Information Security

Unit - I

Define security and important terms used.
The meaning of the term computer security has evolved in the recent years. most puple idea of computer security focus on the physical machine. Traditionally computer resibilities have been physically protected for three resions. These three resions are—
(i) to prevent from damage to the hardware.
(ii) to prevent from damage to the information (software).
(iii) To preavent from theft and damage the service

Computer security is security applied to computing device such as computer and smart phones as well as computer networks such as private and public networks including the whole internet. The field covers all the processes and mechenisms by which digital equipment information and services are protected from unintended and unauthorized acces, change or distruction and are of growing importance in the line with the increasing reliance of computer system. Therefore we have to concious with the physical security as well as the software field it is some time

refers to as "cyber security" or "IT security".

Some important terms used in computer security are :-

1. Vulnerability :-
It is the weakness which allows an attacker to reduce a system information ensurance. Vulnerability is the intersection of three elements -
(a) A system susceptability or flow.
(b) attackers access to the flow.
(c) attackers capability to explored the flow.
It is also known the attack surface.

2. Backdoors - (It is done by hackers)
A backdoor in a computer system is a method of by passing normal authentication, security remode access to a computer obtaining access to plane text and so on. while attempting to resion/remain undetected.

A backdoor may take the form of an installed program or could be a modification to an existing program or hardware device it may take also fake. information about disk and memory uses.

3. Denial of service attack :-
A denial of service (DOS) attack is an attempt to overload a website or network, with the aim of degrading its performance or even making it completely inaccessible.

Typically a successful DOS attack will result in loss of availability of part, or all of a system and consume time and money to analyse, defend and recover from.
Different types of DOS attack target different parts of a system for instance, a DOS attack can target a network's capacity to send & receive traffic or the processor limitations of server.

4. Direct - access attack :-
A direct access attack is an attack where a hacker is able to gain access to a computer and be able to directly download data from it. They will be able to compromise security by modifying that software and adding key loggers, worms etc.
Eavesdropping is listening to a private conversation between hosts & networks.

5. Tempering :-
Tempering is the deliberate and unauthorized modification of digital

content, system settings, or data packets.

Tempering in information security refers to the unauthorized alteration or modification of data or systems. It is a type of security breach where an attacker changes information to deceive, manipulate or cause harm.

6. Computer crime :-

Computer crime is any illegal activity involving a computer, networked device, or network. It include offenses where computer are the tool, target or place of criminal activity.

Classification of computer crimes :-

1. Offenses against confidentiality, integrity & availability.

Hacking :- Unauthorized access to system or data.

Denial of service - Flooding a target to disrupt services.

Malware attacks :- Viruses, worms, ransomware altering or destroying data.

2. Computer as a tool.

Identity theft :- Using stolen personal data to impersonate victims.

Financial fraud :- ATM ~~skimming~~ Skimming, online banking. Trojan attacks.

3. Computer as a target.

Website defacement - unauthorized modification of web content

Data Breaches - stealing sensitive information from ds.

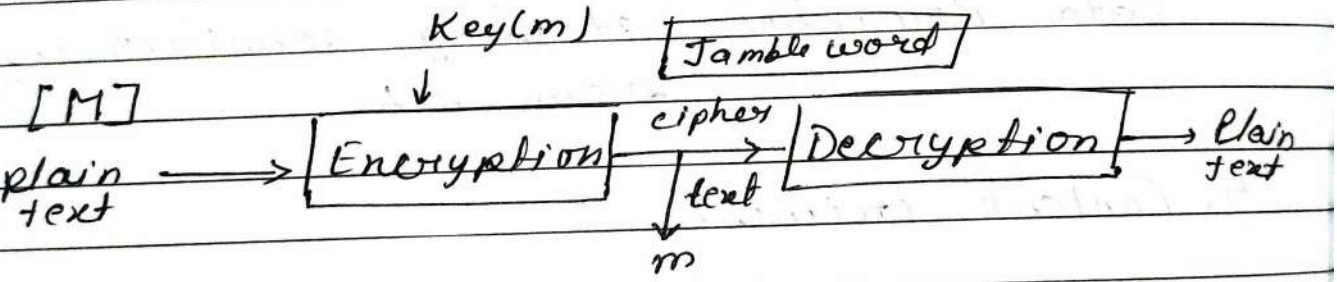
4. Content crimes -

Cyberstalking & Harassment :- Repeated unwanted online contact.

copyright ~~infrig~~ infringement :- Piracy of music, films.

Information Security

Define cryptography ?
Cryptography is a technique of securing information and communication through used of forces so that only those person for the information is intended can understand it an process to information. The prefix "crypt" means hidden and suffix "graphy" means writing.



A Hacker such kind of techniques are called cryptography. It includes the special word known a CIA which means confidentiality, Integrity and availability.

In cryptography the techniques which are used to protect information are obtained from mathematical concept and set of rules based on calculation known as algorithm to convert in message in ~~the~~ which based that make

hard to decode it. This algorithm used for cryptographic Key generation digital sign. varification to protect data privacy. web browsing on internet and to protect confidential transactional such as credit card, debit card transmission.

Why we use the technique of cryptography

Computer cryptography is often associated with the where and ordinary plane text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process known as encryption. The process of convertion of cipher text to plane text this is known as decryption.

Features of cryptography as follows:-

1. Confidentiality :- Information can only be access by person for whom it is intended and no other person accept him can access it.

2. Integrity :- Information can't modified in storage or transsions between sender and

receiver without any addition to information being detected.

3. Authentication :- The identies of sender and receiver are confirmed as well as destination origin of of information in confirms.

4. Non - repudiation :- The creater/sender of information cannot denied on his intension to send information at later stage.

Date - 09/06/2025

Define the types of cryptography :-

In general there are three types of cryptography

(1) Symmetric key cryptography :-
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt message. Symmetric key system are faster and simple but the problem is that sender and receiver have to share some how exchange key in a secure manner. The most popular Syst Symmetric key cryptography system

is Data Encryption system (DES) so the security has to be done in a private way ~~to~~ so that no any disclosed of the security code non-other than the actual authentic person.

2. Hash function :-
There is no uses of any key in this algorithm a hash value with fixed length is calculated as per the plane text which make it impossible for content of plane text to be recovered. Many operating system use hash function to ~~en~~ encrypt password.

3. Asymmetric Key cryptography :-
Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and private key is used for decryption. Public key and private key are different even if the public key is known by everyone the intended receiver can only decode it because he also knowns the private key.

Application of cryptography

(i) Computer Password
(ii) Digital currencies

(iii) Secure web browsing
(iv) Electronic signature
(v) Authentication
(vi) Crypto currencies
(vii) End-to-end encryption.

What is Data encryption standard (DES)

DES stands for data encryption standard there are certain machine that can be used to crack the DES algorithm. The DES algorithm uses a key of 56-bits size using this key the DES takes a block of 64-bits plane text as input and generates a block of 64 bit cypertext.

The DES process has several steps involved in it where each step is called a round. Depending upon the size of the key being used the DES algorithm is a symmetric key block cyper created in the year 1970's by an IBM team and adopted by the national institute of standard and technology (NIFT) The algorithm take the plane text in 64-bit block and converts then into cypertext using 48-bit key since it is a symmtric key algorithm

It employes the same key in both encryption and decrypting the data.

Date 10/06
Page

DES modes of operation

DES have five different modes of operation to choose from:-

(i) electronic code book (ECB)
each 64-bit block is encrypted and decrypted independentaly.

(ii) cipher block chaining (CBC).
each 64-bit block depends on the previous one and uses an initialization factor. vactor.

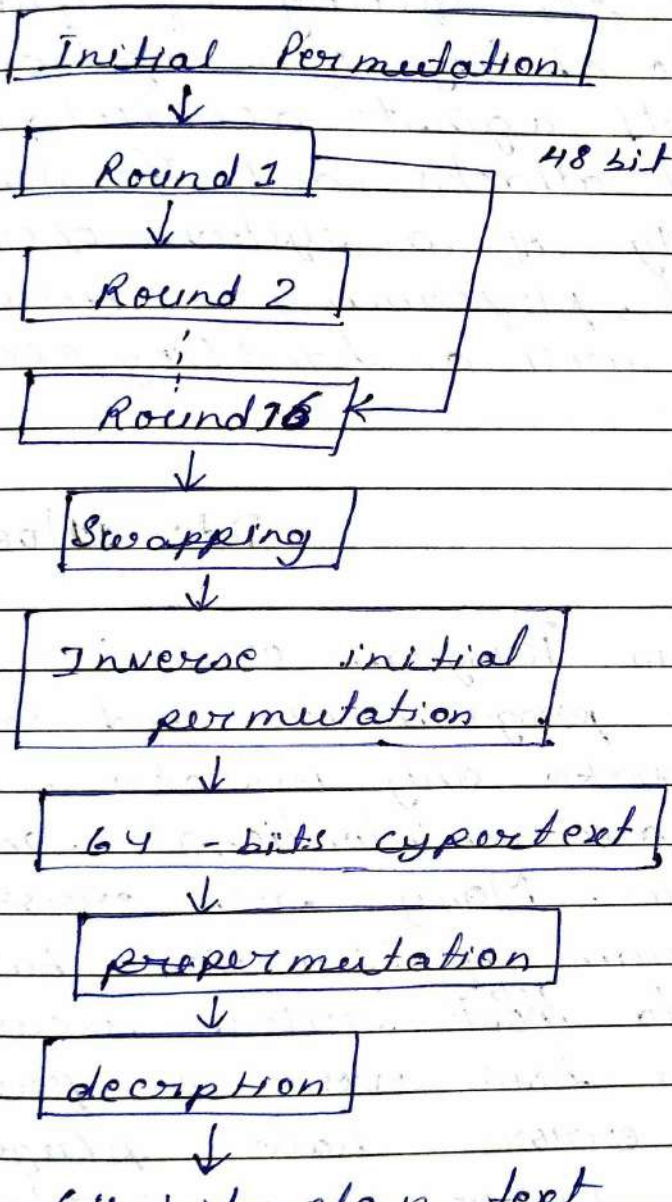
(iii) cipher Feedback (CFB)
The preceding cipher text becomes the input for the encryption algorithm producing which in turn is XORed with plane text building the next cy. cipher text unit.

(iv) Output Feedback (OFB)
which like CFB except that the encryption algorithm input is the output form of the preceding DES.

(v) Counter (CTR)
each plane text block is XORed with an encrypted counter. The counter is then incremented for each subsequent block.

Algorithm 64-bits plain text

64 bit plane text



48+8 = 56
8 bit = parity bit
for checking program

Define Secure Programming.

Security implies some degree of trust that the program enforces expected.

- confidentiality
- Integrity

• availbility

Security and safty are two important aspects ~~to~~ of the quility of software. Safty is the ability of a system to protect itself against accidental or intentional attacks and the safty is the ability of a system operating without risk, performing normal function as well as handling exceptional condition.

Date - 12/06/2025

Non-Malicious Program error :-
Being human programmers and other developers make any mistake, most of which are unintentional and non-malicious. Many such error causes program malfunction but do not lead to ~~most~~ more serious security Vulnuabilities how ever a few classes of errors have pluged and their is no reason to believe they will disappear.

Errors are of three types :-

(1) Buffer overflow :-
A Buffer overflow is the computing equivalent of trying to pour two

literals in a same storage place just like we are trying to fill two liters to ~~of~~ water one liter buckets. Some ~~water~~ water is going to split out and make a mass.

A Buffer (array or string) is a space in which data can be hold. A Buffer ristricts in memories because memory is finite. A buffer capacity is also finite for this reason in many progra-mming language or programmer must declare the buffer maximum size so that the compiler can set a side that an amount of spares to be store the data and the compiler can run and procede easily.

Eg:-
char sample [10]

The compiler sets a side 10 bytes to store this buffer, one bytes of each of the ten elements of the array. So, the sample [0] store the first value and so on.

Date 12/06/25
Page

(II) Incomplete Mediation :-
Incomplete mediation in information security occurs when an application or system fails to properly validate sanitize user input, allowing malicious data to by pass intended security checks and potentially compromise the system. It leads to various attacks, including buffer overflows, SQL injections and other drawbacks that can be exploted to gain unathorized access or modified data.

(III) Time of check to time of user errors :-
"A time of check to time of use" error occurs when the state of resource changes between the time its checked and the time is use causing unexpected behaviour or potential security vulnerabilities. This happens because the system has a window of opportunity where an attacker or another process can modify the resource before it is fully utilized.

What do you mean by information security. Define its application?

Information security is a set of practice designed to ~~prevent~~ private data secure from unauthorized access

and alteration for the duration of storing or terminating from one location to another.

Information security is design and carried out to protect the print, digital and other private, sensitive and private data from unauthorized person. It can be used to secure data from being misused acknowledgement, distruction, alteration and disruption.

Computer network are connected in daily transmission and communication inside the government, private or corporates that need security. The most common or easy method of protecting network support is assigning it with unique name and a crossponding password. The network security includes :—

(a) Protection :- The user needs to be capable of configuring their device and network accurately.

(b) Detection :- The user should detect wheather the the configuration has been modified or get a notification if their are some issues in the network traffic.

(iii) Reaction :- After detecting the issues the user should acknowledge them and should return to a protected positioning as required or needed in the availability.

Network security work with more then one layer of protection at the edges and in among the network. All the security layers implements some technique and follow specified policies.

Application of Information Security

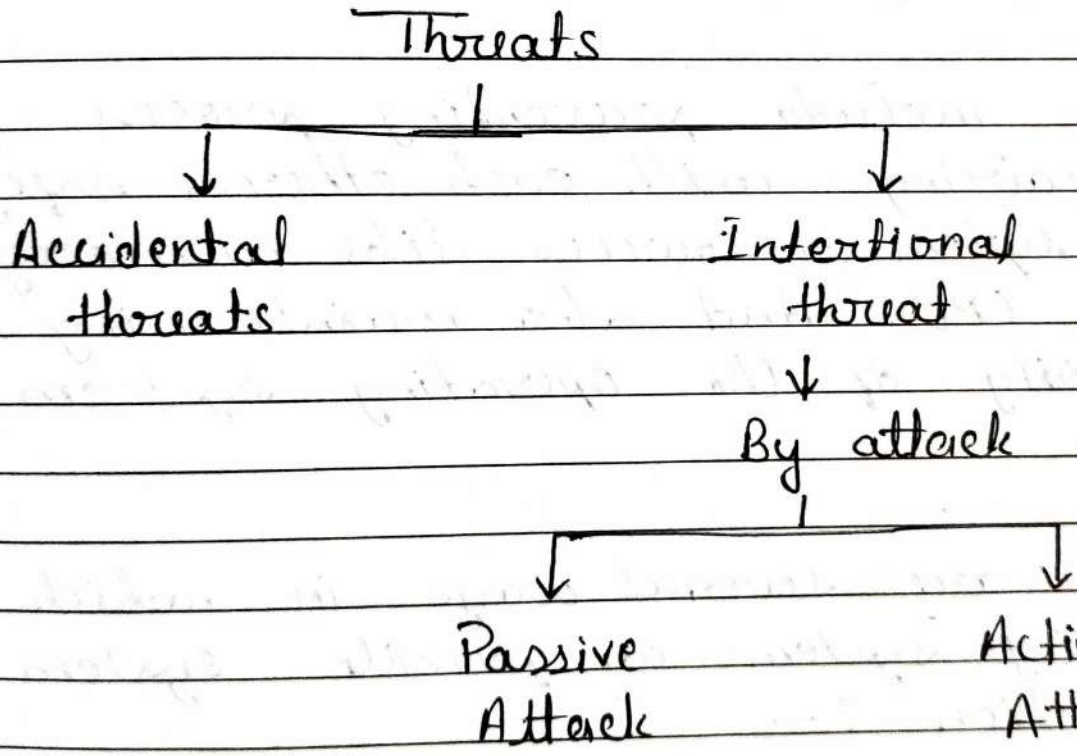
Date 31/06

Unit-4

Threats

A threats is a illegal activity that can damages information system such as loss information data corruption etc.

Eg.:- Data Crash
data interuption
Modification in data



Accidental threat

It is also known as unintentional insider threat are security risk arising from the unintentional action or intent of individuals within an organization.

These threats unlike malicious one from negligence, lack of awareness or simple errors, rather than deliberate harmful intent

Eg - include accidental sending sensitive data to the wrong recipient falling victim to phising attack or configuration system.

Intentional threats

It is to informatic system are deliberate action taken by individual or group with maliciout intent to compromise the security or system data or network this threats are open AND at causing harm. Disruption or financial gain.

Eg:- include malware phising ransomeware and social engering attack

Passive attack

A passive attack is network attack in which system is monitored, analysis, observed the information over the network without altering or interyairing with the target system or network. The primary goal is to gather information such as password credit card debit card or business secrets without the victim's knowledge. This attack are difficult to detact because they do'nt inwalk directly.

Some Key factor of passive Attack

- Monitoring and Eavesdropping (listing in a conversation wheather they are voice calls, vedio call or chat message.)
- Information gathering
  Lack of modification
  Difficult in detection

Active attack :-

An active attack is a type of cyber attack where the attacker actively interferes with a system or network, attempting to modify disrupt, or damage data or

services.

Active attack, often involve direct interaction with the target to achive malicious goals like gaining unauthorized access, altering sensitive information or making system unusable

Key characteristic

(i) Modification of data :-
Attackers directly interact with the target system, inject malicious code or commands and attacker alters/delete data during transmission or storage.

(ii) Disruption :-
Attackers can disrupt services by flooding the system with traffic or causing it to crash. Aims to disrupt normal operations

(iii) Data Fabrication :-
Involves inserting false data or message into the system.

Date 01/07
Page

Q) What do you mean by System Protection in Operating System.
(Note :- Protection in OS - memory and address protection, Access control, file protection, user authentication)

System protection in an operating system refferce to the machenism implemented by the Operating system to ensure the security an ~~interi~~ integrity of the system. System protection involves techniques to prevent unauthorized access, misuse or modification of the Operating system and its resources.

This include preventing process from interfairing with each other, safeguarding system resources like memory and CPU. And also maintaining the integrity of the operating system itself.

There are several ways in which an operating system can provide system protection :-

1) Resource Isolation :-
Protection machenism ensure that one process cannot interfair with the execution and data of another process.

(ii) Authentication and authorized

Authentication is the process of verifying the identity of a user, device, or system. authentication ensure that only authorized entities access system resources. Authorization is the process of the granting or denying access to system resources based on user identity, role or privileges. It ensures that user can only access resources they are permitted to access. Authentication and authorization improve system security by preventing unauthorized access and also protect sensitive data from unauthorized access or modification.

(iii) Access control

Access control refers to the methods and mechanisms used to regulate who or what can view or use resources within a system. This security technique used by OS to control who can access what resources and what action they are allowed to perform (like read, write, execution).

(iv) Encryption :-

Encryption is the process of converting plain text into cipher text using a key. To read It used to secure data by converting it into an unreadable form so that only authorized users can read it.

(v) Privilage levels :-

Diffirents level of privilage (user mode, kernel mode) are used to restrict access to sensitive system operation.

Date 02/07
Page

How it works

1. System call :-
System calls are the interface through which user programs request services from the operating system and they are often protected by the operating system to prevent issues.
Eg:-
(i) Firewall :- A firewall is a system level protection machenism that controls network traffic, preventing unauthorized access to the system through the network.

(ii) File Permission :- File permissions are rules set by O.S. to control who can read, write or execute a file or directory. They are a key part of system protection, helping to secure file from unauthorized access or modification.

(iii) Memory Protection :- Paging and segmentation machenism protect memory from unauthorized access from different processes.

(iv) Antivirus Software :- Antivirus is a security program that scan files, processes and memory to identify known or suspicious malware and protects the system from attacks.

2. Domain of protection :-
The domain of protection is the set of resources that are controlled by a particular protection mechanism. In an Operating System, a domain can be defined as a set of objects that are accessed by a set of subjects. Objects are resources, such as files, memory, and I/O devices, while subjects are entities that access these resources, such as processes, users, and groups. Each domain has a specific set of rule that govern the access to its objects by its subjects.

3. Access Rights :-
An access right is the ability to execute an operation on an object. Access right refer to the permissions or privileges granted to users or systems to access specific resources, data, or systems. Access rights help protect sensitive data from unauthorized access or modification. Access rights help prevent unauthorized access to systems or resources. Access rights help organizations comply with regulatory requirements and industry standards.

Hardware Support :-
Hardware support in threat mitigation

involves various measures to protect devices and systems from potential security breaches. Ensure hardware comes from reputable manufacturers. Outline guidelines for handling hardware, security access, and responding to incidents. Regularly educate employees on security awareness and best practices.

Advantages of system protection in O.S.

(i) Prevents unauthorized Access:- System protection prevents unauthorized access to sensitive data and system resources.

(ii) Protection against malware - System protection helps protect against malware Viruses and other types of malicious software.

(iii) Ensures data Integrity:- System protection ensures the integrity of data by preventing unauthorized modifications or deletions.

(iv) Improve System stability:- System protection ensures the integrity of data by preventing unauthorized modifications or deletions.

(v)

System protection help to ~~em~~ improve malicious software from causing system crashes or instability.

(v) Enhances security:- System protection provides access control mechanisms to restrict user access to sensitive

data and system resources.

- Memory Protection - System protection mechanisms to prevent malicious software from accessing sensitive data in memory.
- File System Protection :- System protection provide file system protection mechanism to prevent unauthorized access to sensitive files and directories.

Disadvantages of System protection in O.S.

(i) Perform Overhead - System protection mechanism can introduce perform overhead, slowing down system operations.

(ii) Complexity - System protection mechanisms can be complex to implement and manage, requiring significant expertise.

(iii) Additional Resource Requirements :- System protection mechanisms can required additional resources, such as memory or CPU cycles, which can impact system performance.

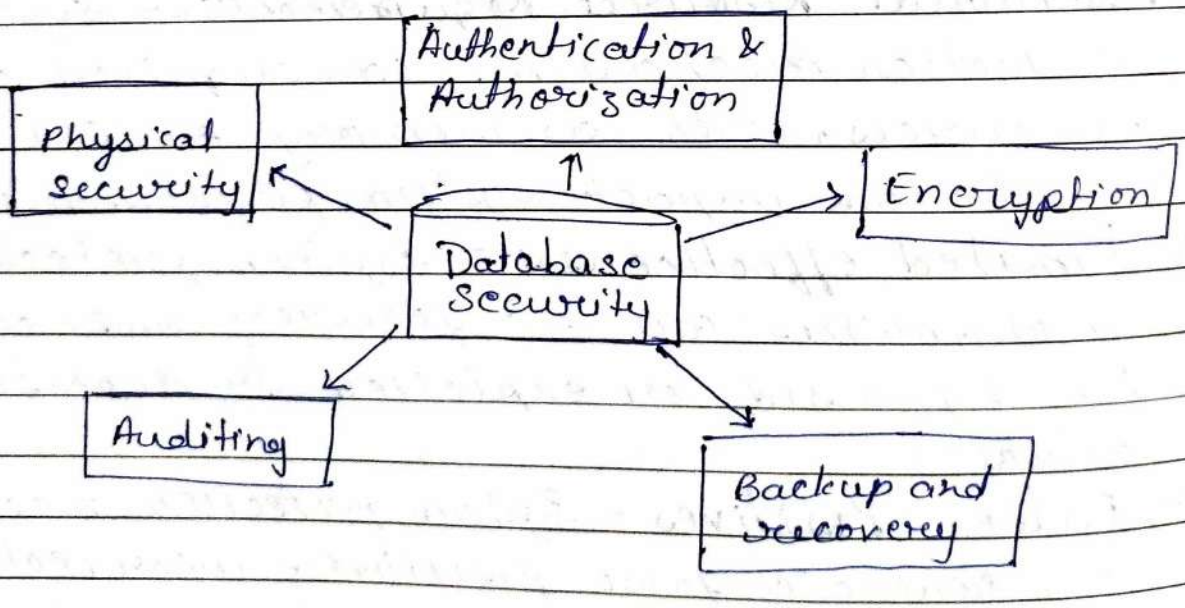
(iv) Limited effectiveness - System protection mechanisms are not foolproof and can be be bypassed or exploited by sophisticated attacks

(v) False Positives - System protection mechanism can generate false positives, incorrectly identifying legitimate users of applications, causing system activity as malacious.

Date 03/07
Page

What is Data security? Explain authorization in full explanation.

Database security is a critical aspects of information security, incompressing measures to protect database from unauthorized access, misuse or distruction. It involves implementing various catogories and technologies to ensure that only authorized individuals or entities can access and utilized the data stored with in the database. This includes protecting the database itself. The data it contains the database management system (DBMS) and the applications that access it.



1. Physical Security :-
The safe guarding of actual infor infra-structure that contains the database

is refer to as a physical security. This covers the server rooms physical security as well as the security of the networks and storage system. Only authorized workers should be able to enter the server room and CCTV camera should be placed to keep on eye on the space. Utilizing firewalls, instruction detection system and other security measures.

(2) Authentication & authorization
In Database Mangement system ensuring data securing and proper authorization is needed to protect sensitive information and maintain data integrity. User authorization and authentication are essential aspects of database security.

(i) User Authentication :- Authentication verifies the to identify of users attempting to access the database. It ensure that only legal user with valid credentation allowed to access.

Common authentication method includes :-
- Username and Password
- Biometric scanner
- Token based etc.

Eg:- When an employee logs into the company database. They must enter there unique username and password The system verifies the credentials before granting access.
Enter the username : System
Enter the password : 12345

(ii) Authorization :- Authorization determines what authentication users are permited to do with in the database.
Eg:- User 'ROHIT' have previlages to connect, insert, select, alter data in the 'Customer table'. Now Rohit can do only provided previtages in the database. But he cannot delete anything from the database.

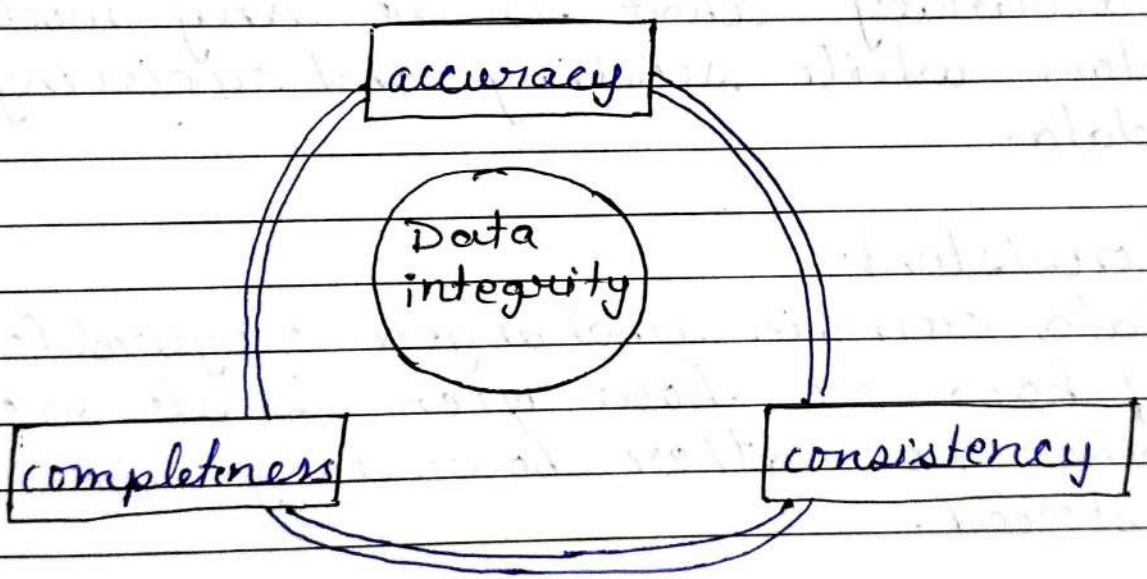
Enter user Name : System
Enter password : 12345
SQL> show user;
User is 'system'
SQL> Create user 'ROHIT' identified by ROHIT123;
user created
SQL> commited;
commit complete
SQL> grant connect to ROHIT;
Grant succeded

SQL> commit
commit complete.

Date 04/07/25
Page

Define Integrity in database Security?

Data integrity in database security is refers to ensuring data accuracy, consistency and completeness throughout its life cycle. from creating deleting deletion. It is about preventing unauthorized modification ensuring data correctness and maintaining data reliability this includes protecting data from accidental or milicious alterations, errors and inconsistencies.



Data Integrity can be compromised in several ways. each time data is replicated or transfered it should remain intect unaltered between update error checking method and validate procedures are tipicaly ensure the integrity of data that is transfered or reproduced without the intention of alteration.

