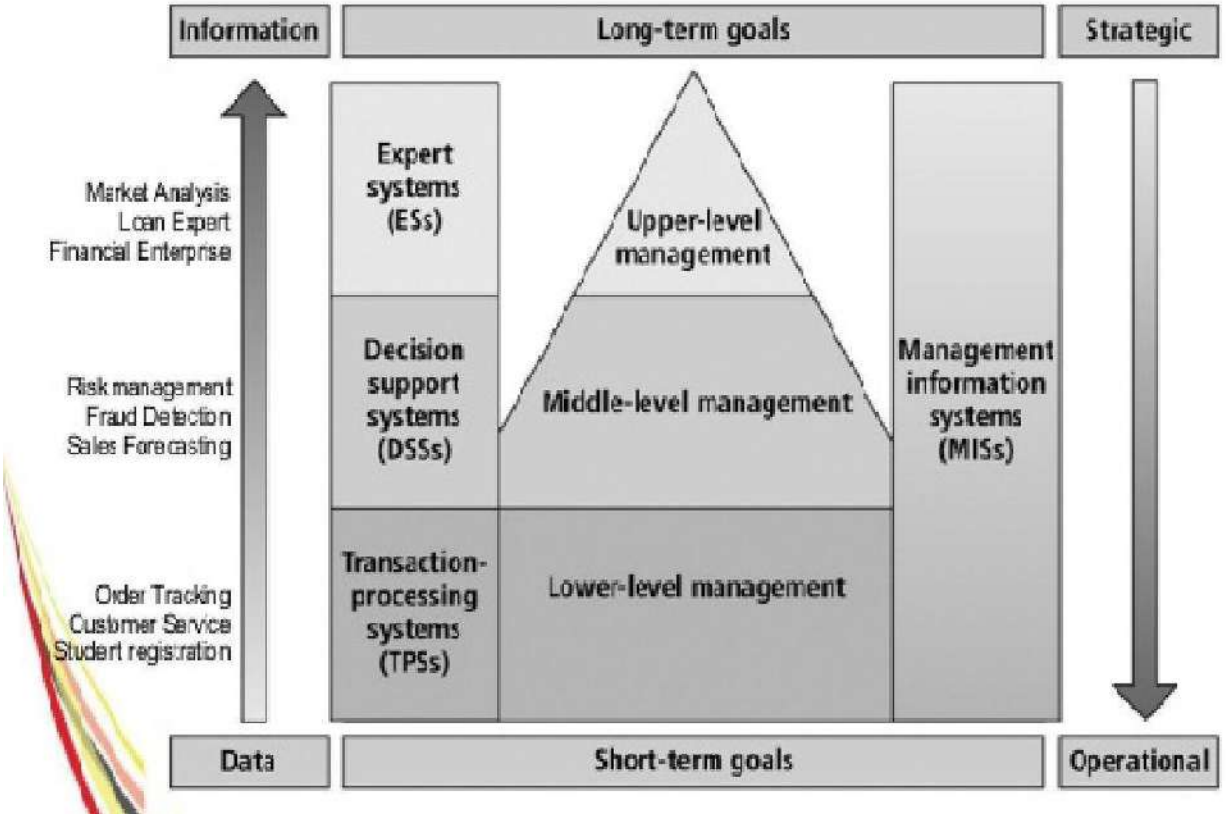
Unit 1 - Security Architecture

Security Architecture: Introduction

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

Information System

1. In today's global market, corporate companies all over the world to gain a portion of market share.
2. Wise decisions are not made without accurate and timely information.
3. At the same time integrity of information is more important.
4. The integrity of the information depends on the integrity of its data source and the reliable processing of the data.
5. Data is processed and transformed by a collection of components working together to produce and generate accurate information
6. These components are known as INFORMATION SYSTEM.
7. 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.
8. Information systems are categorized based on usage.
9. The following figure shows the typical use of system applications at various management levels



Information System mainly classified into three categories

1) **TransactionProcessingSystem(TPS)**
2) **DecisionSupportSystem(DSS)**
3) **ExpertSystem(ES)**

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)	▪ Ordertracking ▪ Customerservice ▪ Payroll ▪ Accounting ▪ StudentRegistration ▪ Sales
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	▪ RiskManagement ▪ FraudDetection ▪ Salesforecasting ▪ Caseresolution

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

Components of Information System

- ✔ Data – The information stored in the Database for future or processing
- ✔ Procedures – 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
- ✔ People – DBA, System Admin, Programmers, Users, Business Analyst, System Analyst

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

DBMS

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

Purpose of DBMS

1. Data redundancy and inconsistency
2. Difficulty in accessing data
3. Data isolation – multiple files and format
4. Integrity problems
5. Atomicity of updates
6. Concurrent access by multiple users
7. Security problems

