

(A) Security Architecture (Introduction):

- Security means avoiding unauthorized access.
- Security breaches include: virus alerts, email spamming, identity theft, data theft, etc.
- Database security is the degree to which all the data is fully protected from tampering or unauthorized acts.

Information Systems: (Security Architecture):

- Wise decisions cannot be made without accurate and timely information. At the same time, integrity of information is important.
- The integrity depends on the source and 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.
- Information system can be a backbone of day to day operations of a company.
- Information Systems can be categorized based on usage.
- Information System can be classified into three categories:
 - ① Transaction Processing System (TPS)
 - ② Decision Support System (DSS)
 - ③ Expert System (ES)



(iv) Transaction Processing System (TAS): Characteristics.

- Also known as online Transaction Processing.
- Used for operational tasks.
- Provides solution for structured problems.
- Includes business transactions.

Typical Application System:

Order tracking, customer Service, Payroll, accounting, Student Registration, sales.

(*) Decision Support System (DSS): Characteristics.

- Deals with unstructured problems.
- Provides recommendations or answer to solve these problems.
- Capable of what-if? Analysis.
- Contains collection of business models.

Typical Application System:

Risk Management, fraud Detection, Sales forecasting, etc.

(**) Expert System (ES): Characteristics.

- Captures reasoning of Human Experts.
- Used by top level management.
- Branch of Artificial Intelligence.
- Concepts of Knowledge Base, Inference Engine, Rules.
- People consist of Domain Experts, Knowledge Engineers, Power users.

Typical Application System:

Virtual University Simulation, loan Expert, Market Analysis, Statistical tracking, Financial Enterprise.

Components of Information System:

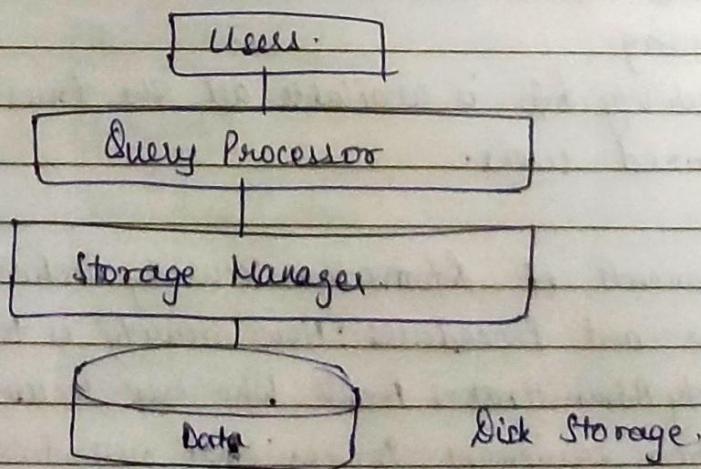
- ① Data
- ④ Software tools
- ② Procedures
- ⑤ Network
- ③ Hardware
- ⑥ People. (Users, System Analysts, Business Analysts, etc.)

(x) Database Management System:

- A collection of meaningful integrated information system.
- Both Physical and logical.
- Represents logical information in physical device.
- Mainly used for storing and retrieving data for processing.
- Uses client/server architecture.
- There is a set of programs to access the database.

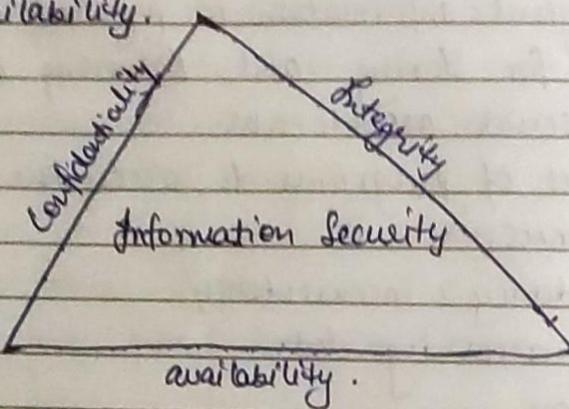
Purpose of DBMS:

- ① Data redundancy & inconsistency.
- ② Difficulty in accessing data.
- ③ Data Isolation
- ④ Integrity Problems.
- ⑤ Atomicity
- ⑥ Concurrent access.
- ⑦ Security Problems.



