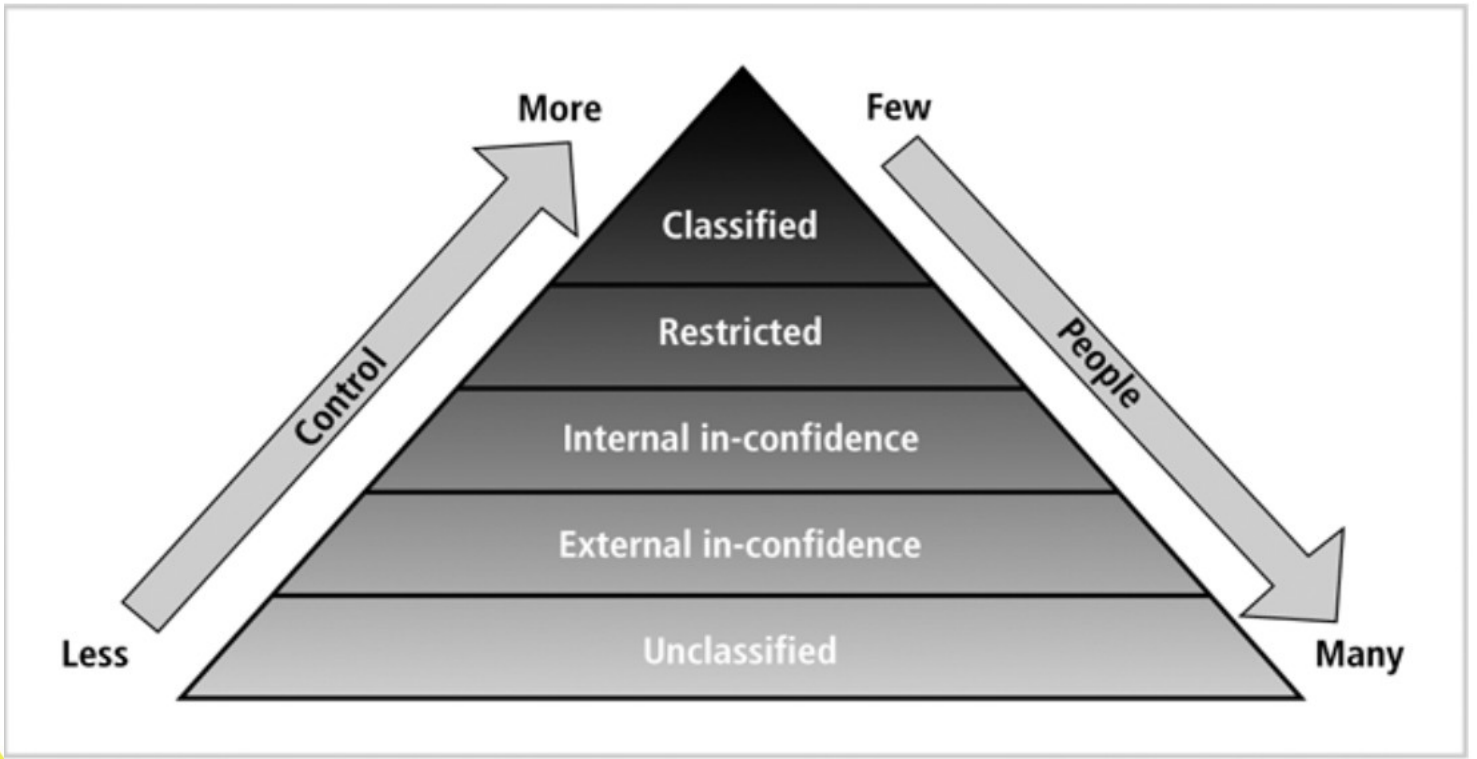
- Information / data is one of the most valuable asset for any organization.
- Its security consist of procedures and measures taken to protect information systems components.

Information Security Triangle



Information Security C.I.A Triangle

Confidential Classification (CIA Triangle)



Integrity (CIA Triangle)

- **Data Integrity** refers to the overall completeness, accuracy and consistency of **data**.
- Integrity has two types physical and logical.
- **Physical integrity:** Physical integrity deals with challenges associated with correctly storing and fetching the data itself.
  - Challenges: electromechanical faults, physical design flaws, natural disasters etc.
- **Logical Integrity: C**oncerned with referential integrity and entity integrity in a relational database
  - Challenges: software bugs, design flaws, and human errors.

Integrity by Example (CIA Triangle)

Employee A learns that his similar designation coworker is earning higher salary then he is. Employee A get this information through the access of an application program by accounting dept and manipulates the vacation hours and overtime hours of his colleague.