DBMS Architecture

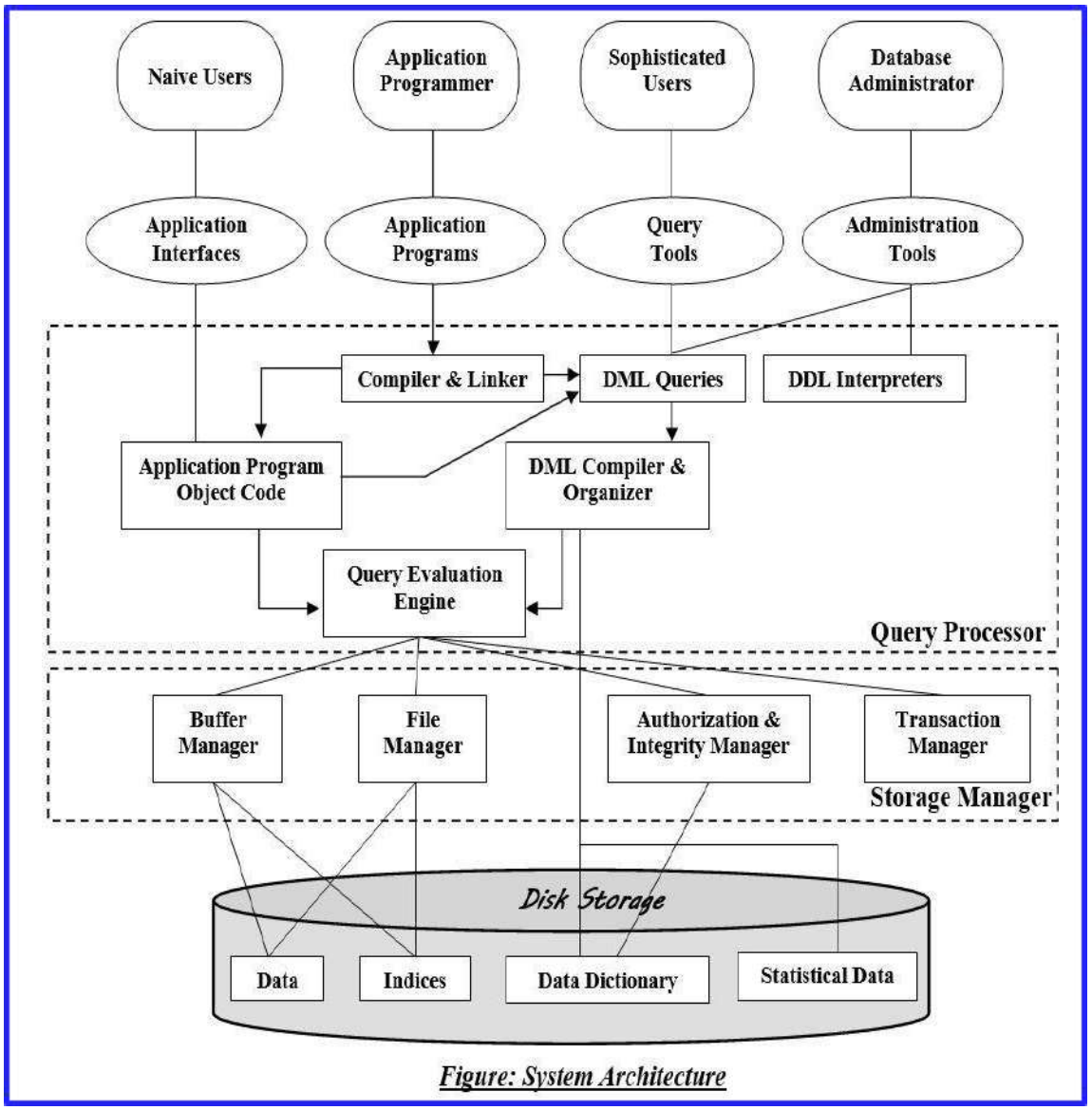


Figure: System Architecture

Information Security Architecture

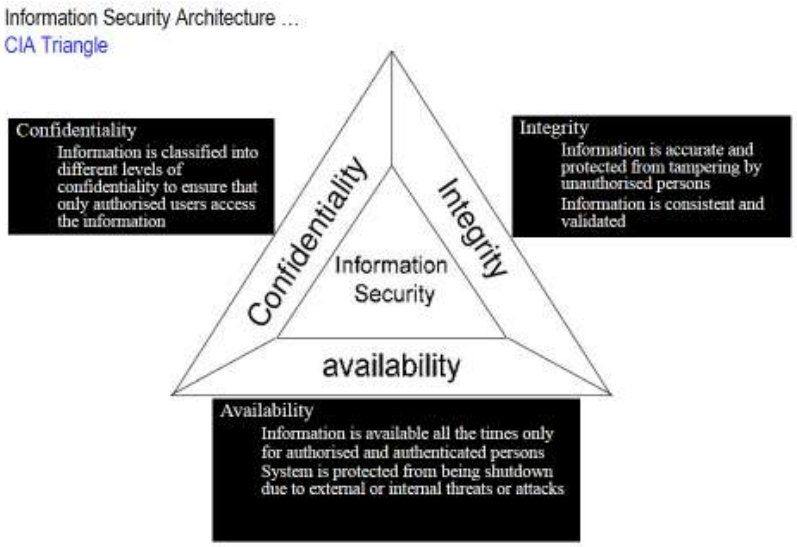
Information Security

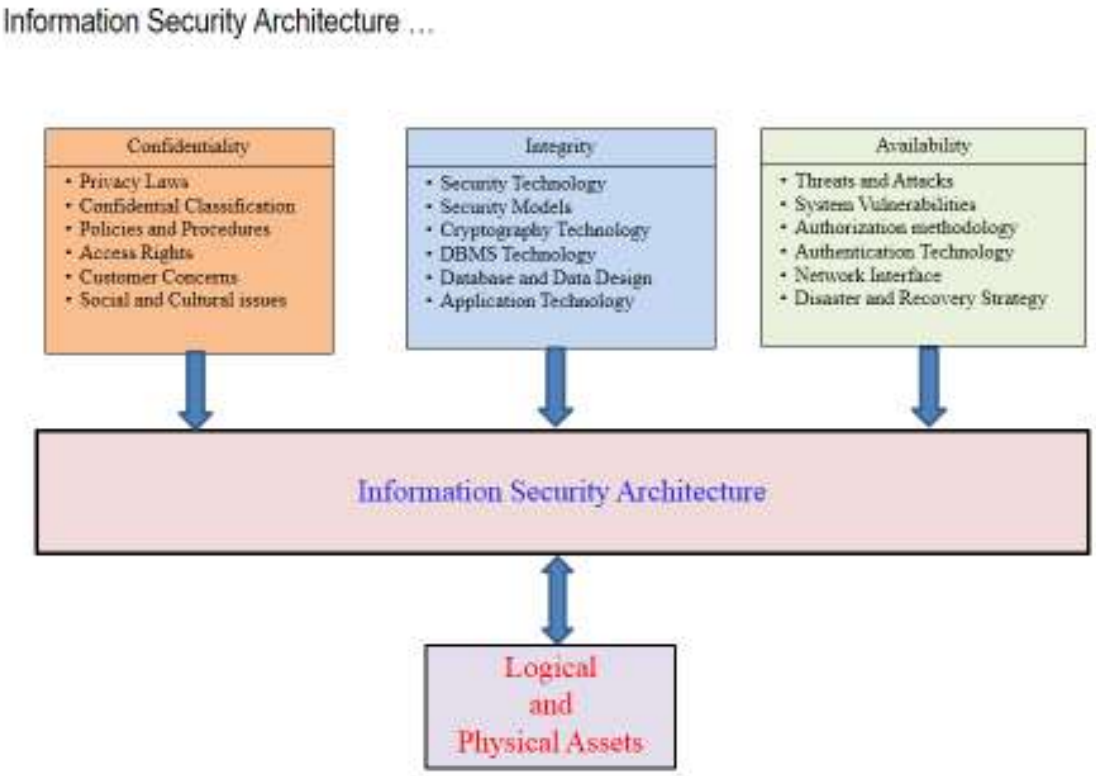
✔ Information is one of the most valuable asset in an organization

✔ Many companies have Information Security Department

✔ Information Security consists of the procedures and measures taken to protect each component of the information systems involved in protecting information

✔ According to the National Security Telecommunications and Information Systems Security Committee (NSTISSC) , the concept of CIA Triangle , in Which “C” stands for “Confidentiality”, “I” stands for “Integrity” and “A” stands for “Availability”





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

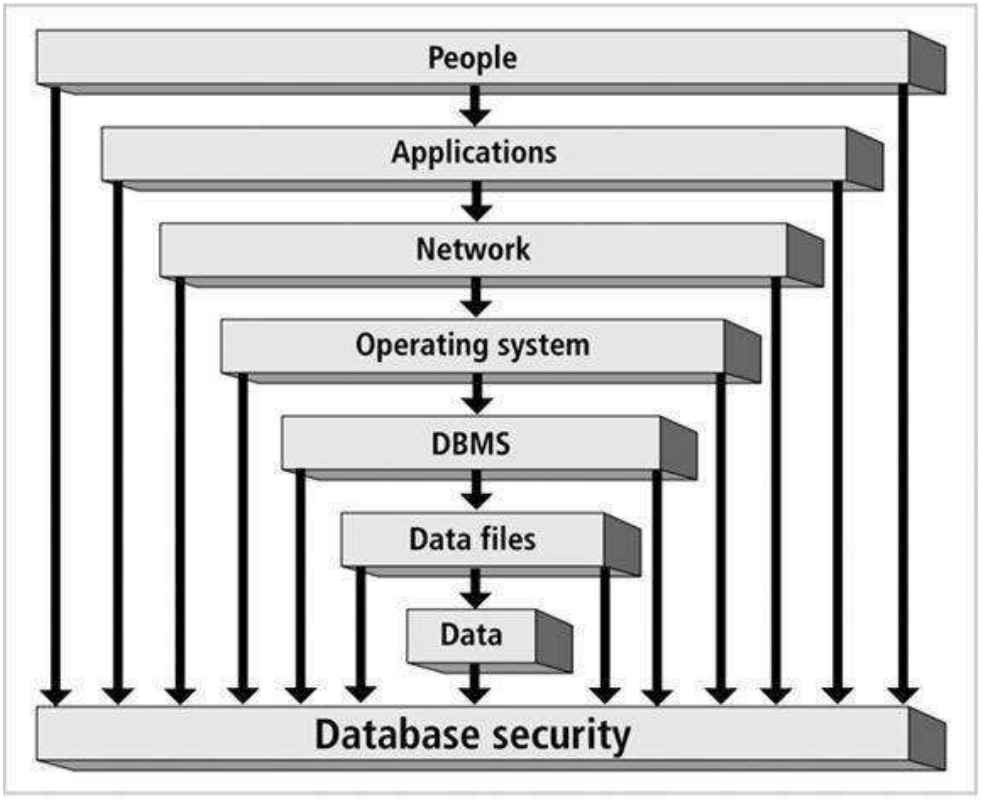
✔ Auditing Procedures and Tools
- Checks and Controls put in place to ensure that security measures are working

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

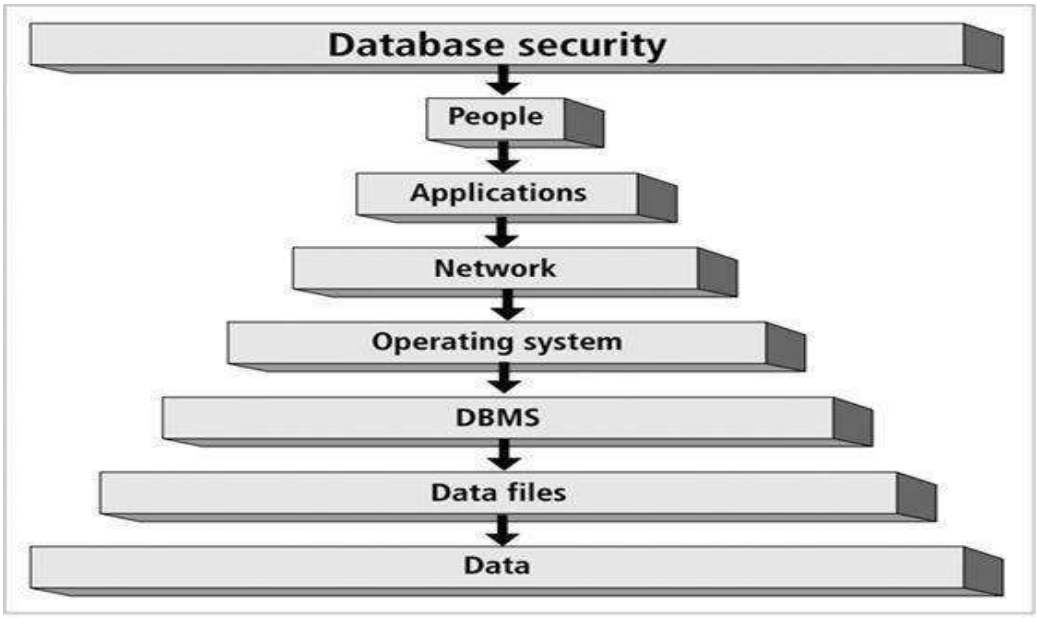
✔ The Security access points illustrated in the below figure



Database Security Access Points

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

Database security enforcement



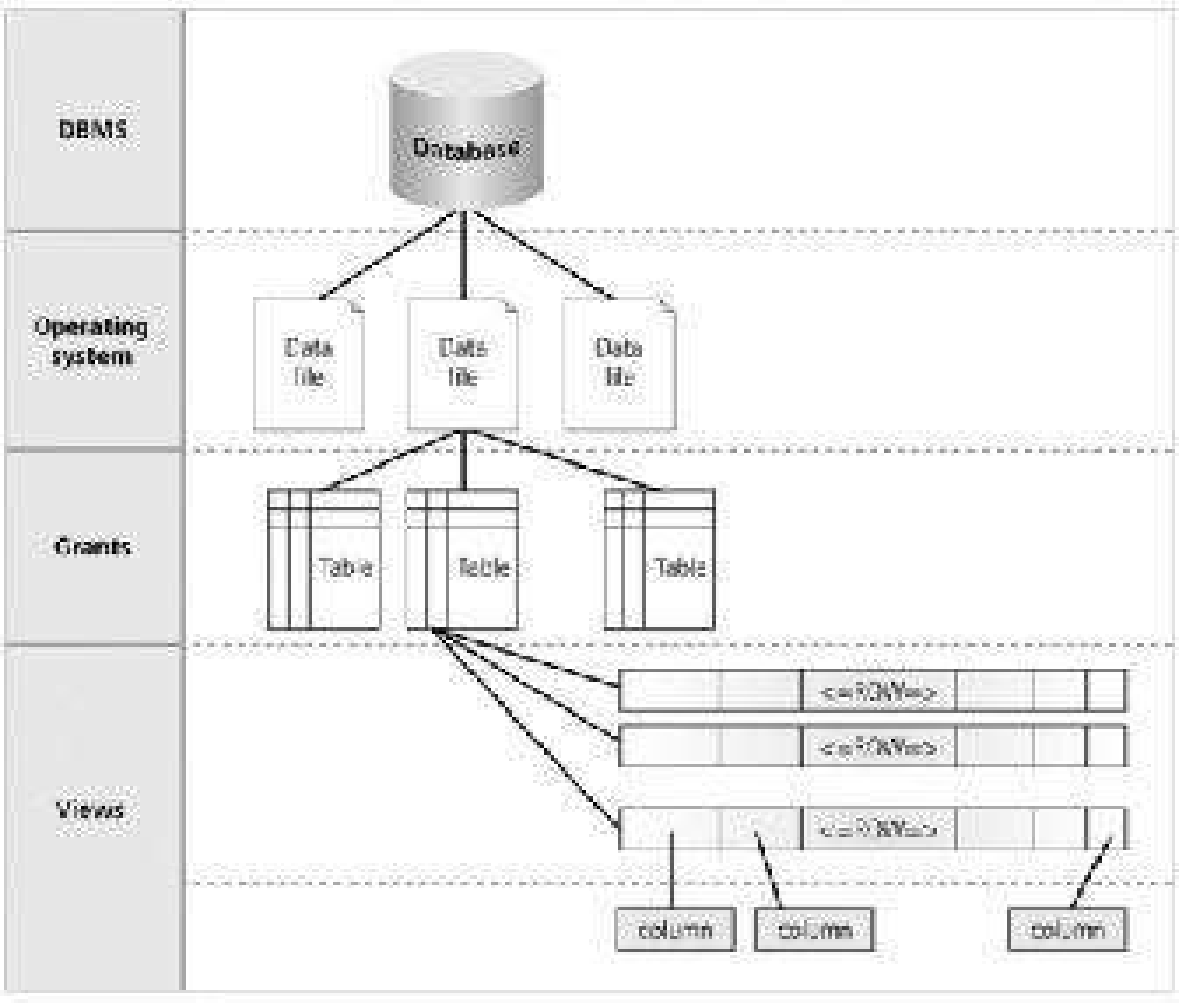
Data Integrity violation process

✔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.

Database Security Levels



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.

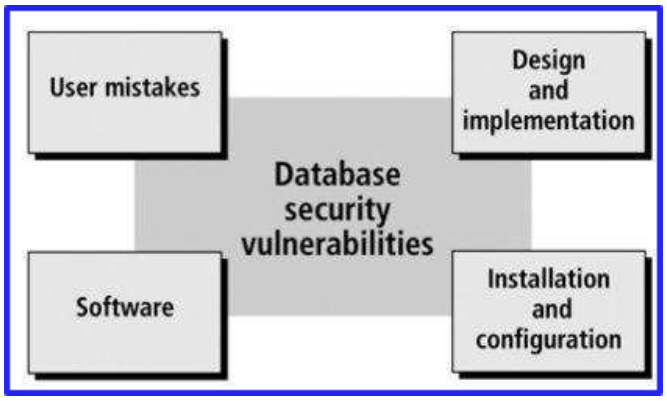
✔ Hackers usually explore the weak points of a system until they gain entry

✔ 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



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

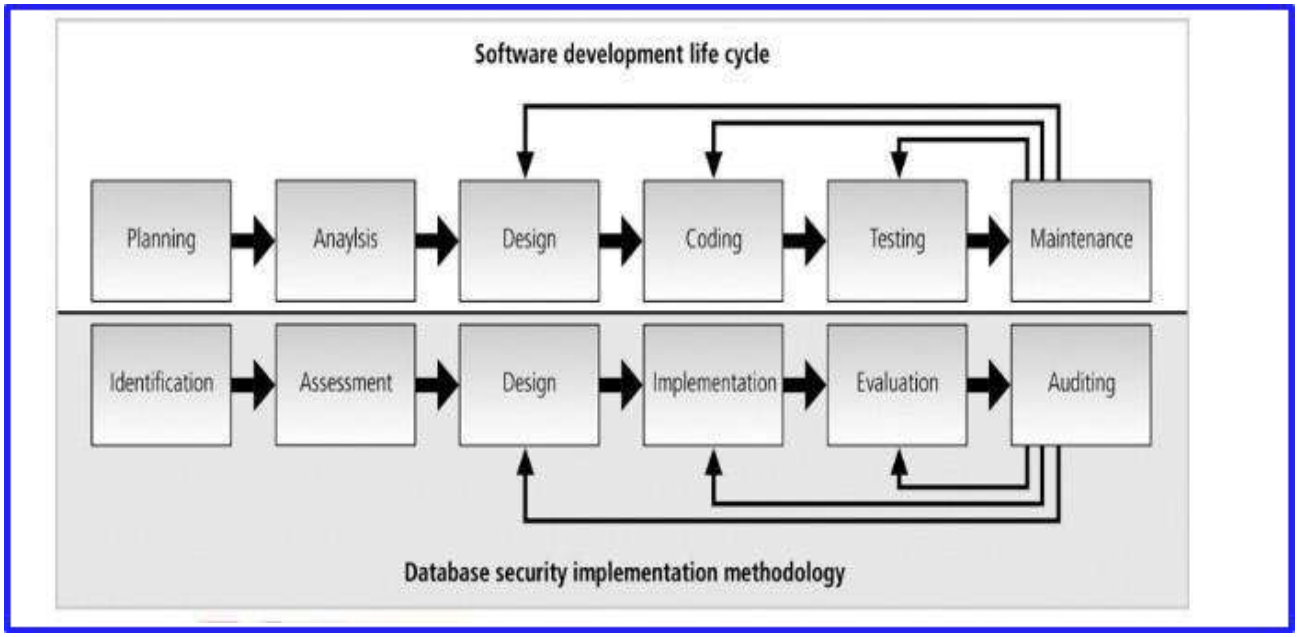
Security methods used to protect database environment components

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

Database Security Methodology

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



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 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 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 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 un authorised 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 …

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

- ✓ Multitasking
- ✓ Multisharing
- ✓ 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

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

Operating System Security Fundamentals

...

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

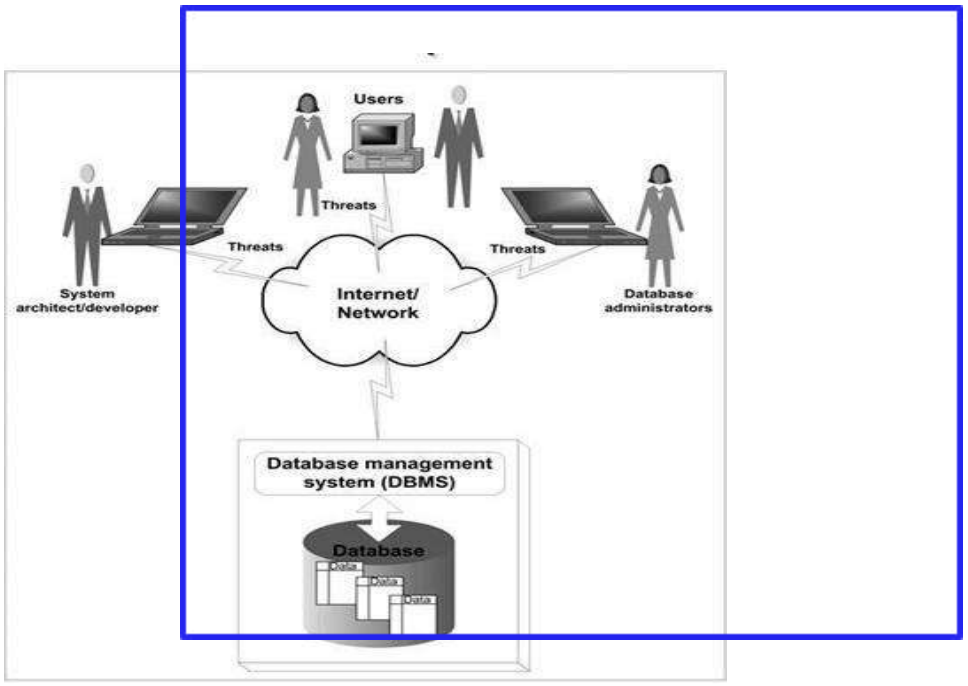
- ✓ Multitasking
- ✓ Multisharing
- ✓ Managing computer resources
- ✓ Controls the flow of activities
- ✓ Provides a user interface to operate the computer
- ✓ Administers user actions and accounts
- ✓ Runs software utilities and programs
- ✓ Provides functionalities to enforce the security measures
- ✓ Schedules the jobs and tasks to be run
- ✓ Provides tools to configure the OS and hardware

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**

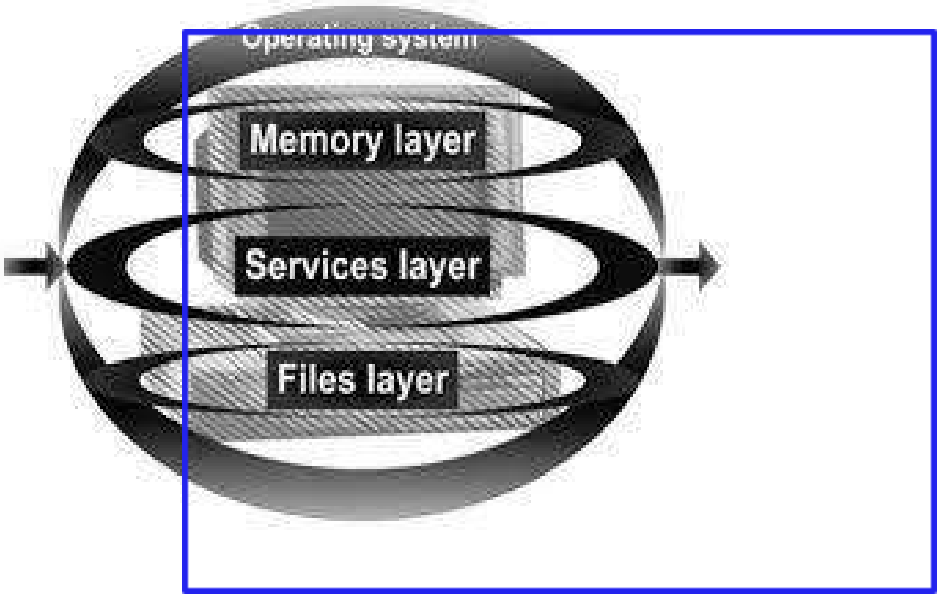
The OS Security Environment

- ✔ **A compromised OS can compromise a Database Environment**
- ✔ **Physically protect the computer running the OS(Padlocks, Chain locks, Guards, Cameras)**
- ✔ **Model :**
  - **BankBuilding–OS**
  - **Safe–DB**
  - **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.

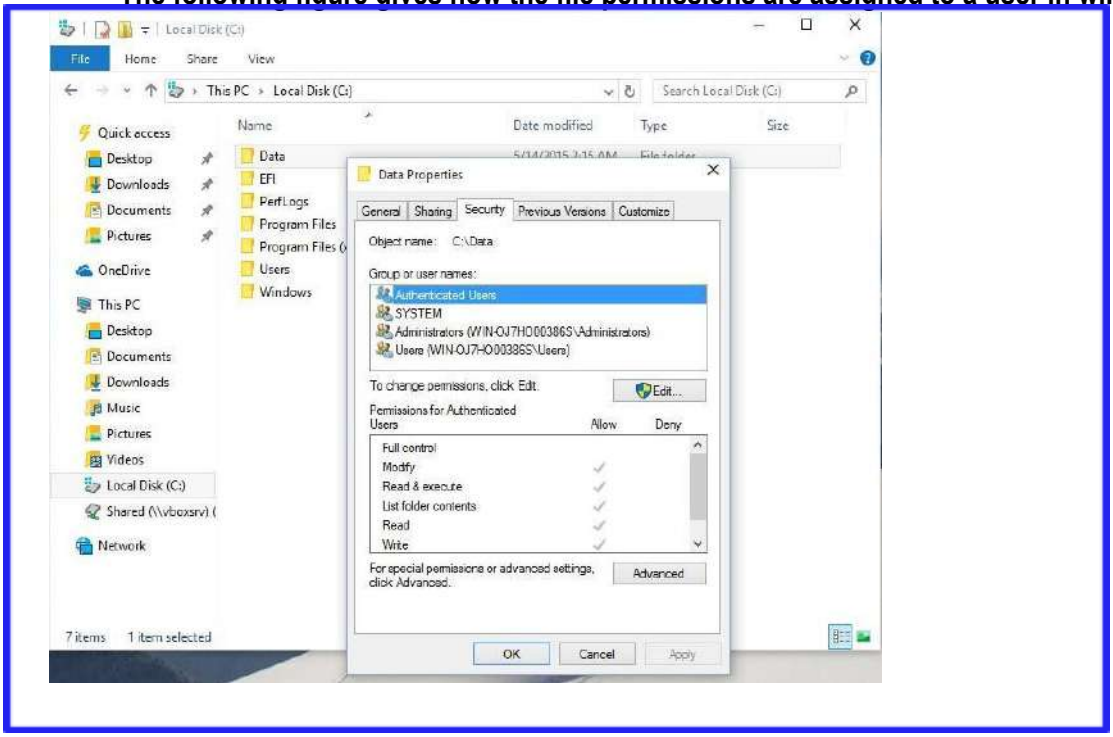
Files

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

Files …

File Permission

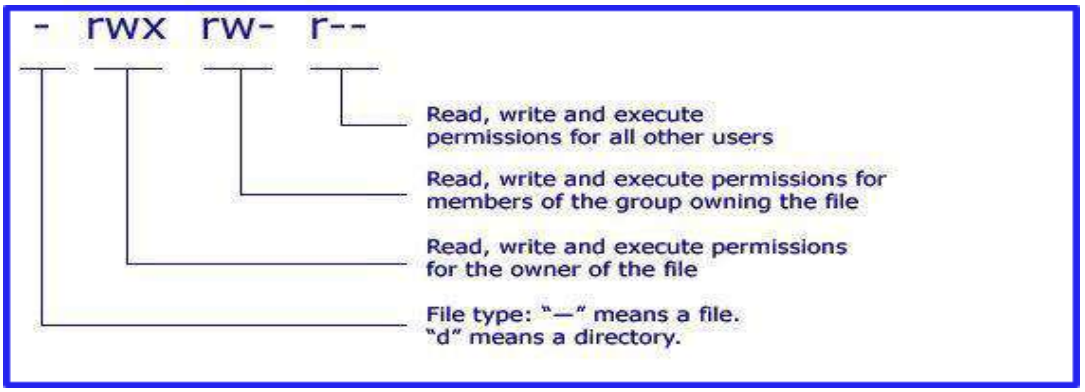
- **Every OS has a method of implementing file permission to grant read, write or execute privileges to different users.**
- **The following figure gives how the file permissions are assigned to a user in windows**



✔ 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.
✔ 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. FirstrwxisOwnerofthefile
2. SecondrwxisGrouptowhichownerbelongs
3. ThirdrwxisAllotherusers

✔ The given images gives the details of UNIX file permission.



Security Environment

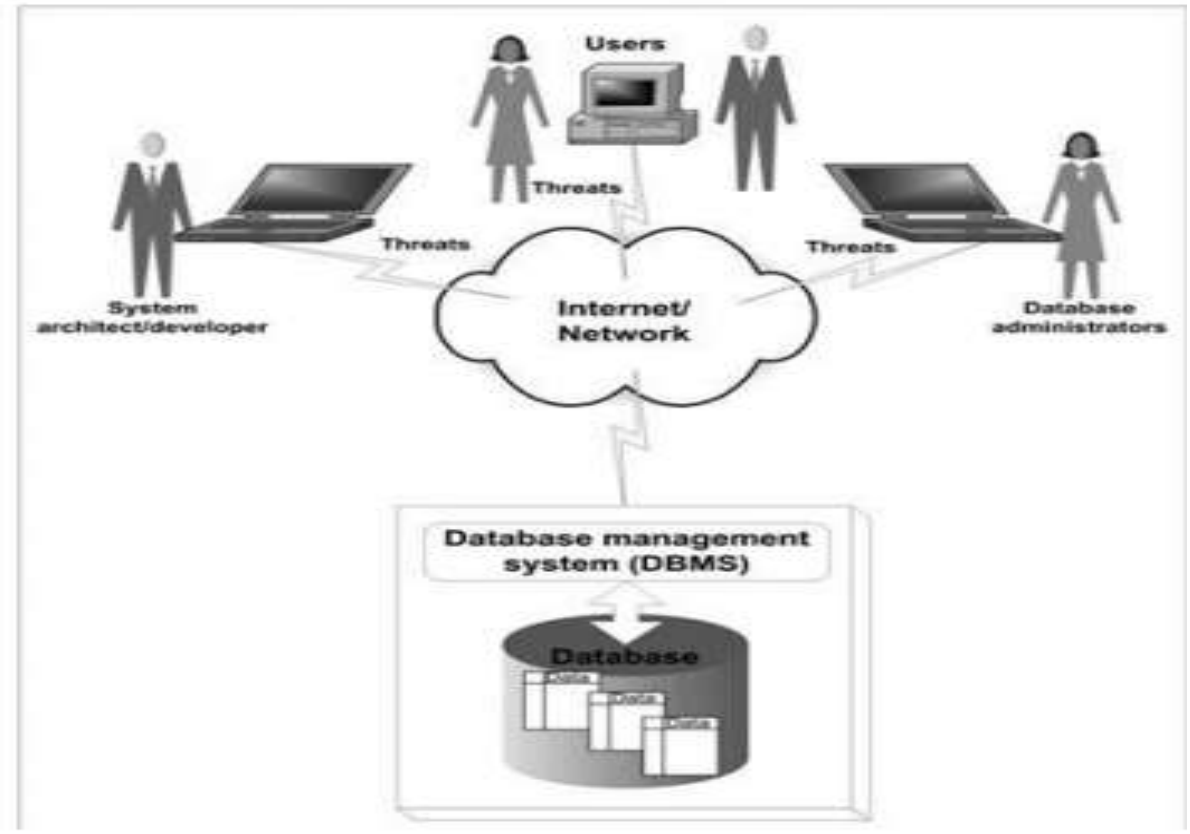
A compromised OS can compromise a

Database Environment

✔ Physically protect the computer running the OS(Padlocks, Chain locks, Guards, Cameras)

✔ Model :

- Bank Building – OS
- Safe – DB
- Money - Data



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

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

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

It is a process to very the user identity

Authentication is the fundamental service of the OS

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 identity of the user by means of digital mechanism or software

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 commun

Authentication is the process of providing that users really are who they claim to be.

Authorization

✔ 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

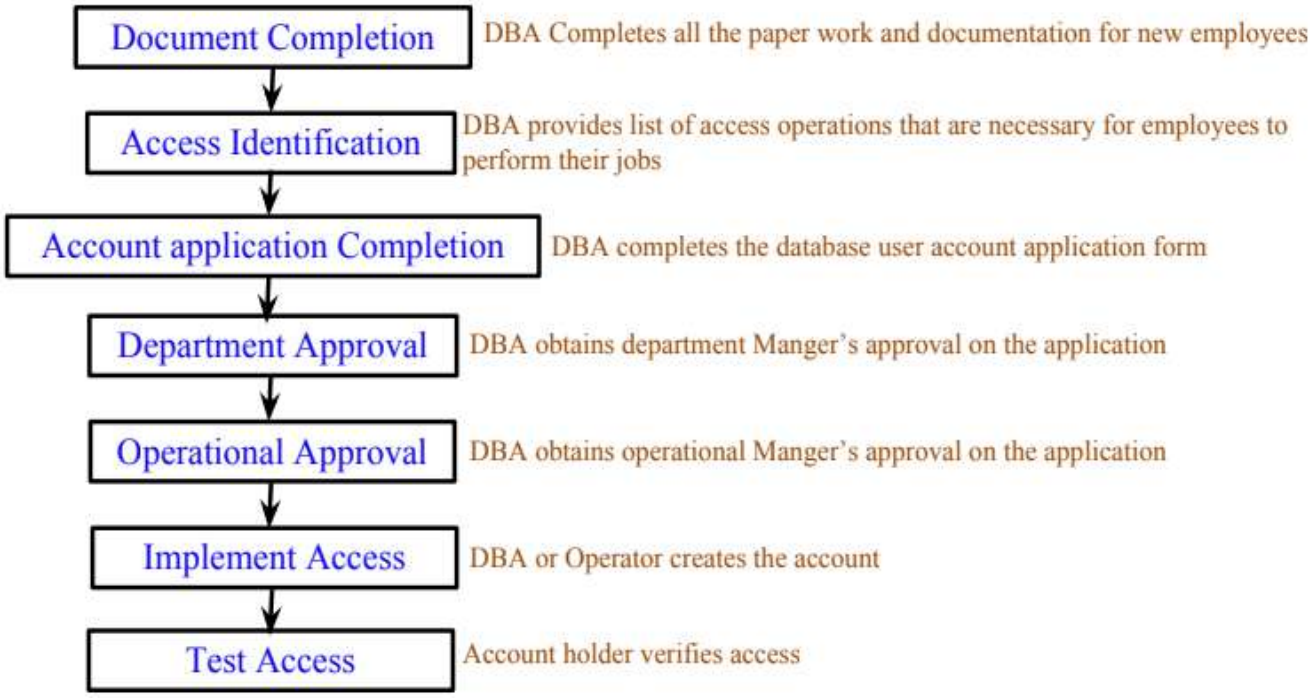
Administrators use this functionality to create user accounts, set password policies and grant privileges to user.

- ✔ Improper use of this feature can lead to security risks and threats. At every type of organization, many security violations are caused by negligence and ignorance and in particular by failing to consider documentation
- ✔ Documentation is a main part of administration process
- ✔ There top three excuses for failing to incorporate documentation
- ▪ Lack of Time
- ▪ Belief that the administration process is already in documented in the system
- ▪ Reluctance to complicate a process that is simple
- ✔ Everything is documented for two reasons
- ▪ To provide a paper trail to retrace exactly what happened when breach of security occurs
- ▪ To ensure administration consistency

Documentation in Administration

Administration Policies

- ▪ Documentation includes all policies for handling new and terminated employees, managers, system and database administrator, database managers, operation managers, and human resources.
- ▪ A detailed document should describe guidelines for every task that is required for all common administrative situations.
- ✔ Security Procedures
- ▪ This is an outline of a step-by-step process for performing administrative task according to company policies.
- ✔ Procedures implementation scripts and programs
- ▪ This is documentation of any script or program used to perform an administrative task.
- ▪ This includes user's manual and operational manual



Password policies

Password is key to opening the user account.

✔ The stronger the password, the longer it takes a hacker to break it.

✔ Many hackers security violations begin with breaking password.

✔ If you joining any financial company the orientation program on security administration including password selection, password storage, and the company's policies on password.Password policy is a set of guidelines that enhances the robustness

of the password and reduces the likelihood of its being broken

✔ Importance of Password Policies

▪ The frontline defence of your account is your password.

▪ If your password is weak, the hacker can break in, destroy your data, and violate your sense of security .

▪ For this specific reason, most of the companies invest considerable resources to strengthen authentication by adopting technological measures that protect their assets.

Designing password policies

Most companies use a standard set of guidelines for their password policies

✔ These guidelines can comprise one or more of the following

✔ Password Complexity – A set of guidelines used when selecting password, for example minimum

8 characters, 1 special character, 1 Capital letter, etc.,

The purpose of password complexity is to decrease the chances of a hacker guessing or breaking a password.

✔ Password Aging – Indication of how long the password can be used before it expires

✔ Password usage – Indication of how many times the same password can be used

✔ Password storage – A method of storing a password in an encrypted manner

Vulnerabilities of OS

A vulnerability is effectively an error in the code or the logic of operation within the OS or the application software. Because today's OSs and applications are very complex and include a lot of functionality, it's difficult for a vendor's development team to create software that contains no errors.

- **Application vulnerabilities**
  The Nimda and Aliz mail worms exploited Microsoft Outlook's vulnerabilities. When the victim opened an infected message – or even placed their cursor on the message, in the preview window – the worm file launched.
- **Operating system (OS) vulnerabilities**
  CodeRed, Sasser, Slammer and Lovesan (Blaster) are examples of worms that exploited vulnerabilities in the Windows OS – whereas the Ramen and Slapper worms penetrated computers via vulnerabilities in the Linux OS and some Linux applications.

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 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

Types of Email Attacks

Phishing

A phishing attack targets users by sending them a text, direct message, or email. The attacker pretends to be a trusted individual or institution and then uses their relationship with the target to steal sensitive data like account numbers, credit card details, or login information.

Spoofing

Spoofing is a dangerous email threat because it involves fooling the recipient into thinking the email is coming from someone other than the apparent sender. This makes spoofing an effective business email compromise (BEC) tool. The email platform cannot tell a fake email from a real one because it merely reads the metadata—the same data

the attacker has changed.

Internet Security

Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

Types of internet security threats

Malware: Short for "malicious software," malware comes in several forms, including computer viruses, worms, Trojans, and dishonest spyware.

Computer worm: A computer worm is a software program that copies itself from one computer to the next. It does not require human interaction to create these copies and can spread rapidly and in great volume.

Spam: Spam refers to unwanted messages in your email inbox. In some cases, spam can simply include junk mail that advertises goods or services you aren't interested in. These are usually considered harmless, but some can include links that will install malicious software on your computer if they're clicked on.

Phishing: Phishing scams are created by cybercriminals attempting to solicit private or sensitive information. They can pose as your bank or web service and lure you into clicking links to verify details like account information or passwords.

Botnet: A botnet is a network of private computers that have been compromised. Infected with malicious software, these computers are controlled by a single user and are often prompted to engage in nefarious activities, such as sending spam messages or denial-of-service (DoS) attacks.