Data integrity discribes data that is kept complete, accurate, consistent and safe throughout its life cycle in the following ways

Complete
Data is maintained in its full form and no data elements are filtered, ~~toar~~ truncated and lost.

Accurate
Data can be transfer in a form of accuracy that is no any modification done while sending and recieving the data.

Consistent
Data remain unchanged regardless of how or how often, its accessed and no matter how long it stored.

Safe
Data is maintained in a secure manner and can only be accessed and used by authorized application or indivisuals. Further safe data cannot readily be exploited by malicious.

Data Security involves considerations such as authentication, authorization

encryption, backups and access logging.

Types of Data Integrity :-

Entity Integrity
A feature of relation database systems that stores data within tables, which can be used and linked in various ways. Entity integrity relies on unique key and value created to identify data, ensuring the same data isn't listed numerous times and table field are correctly populated.

Referential integrity
A series of processes ensuring data is uniformly stored and used. Database structures incorporate rules that enforce the presence of matching records in linked tables, preventing orphaned records and maintaining the consistency of the data across the database.

Domain integrity
A domain is defined by a specific set of values for a table's columns, including restrictions and rules that governs the quantity, format and data that can be input. Domain integrity helps to ensure the precision of data elements within a domain.

User-defined integrity
When users create rules and constraints around data to align with their unique specifications. This method is generally employed with other processes that don't guarantee data safety and security.

Physical integrity
Protects data's accuracy, correctness and wholeness as it is being stored and retrieved. Physical integrity can be compromised by power outages, storage erosion, hacker and natural disasters.

Date 08/07/25
Page

Define multilevel security?

In todays world organizations must be conscious about protecting data and safeguarding the exchange of information, on top of that digital transformation has become covering everything (anything from the organizations top secret business leads to unclassified day to day operational information.

A multilevel security (MLS) approaches is crucial is privacy conscious prioritywise data security since, A single security system often cannot gurntee safety from data breaches. The multilevel security approach has become the fundamental requirement for security and organization data.

Multilevel security (MLS) in database security is a system that allows simultaneous accurs to data with different sensitivity labels which enforcing strict access information by an authorized to see it categoried both data and user based on a hierarchical security system, preventing unauthorized access based on clearance levels, Multilevel security provides the capability to prevent unauthorized users from accessing information.

08/07/25

The two primary goals of multilevel security are as follows:-
(i) Prevent unauthorized access to information.
(ii) Deter individual from declassifying information.

Dynamic policy enforcement and multi-level security methodology can ensure that separation and protection are inplaced for contextual access to information without hindering authorized collabration.

Advantages of multilevel Security :-

1. **Protection of sensitive information** :- MLS ensures that sensitive information is protected from unauthorized access.

2. **Compartmentalization** :- MLS allows for compartmentalization of information, limiting access to only those who need it.

3. **Reduced Risk** :- MLS reduces the risk of data breaches and authorized disclosure.

4. **Flexibility** :- MLS allows for different levels of access control, enabling organizations to tailor security to specific needs.

5. High-Security Environment - MLS is suitable for high-security environments, such as military government and financial institutions.

Disadvantages of Multilevel Security.

(i) Complexity :- Implementing MLS can be complex and require significant resources.

(ii) User Management :- Managing user clearances and access control can be time-consuming and prone to errors.

(iii) Data Classification :- Classifying information correctly is crucial to ensure that MLS is effective, which can be challenging.

(iv) Cost - Implementing and maintaining MLS can be costly especially for large organizations.

(v) Limited Flexibility - MLS can be inflexible, making it difficult to adapt to changing security requirements or organizational needs.

(vi) Potential of over-Classification :- Over-classification can lead to unnecessary can lead to unnecessary restrictions on access, hindering.

(vii) Potential for under-classification :- Under classification can lead to sensitive information being exposed to unauthorized individuals.

Security in Network :-

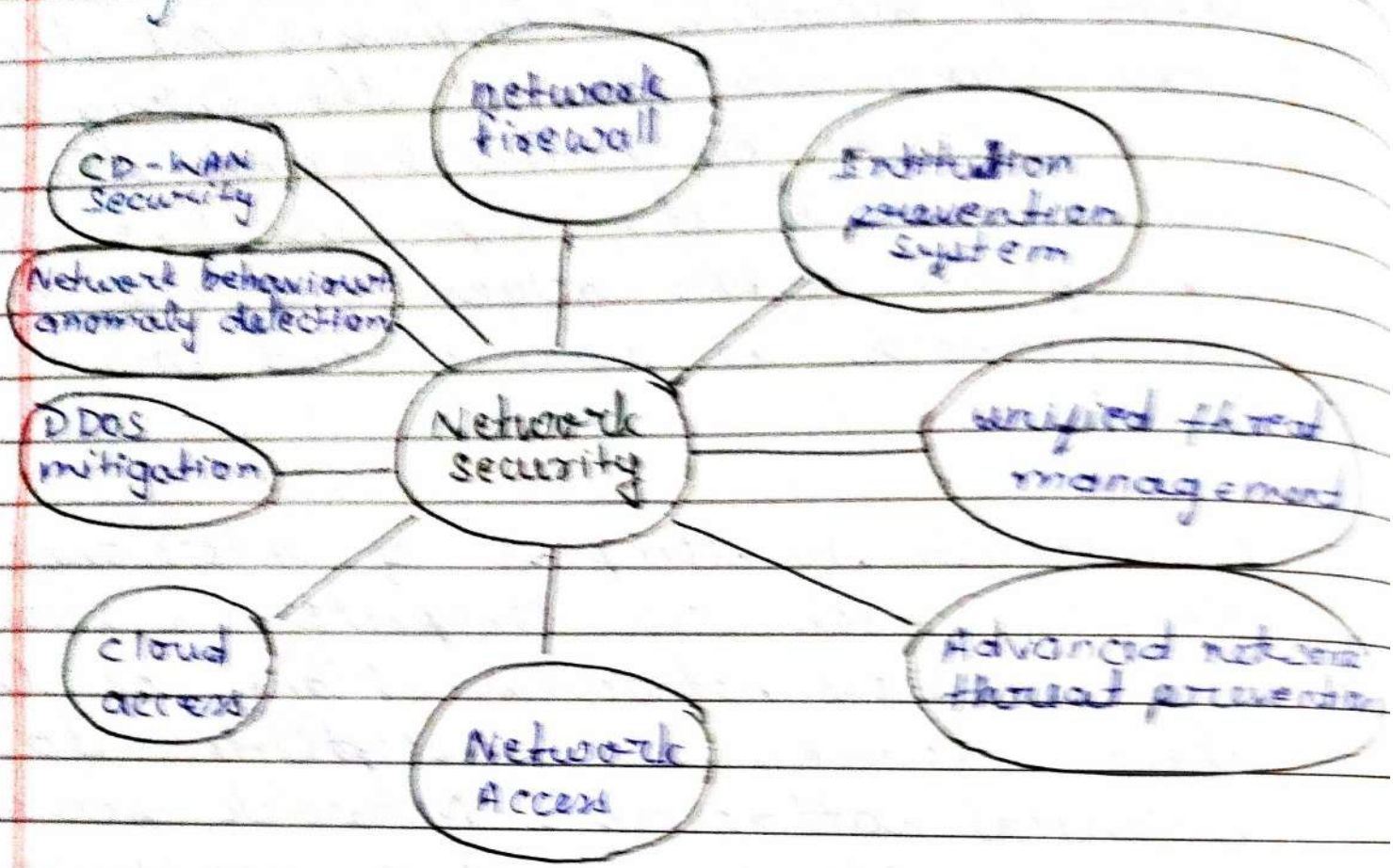
Network security encompasses all the steps taken to protect the intrigrity of a computer network and the data with in it. Keep sensitive data safe from cyber attack and ensure the networks is usable and trust worthy.

A network is compose of interconnected devices such as computers, severs and wireless networks. Many of these these devices are susceptible to potential attackers. Network security envolves ~~it~~ the use of a verity of software as a service. Security become more important as network grow more complex and interprises. security mode must involves threat actors create new attack modes on this increasing complese networks.

Network security is inforced using a combination of hardware and software tools. The primary goal of network security is to prevent unauthorized access into or between parts of a network.

Network Security encompasses multiple

They are as follows.



Types of network Security

1. Firewalls :-

It put up a barrier between your trusted internal network and untrusted outside networks such as the internet. They use a set of defined rules to allow & block traffic a firewall can be hardware, software or both.

Eg:- Cisco offers unified threat management (UTM) devices and threat-focused next generation fire-wall.

2. Email Security :-

Email getways are the no. one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to use recipants and send them to sides serving upmalware An email security application incomming attacks and control out bound messages to prevent loss of data.

4. Network Segmentation :-

Software define segmentation puts network traffic into different classification and makes enforcing security policies easier Ideally the classification are based on endpoint Identity, not IP address assign access rights based on roles, location, so that

the right level of access is given to the right puple.

Application Security :—
Any software we use to run our business need to be protected weather It is build it wheather you by it. Unfortunately any application may contain defects that attackers can use to infilterate your network. Application security maintain and manage the hardware and software.

Anti-Virus and Anti-malware.
Antivirous and antimalware software are essential components of network security that help protect against malicious software (malware) and viruses. Scans files and programs in real-time to detect and block malware. Regularly updates virus definitions to stay protected against new threats. Removes detected malware from the system. Integrates with firewalls to block malicious traffic.

Access control
Access control is a security mechanism that regulates user access to network resources based on user identity, role or privileges. Verifies user identity before granting access to network

resource. Determines user access levels and privileges. Track user activity and resource usage.

Date - 15/07/2025

Administrating Security

Administrating security in information security involves implementing and maintaining a comprehensive security statigies to protect an organization information ~~assets~~ assets. This includes identifiying critical information analyzing thread and vulnerabilities, accessing risk and applying appropriate counter measures.

Administrating security includes four features:-

- Planning - prepare and study what will verify our implementation meets security needs of todays and tommorow.
- Risk analysis :- cost / benefit analysis of controles
- Policy :- Establish a framework of ~~verifying~~ security needs are met.
- Physical control :- what aspects of the computing environment have an impact on security.

Date 16/07/25
Page

Security Planning :-

The system security plan should be viewed as documentation of the structure process of planning adequate, cost effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needed.

Contents of security plan

- **Policy** - The goal of the computer security.
- **Current state** - describe current states.
- **Requirements** - how to meet goals, legal etc.
- **Recommended controls** :- map controls, remata vulnerability identified
- **Accountability** :- who is responsible for any task.
- **Timetable** - due dates for tasks.
- **Continuous attention** - keep it up to date.

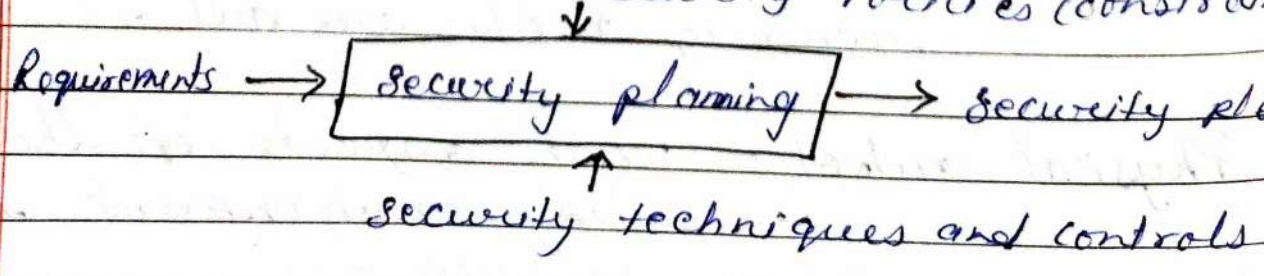


Fig :- Inputs to the Security Plan.

Risk Analysis :-
Risk analysis in administrating security is a crucial process that identifies, accesses and prioritywise potential security threads and vulnerabilities to an organization assets. It involves evaluating the likelyhood and potential impact of security breaches allowing organization to develop and implement those risk.

Date - 17/07/2025

It is a process of identifying and accessing the likelyhood and impact of potential event that could harm your organization. Their are some important things to remember on you mind while risk analysis.

- Context criticality and sensitivity of system :- System containing sensitive information should be given priority and given special treatment as like security provide from the unauthorized person.

- Dependency of the system :-
Like e-commerce websites or any payment based sites depend on other or external payment processors. So users are directly depend upon the other ERT system for payment or any other purpose.

- Operational procedures configuration and management of the system.
These type of risk are arises if the system is not properly configured It is easily invite Vulnerable to attack.

- Effectiveness of the controls and monitoring of the system:-
It is difficult to detect events if controls are not effective manner in which data or system components are connected to each other. To transfer the data one environment to another.

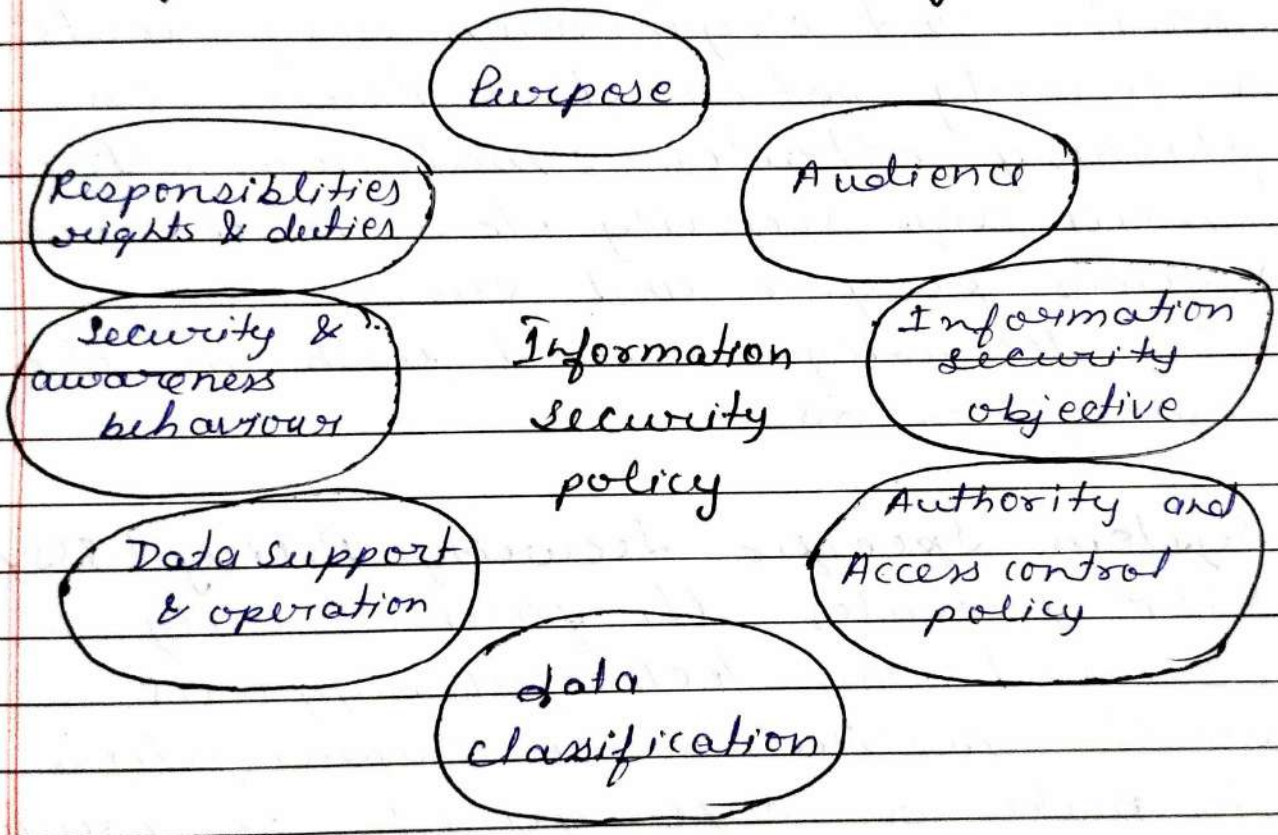
17-25

3. Policy of Administration Security
Security policy in the context in the administration sucurity ouline the rules guide lines and ~~procedural~~ procedures an organization use to protect its information assits and systems. It reffers to the ~~produ~~ procedure techniques or technology created and use to safe guard confidential company data and data assits. If Information security is primitively concerned with availability and intigrity of the system. It defines how an organization will manage and protect sensitive data. control access and impliment measures to prevent unauthorized

access and data breaches.

Information security policy needs to do robust and protect the organization from internal and external threat. Its scope should be updates and edits to keep pace and the changing over system.

Policy of Information security Framework



Security Policy :-

There are three types of security - defined by the management. They are as follows :-

(I) General or Security program policy

(II) Issue - Specific Security policy

(III) System Specific Security policy

1. General or Security program policy (SPP)
It is also known as a general security policy. Information security policy or IT security policy. The general security policy discribe the whole organization security objectives and its commitments for information security policy.

2. Issue - Specific security policy (ISSP)
ISSP provides the guide line for specific threats and organization may create a security policy that focuses on phishing attackes, malware attackes email ~~dog~~ security etc. There are various purpose and processes and also technologies used with in the organization. ~~SS~~

3. System Specific Security Policy (SSSP)
SSSP provides the final security observed and technical supports for the institution or organization to make a safe guard of your data and company assits.