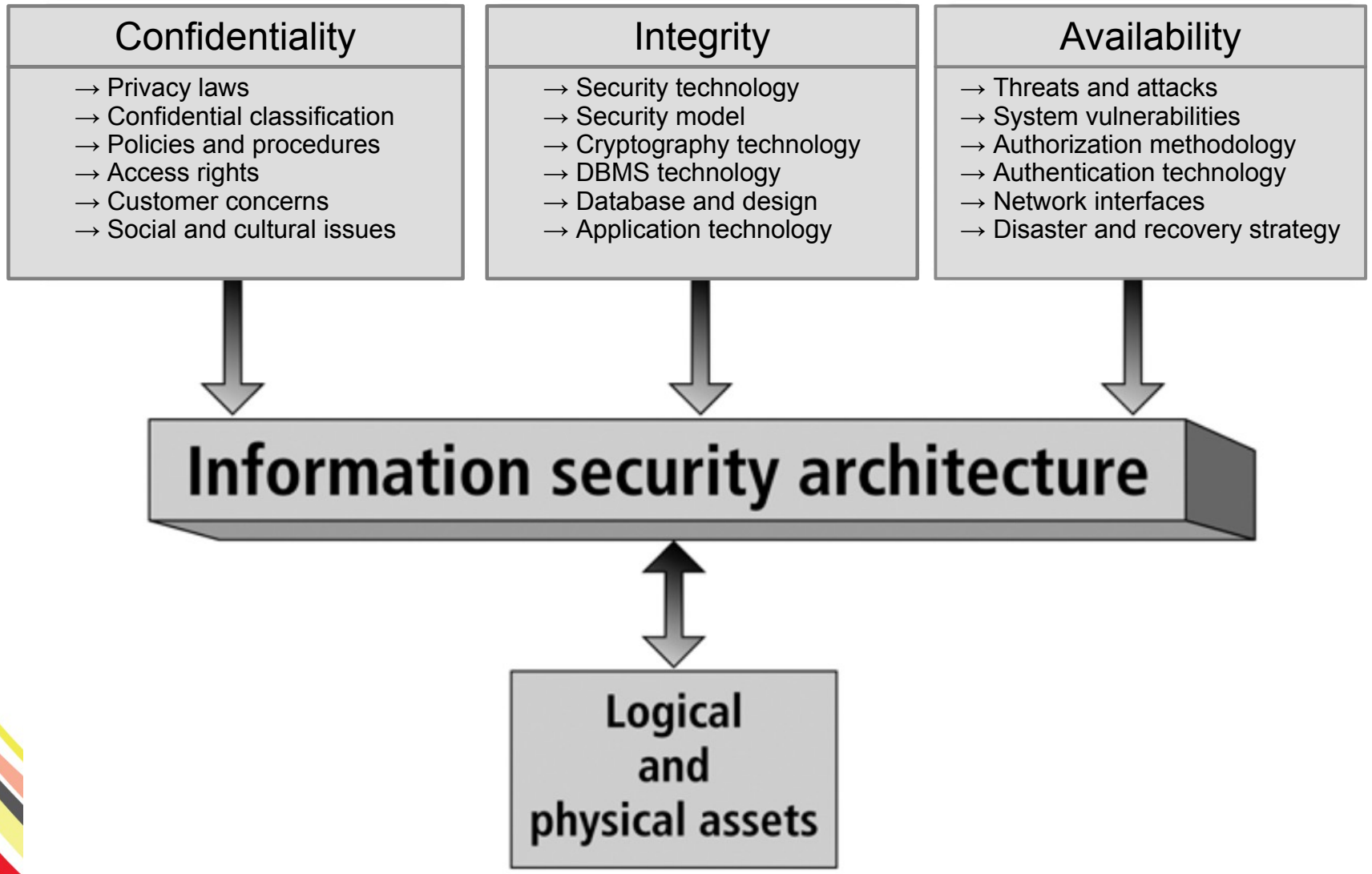
Two security violations:

- Confidential data is disclosed inappropriately.
- An application to modify data was access inappropriately.

Availability (CIA Triangle)

- Systems must be always available to authorized users.
- Systems determines what a user can do with the information.
- System might not be visible in some conditions.

Information Security Architecture

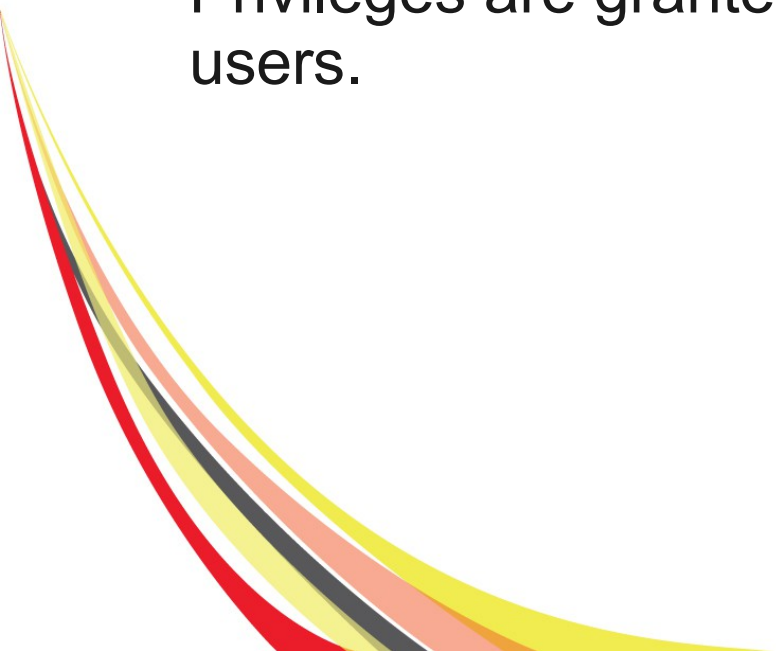


Database Security

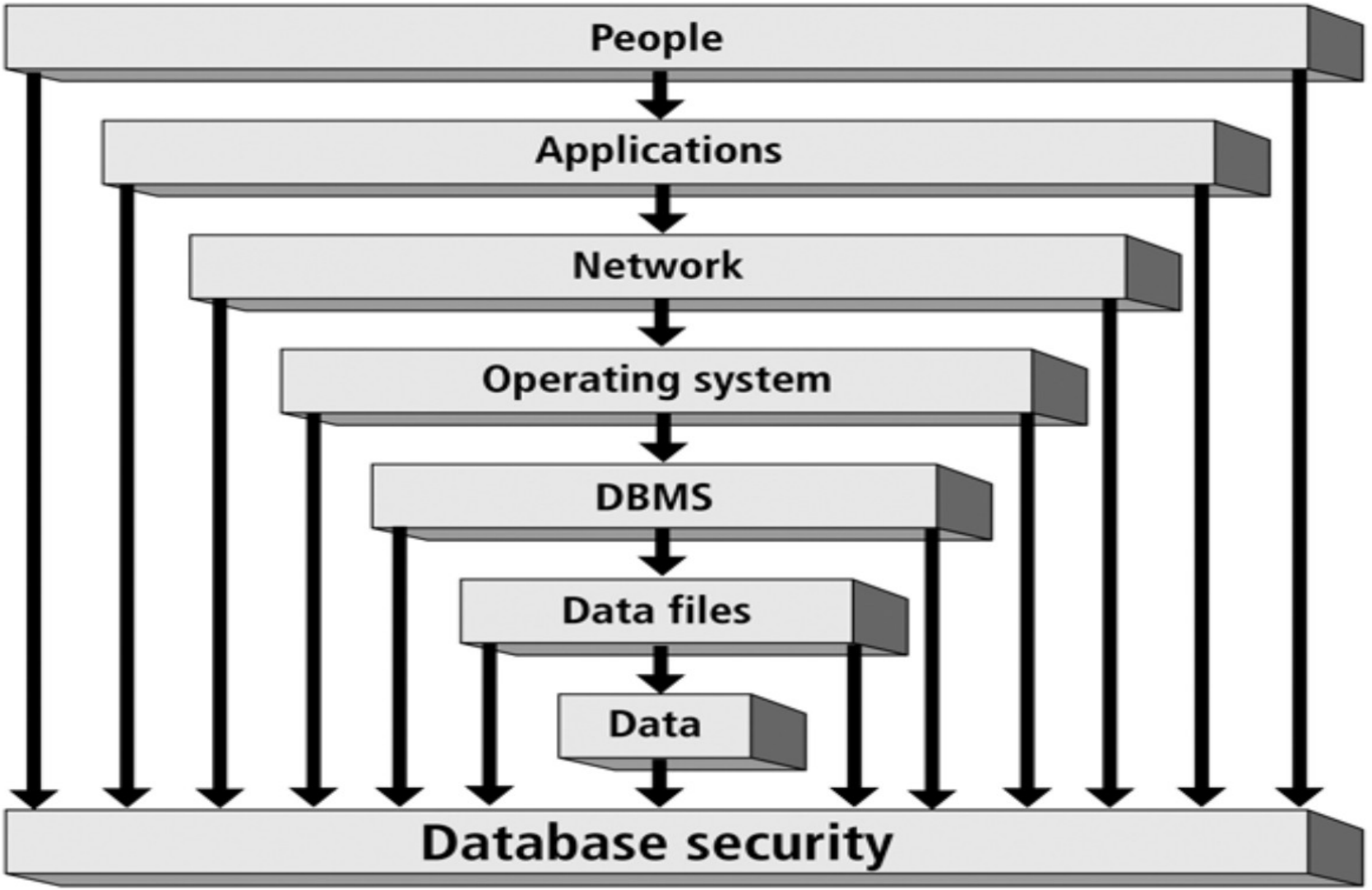
Database security entertain allowing or disallowing user actions on the database and the objects within it.

DMBS contains Discretionary access control regulates all user access to named objects through privileges.

A privilege is permission to access a named object in a prescribed manner; for example, permission to query a table. Privileges are granted to users at the discretion of other users.

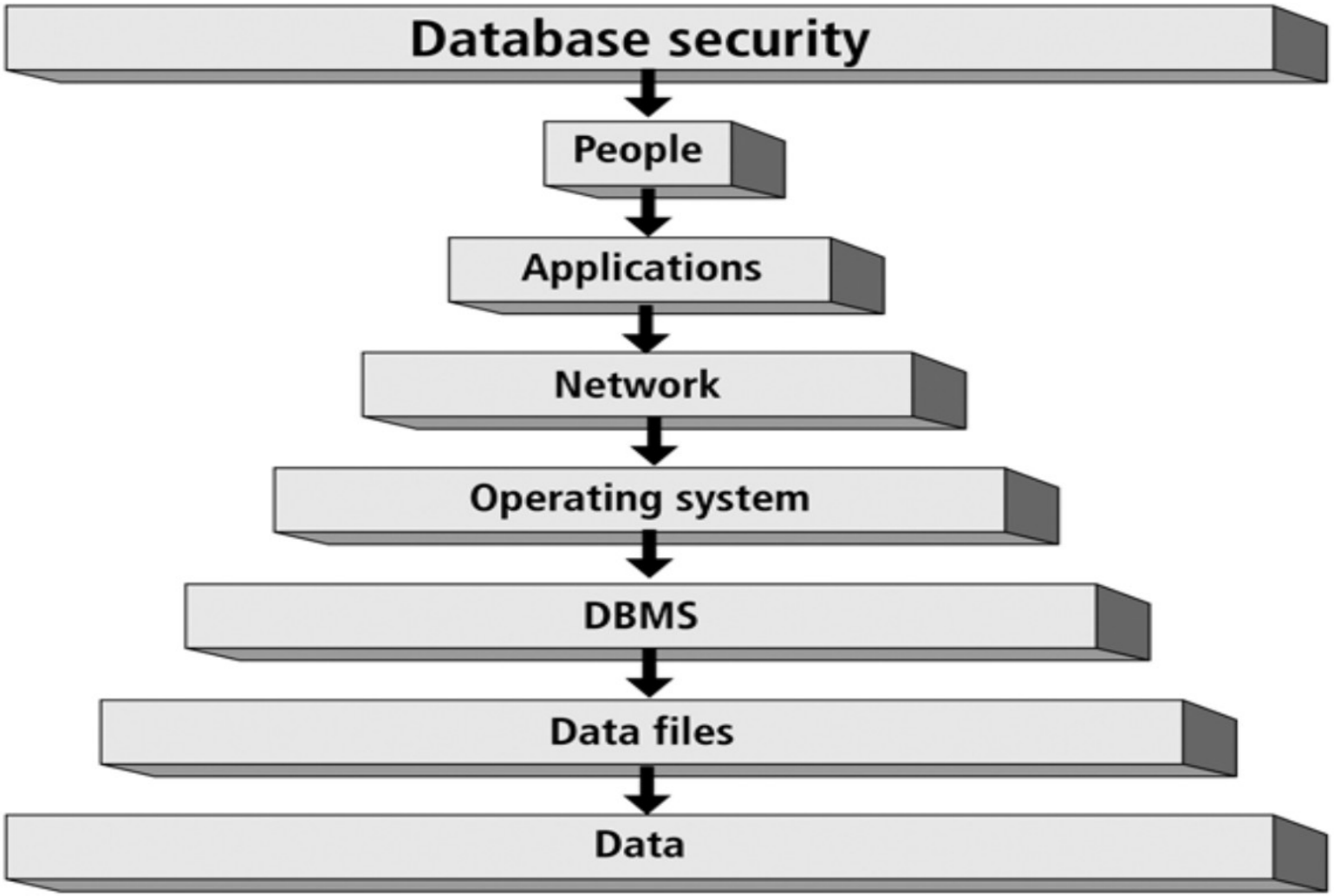


Database Security ...



