Network Security AND Cryptography

Unit - 01

Intro :- Computer security concept, Need for security, Security in Networks : Threats in networks, ~~Network Secur~~ Network security control - The OSI security, Architecture, Fundamental security : Design Principle, Security Attacks, security services, Security mechanism, Attack surface and Attack trees, A model of Network security.
Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots.
Proxy Servers and Anonymizers, Firewall, Types of Firewall, Password Cracking Techniques.

Computer Security Concept.

Definition and objective

Computer security, also known as cybersecurity, refers to the protection of computer systems and networks from unauthorized access, data theft, damage, or disruption. The goal is to ensure the confidentiality, integrity, and availability of information - often referred to as the CIA triad

Computer security applies to software, hardware, data, networks, and user access, and is essential for preventing

Cyber threats such as malware, hacking, phishing, and denial-of-service attacks. Security ensures that only authorized users can access and manipulate data and that the systems operate reliably.

Core Principles (CIA Triad)

The foundation of computer security is based on the following three principles:-

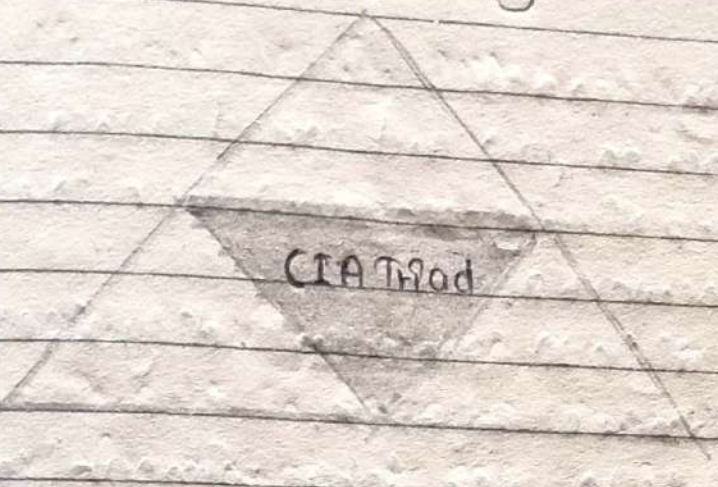
- Confidentiality: Ensures that information is not accessed by unauthorized individuals. It involves data encryption, secure access controls, and authentication methods.

- Integrity:- Guarantees that data is accurate, consistent, and unaltered during storage or transmission. It includes checksums, hashing, and data validation mechanisms.

- Availability:- Ensures that systems and data are accessible to authorized users when needed. It includes redundancy, failover systems, and protection against denial-of-service attacks.

Rajshree
PAGE NO.:
DATE:

Confidentiality.



Need for Computer Security.

With the increasing dependence on digital systems and the rise in cyber threats, computer security is crucial for protecting sensitive information, maintaining trust in communication systems, complying with legal standards, and ensuring business continuity.

Security in Networks.

Threats in Networks.

Network security threats refer to any action or event that compromises the confidentiality, integrity, or availability of data being transmitted across computer networks. These threats can be internal or external, intentional or accidental, and they continue to evolve with advancements in technology.

Common Threats in Networks :-

1. Malware Attacks
   - Viruses :- Attach to files and spread when executed.
   - Worms :- self-replicating programs that spread over networks.
   - Trojans :- Malicious programs disguised as legitimate software.
   - Spyware :- Collects user data without consent.
   - Ransomware :- Encrypts data and demands payment for access.

2. Denial-of-service (DoS) and Distributed DoS (DDoS) Attacks
   - Overwhelm network resources with traffic to make service unavailable.
   - DDoS uses multiple compromised systems to launch large-scale attacks.

3. Phishing and social Engineering
   - Tricks users into revealing sensitive information (eg. passwords).
   - often involves fake emails, websites, or calls mimicking legitimate sources.

4. Man-in-The-Middle (MitM) Attacks
   - An attacker secretly intercepts or alters communication between two parties.
   - Common in unencrypted public Wi-Fi networks.

5. Eavesdropping (Sniffing)
- Unauthorized monitoring of data transmitted over a network.
- Attackers use packet sniffers to capture sensitive information.

6. IP spoofing
- Attackers sends packets with a forged source IP to impersonate another system.
- Used to bypass firewalls or perform MitM attacks

7. SQL Injection
- Exploits vulnerabilities in web applications to execute malicious SQL commands.
- Can expose, delete, or manipulate database conten

8. Session Hijacking
- Attacker takes over a user's active session to gai unauthorized access.
- Exploits weak session management.

9. DNS spoofing (Cache Poisoning)
- Redirects users to fake websites by corrupting DNS cache information.

10. Insider Threats
- Employees or trusted individuals misuse access rights. harm the network.

Network security Control

The OSI security :- Architecture

The OSI security Architecture is defined by the ITU-T X800 7498-2 standard, and it provides a structured framework to ensure secure communication over a network. It defines security services and mechanisms applicable at each layer of the OSI model, which helps in building layered and effective security solutions.

This model does ~~not~~ not change the OSI 7-layer structure but adds a parallel view of security that can be applied at any layer.

Security services :-

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non-Repudiation

Security mechanisms :

Encryption : Protects data confidentially by making it unreadable to unauthorized users.

Digital signatures: Provide data integrity and authentication

Authentication protocols: Verify user or system identities

Traffic padding: hides traffic patterns by adding dummy data.

Routing control: Ensures secure route selection and data forwarding.

Notarization: Third-party validation for certain operations or agreements.

Diagram:- OSI security Architecture

Application layer → security services
Presentation layer → Encryption/decryption
Session layer → Authentication
Transport layer → Secure channels
Network layer → Secure Routing
Data link layer → Error checking
Physical layer → Physical safeguards

Fundamental Security.

- Fundamental security under network security control refers to the core principles, policies, and technologies implemented to protect networks and data from threats. These controls act as preventive, detective, and corrective mechanisms that ensure the CIA triad (Confidentiality, Integrity, Availability) is maintained throughout network operations.

These security controls are essential for securing data in transit, controlling access to systems, and ensuring that malicious activities can be monitored and mitigated.

Categories of security Controls.

Preventive Controls :- Aim to prevent security breaches (e.g. Firewalls, encryption, access control lists).

Detective Controls :- Identify and report security incidents (e.g. Intrusion detection systems, logging).

Corrective Controls :- Respond to and fix security breaches (e.g. backup recovery, patch management).

Rajshree
PAGE NO.
DATE

Key Mechanisms in NSC

Access Control :- Limits user access based on identity and role.
Firewalls :- Filter traffic between trusted and untrusted networks.
Intrusion Detection System (IDS) :- Monitor traffic for suspicious activity.
Encryption :- Secures data in ~~transmit~~ transit from eavesdropping or tampering.
Security Policies :- Define acceptable use, roles, and responsibilities within a network.

Diagram :- layered security model.

Policies & Procedures
Network Access Control
Encryption Mechanisms
Firewalls & IDS
Physical Security

"Defense in Depth" model.

Design Principles:-

Principle :- Security should be an integral part of system design.
→ Security features must be built from the start, not added later.

Principle :- least privilege
→ Each user/process should have only the minimum access rights needed to perform tasks.

Principle :- Defense in Depth :-
→ Multiple security layers (physical, network, application) are applied to protect systems.

Principle :- Open Design
→ Security should not depend on secrecy of design, but on secrecy of keys/credentials.

Principle :- Seperation of Duties
→ Responsibilities are divided to reduce fraud or misuse risk.

Principle :- Fail-Safe Defaults
→ Default state should be "deny access" unless explicitly allowed.

Principle :- Auditability.

→ Systems should maintain logs for tracking and investigating security events.

Security Attacks :-

A security attack is any action that compromises the security of information systems, targeting confidentiality, integrity, or availability.

The OSI security architecture classifies attacks mainly into Passive and Active types.

classification of security attacks.

Passive Attacks :- Eavesdropping

Attempt to intercept or monitor transmissions without altering them. Goal :-

Goal : gain information.

Ex : Release of message contents -

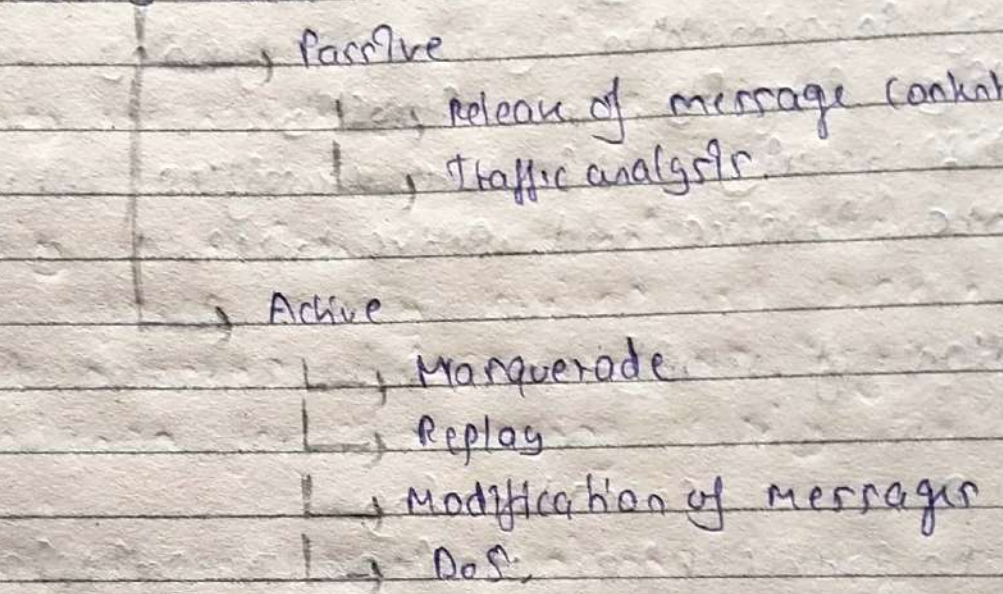
reading confidential emails.

Traffic Analysis - Analysing communication patterns to infer sensitive info.

Active attacks :- Tampering

Attempt to modify, disrupt, or fabricate Communication

Ex :- Masquerade :- Pretending to be another user.
Replay :- using captured data packets.
Modification of messages :- altering message content
Denial of service (DoS) :- making resources unavailable



Security services.

Security services are mechanisms that provide specific kinds of protection to ensure the confidentiality, integrity, and availability of information in computer networks

Main Security services.

1. Authentication :
   - Ensures that the communicating entity (user, device, or system) is genuine

Example :- login with username & password, digital certificates.

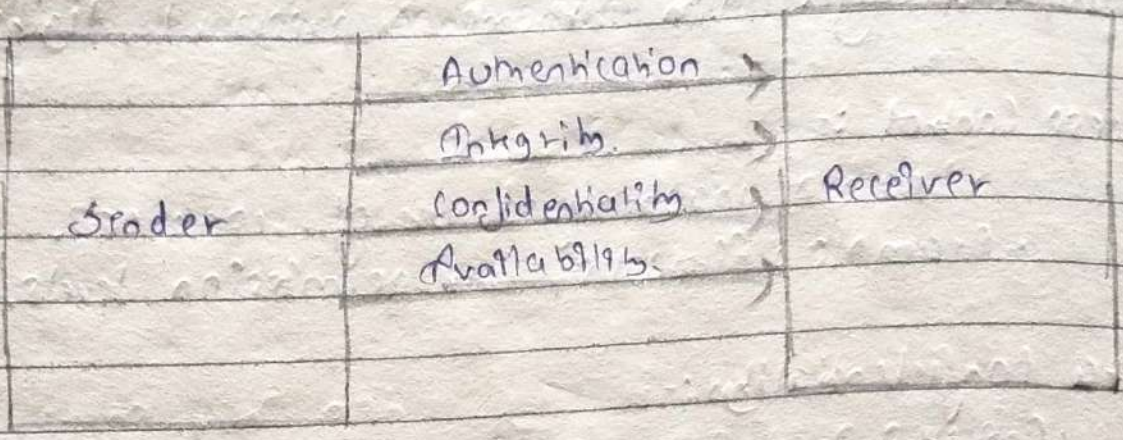
2. Access Control :-
- Prevents unauthorized use of resources.
- Example : Firewalls, user permission levels.

3. Data Confidentiality :-
- Ensures that information is not disclosed to unauthorized parties
- Achieved through encryption techniques (e.g. AES, RSA).

4. Data Integrity
- Protects data from unauthorized alteration, addition, or deletion
- Ensures that the received data is exactly as sent.
- Example : Hash functions (SHA, MD5)

5. Non-Repudiation
- Prevents a sender from denying that they sent a message and a receiver from denying reception
- Example : Digital signatures.

6. Availability
- Ensures that network services and resources are available to authorized users when needed.
- Example : Protection against Denial-of-Service (DoS) attacks.



Security Mechanism

Security mechanisms are techniques, tools, and procedures that enforce security services and protect data, systems, and networks against attacks. They act as the function foundation for implementing security services.

Types of Security Mechanisms

1. Encipherment (Encryption/Decryption)
   - Transforms data into an unreadable form (cipher text) using algorithms and keys.
   - Provides confidentiality and helps in Integrity
   - Example: AES, RSA

2. Digital signatures
   - Ensures authentication, integrity, and non-repudiation.
   - Sender signs message with private key, receiver verifies with public key.

3. Access Control Mechanism
- Regulates access of users, processes, and devices to system resources.
- Example :- Passwords, biometrics, Role-Based Access Control (RBAC)

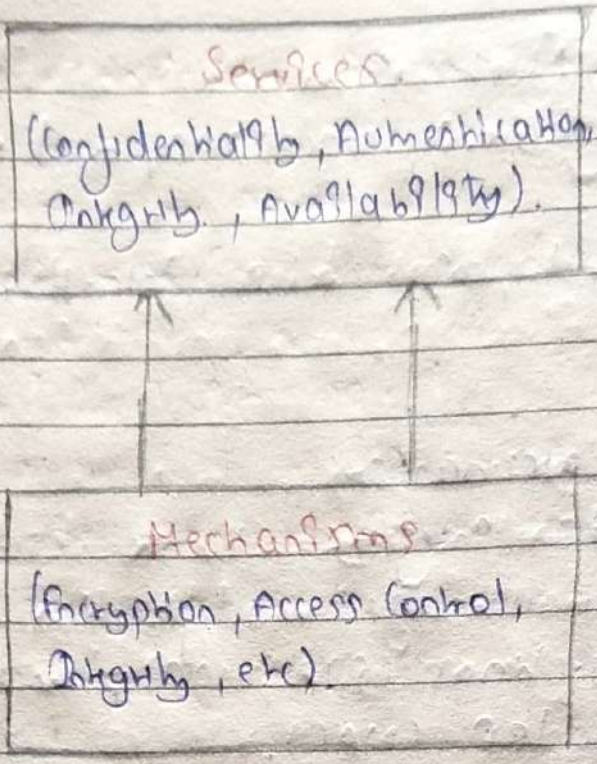
4. Data Integrity Mechanism
- ~~Ensures~~ authentication, integrity and non-repudiation
- ~~order~~ : Detects unauthorized modification of data.
- Example: Hash functions (SHA, MD5), checksums, message authentication codes (MAC).

5. Authentication Exchange.
- Mechanism by which communicating entities prove their identity.
- Example : challenge-response protocols, ~~Kerbore~~ Kerberos.

6. Traffic Padding.
- Inserts dummy data into traffic analysis attacks.

7. Routing Control.
- Chooses secure and trusted routes for transmitting data in a network.

8. Notarization.
- