UNIT - 1

18CSE455T – DATABASE SECURITY AND PRIVACY

18CSE455T – DATABASE SECURITY AND PRIVACY

UNIT I : SECURITY ARCHITECTURE & OPERATING SYSTEM SECURITY FUNDAMENTALS

- ✓ Security Architecture:
  - Introduction
  - Information Systems
  - Database Management Systems
  - Information Security Architecture
  - Database Security
  - Asset Types and value
  - Security Methods
- ✓ Operating System Security Fundamentals:
  - Introduction
  - Operating System Overview
  - Security Environment
  - Components
  - Authentication Methods
- ✓ User Administration
- ✓ Password Policies
- ✓ Vulnerabilities
- ✓ E-mail Security

Security Architecture: Introduction

- ✓ Security is Avoiding unauthorised access (with limited time duration , not always)
- ✓ There is no 100% Security in all kind of software and hardware .
- ✓ Security violations and attacks are increased globally at an average rate of 20%.
- ✓ Statistics shows that virus alerts, email spamming, identity theft, data theft, and types of security breaches on the rise.
- ✓ Database Security is the degree to which all the data is fully protected from tampering or unauthorised acts.
- ✓ The great challenge is to develop a new database security policy to secure data and prevent integrity data violations.
- ✓ Most of the DBMS did not have a security mechanism for authentication and encryption until recently.

Security Architecture: Introduction

You serve as a database administrator to enforce security policies. Responsibilities can be:

- ✓ Design and implement a new DB security policy.
- ✓ Enforce a stringent security policy.
- ✓ Implement functional specification of a module, i.e. encrypt the stored data, replace sensitive data using the data masking pack.

Security Architecture: Introduction

- Security measures
  - Prevent physical access to the servers where the data resided.
  - Operating systems require authentication of the identity of computer users.
  - Implement security models that enforce security measures.
- DBA should manage databases and implement security policies to protect the data (assets).

Information Systems

- ✓ In today's global market , corporate companies all over the world to gain a portion of market share.
- ✓ Wise decisions are not made without accurate and timely information.
- ✓ At the same time integrity of information is more important.
- ✓ The integrity of the information depends on the integrity of its data source and the reliable processing of the data.
- ✓ Data is processed and transformed by a collection of components working together to produce and generate accurate information. These components are known as INFORMATION SYSTEM.

Security

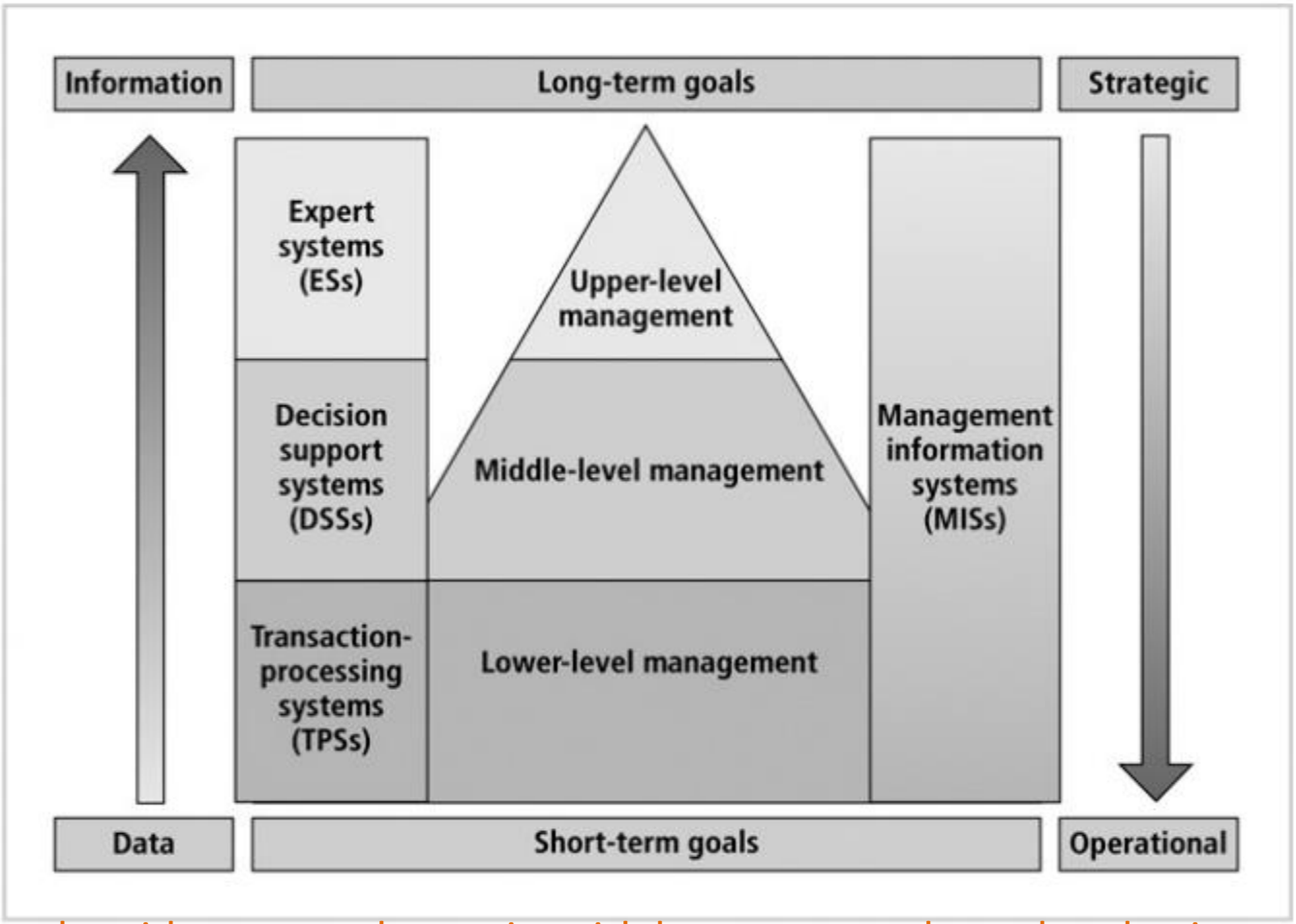
- **Database security:** degree to which data is fully protected from tampering or unauthorized acts comprises information system and information security concepts.
- Wise decisions require:
  - Accurate and timely information
  - Information integrity
- Information system: comprised of components working together to produce and generate accurate information
- Categorized based on usage: low-level, mid-level and high-level

Information Systems …

- ✓ An information can be a back bone of the day-to-day operations of a company as well as the beacon of long-term strategies and vision.
- ✓ Information systems are categorized based on usage.
- ✓ The following figure shows the typical use of system applications at various management levels.

Low-level management uses information Systems that assist management and employees with operation Tasks, such as inventory systems or point of sale(POS) systems

Middle-level management uses systems that deals with mid term goals, such as forecasting systems



Upper-level management works with systems that assist with long-term goals, such as business Model simulation and reasoning

Information Systems ...

- ✓ Information System mainly classified into three categories

    1) Transaction Processing System (TPS)

    2) Decision Support System (DSS)

    3) Expert System (ES)

INFORMATION SYSTEMS ...

Characteristics of Information System categories

Category	Characteristics	Typical Application System
Transaction Processing System (TPS)	✓ Also Known as ONLINE TRANSACTION PROCESSING (OLTP) ✓ Used for operational tasks ✓ Provides solutions for structured problems ✓ Includes business transactions ✓ Logical Components of TPS applications (Derived from business procedures , business rules and policies)	▪ Order tracking ▪ Customer service ▪ Payroll ▪ Accounting ▪ Student Registration ▪ Car Sales
Decision Support System (DSS)	✓ Deals with nanostructured problems and provide recommendations or answer to solve these problems ✓ Is capable of "What-if?" analysis ✓ Contains collection of business models ✓ Is used for tactical management tasks	▪ Risk Management ▪ Fraud Detection ▪ Sales forecasting ▪ Case resolution

Information Systems ...

Characteristics of Information System categories ...

Category	Characteristics	Typical Application System
Expert System (ES)	✓ Captures reasoning of human experts ✓ Executive Expert Systems(EESs) are a type of expert system used by top level management for strategic management goals ✓ A branch of Artificial Intelligence within the field of computer science studies ✓ Software consists of : Knowledge Base Inference Engine Rules ✓ People Consists of : Domain Experts Knowledge Engineers Power Users	✓ Virtual University Simulation ✓ Financial Enterprise ✓ Statistical Trading ✓ Loan Expert ✓ Market Analysis

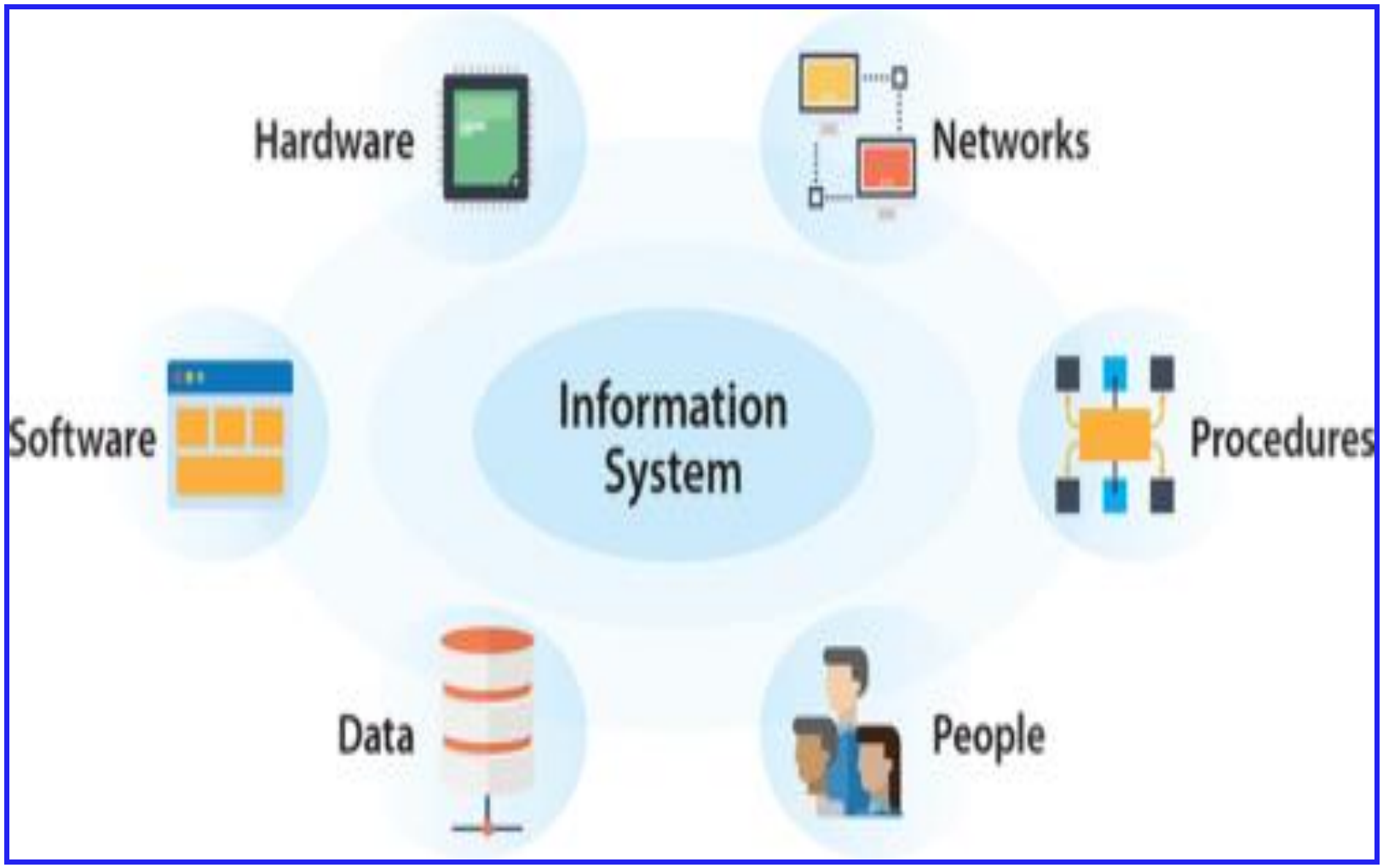
Information Systems ...

Components of Information System

- ✓ Data – Collected data and facts used as input for system processing and data stored in the Database for future reference or processing
- ✓ Procedures – includes Manual , Guidelines, Business rules and Policies
- ✓ Hardware – Computer System, Fax, Scanner, Printer, Disk
- ✓ Software – DBMS, OS, Programming Languages, Other Utilities or Tools
- ✓ Network – Communication Infrastructure to connect client processes to the system.
- ✓ People – DBA, System Admin, Programmers, Users, Managers, Business Analyst, System Analyst

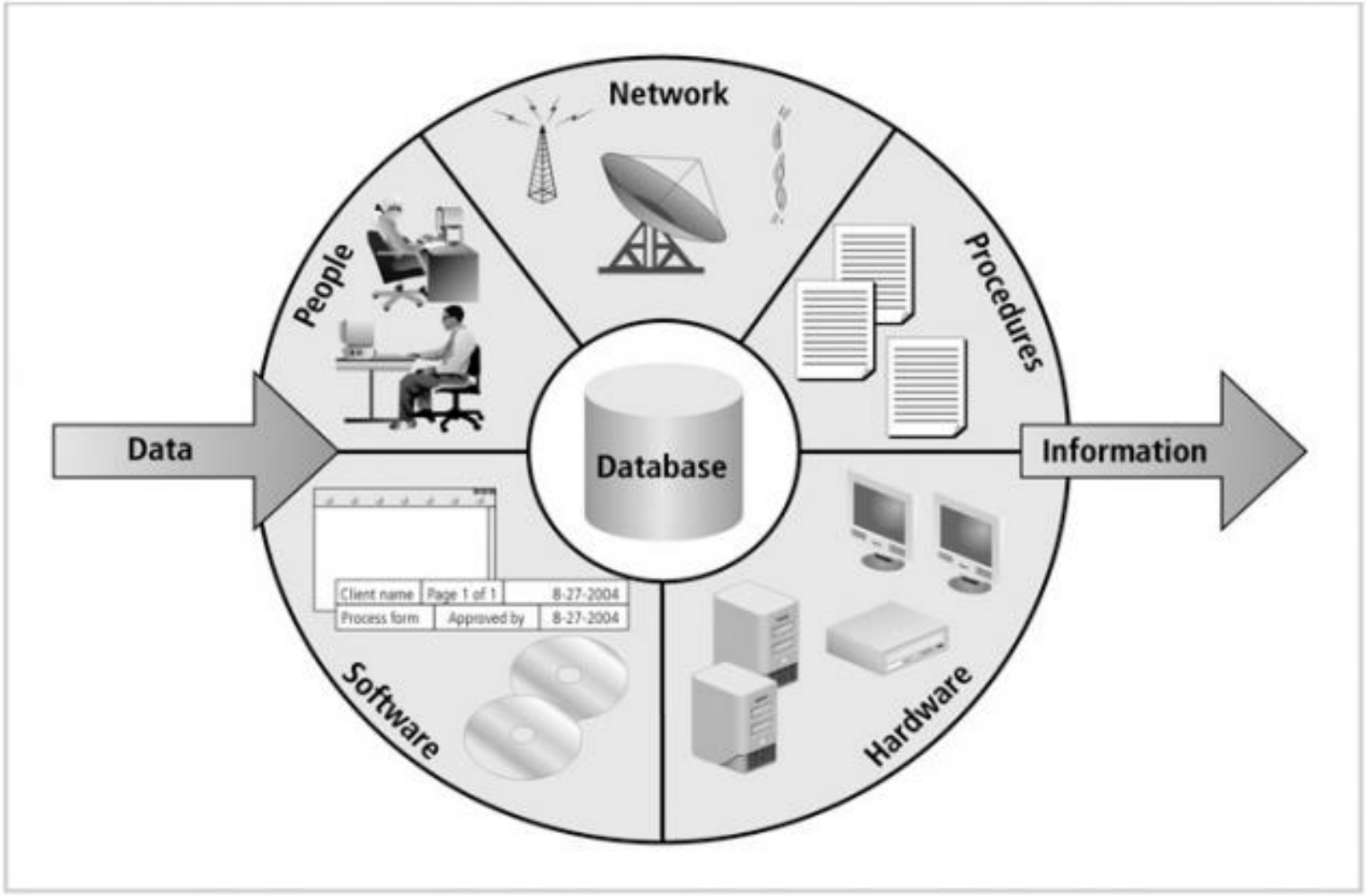
Information Systems ...

- Components of Information System ...



Information Systems ...

- Components of Information System ...



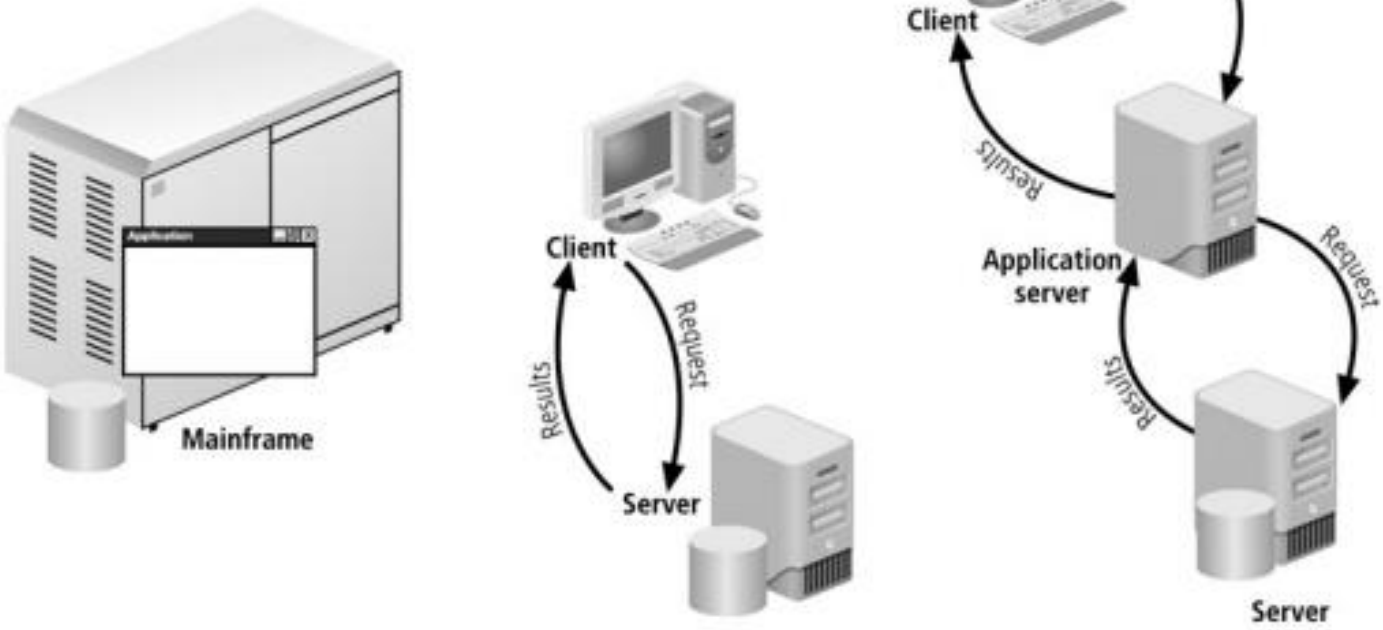
Information Systems ...

- Client/server architecture:
  - Based on the business model
  - Can be implemented as one-tier; two-tier; n-tier
  - Composed of three layers
- Tier: physical or logical platform
- Database management system (DBMS):

  Collection of programs that manage database

Information Systems ...

Client and server components residing on the same hardware



Examples of different client/server tier design

User interface

Network interface (Application architecture)

Core (Client and server Architecture – database Server layer))

Database Management System

Database :

- ✓ A collection of meaningful Integrated Information System
- ✓ It is both Physical and Logical
- ✓ Representing the logical information in a physical device
- ✓ Mainly used for storing and retrieving the data for processing
- ✓ Using CLIENT / SERVER Architecture
- ✓ Request and Reply protocols are used to communicate client and server

Database Management System

Database Management :

- Essential to success of information system

DBMS functionalities:

- ✓ Allow developer and administrators to Organize data
- ✓ Allow user to Store and retrieve data efficiently
- ✓ Allow user to Manipulate data (update and delete)
- ✓ Enforce referential integrity and consistency
- ✓ Enforce and implement data security policies and procedures
- ✓ Back up, recover, and restore data

Database Management System

DBMS components include:

- Data
- Hardware
- Software
- Networks
- Procedures
- Database servers

Database Management System

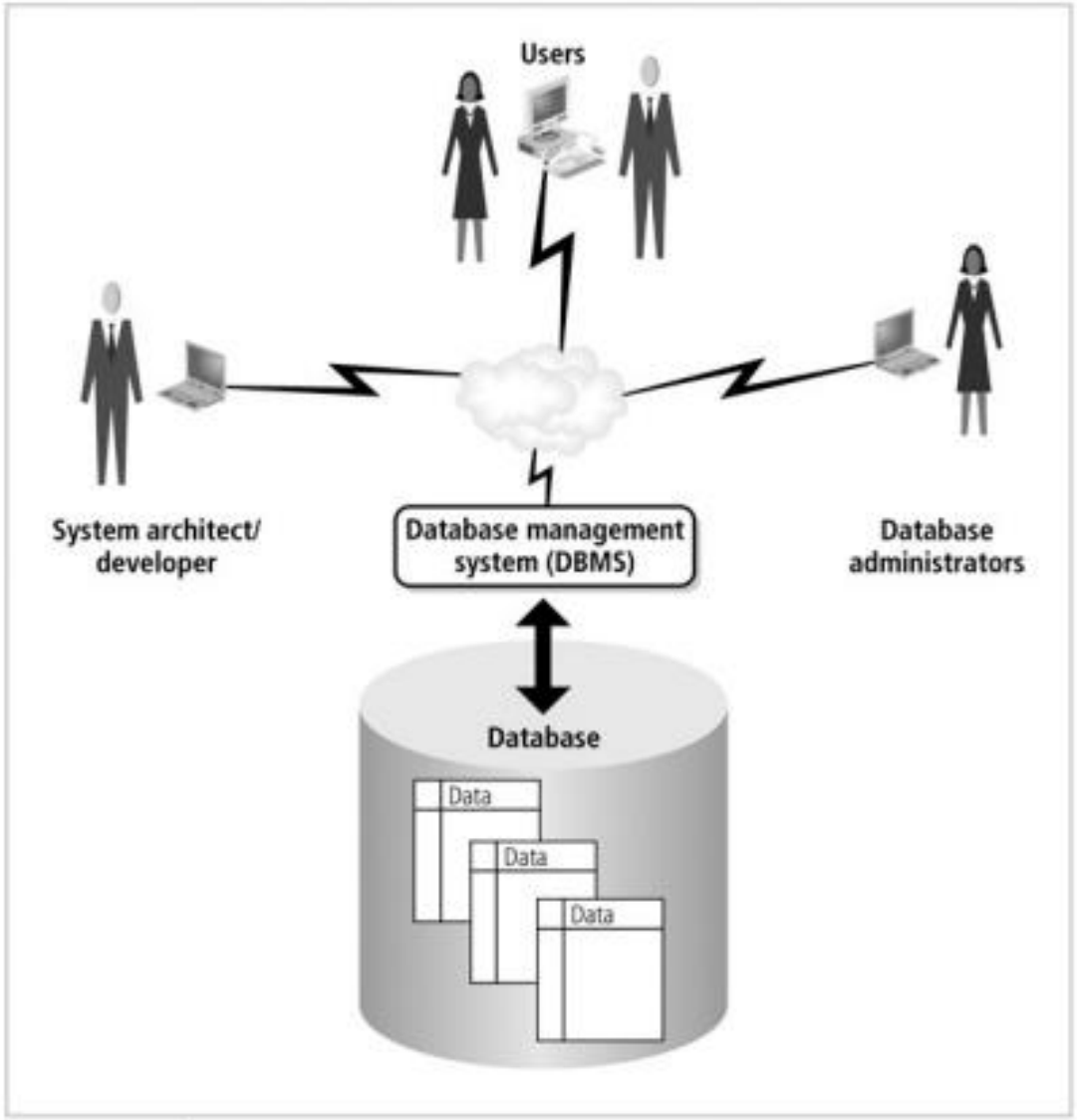


FIGURE 1-4 Database and DBMS environment

Database Management System ...

DBMS

- ✓ Set of programs to access the database for data manipulation or processing.
- ✓ DBMS contains information about a particular enterprise
- ✓ DBMS provides an environment that it both convenient and efficient to use.

Purpose of DBMS

- ✓ Data redundancy and inconsistency
- ✓ Difficulty in accessing data
- ✓ Data isolation – multiple files and format
- ✓ Integrity problems
- ✓ Atomicity of updates
- ✓ Concurrent access by multiple users
- ✓ Security problems

Database Management System ...

DBMS Architecture

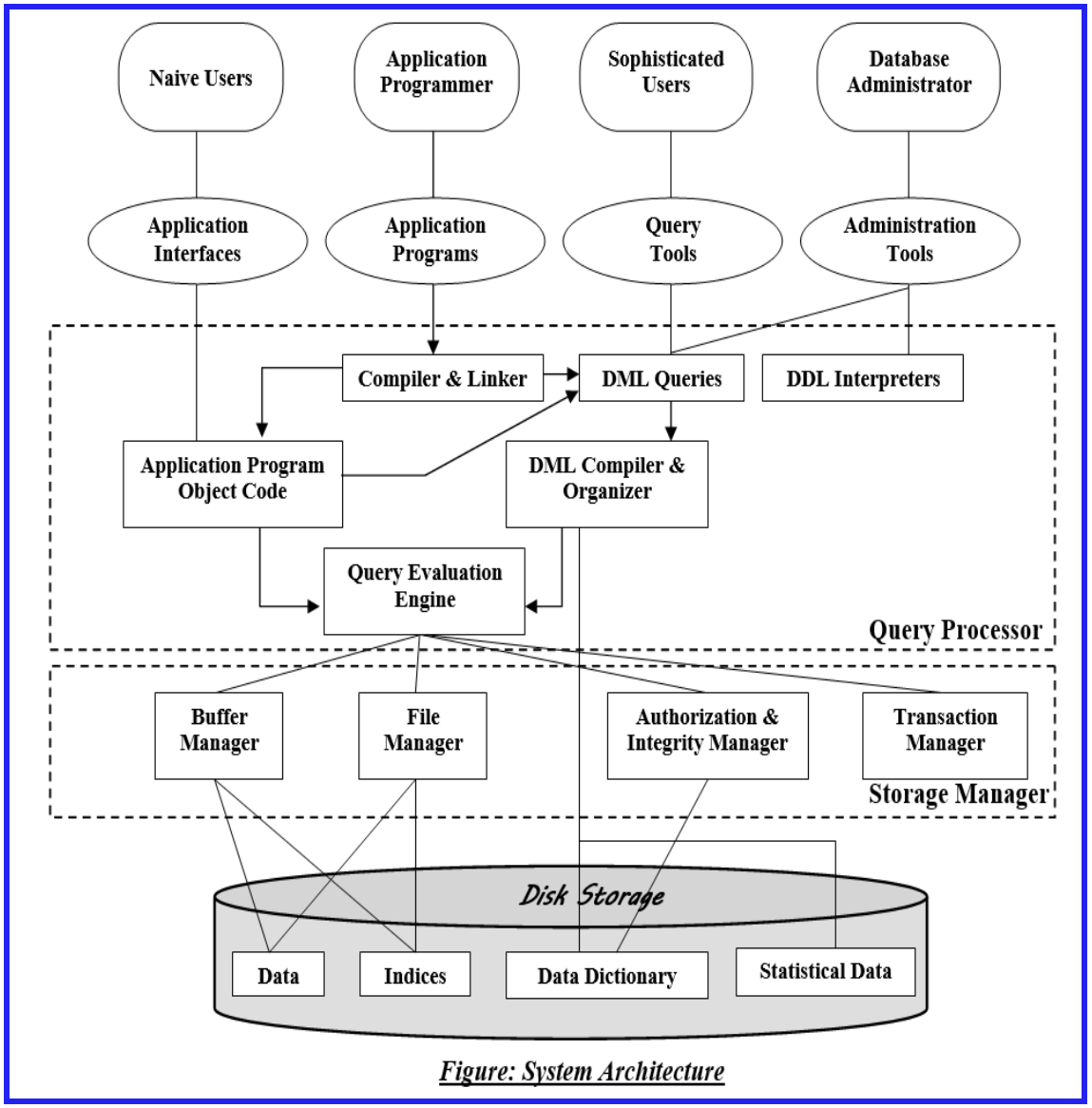


Figure: System Architecture

INFORMATION SECURITY

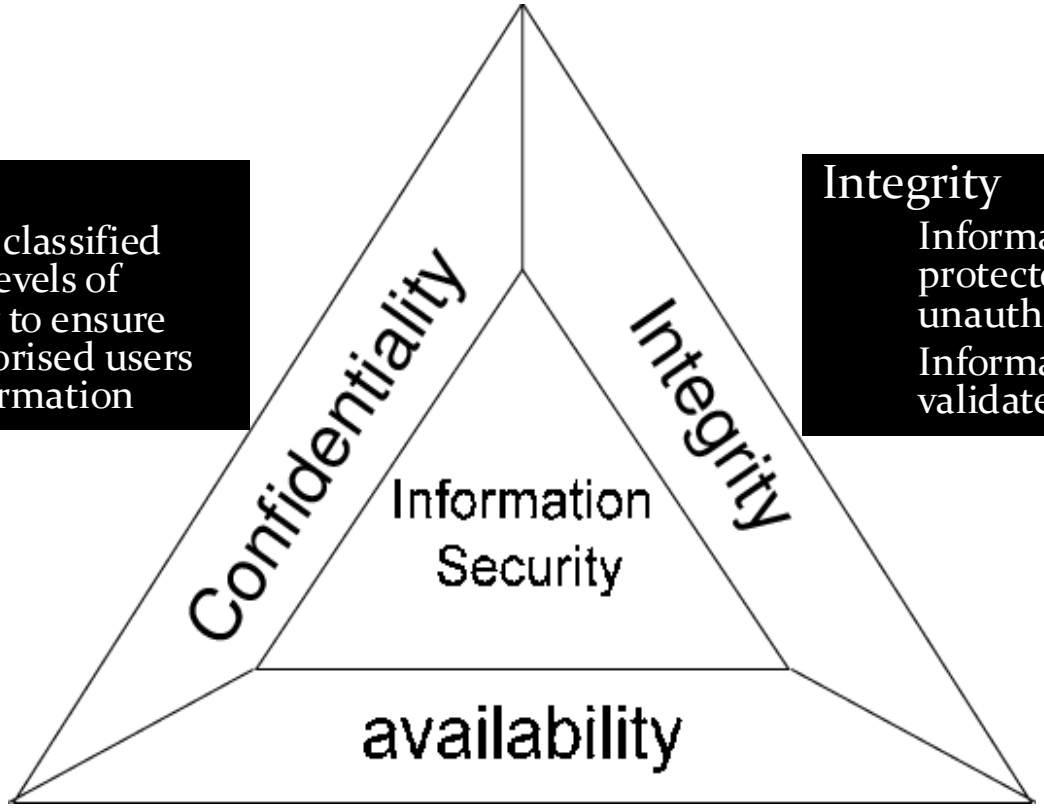
- Information is one of an organization's most valuable assets
- Information security: consists of procedures and measures taken to protect each components of the information systems involved in producing information.

- According to NSTISSC - National Security Telecommunications & Information Systems Security Committee – the concepts of information system is based

  C.I.A. triangle: Confidentiality, Integrity, Availability
- CIA – Frame work for protecting information.
- Security policies must be balanced according to the C.I.A. triangle

Information Security Architecture ...

CIA Triangle



Confidentiality

Information is classified into different levels of confidentiality to ensure that only authorised users access the information

Integrity

Information is accurate and protected from tampering by unauthorised persons

Information is consistent and validated

Availability

Information is available all the times only for authorised and authenticated persons

System is protected from being shutdown due to external or internal threats or attacks

Information security : Confidentiality

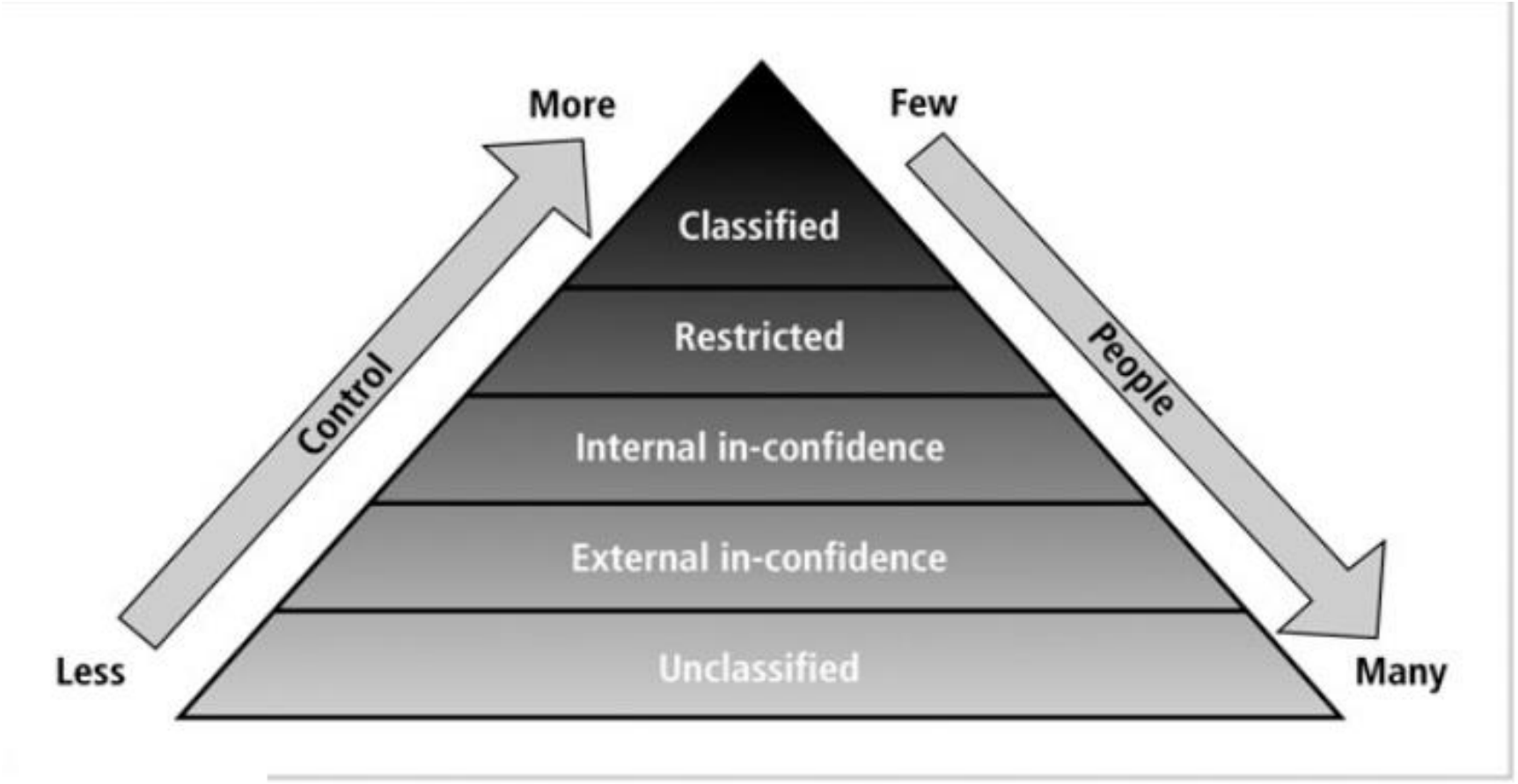
Addresses two aspects of security:

- Prevention of unauthorized access
- Process of safeguarding confidential information and Information disclosure based on classification (only to authorized users)

Classify company information into levels:

- Each level has its own security measures
- Usually based on degree of confidentiality necessary to protect information

Information security : Confidentiality



Confidentiality classification

Information security : INTEGRITY

- One of the pitfalls is losing read constancy.
- When working with data that has read consistency, each user sees only his own changes and those that have been committed by other users.

Information security : INTEGRITY

Integrity

- Consistent and valid data, processed correctly, yields accurate information
- Information has integrity if:
  - It is accurate
  - It has not been tampered with
- Read consistency: each user sees only his changes and those committed by other users

Integrity -- Example

- Employee A learns that his adversarial coworker is earning higher salary then he is.
- A access 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.
- There should be a control to cross-check overtime hours against actual time cards, computes vacation hours, and verifies entered values. If they are different, the app requires override from another person. (data validation)

TABLE 1-2 Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Invalid data	Indicates that not all the entered and stored data is valid without exception; checks and validation processes (known as database constraints) that prevent invalid data are missing.	■ User enters invalid data mistakenly or intentionally. ■ Application code does not validate inputted data.
Redundant data	Occurs when the same data is recorded and stored in several places; this can lead to data inconsistency and data anomalies.	■ Faulty data design that does not conform to the data normalization process. (**Normalization** is a database design process used to reduce and prevent data anomalies and inconsistencies.)

TABLE 1-2 Degradation of data integrity

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Inconsistent data	Occurs when redundant data, which resides in several places, is not identical.	■ Faulty database design that does not conform to the data normalization process.
Data anomalies	Exists when there is redundant data caused by unnormalized data design; in this case, data anomalies occur when one occurrence of the repeated data is changed and the other occurrences are not.	■ Faulty data design that does not conform to the data normalization process.

TABLE 1-2 Degradation of data integrity (continued)

Type of Data Degradation	Description	Reasons for Data Losing Integrity
Data read inconsistency	Indicates that a user does not always read the last committed data, and data changes that are made by the user are visible to others before changes are committed.	■ DBMS does not support or has weak implementation of the read consistency feature.
Data nonconcurrency	Means that multiple users can access and read data at the same time but they lose read consistency.	■ DBMS does not support or has weak implementation of the read consistency feature.

Information security : AVAILABLITY

- Systems must be always available to authorized users
- Systems determines what a user can do with the information

INFORMATION SECURITY : AVAILABLITY

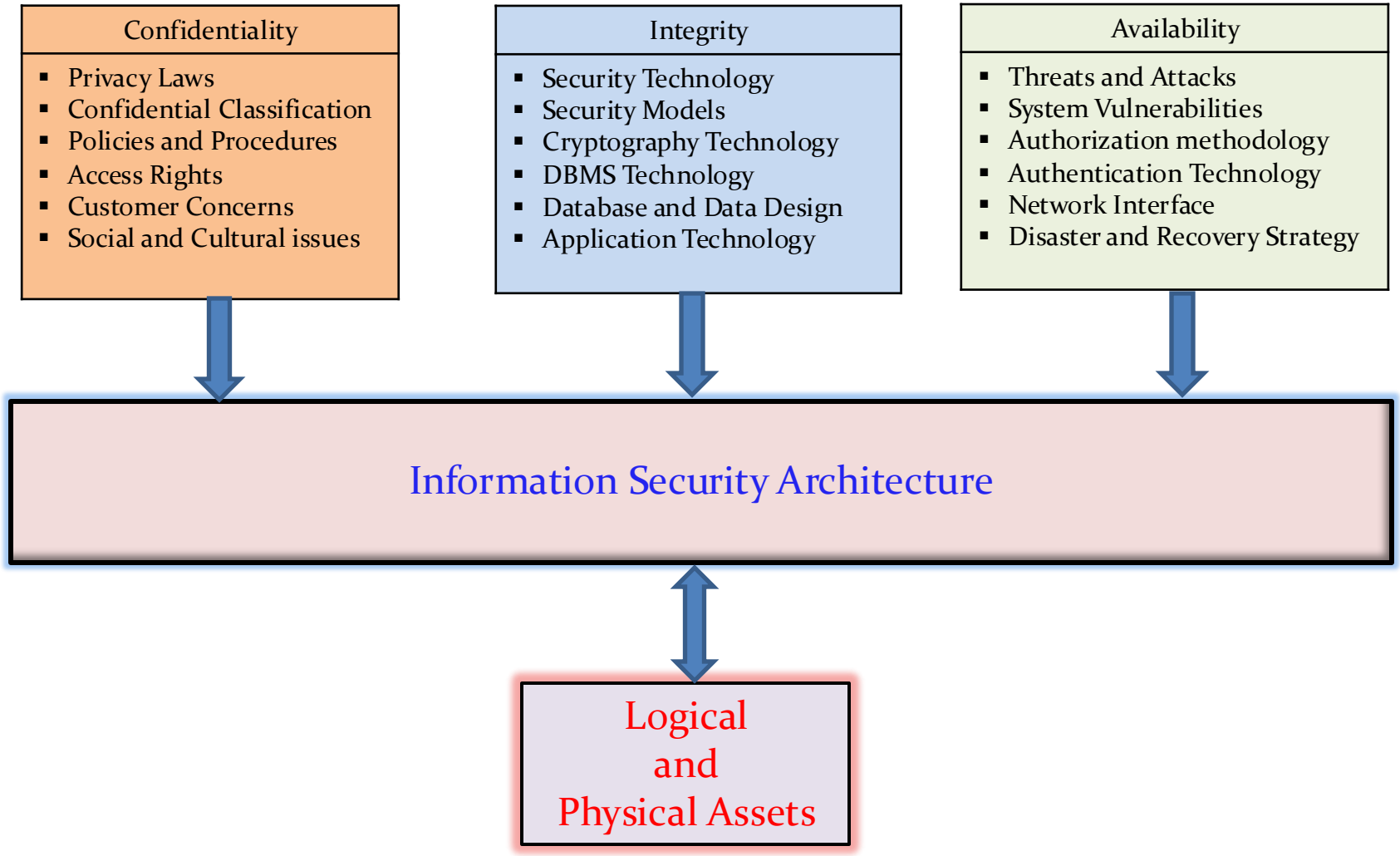
Reasons for a system to become unavailable:

- External attacks and lack of system protection
- System failure with no disaster recovery strategy
- Overly stringent and obscure security policies
- Bad implementation of authentication processes

Information Security Architecture ...

- Protects data and information produced from the data
- Model for protecting logical and physical assets
- Is the overall design of a company's implementation of C.I.A. triangle
- CIA is violated → Fail to protect the company's Logical and physical assets.

Information Security Architecture ...



Information Security Architecture ...

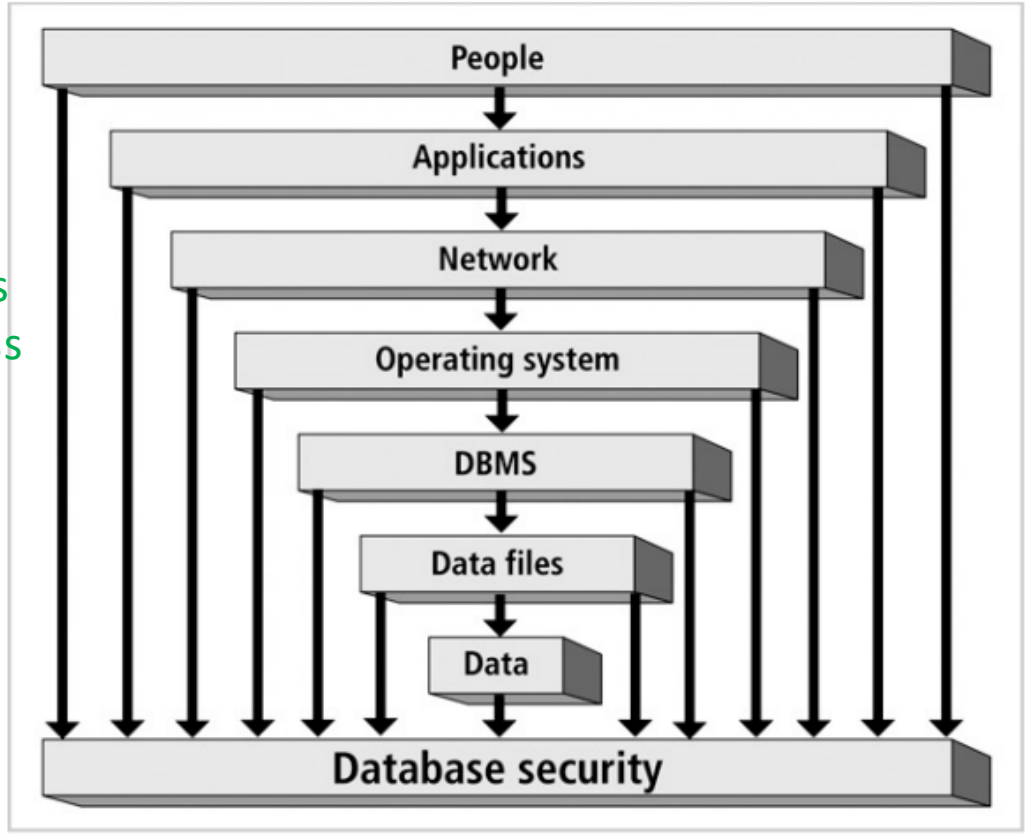
Outlines the Components of Information Security Architecture

- ✓ Policies and Procedures
  - Documented procedures and company policies that elaborate on how security is to be carried out
- ✓ Security personnel and Administrators
  - People who enforce and keep security in order
- ✓ Detection equipment
  - Devices that authenticate employees and Detect equipment that is prohibited by the company
- ✓ Security Programs
  - Tools that protect computer systems' server
- ✓ Monitoring Equipment
  - Devices that monitor physical properties , employees and other important assets
- ✓ Monitoring Applications
  - Utilities and applications used to monitor network traffic and Internet activities
- ✓ Auditing Procedures and Tools
  - Checks and Controls put in place to ensure that security measures are working

Database Security

- ✓ One of the functions of DBMS is to empower DBA to implement and enforce security at all levels of security
- ✓ A security access point is a place **where database security must be protected and applied (enforced and audited)**
- ✓ The Major Security access points illustrated in the below figure

Data – valuable assets and need highest levels of protection, so access Point is smallest



Database security access points

Database Security Access Points

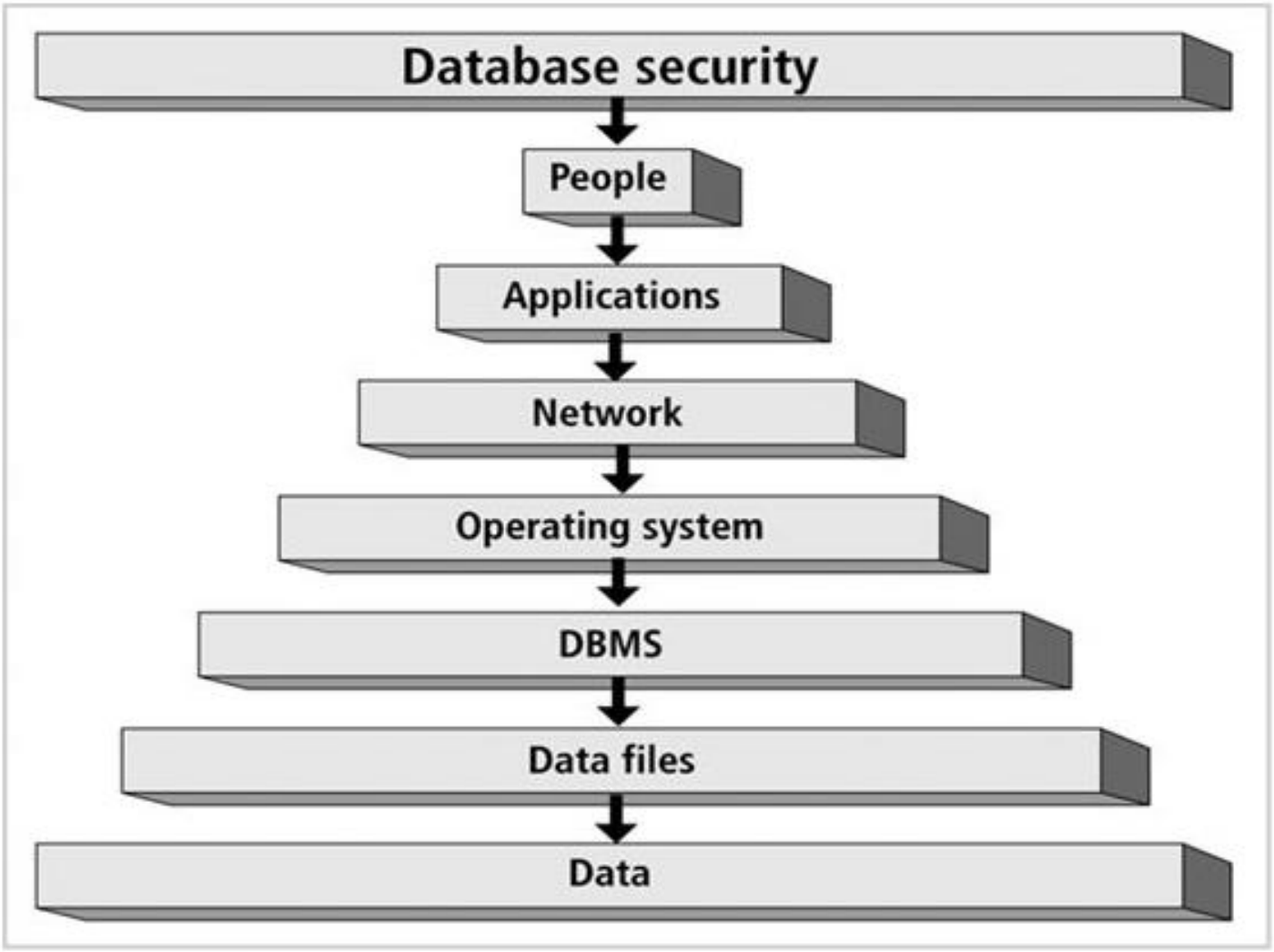
- ✓ People – Individuals who have been granted privileges and permissions to access networks, workstations, servers, databases, data files and data
- ✓ Applications – Application design and implementation , which includes privileges and permissions granted to people
- ✓ **Network** – One of the most sensitive security access points. Protect the network and provide network access only to applications, operating systems and databases.
- ✓ **Operating Systems** – This access point is defined as authentication to the system, the gateway to the data
- ✓ **DBMS** – The logical structure of the database, which includes memory , executables and other binaries
- ✓ **Data files** – Another access point that influences database security enforcement is access to data files where data resides.
- ✓ **Data** – The data access point deals with data design needed to enforce data integrity

Database Security Access Points

- ✓ Reducing access point size reduces security risks
- ✓ Security gaps are points at which security is missing, and thus system is vulnerable.
- ✓ Vulnerabilities are kinks in the system that can become threats
- ✓ Threat: security risk that can become a system breach

(either intentional or unintentional actions)

Database security enforcement



Reducing the access point size reduces security risks, which in turn increase database security

- ✓ Security gaps are points at which security is missing and the systems is vulnerable.
- ✓ Vulnerabilities are kinks in the system that must be watched because they can become threats.
- ✓ In the world of information security , a threat is defined as a security risk that has high possibility of becoming a system breach.

DATA INTEGRITY VIOLATION PROCESS (PROCESS OF SECURITY GAP)

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

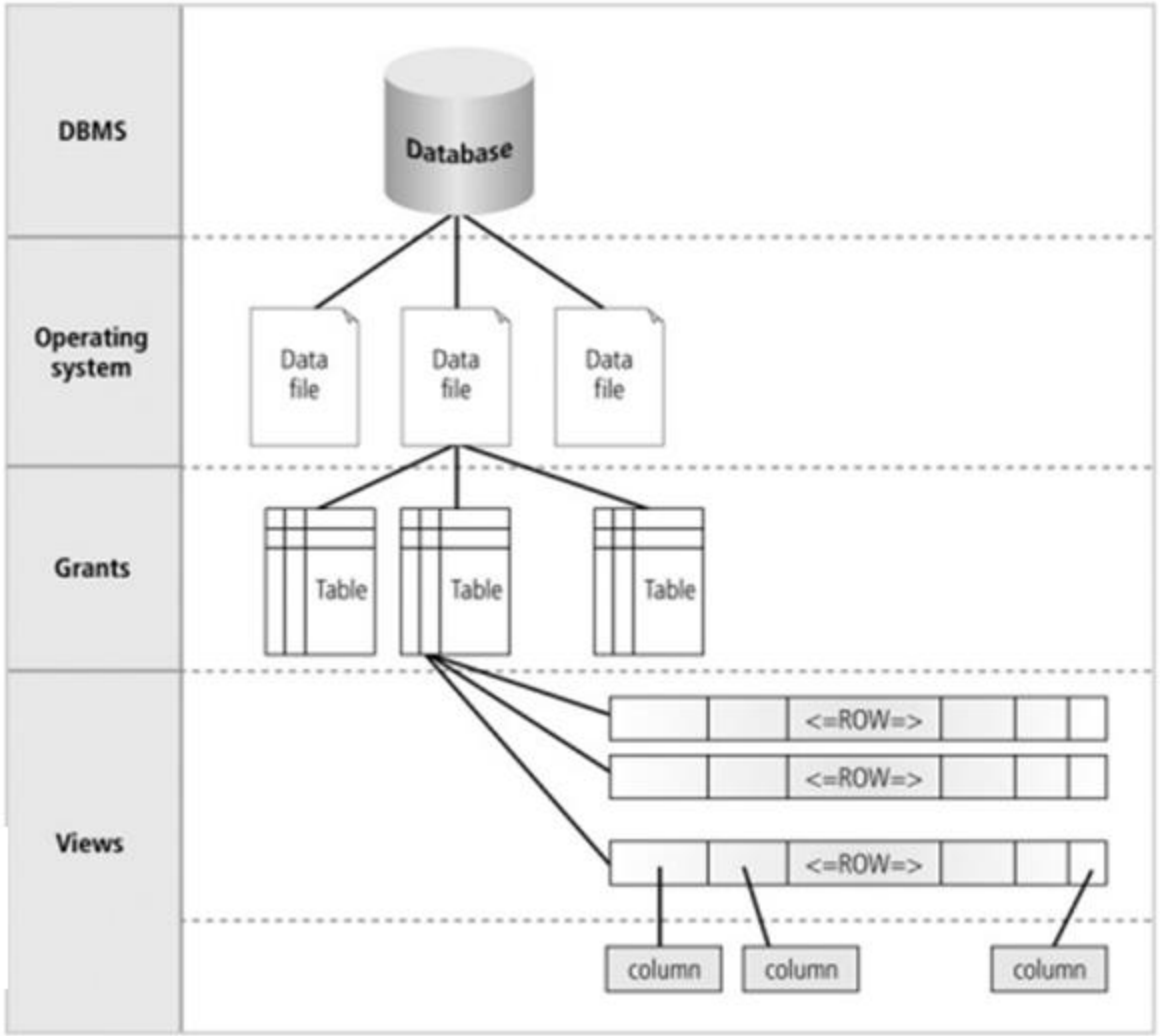
Structure of database is organized in levels, and each level can be protected by a different security mechanisms.

By database management system through user accounts and password

Through file permission

Schema owners/security administrator grant or revoke privileges

Column can be protected by using a VIEW database object.



Levels of database security

Menaces to Databases

Security vulnerability

– A weakness in any of the information system components that can be exploited to violate the integrity , confidentiality, or accessibility of the system

Security Threat

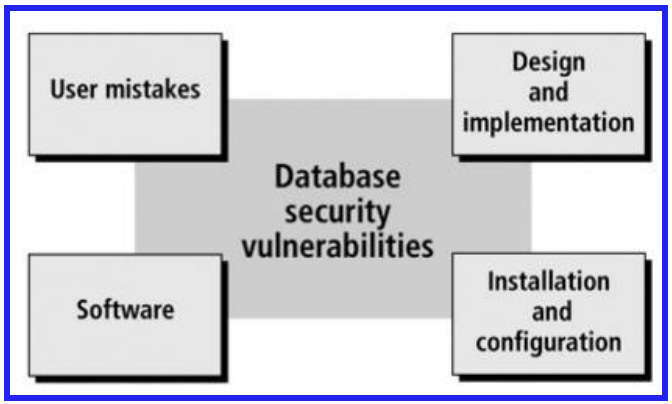
– A security violation or attack that can happen any time because of a security vulnerability

Security risk

– A known security gap that a company intentionally leaves open

Types of Vulnerabilities

- ✓ Vulnerability means " Susceptible to Attacks" (Source :www.dictionary.com)
- ✓ Intruders, Attackers and Assailers exploit vulnerabilities in Database environment to prepare and start their attacks.
- ✓ Hackers usually explore the weak points of a system until they gain entry
- ✓ Once the intrusion point is identified , Hackers unleash their array of attacks
  - Virus
  - Malicious Code
  - Worms
  - Other Unlawful violations
- ✓ To protect the system the administrator should understand the types of vulnerabilities
- ✓ The below figure shows the types of vulnerabilities



Types of Vulnerabilities …

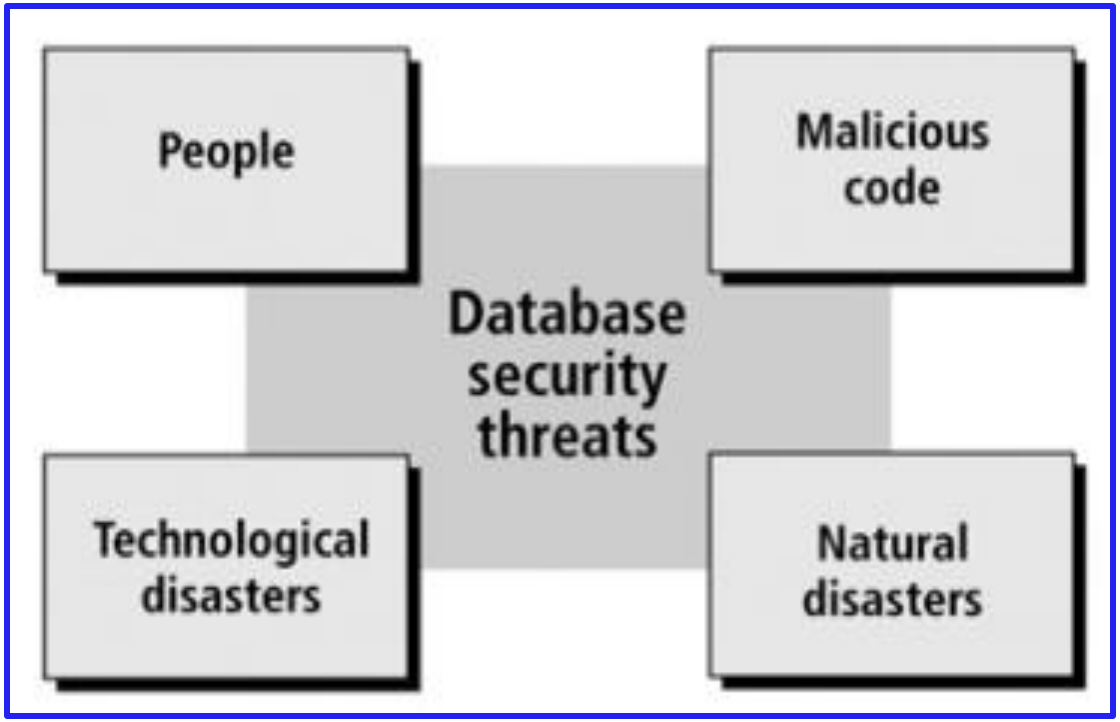
Category	Description	Examples
Installation and Configuration	✓ Results from default installation ✓ Configuration that is known publicly ✓ Does not enforce any security measures ✓ Improper configuration or Installation may result in security risks	✓ Incorrect application configuration ✓ Failure to change default passwords ✓ Failure to change default privileges ✓ Using default installation which does not enforce high security measures
User Mistakes	✓ Security vulnerabilities are tied to humans too ✓ Carelessness in implementing procedures ✓ Failure to follow through ✓ Accidental errors	✓ Lack of Auditing controls ✓ Untested recovery plan ✓ Lack of activity monitoring ✓ Lack of protection against malicious code ✓ Lack of applying patches as they are released ✓ Bad authentication or implementation ✓ Social Engineering ✓ Lack of technical information ✓ Susceptibility to scam

Types of Vulnerabilities …

Category	Description	Examples
Software	✓ Vulnerabilities found in commercial software for all types of programs (Applications, OS, DBMS, etc.,)	✓ Software patches that are not applied ✓ Software contains bugs ✓ System Administrators do not keep track of patches
Design and Implementation	✓ Related to improper software analysis and design as well as coding problems and deficiencies	✓ System design errors ✓ Exceptions and errors are not handled in development ✓ Input data is not validated

Types of threats

- ✓ Threat is defined as " An indication of impending(i.e. will happen soon) danger or harm"
- ✓ Vulnerabilities can escalate into threats
- ✓ DBA , IS Administrator should aware of vulnerabilities and threats
- ✓ Four types of threats contribute to security risks as shown in below figure



Types of threats , definitions and examples

Threat type	Definition	Examples
People	People intentionally or unintentionally inflict damage, violation or destruction to all or any of the database components (People, Applications, Networks, OS, DBMS, Data files or data)	✓ Employees ✓ Govt. Authorities or Person who are in charge ✓ Contractors ✓ Consultants ✓ Visitors ✓ Hackers ✓ Organised Criminals ✓ Spies ✓ Terrorists ✓ Social Engineers
Malicious Code	Software Code that in most cases is intentionally written to damage or violate one or more database environment components (People, Applications, Networks, OS, DBMS, Data files or data)	✓ Viruses ✓ Boot Sector Viruses ✓ Worms ✓ Trojon Horses ✓ Spoofing Code ✓ Denial-of-service flood ✓ Rookits ✓ Bots ✓ Bugs ✓ E-Mail Spamming ✓ Back Door

Types of threats , definitions and examples

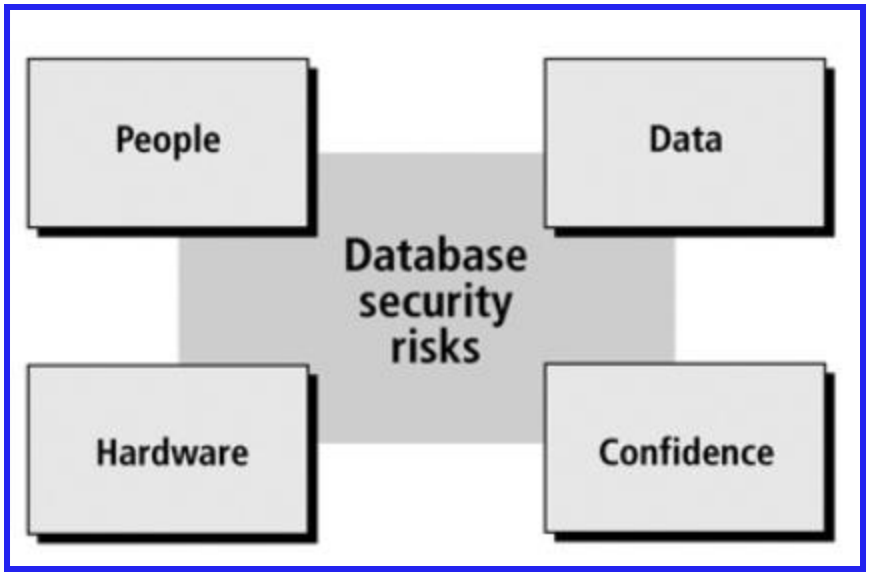
Threat type	Definition	Examples
Natural Disasters	Calamities caused by Nature, which can destroy any or all of the Database Components (People, Applications, Networks, OS, DBMS, Data files or data)	✓ Hurricanes ✓ Tornados ✓ Eartquakes ✓ Lightning ✓ Flood ✓ Fire
Technological Disasters	Often caused by some sort of malfunction in equipment or hardware. Technological disasters can inflict damage to Networks, OS, DBMS, Data files or data	✓ Power failure ✓ Media failure ✓ Hardware failure ✓ Network failure

Terms used in the table

- ✓ Virus – Code that compromises the integrity and state of the system
- ✓ Boot Sector Virus – Code that compromises the segment in the hard disk that contains the program used to start the computer
- ✓ Worm – Code that disrupts the operation of the system
- ✓ Trojon Horses – Malicious code that penetrates a computer system or network by pretending to be legitimate coded
- ✓ Spoofing Code – Malicious code that looks like a legitimate code
- ✓ Denial-of-service-flood – The act of flooding a web site or network system with many requests with the intent of overloading the system and forcing it to deny service legitimate requests
- ✓ Rootkits and Bots – Malicious or Legitimate code that performs such functions as automatically retrieving and collecting information from computer system
- ✓ Bugs - Code that is faulty due to bad design, logic or both
- ✓ E-Mail Spamming – E-Mail that is sent to may recipients without their permission
- ✓ Back door – An intentional design element of software that allows developers of the system to gain access to the application for maintenance or technical problems

Types of Risks

- ✓Risks are simply the a part of doing business
- ✓Managers at all the levels are constantly working to assess and mitigate risks to ensure the continuity of the department operations.
- ✓Administrators should understand the weakness and threats related to the system
- ✓Categories of database security risks are shown in the below figure

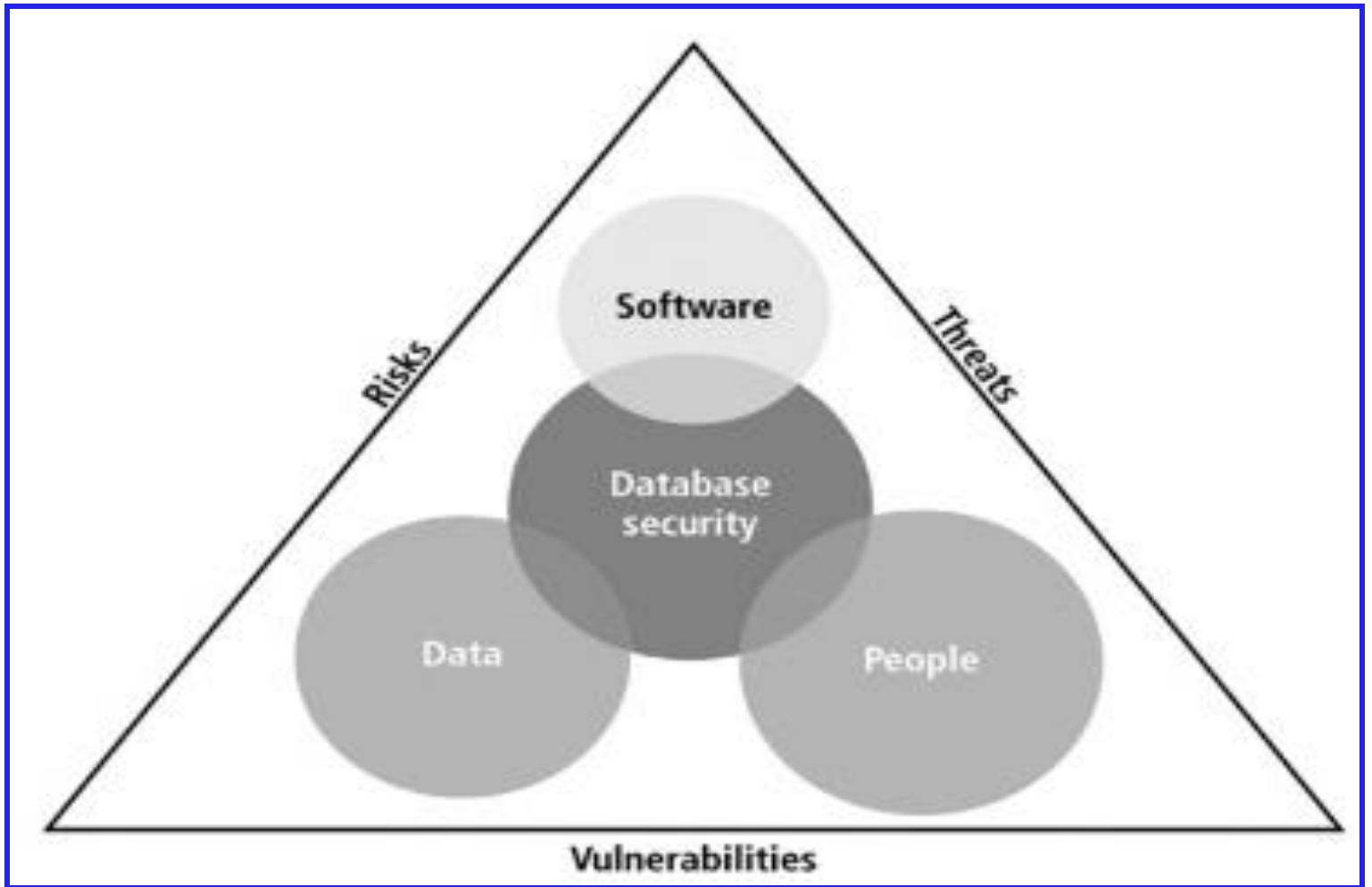


Definitions and examples of Risk types

Risk Type	Definition	Examples
People	The loss of people who are vital components of the database environments and know critical information can create risks	✓ Loss of key persons (Registration, Migration, Health problems) ✓ Key person downtime due to sickness personal or family problems, or burnout
Hardware	A risk that mainly results in hardware unavailability or interoperability	✓ Downtime due to hardware failure, mal functions, or inflicted damages ✓ Failure due to unreliable or poor quality equipment
Data	Data loss or data integrity is a major concern of the database administration and management	✓ Data loss ✓ Data corruption ✓ Data Privacy loss
Confidence	The loss of public confidence in the data produced by the company causes a loss of public confidence in the company itself ie. Customer satisfaction fails	✓ Loss of procedural and policy documentation ✓ DB performance degradation ✓ Fraud ✓ Confusion and uncertainty about database information

Integration of security vulnerabilities, therats and risks in a database

if you were to rate vulnerabilities, threats, and risks according to most the common and important factors you would list three factors: people, software and data. The remaining factors act as amplifiers or supporters.



Asset Types and Their Values

- ✓ People always tend to protect assets regardless of what they are
- ✓ Corporations treat their assets in the same way
- ✓ Assets are the infrastructure of the company operation

There are four main types of assets

- Physical assets – Also known as tangible assets, these include buildings, cars, hardware and so on…
- Logical assets – Logical aspects of an information system such as business applications, in-house programs, purchased software, OS, DBs, Data
- Intangible assets – Business reputation, quality, and public confidence
- Human assets – Human skills, knowledge and expertise

Database Security Methods

Security methods used to protect database environment components

Database Component Protected	Security Methods
People	✓ Physical limits on access to hardware and documents ✓ Through the process of identification and authentication make certain that the individual is who is claim s to be through the use of devices, such as ID cards, eye scans, and passwords ✓ Training courses on the importance of security and how to guard assets ✓ Establishment of security policies and procedures
Applications	✓ Authentication of users who access applications ✓ Business rules ✓ Single sign-on (A method for signing on once for different applications and web sites)
Network	✓ Firewalls to block network intruders ✓ Virtual Private Network (VPN) ✓ Authentication

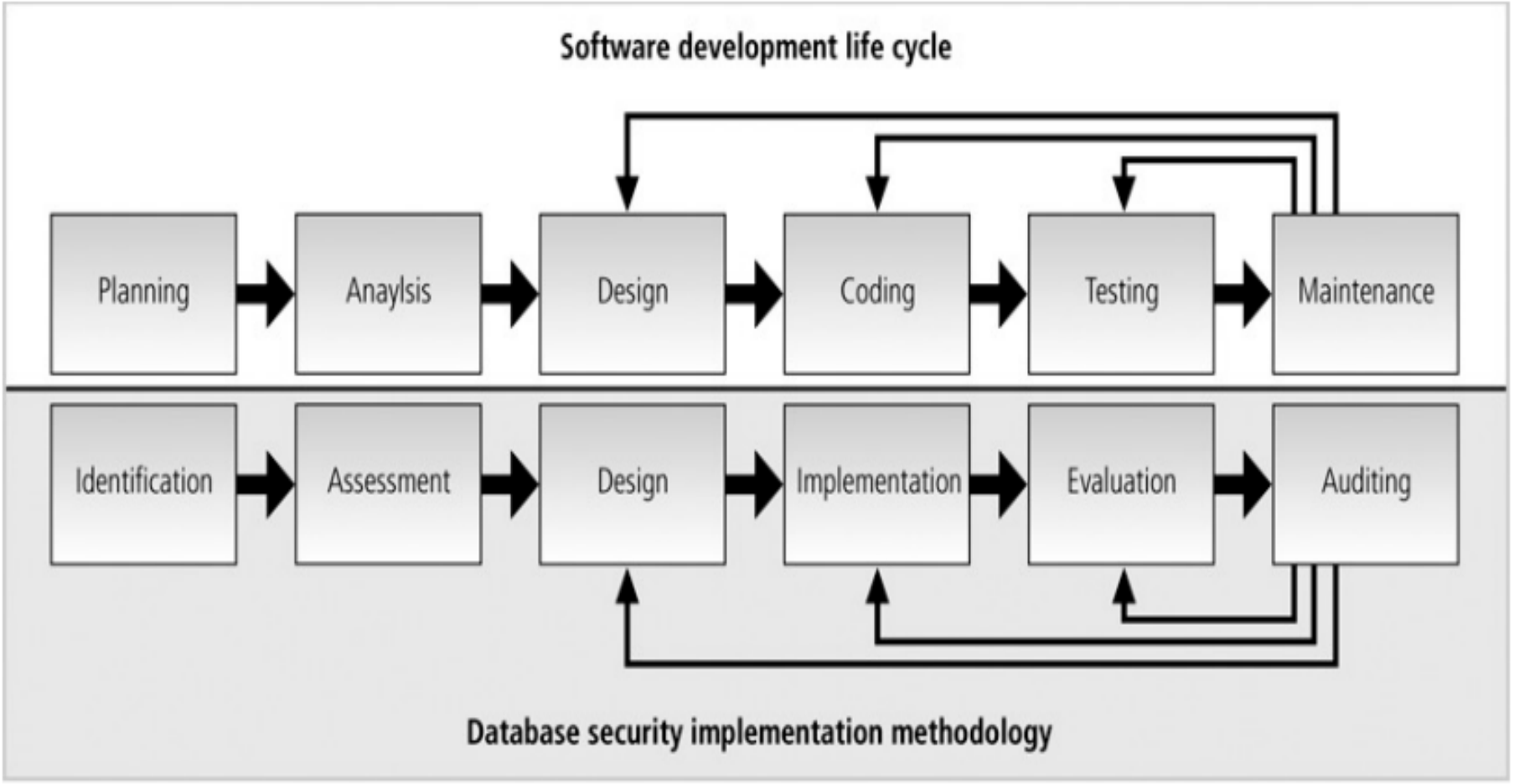
Database Security Methods ...

Database Component Protected	Security Methods
OS	✓ Authentication ✓ Intrusion Detection ✓ Password Policies ✓ User accounts
DBMS	✓ Authentication ✓ Audit Mechanism ✓ Database resource limits ✓ Password poilicy
Data files	✓ File permission ✓ Access Monitoring
Data	✓ Data Validation ✓ Data Constraints ✓ Data Encryption ✓ Data Access

Database Security Methodology

The below figure presents database security Framework and methodology side by side with the software development life cycle (SDLC) methodology.

- Figure - Assist you to building a database security in each phase



Database Security Methodology...

The following list presents the definition of each phase of the database security methodology

Identification – Entails the identification and investigation of resources required and policies to be adopted

Assessment – This phase includes analysis of vulnerabilities, threats and risks for both aspects of DB security

Physical – Data files

Logical – Memory and Code

Design – This phase results in a blueprint of the adopted security model that is used to enforce the security

Implementation – Code is developed or tools are purchased to implement the blueprint outlined in the previous phase

Evaluation – Evaluate the security implementation by testing the system against attacks, hardware failure, natural disasters and human errors

Auditing – After the system goes into production , security audits should be performed periodically to ensure the security state of the system

Database Security Definition Revisited

- At the start of the chapter database security was defined as "the degree to which all the data is fully protected from tampering and unauthorised acts".
- After discussing a lot of database security , various information systems and information security the definition of database security can be expanded as follows:

Database security is a collection of security polices and procedures, data constraints, security methods , security tools blended together to implement all necessary measures to secure the integrity, accessibility and confidentiality of every component of the database environment.

Operating System Security Fundamentals

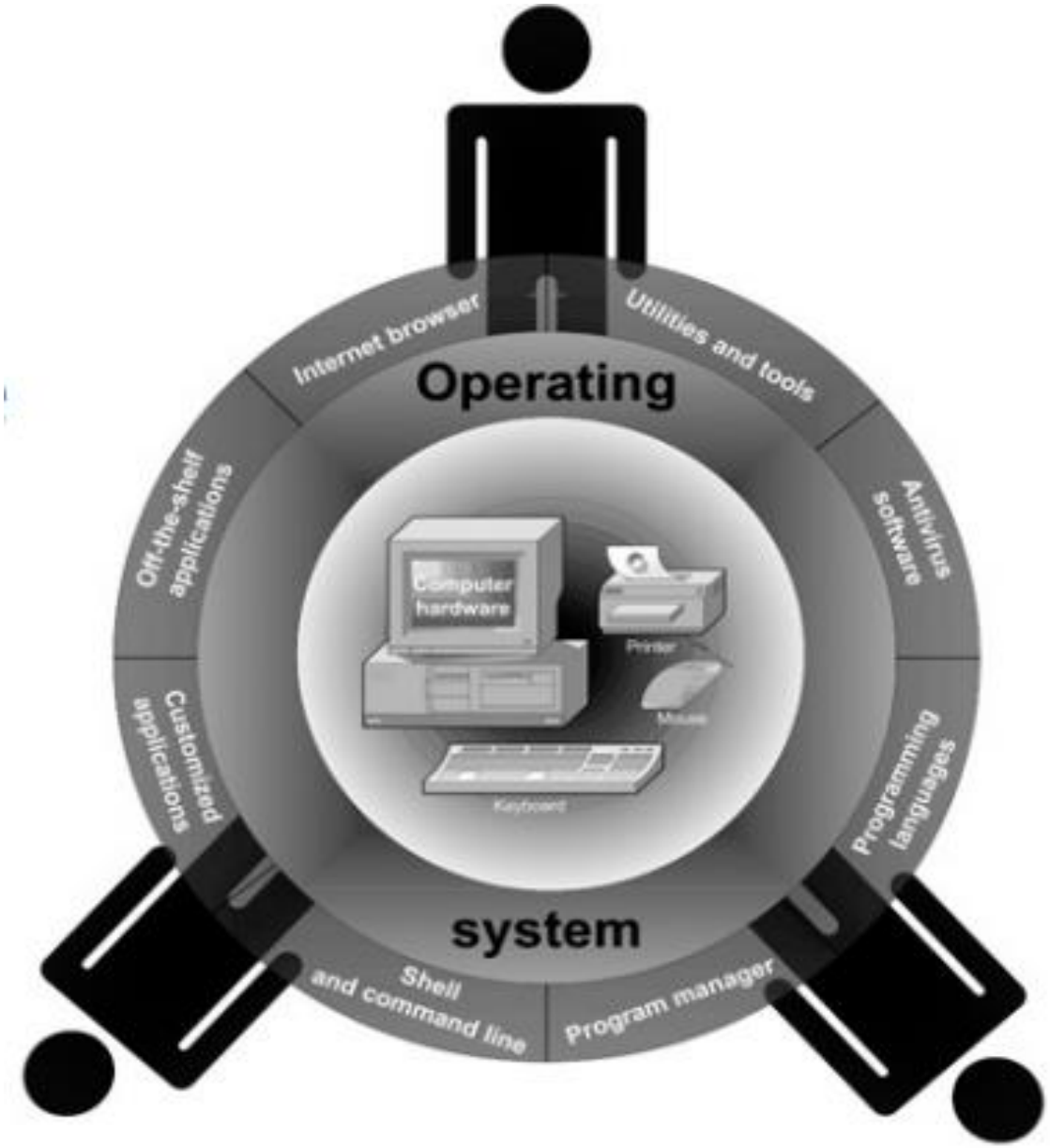
An Operating System (OS) is a collection of programs that allows the to operate the computer hardware.

- ✓ OS is also known as " RESOURCE MANAGER"
- ✓ OS is one of the main access point in DBMS

A computer system has three layers

- The inner layer represents the hardware
- The middle layer is OS
- The outer layer is all different software

Operating System Security Fundamentals



Operating System Security Fundamentals ...

An OS is having number of key functions and capabilities as outlined in the following list

- ✓ **Multitasking (runs multiple tasks at same tme)**
- ✓ **Multisharing (resource sharing)**
- ✓ **Managing computer resources**
- ✓ **Controls the flow of activities**
- ✓ **Provides a user interface to operate the computer**
- ✓ **Administers user actions and accounts**
- ✓ **Runs software utilities and programs**
- ✓ **Provides functionalities to enforce the security measures**
- ✓ **Schedules the jobs and tasks to be run**
- ✓ **Provides tools to configure the OS and hardware**

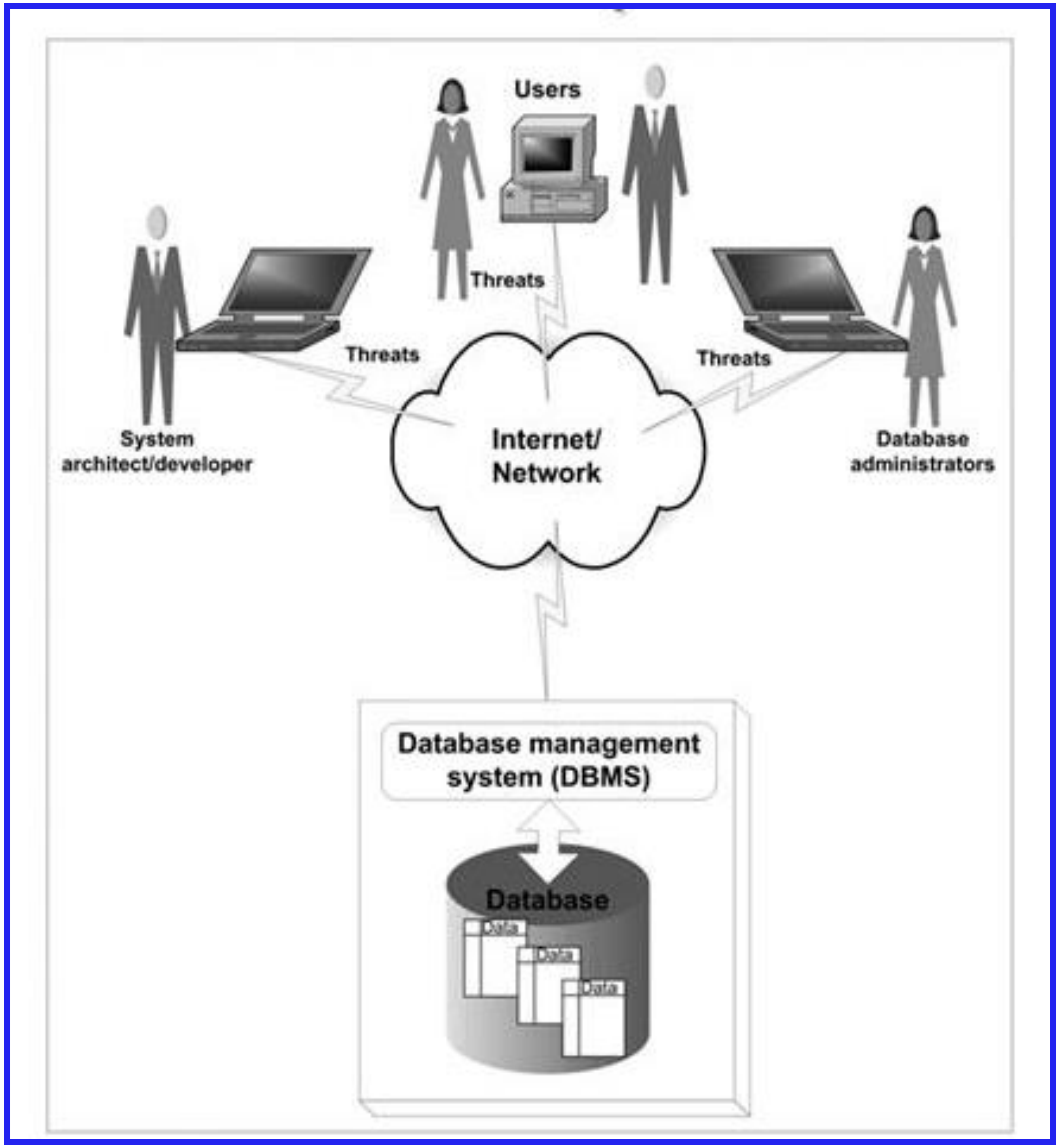
Operating System Security Fundamentals …

There are different vendors of OS

- ✓ *Windows by Microsoft*
- ✓ *UNIX by companies such as Sun Microsystems, HP and IBM*
- ✓ *LINUX "flavours" from various vendors such as Red Hat*
- ✓ *Macintosh by Apple*

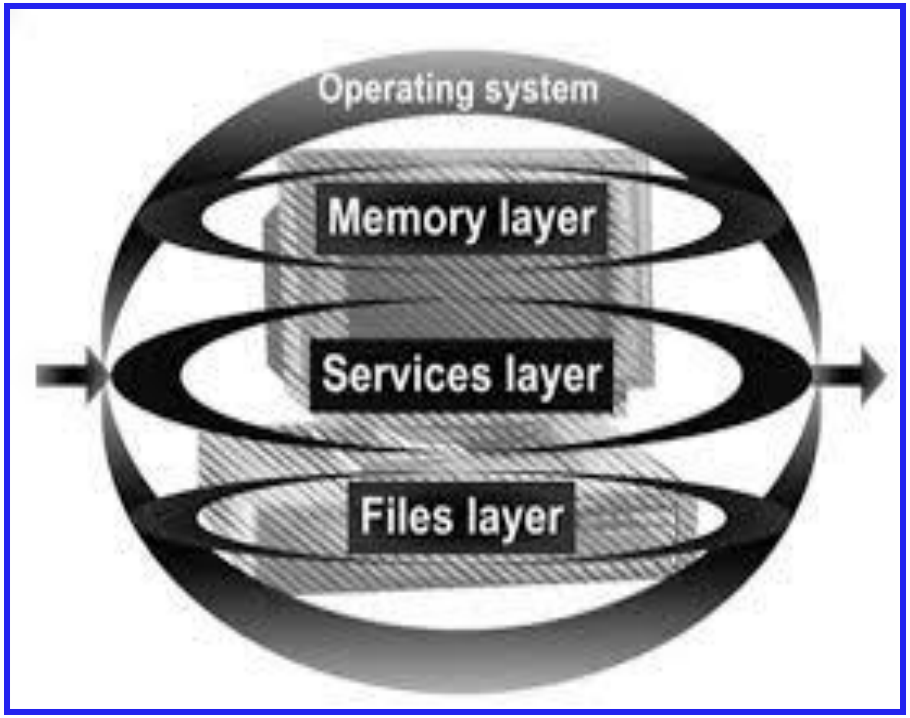
The OS Security Environment

- ✓ A compromised OS can compromise a Database Environment
- ✓ Physically protect the computer running the OS(Padlocks, Chain locks, Guards, Cameras)
- ✓ Model :
  - Bank Building – OS
  - Safe – Database
  - Money - Data



The Components of an OS Security Environment

- ✓ The three components (layers) of the OS are represented in the figure
- ✓ Memory component is the hardware memory available on the system
- ✓ Files component consists of files stored on the disk
- ✓ Service component compromise such OS features and functions as N/W services, File Management and Web services



Services

The main component of OS security environment is services.

- ✓ It consists of functionality that the OS offers as part of its core utilities.
- ✓ Users employ these utilities to gain access to OS and all the features the users are authorised to use.
- ✓ If the services are not secured and configured properly, each service becomes a vulnerability and access point and can lead to a security threat.

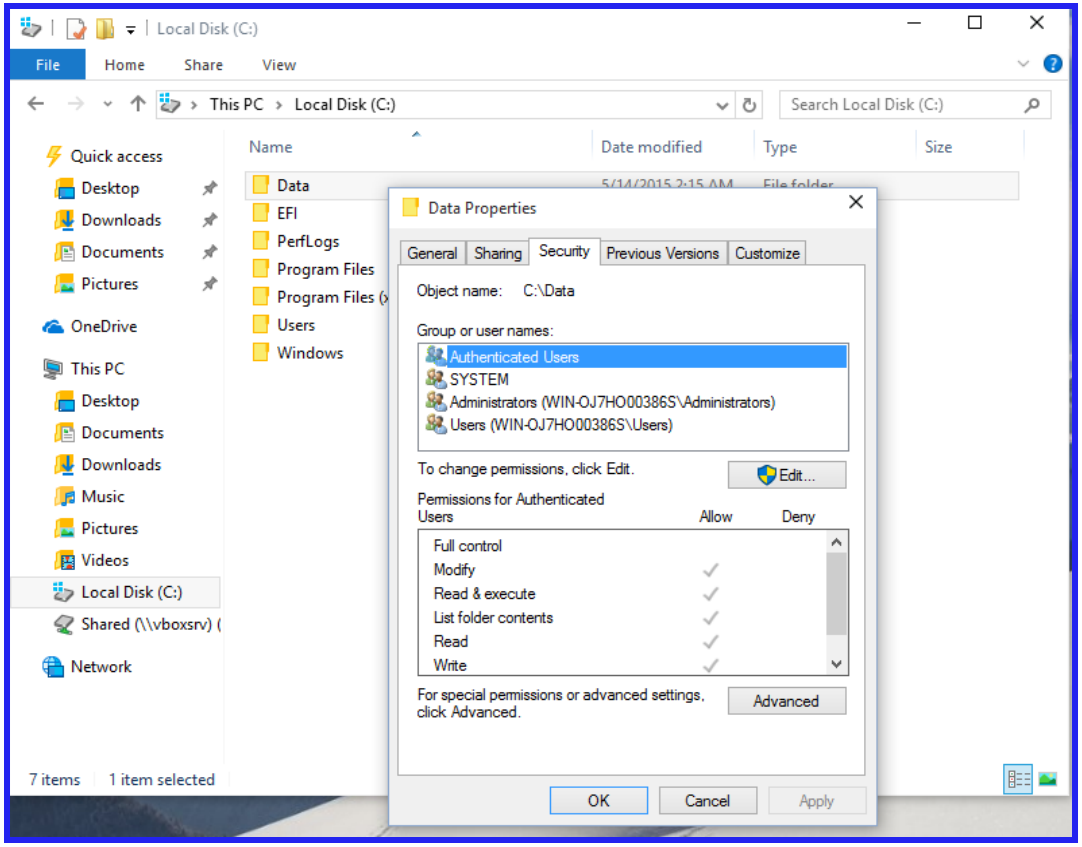
Files

- ✓ Files are another one component of OS.
- ✓ It has more actions
  - ✓ File Permission
  - ✓ File Transfer
  - ✓ File Sharing

FILES …

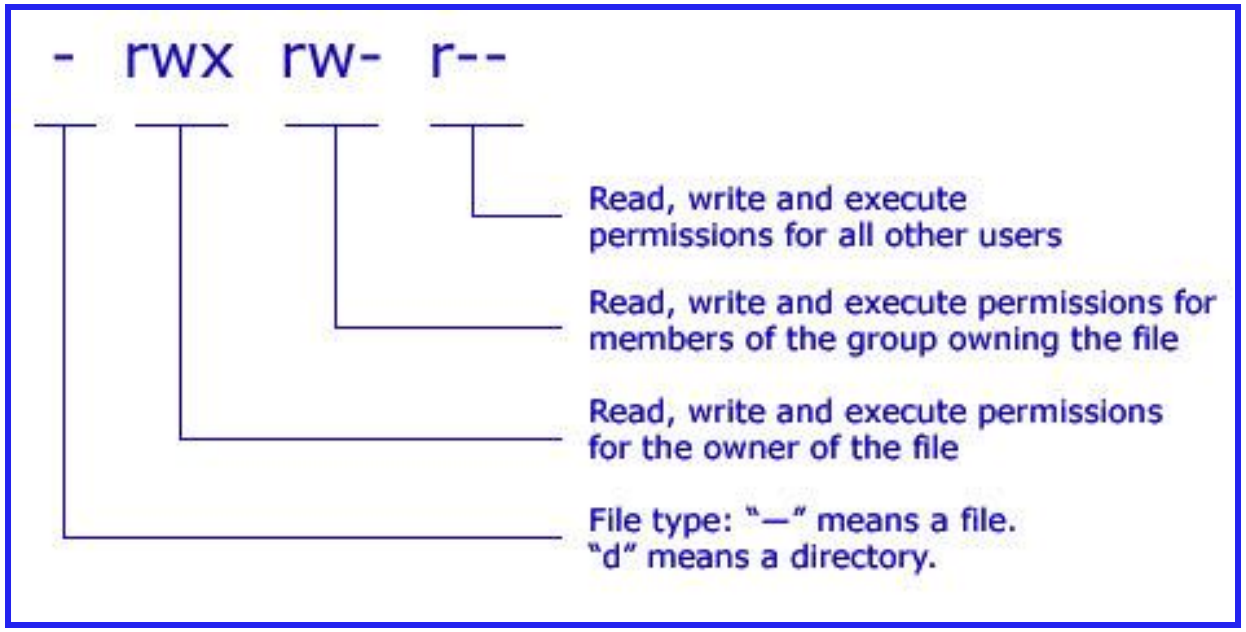
File Permission

- Every OS has a method of implementing file permission to grant read, write or execute privileges to different users.
- The following figure gives how the file permissions are assigned to a user in windows



Files …

- ✓ In UNIX, file permissions work differently than windows.
- ✓ For each file there are three permission settings
- ✓ Each setting consists of rwx (r – read, w – write and x – execute)
  1. First rwx is Owner of the file
  2. Second rwx is Group to which owner belongs
  3. Third rwx is All other users
- ✓ The given images gives the details of UNIX file permission.



Files …

File Transfer – moving the file from one location to another location in a disk/web/cloud

- ✓ FTP is an Internet service that allows transferring files from one computer to another
- ✓ FTP clients and servers transmit usernames and passwords in plaintext format(Not Encrypted). This means any hacker can sniff network traffic and be able to get the logon information easily.
- ✓ Files also transferred as plaintext format
- ✓ A root account cannot be used to transfer file using FTP
- ✓ Anonymous FTP is the ability to log on to the FTP server without being authenticated.
- ✓ This method is usually used to provide access to files in the public domain.

Files …

Here are some best practices for transferring files

- ✓ Never use the normal FTP Utility. Instead, use the secure FTP utility , if possible.
- ✓ Make two FTP directories: one for file uploads with write permission only and another one file is for file downloads with read permission.
- ✓ Use specific accounts for FTP that do not have access to any files or directories outside the file UPLOAD and DOWNLOAD directories.
- ✓ Turn on logging , and scan the FTP logs for unusual activities on a regular basis.
- ✓ Allow only authorized operators to have FTP privileges.

Files …

- ✓ **Sharing files** naturally leads to security risks and threats
- ✓ The peer-to-peer technology is on rise(very well developed now)
- ✓ Peer-to-Peer programs allow users to share the files over internet
- ✓ If you were conduct a survey of users that use Peer-to-Peer programs, majority of the users' machines are infected with some sort of virus, spyware, or worm.
- ✓ Most companies prohibit the use of such programs.
- ✓ The main reason for blocking these programs are
  - Malicious Code
  - Adware and spyware
  - Privacy and confidentiality
  - Pornography
  - Copy right issues

Memory

- ✓ You may wonder how memory is an access points to security violations
- ✓ There are many badly written programs and utilities that could change the content of memory
- ✓ Although these programs do not perform deliberate destructions acts.
- ✓ On the other hand , programs that intentionally damage or scan data in memory are the type that not only can harm the data integrity, but may also exploit data for illegal use.

Authentication Methods

- ✓ Authentication is the fundamental service of the OS
- ✓ It is a process to very the user identity

Most security administrators implement two types of authentication methods

- ✓ Physical authentication method allows physical entrance to the company properties
  - ✓ Most companies use magnetic cards and card readers to control the entry to a building office, laboratory or data center.
- ✓ The Digital authentication method is a process of verifying the identify of the user by means of digital mechanism or software

Digital Authentication used by many OS

- ✓ Digital Certificate
  - Widely used in e-commerce
  - Is a passport that identifies and verifies the holder of the certificate
  - Is an electronic file issued by a trusted party (Known as certificate authority) and cannot be forged or tampered with.
- ✓ Digital Token (Security Token)
  - Is a small electronic device that users keep with them to be used for authentication to a computer or network system.
  - This device displays a unique number to the token holder, which is used as a PIN (Personal Identification Number) as the password
- ✓ Digital Card
  - Also known as security card or smart card
  - Similar to credit card in dimensions but instead of magnetic strip
  - It has an electronic circuit that stores the user identification information
- ✓ Kerberos
  - Developed by Massachusetts Institute of Technology (MIT) , USA
  - It is to enable two parties to exchange information over an open network by assigning a unique key. Called ticket , to each user.
  - The ticket is used to encrypt communicated messages

Digital Authentication used by many OS ...

- ✓ Lightweight Directory Access Protocol (LDAP)
  - Developed by University of Michigan, USA
  - Uses centralized directory database storing information about people, offices and machines in a hierarchical manner
  - LDAP directory can be easily distributed to many network servers.
  - You can use LADP to store information about
    - Users (User name and User id)
    - Passwords
    - Internal telephone directory
    - Security keys
  - Use LADP for these following reasons
    - LDAP can be used across all platforms (OS independent)
    - Easy to maintain
    - Can be employed for multiple purposes
  - LDAP architecture is Client / Server based

Digital Authentication used by many OS ...

- ✓ NTLM (Network LAN Manager)
  - Was developed by Microsoft
  - Employs challenge / response authentication protocol uses an encryption and decryption mechanism to send and receive passwords over the network.
  - This method is no longer used or supported by new versions of Windows OS
- ✓ Public Key Infrastructure (PKI)
  - Also known as Public Key Encryption
  - It is a method in which a user keeps a private key and the authentication firm holds a public key .
  - The private key usually kept as digital certificate on the users system.
- ✓ RADIUS (Remote Authentication Dial-In User Services)
  - It is a method commonly used by a network device to provide centralized authentication mechanism.
  - It is Client / Server based, uses a dial-up server, a Virtual Private Network (VPN) , or a Wireless Access Point communicating to a RADIUS server

Digital Authentication used by many OS ...

- ✓ SSL (Secure Sockets Layers)
  - Was developed by Netscape Communications
  - To provide secure communication between client and server.
  - SSL is a method in which authentication information is transmit over the network in encrypted form.
  - Commonly used by websites to source client communications.
- ✓ SRP (Secure Remote Password)
  - Was developed by Stanford University, USA
  - It is a protocol in which the password is not secure locally in an encrypted or plain text form.
  - Very easy to install.
  - Does not require client or server configuration .
  - This method is invulnerable to brute force or dictionary attacks.

Authorization

- ✓ Authentication is the process of providing that users really are who they claim to be.
- ✓ Authorization is the process that decides whether users are permitted to perform the functions to they request.
- ✓ Authorization is not performed until the user is authenticated.
- ✓ Authorization deals with privileges and rights that have been granted to the user.

User Administration

- ✓ Administrators use this functionality to create user accounts, set password policies and grant privileges to user.
- ✓ Improper use of this feature can lead to security risks and threats.
- ✓ Note : User Administration and Password policies will be discussed in Next Unit (Chapter III and Chapter IV in Text book)

Password Policies

A good **password policy** is the first line of defense against the unwanted accessing of an operating system. Usually, hackers try to access the system through the front door using an account and password. If this method fails, they try other methods. In fact, most hackers utilize tools that use the dictionary method to crack passwords. These tools use the permutation of words in the dictionary to guess the password. As the system administrator, you should work with the security manager to establish a password policy to make it difficult for hackers to enter your system.

There are many different practices and policies that you can adopt for your company. However, the best password policy is the one that matches your company missions and is enforced at all levels of the organization. The following password practices—all or a combination of them—can be employed to devise a policy plan that suits your company.

- **Password aging**—Tells the system how many days a password can be in effect before it must be changed. Most companies practice a three-month policy, but you should determine the number of days based on your business and security requirements.

- **Password reuse**—This practice can be interpreted and applied in three different ways:
  - Tells the system how many times you can reuse a password
  - Indicates the number of days that must pass before you can reuse a password
  - Determines whether the system allows passwords to be reused
- **Password history**—This practice is related to password reuse, and it tells the system how many passwords it should maintain for an account. The password history can be used to determine if a password can be reused or not.
- **Password encryption**—A method that encrypts (scrambles) the password and stores it in a way that it cannot be read directly.
- **Password storage**—The place where the password is stored and kept hidden from the public.
- **Password complexity**—This is one of the most important password practices that should be implemented for any password policy. Complex passwords are those that are made up of a combination of upper- and lowercase letters, digits, and symbols. Having a password complexity requirement forces users to choose a password that is not easily cracked. The following is a list of standards that can be used when creating complex passwords:
  - The password must contain digits, symbols, and alphabetic characters (a-z, A-Z, 0-9, !@#$%^&*()_+}{":><?).
  - The password must have a minimum length which is usually six characters, but eight characters are recommended.
  - The alphabetical characters must use mixed letter cases (uppercase and lowercase).
  - The password must not contain any part of your account, first name, last name, birthday, telephone number, license number, registration number, employee number, spouse's name, child's name, parent's name, sibling's name, city you live in, or country in which you reside.

- **Logon retries**—A good practice is to allow a user to unsuccessfully try to log on up to three times before the account is locked and an administrator is contacted.
- **Password protection**—Although this practice is very hard to enforce, you, the manager, system administrator, security manager, or human resources manager, must train your employees and make them aware of the danger of concealing a password in a place from which it can be retrieved in case it is forgotten. It is bad practice to record a password on paper even if the paper is stored in a locked place. If you must record a password, use an encrypted file that can be accessed only by you.
- **Single sign-on**—Single sign-on allows you to sign on once to a server (host machine) and then not have to sign on again if you go to another server where you have an account. Although a single sign-on provides great convenience, it should not be practiced for mission-critical operations, financial institutions, government agencies, or other similar organizations.

Vulnerabilities of OS

- ✓ The top vulnerabilities to Windows Systems
  - IIS (Internet Information Server)
  - MSSQL (Microsoft SQL Server)
  - Windows Authentication
  - IE (Internet Explorer)
  - Windows Remote Access Services
  - MDAC (Microsoft Data Access Components)
  - WSH (windows Scripting Host)
  - Microsoft Outlook and Outlook Express
  - Windows Peer-to-Peer File Sharing (P2P)
  - SNMP (Simple Network Management Protocol

- ✓ The top vulnerabilities to UNIX Systems
  - BIND Domain Name System
  - RPC (Remote Procedure Call)
  - Apache Web Server
  - General UNIX authentication accounts with no / weak passwords
  - Clear text services
  - Sendmail
  - SNMP (Simple Network Management Protocol
  - Secure Shell
  - Misconfiguration of Enterprise Services NIS/ NFS
  - Open SSL (Secure Socket Layer)

E-mail Security

- ✓ E-mail may be the tool most frequently used by hackers to exploit viruses, worms, and other computer system invaders.
- ✓ E-mail is widely used by public and private organizations as a means of communication
- ✓ E-mail was the medium used in many of the most famous worm and virus attacks
- ✓ For example :
  - Love Bug Worm
  - I LOVE YOU worm
  - Mydoom worm
  - Melissa virus
- ✓ E-mail is not only to used to send viruses and worms, nut to send spam e-mail, private and confidential data as well as offensive messages
- ✓ To prevent from these activities ,
  - Do not configure e-mail server on a machine in which the sensitive data resides
  - Do not disclose the e-mail server technical details

CT-1 Question pattern

Total Marks - 25

MCQ - **Part – A** (10 * 1 Mark = 10 Marks)

Descriptive - **Part – B** (3 * 5 Marks = 15 Marks)

(Answer any three question out of four questions)

References :

1) Hassan A. Afyouni, “Database Security and Auditing”, Third Edition, Cengage Learning, 2009

2) Charu C. Aggarwal, Philip S Yu, “Privacy Preserving Data Mining”: Models and Algorithms, Kluwer Academic Publishers, 2008

3) Ron Ben Natan, ”Implementing Database Security and Auditing”, Elsevier Digital Press, 2005.