Database Security Access Points

Database Security ...



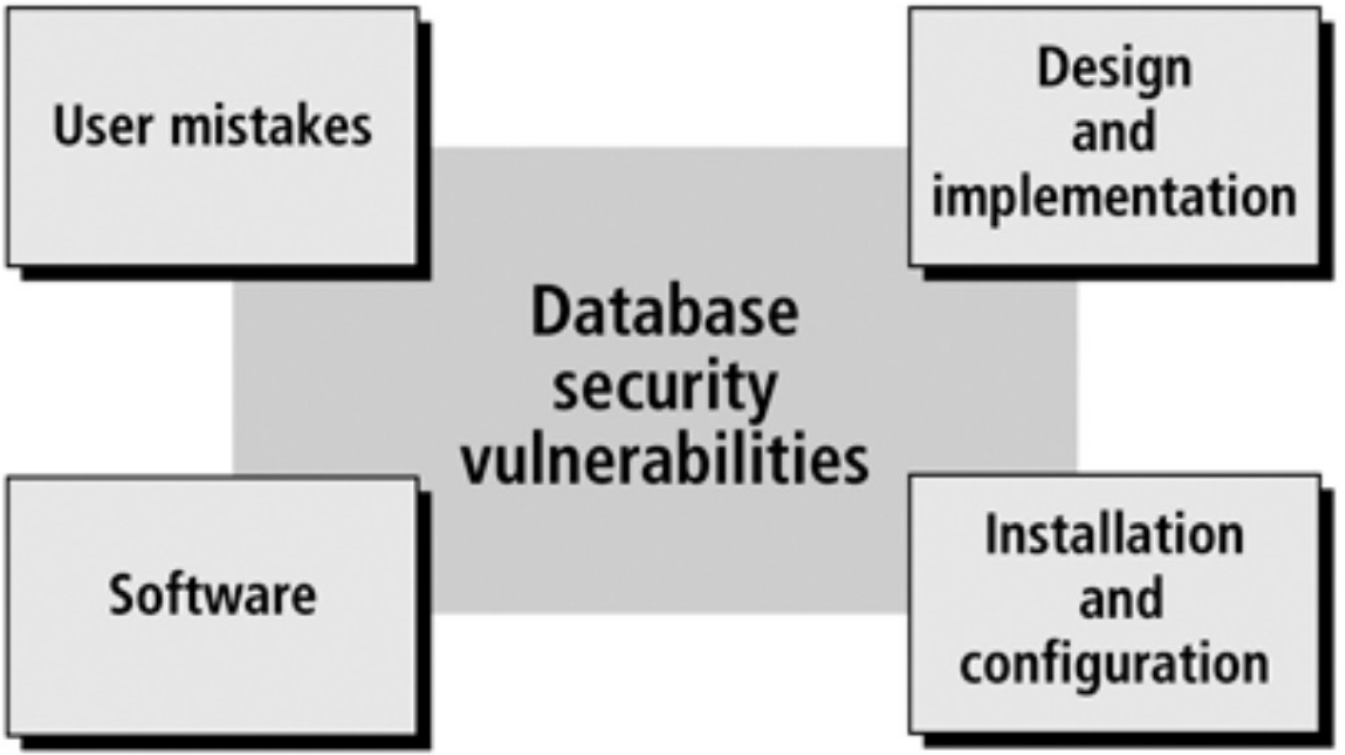
Security Levels

- **Database System:** Since some users may modify data while some may only query, it is the job of the system to enforce authorization rules.
- **Operating System:** No matter how secure the database system is, the operating system may serve as another means of unauthorized access.
- **Network:** Since most databases allow remote access, hardware and software security is crucial.
- **Physical:** Sites with computer systems must be physically secured against entry by intruders or **terrorists**.
- **Human:** Users must be authorized carefully to reduce the chance of a user giving access to an intruder.

Data Integrity Violation

Dangers for Databases

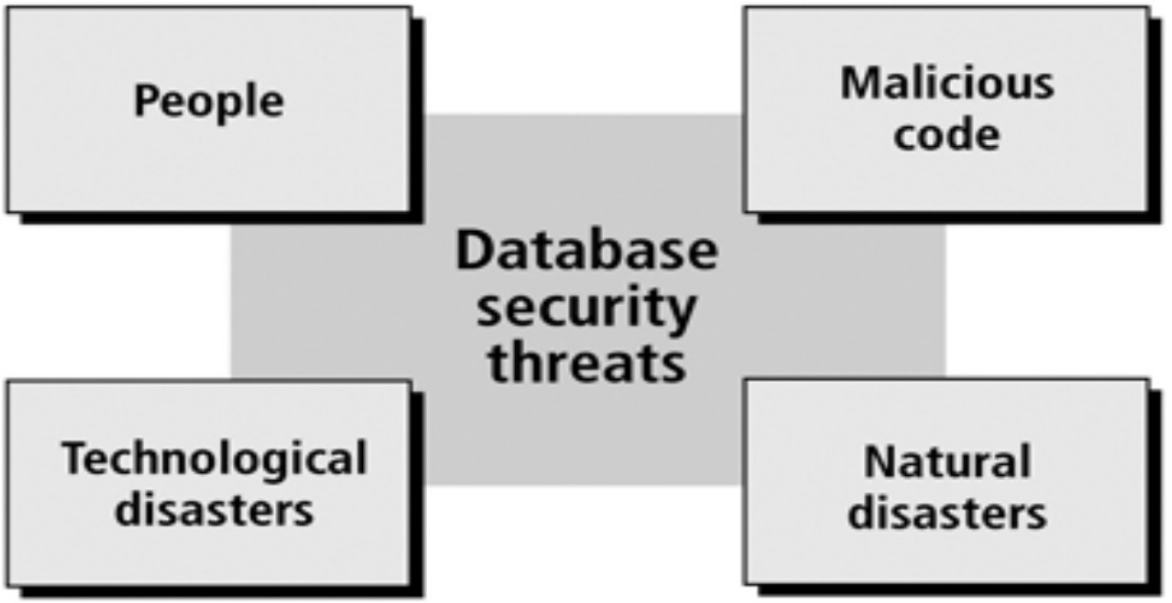
Security vulnerability: a weakness in any information system component.



Categories of Security Vulnerabilities

Dangers for Databases ...

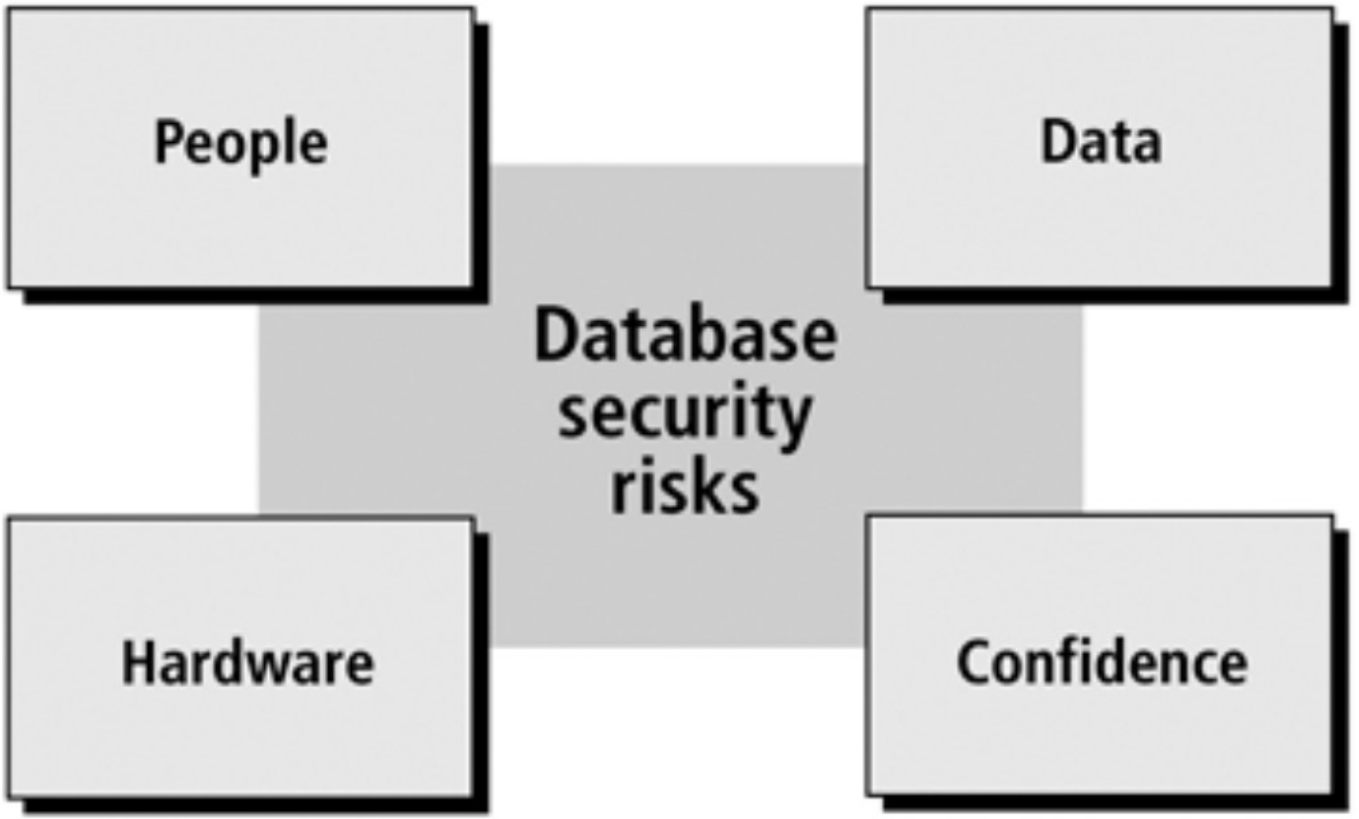
Security threat: a security violation or attack that can happen any time because of a security vulnerability.



Categories of Security Threats

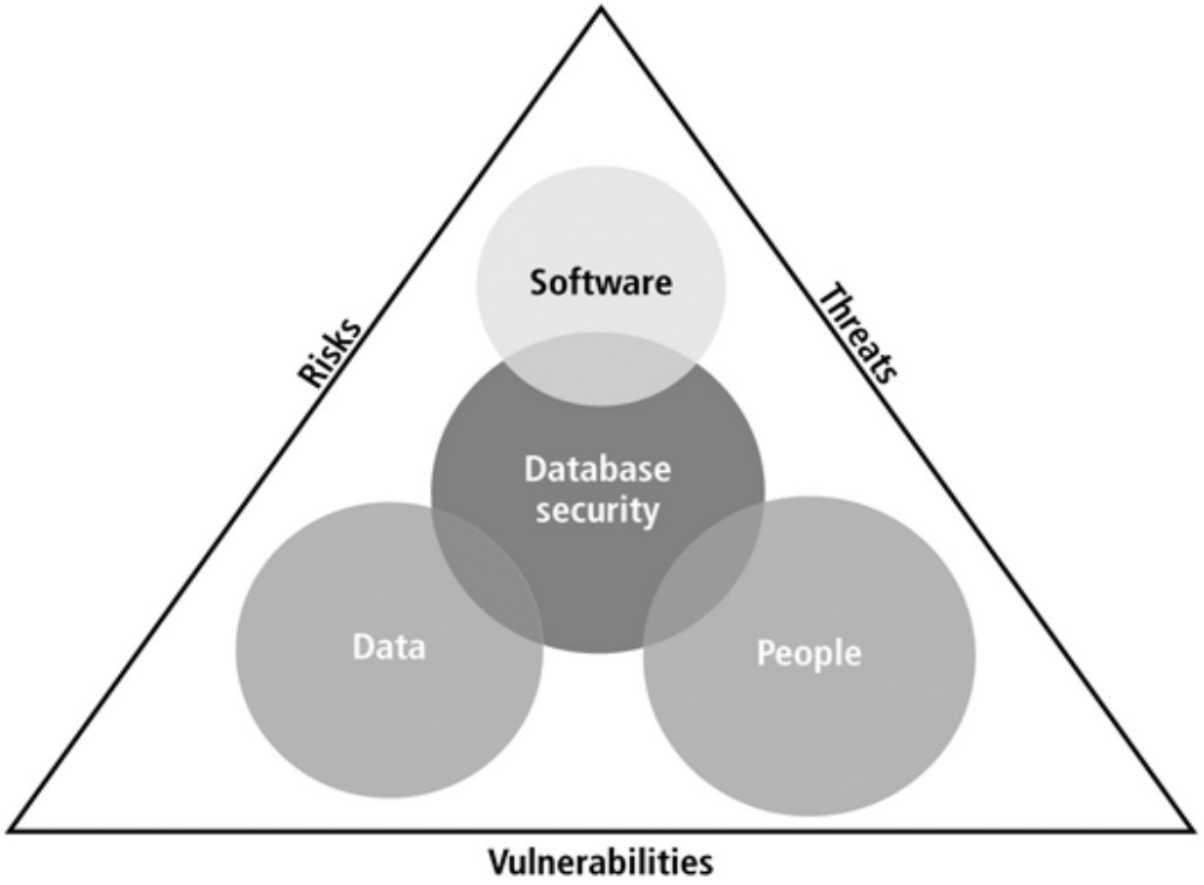
Dangers for Databases ...

Security risk: a known security gap left open.



Categories of Security Risks

Dangers for Databases...



Integration of Security Vulnerabilities, Risks and Threats in Database Environment

Security Methods

Database Component Protected	Security Method
People	• Physical limit to access hardware and documents. • Through the process of identification and authentication make sure right user is going to access the information • Conduct training courses on the Importance of security and how to guard assets • Establishment of security policies and procedures.
Applications	• Authentication of users who access the application. • Apply business rules. • A Single sign on

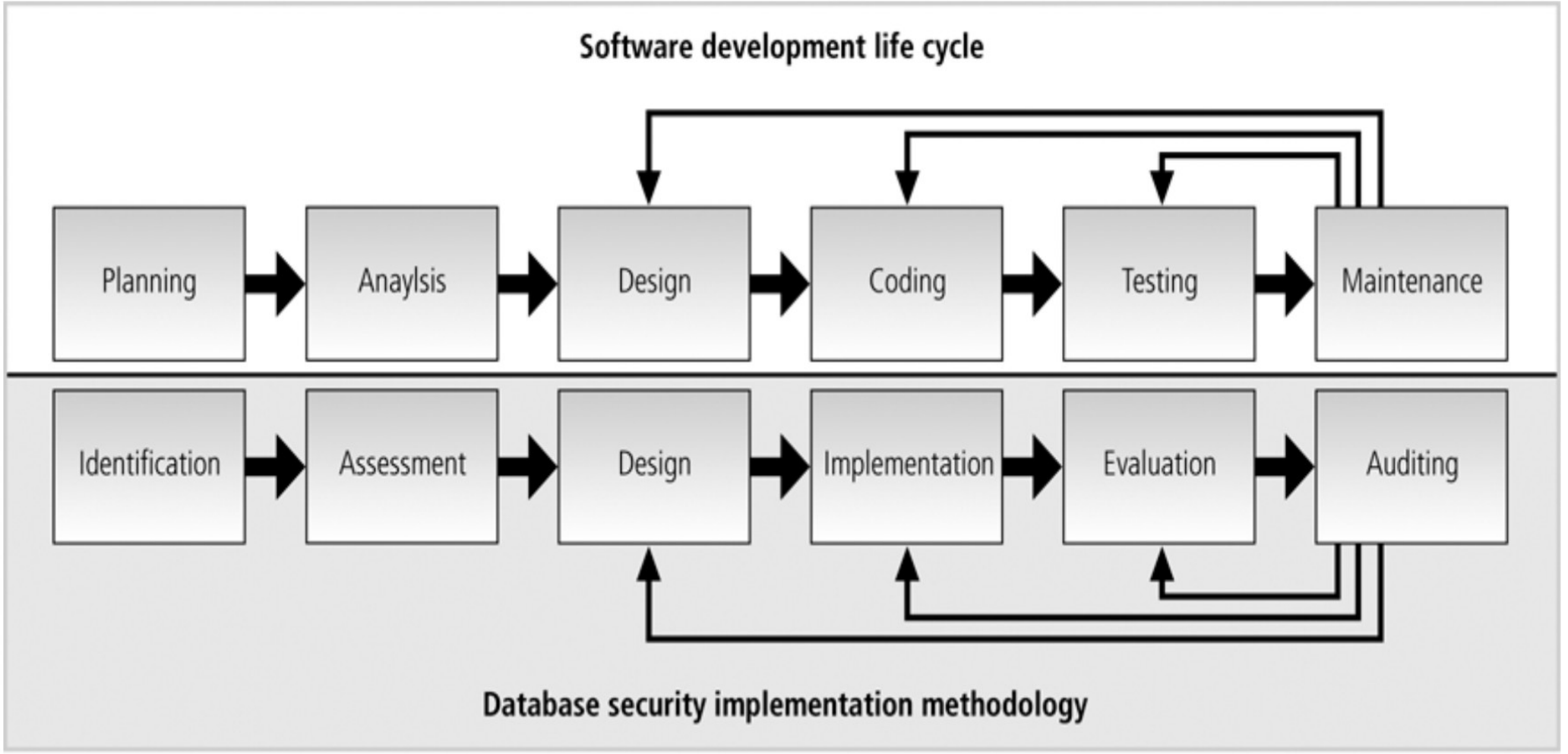
Security Methods ...

Database Component Protected	Security Method
Network	• Network firewall to block the intruders. • VPN • Network Authentication
Operating System	• Authentication • Password policy • User accounts
DBMS	• Authentication • Audit mechanism • Database resource limits • Password policy • Data encryption
Data Files	• Files / Folder permissions • Access monitoring

Security Methods ...

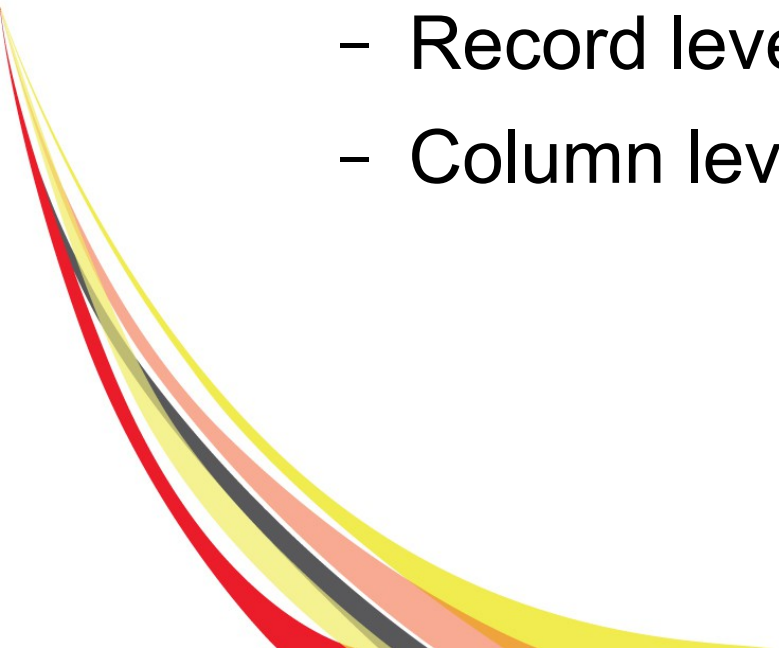
Database Component Protected	Security Method
Data	• Data Validation • Data constraints • Data Encryption • Data Access

Databases Security Methodology



Security Layers in DBMS

- Authentication
- Authorization
  - Data File level
  - Database level
  - Table level
  - Record level
  - Column level

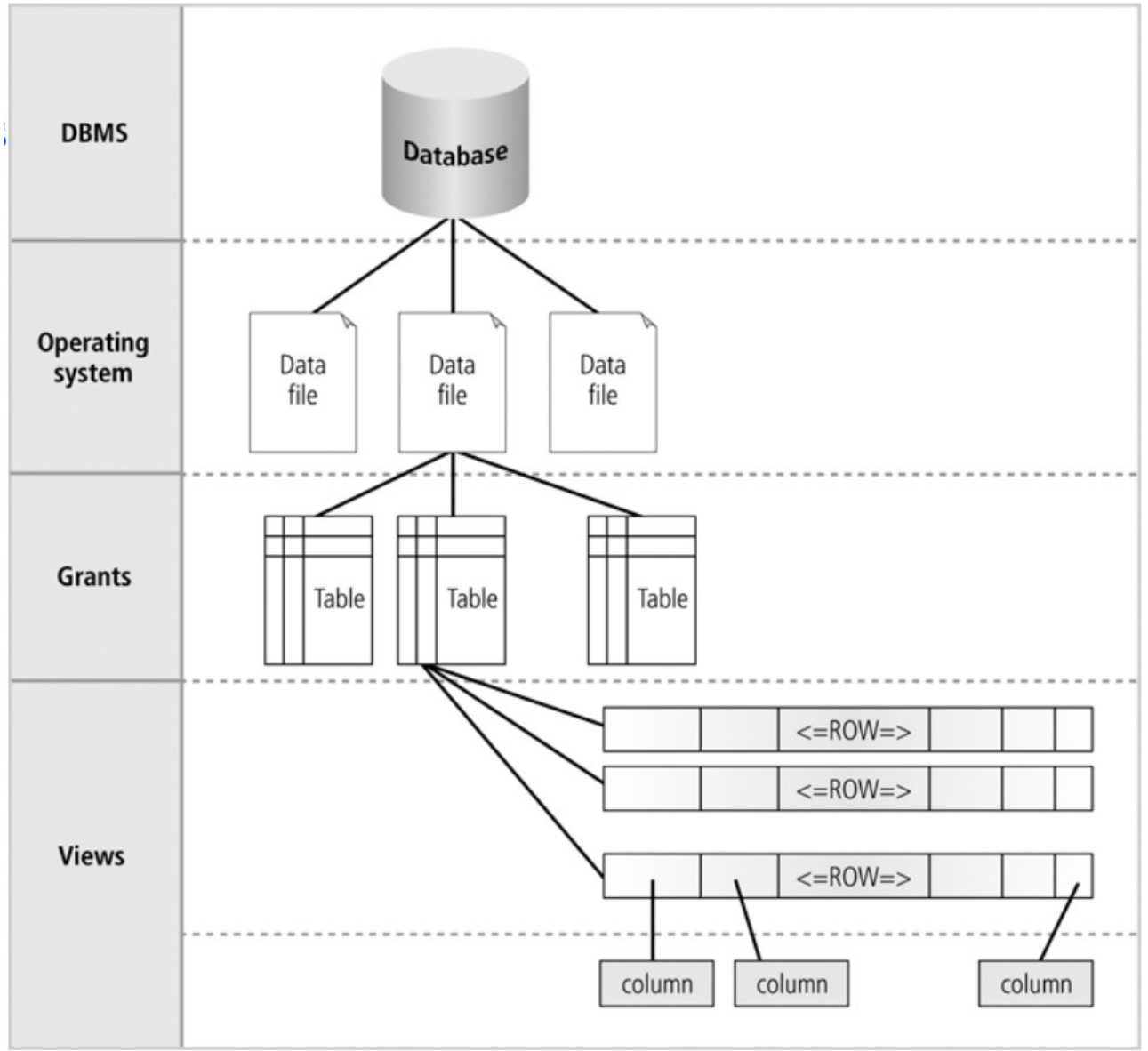


Security Layers in DBMS ...

By Database Management System through username and password

Through Files Permissions

Schema owners/security administrator grant or revoke privileges



Overview of Authentication Methods

Several DBMS support different user authentication method for security purpose. Some of the authentication methods are..

Authentication by the Operating System: Once user authenticated by the operating system, users can connect to database more conveniently, without specifying a user name or password. (e.g. In EDB/Postgres peer/ident authentication method use for this purpose).

Password Authentication: Users are created with some password in database and after assignment of some set of privileges register user can communicate with DBMS.

Overview of Authentication Methods ...

Trust Authentication: Registered user can connect with database and perform operations as per authority on different objects.

Overview of Authentication Methods ...

Authentication by the Network: In network base authentication scheme there are three branches

1. Third Party-Based Authentication Technologies:

If network authentication services are available to you (such as DCE, Kerberos, or SESAME), Oracle Database can accept authentication from the network service.

2.Certificate Authentication: This authentication method uses SSL client certificates to perform authentication. It is therefore only available for SSL connections. When using this authentication method, the server will require that the client provide a valid certificate. No password prompt will be sent to the client.

Overview of Authentication Methods ...

3. Remote Authentication

Oracle Database supports remote authentication of users through Remote Dial-In User Service (RADIUS), a standard lightweight protocol used for user authentication, authorization, and accounting.

Authorization

- For security purposes, we may assign a user several forms of authorization on parts of the databases which allow:
  - Read: read tuples.
  - Insert: insert new tuple, not modify existing tuples.
  - Update: modification, not deletion, of tuples.
  - Delete: deletion of tuples.
- We may assign the user all, none, or a combination of these.

Authorization ...

In addition to the previously mentioned, we may also assign a user rights to modify the database schema:

Index: allows creation and modification of indices.

Resource: allows creation of new relations.

Alteration: addition or deletion of attributes in a tuple.

Drop: allows the deletion of relations.

In SQL DCL used for authorization assignments on different database objects

DCL and Authorization

- DCL commands are used to enforce database security in a multiple database environment.
- Two types of DCL commands are
  - Grant
  - Revoke
- Database Administrator's or owner's of the database object can provide/remove privileges on a database object through Grant and Revoke in RDMS.

DCL and Authorization

- GRANT Syntax

  GRANT privilege_name ON object_name

  TO {user_name | PUBLIC | role_name}
  [with GRANT option];

- Here, privilege_name: is the access right or privilege granted to the user.
- object_name: is the name of the database object like table, view etc.,.
- user_name: is the name of the user to whom an access right is being granted.
- Public is used to grant rights to all the users.
- With Grant option: allows users to grant access rights to other users.

DCL and Authorization

- REVOKE Syntax:

  REVOKE privilege_name ON object_name

  FROM {User_name | PUBLIC | Role_name}

- For Example:

  GRANT SELECT ON employee TO user1

- This command grants a SELECT permission on employee table to user1.

  REVOKE SELECT ON employee FROM user1

- This command will revoke a SELECT privilege on employee table from user1.

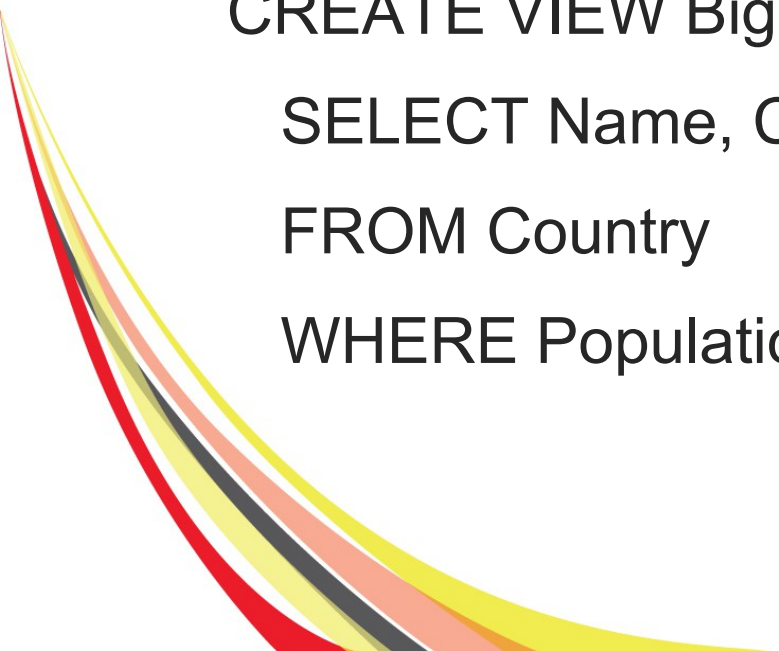
Views and Data Security

- Views can serve as security mechanism by restricting the data available to users. Through views you can restrict users on limited columns and give the rights to specific users.
- Example: Table emp contains employee salaries which should not visible to all users and all user can read the data other then salary.
  - Emp (id, name, address, designation, salary)
  - Create view emp_basic_info as select (id, name, address, designation) from emp;
  - Grant select (id, name,address) on emp_basic_info to 'qasim'
  - Grant select (id, name, address, designation) on emp_basic_info to 'Haider'

Views and Data Security

```
CREATE VIEW EuropeanCountry AS
   SELECT Name, Continent, Population, HasCoast
   FROM Country
   WHERE Continent = "Europe"

CREATE VIEW BigCountry AS
   SELECT Name, Continent, Population, HasCoast
   FROM Country
   WHERE Population >= 30000000
```



Virtual Private Database

Virtual Private Database (VPD) is a feature which enables Administrator to create security around actual data (i.e row/columns) so that multiple users can access data which is relevant to them.

- Steps for VPD
  - Create an Application Context: Create users, objects and permissions on the objects.
  - Create security policies functions
  - Apply security policies to tables

Reference Postgres Plus Advanced Server Guide:

http://get.enterprisedb.com/docs/Postgres_Plus_Enterprise_Edition_Guide_v9.5.pdf

Section 9.11 DBMS_RLS

Data Auditing

Database auditing involves observing a database for user/transaction actions. Database administrators and consultants often set up auditing for security purposes.

In EDB data auditing manage control through audit logs.

EDB / PostgreSQL maintained Audit log on ..

- When a role establishes a connection to an Advanced Server database
- What database objects a role creates, modifies, or deletes when connected to Advanced Server.
- When any failed authentication attempts occur.