(ii). Information Security Architecture:

- Information is one of the most valuable asset in an organization.
- Many companies have Information security Department.
- It consists of the procedures and measures taken to protect each component of information systems.
- CIA triangle:
 - C → Confidentiality
 - I → Integrity.
 - A → Availability.

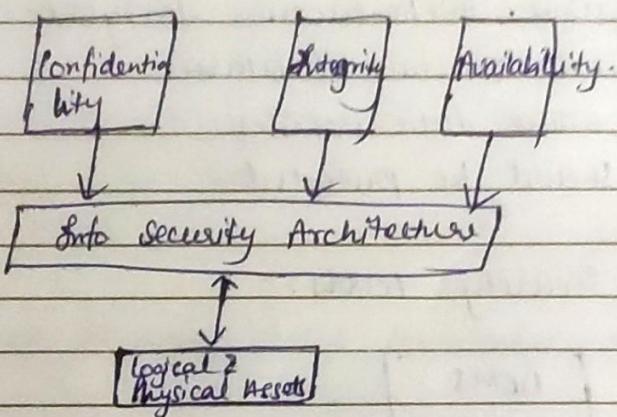


- Confidentiality: Info is classified into different levels of confidentiality to ensure only authorised users access the info.
- Integrity: Info is accurate and protected from tampering.
- Availability: Info is available all the times only for authorized users.

Components of Information Security Architecture:

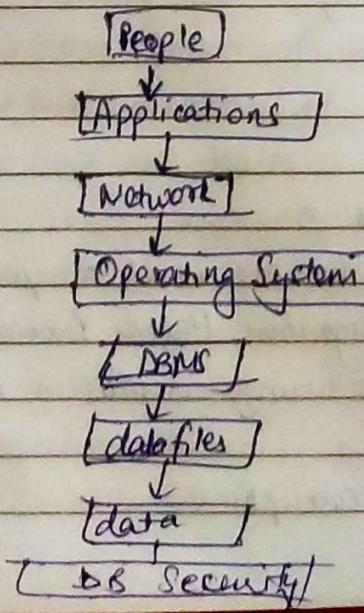
- ① Policies and Procedures: How security is to be carried out.
- ② Security Administrators: People who keep security in order.
- ③ Detection equipment: Devices that authenticate users.

- ④ Security Programs: Tools to protect computer systems & servers.
- ⑤ Monitoring Equipments: To monitor physical properties, employees, etc.
- ⑥ Monitoring Applications: Applications used to monitor network traffic.
- ⑦ Auditing, Procedures and tools: Ensures that security measures are working.



⑧ Database Security:

- One of the functions of DBMS is to empower DBA to implement security at all levels.
- Security access point: A place where database security must be applied.
- Database security Access points:



Database Security Access Points:

- ① People: Individuals who have been granted privileges and permissions.
 - ② Applications: Application design and implementation
 - ③ Network: Protect the N/W. Most sensitive. See APIs.
 - ④ Operating systems: Authentication to system.
 - ⑤ DBMS: logical structure of database.
 - ⑥ Data files: where data resides.
 - ⑦ Data: ~~data~~ should be protected.
- (*) Database Security levels:

DBMS
Operating Systems
Grants
Views.

Menaces to databases:

- ① Security Vulnerability
- ② Security Threat
- ③ Security Risk.

Examples of Risk Types:

- ① People: loss of people who are vital components.
eg: loss of key person (Migration, Health problems).
- ② Hardware: A risk that mainly results in hardware unavailability.
- ③ Data: Data loss or data corruption.

- ① Confidence: loss of procedural data, frauds, etc.
- (*) Asset Types and their values:
- Infrastructure of company operation.
 - 4 main types: also called tangible assets.
- ② Physical Assets: include buildings, cars, hardware, etc.
- ③ Logical Assets: logical aspects of Information System such as business applications, in-house programs, purchased software, OS, databases, data, etc.
- ④ Intangible assets: Business reputation, quality, public confidence.
- ⑤ Human assets: Human skills, knowledge and expertise.

(*) Database Security Methods:

Component	Security Methods.
① People	<ul style="list-style-type: none"> → Physical limits on access to hardware & documents. → Thorough process of identification & authentication. eg → ID cards, eye scans, passwords, etc. → Training courses on importance of security. → Establishment of security policies and procedures.
② Application.	<ul style="list-style-type: none"> → Authentication of users who access applications. → Business rules. → Single sign-on.
③ Network	<ul style="list-style-type: none"> → firewalls to block new intruders. → Use of VPN (Virtual Private N/w). → Authentication.
④ OS	<ul style="list-style-type: none"> → Authentication, → Intrusion detection. → Password Policies → User accounts.

Components

Security Methods.

- | | |
|---------------|---|
| ⑤. DBMS | → Authentication → Audit Mechanism |
| | → Database Resource Limits → Password Policy. |
| ⑥. Data files | → File Permission. |
| | → Access Monitoring. |
| ⑦. Data | → Data Validation → Data constraints. |
| | → Data Encryption |
| | → Data Access. |

Software development life cycle

Planning → Analysis → Design → Coding → Testing → Maintenance

Identification → Assessment → Design → Implementation → Evaluation → Auditing

Database security implementation methodology.

- Identification: Identification and investigation of resources required and policies to be adopted.
- Assessment: Analysis of vulnerabilities, threats, etc for both physical and logical DB security.
- Design: results in a blueprint of the adopted security model.
- Implementation: Code is developed or tools are purchased to implement the blueprint.
- Evaluation: Evaluate by testing the system against attack hardware failures, natural disasters & human errors.

→ Auditing: After production, security audits should be performed periodically to ensure security of the system.

(x) Operating System Security Fundamentals:

- Operating System is a collection of programs that allows the user to operate the computer hardware.
- OS is also known as "Resource Manager".
- OS is one of the main access points in DBMS.
- Computer System has 3 layers → ① Inner layer represents the hardware.
 ② Middle layer is the OS.
 ③ Outer layer is all different software.

→ Key functions and capabilities of operating system:

- ① Multitasking
- ② Multi sharing
- ③ Managing Computer resources.
- ④ Controls the flow of activities
- It also provides functionalities to enforce security.
- Different vendors of OS include:

⑤ Provides a user interface.

⑥ Administers user Actions.

⑦ Schedules jobs and tasks

⑧ Provides tools to configure OS &

Hardware.

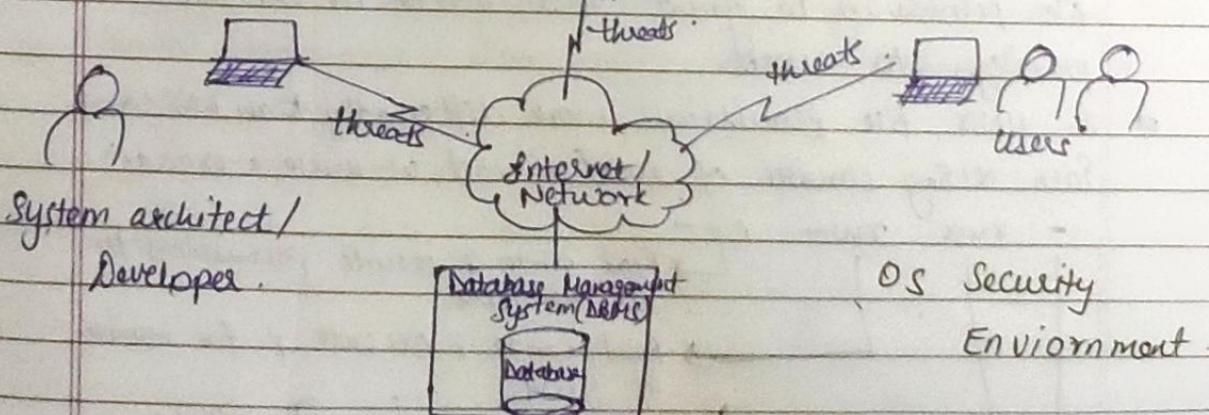
① Windows by Microsoft.

② UNIX by Sun Microsystems, HP & IBM.

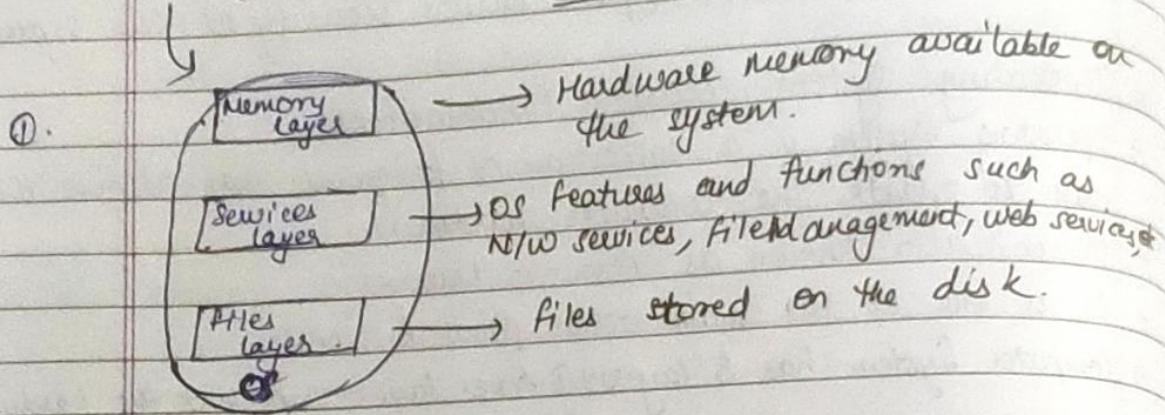
③ LINUX

④ Macintosh by Apple.

Q (Database Administrator)



Q8. 3 layer architecture: Component of OS Security Environment



②. Services:

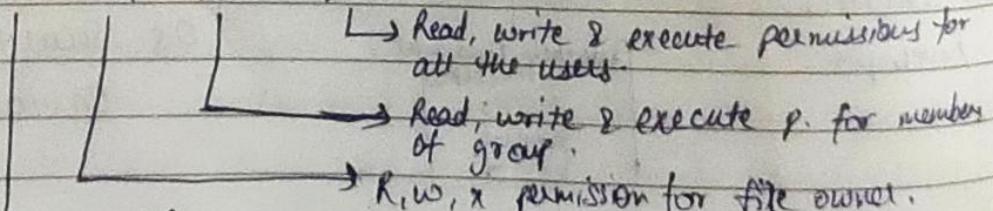
- Main component of OS security environment.
- Consists of functionalities that OS offer.
- Users employ these utilities to gain access to OS.
- If services are not secured and configured properly, each service becomes a vulnerability.

③. Files: Actions : ①. File Permission ②. File transfer ③. File sharing.

- File Permissions: Every OS has a method of implementing file permission to grant read, write or execute privileges to users.

● In UNIX, file permission work differently than Windows. Each setting consists of rwx (r-read, w-write, x-execute)

- rwx rw- r--



→ R, W, X permission for file owner.
→ File type. "-" means a file. "d" means a directory.

- file transfer:
 - ① Moving the files from one location to another in a disk / web / cloud.
 - ② FTP is an internet service that allows transferring of files.
 - ③ FTP clients and servers transmit username & passwords in plain text format (Not Encrypted).
 - ④ Any Hacker can sniff the traffic & get the login info.
 - ⑤ Some best practices for file transferring include:
 - Using the secure FTP utility.
 - Allow only authorized operators to have FTP privileges.
- File sharing① Sharing files naturally leads to security threats and risks.
 - ② Peer-to-Peer programs allow user to share files over internet.
- ④ Memory:
 - Memory is an access point to security violations.
 - There are many badly written programs that could change the content of the memory.
 - These programs do not perform deliberate destruction acts.
 - Programs that intentionally damage or scan data in the memory are the type that not only can harm the data integrity, but may also exploit data for illegal usage.

(*) Authentication Methods:

- Authentication is fundamental service of os.
- Process to verify the user identity.
- Two types:
 - ① Physical Authentication: Using magnetic cards and card readers to control entry in a building office, laboratory or data center.
 - ② Digital Authentication: Process of verifying the identity of user by means of digital mechanism or software.

(**) Digital Authentication Methods:

- ① Digital Certificates: Widely used in e-commerce.
 - File issued by a trusted party that verifies the identity of the holder.
- ② Digital token (Security Token):
 - Small electronic device that users keep with them to be used for authentication.
 - It displays a unique number to the token holder which is used as a pin (Personal Identification Number).
- ③ Digital Card: → Also known as security card or smart card.
 - Similar to credit card without magnetic strip.
 - It has electronic circuit that stores identification info.
- ④ Kerberos: Enables two parties to exchange info. over network by assigning a unique key. This key is used to encrypt communicated messages.

- ⑤ LDAP (Lightweight Directory Access Protocol):
→ developed by University of Michigan, USA.
→ uses centralized directory database.
→ It is OS independent, it can be used across all platforms.
→ LDAP architecture is client / server based.
- ⑥ NTLM (Network LAN Manager):
→ developed by Microsoft.
→ employs authentication protocol.
- ⑦ Public Key Infrastructure (PKI):
→ Also known as Public Key Encryption.
→ A method in which user keeps a private key and authentication firm holds the public key.
- ⑧ RADIUS (Remote Authentication Dial-In-User Services):
→ Provides centralized authentication mechanism.
→ Client / server based, uses a dial-up server, a VPN or a wireless Access Point.
- ⑨ SSL (Secure Socket Layer):
→ Developed by Netscape Communications.
→ To provide secure communication b/w Client & Server.
- ⑩ SRP (Secure Remote Password):
→ Developed by Stanford University, USA.
→ Easy to install, does not require client server configuration.

(*) Authorization:

- Process that decides whether users are permitted to perform the functions for which they request.
- Authorization is not performed until the user is authenticated.
- ~~Authenticates~~ deals with privileges and rights that have been granted to the user.

(*) User Administration:

- ^{Authentication} ~~Administration~~ and authorization are essential services that every OS provides in order to secure access to computer's logical and physical resources.
- Another related service is User Administration.
- Administrators use this functionality to:
 - ① Create User Accounts.
 - ② Set Password Policies
 - ③ Grant Privileges to users.
- Improper use of this feature can lead to security risks and threats.
- Best practices for user Administration:
 - ① Use a consistent naming convention.
 - ② Always provide a password to user and force them to change it on first log on.
 - ③ Make sure that all the passwords are encrypted.
 - ④ Do not use default passwords.
 - ⑤ If a machine is compromised, change all the passwords of all existing accounts.
 - ⑥ Create a specific file system.
 - ⑦ Lock accounts that are not used for a specific time period.
 - ⑧ Perform random auditing procedures.

- ⑨ Do not grant privileges to all the machines, but only to those who are actually in need.
- ⑩ When a computer system is compromised, isolate the system from other systems.

(*) Password Policies:

- Usually hackers try to access the system using an account and a password. If this method fails, they try other methods.
- Most hackers utilise the tools that use dictionary method to crack passwords. These tools use permutations of the words in dictionary to guess the password.
- There are many different practices and policies that you can adopt for your company:
 - ① Password aging: Tells a system how many days a password can be effective before it must be changed. Many companies practice 3 month policy.
 - ② Password reuse: Tells the system how many times you can reuse a password or indicates the no. of days that must pass before you reuse a password. Also tells if you can reuse the password or not.
 - ③ Password history: Related to password reuse. Tells the system how many passwords it should maintain for an account.
 - ④ Password encryption: A method that encrypts a password and stores it in a way that it cannot be read directly.
 - ⑤ Password storage: The place where password is stored and kept hidden from the public.
 - ⑥ Password complexity: Complex passwords are the ones that are made up of a combination of upper case, lower case letters, symbols and numbers. The password must have a minimum length of 6 characters.

- ⑦ Logon retries: A good practice is to allow a user to try 3 times before the account is locked and administrator is contacted.
- ⑧ Password Protection: This practice is hard to enforce. If you record a password, use an encrypted file that can only be accessed by you.
- ⑨ Single sign-on: Allows you to sign on once to a server and not have to sign in again on a different server if you have an account.

(*) Vulnerabilities of Operating Systems:

- Vulnerability means Susceptible to Attacks.
- Hackers usually explore the weak points of the system until they get an entry.
- Types of Vulnerabilities:
 - (a) Installation and configuration: Results from default installation configuration that is known publically. Does not enforce any safety measures.
 - (b) User mistakes: Carelessness in implementing procedures, accidental errors, failure to follow through, etc.
 - (c) Lack of auditing controls, untested recovery plan, lack of activity monitoring, lack of protection against malicious codes, etc.
 - (d) Software: Software contains bugs, etc.
 - (e) Design and Implementation: Related to improper designs, coding problems, input data not validated, etc.
- Vulnerabilities of OS:
 - ① IIS (Internet Information Server)
 - ② MSSQL (Microsoft SQL Server)

- ④ windows Authentication
 - ⑤ IE (Internet Explorer)
 - ⑥ Microsoft Outlook & Outlook Express
 - ⑦ windows Peer to peer file sharing (P2P)
- Top vulnerabilities to UNIX Systems:
- ① BIND domain Name
 - ② RPC (Remote Procedure call)
 - ③ Apache web server
 - ④ clear-text services
 - ⑤ sendmail
 - ⑥ Open SSL (Secure Socket Layer)

* E-mail Security :-

- As email is widely used method of communication, it is susceptible to various security risks, including unauthorized access, data breaches, phishing attacks, malware infections and spam.
- Here are some key aspects of email security :-

1. Encryption :-

2-types of e-mail encryption

TLS

end-to-end encryption

(Transport layer security)

securing the connection

betⁿ mail servers

2. Secure protocols :-

→ Using secure protocols such as SSL or TLS is essential for encrypting the connection betⁿ email clients and servers.

→ These protocols prevent eavesdropping and man-in-the-middle attacks.

3. Strong authentication.

4. Anti-malware and anti-spam filters.

5. User awareness and training.

6. E-mail gateway security :- analyze incoming and outgoing email traffic, detect threats and block malicious content before it reaches the user's inbox.
7. E-mail retention and archiving :- ensures that important emails are securely stored and can be retrieved when needed.
8. Regular updates and patching
9. Data loss prevention, :- DLP mechanism monitor and control outgoing email contents to enforce security policies.
10. Incident response and monitoring :- This includes monitoring for suspicious activity, investigating potential breaches and promptly addressing any security issues.

* Internet Security :-

- Refers to the practice of protecting communication and data transmitted over the internet from unauthorized access, theft and other security threats.
 - Two commonly mentioned used security protocols are :-
- (i) IPsec (ii) SSL/TLS
-
- IPsec :-
 - Securing IP communications
 - operates at the new layer of TCP/IP and offers a range of security services including authentication, encryption and data integrity.
 - IPsec can be used to establish secure virtual private networks (VPNs) between networks or individual

RANKA
DATE / / /
PAGE / / /

devices ensuring data transmitted between them remains secure and protected

(ii) SSL/TLS :-

- provides security at transport layer.
- TLS is updated and more secure version than it is widely used today.
- primarily used to secure communication b/w web browsers and web servers.
- SSL/TLS uses a combination of symmetric and asymmetric encryption algorithms to establish a secure, encrypted connection b/w a client (e.g., web browser) and a server (web server).
- prevents from eavesdropping or unauthorized access of login credentials or financial data.

Other notable protocols ~~and~~ and technologies include → firewalls

- IDS (Intrusion Detection System)
- Antivirus s/w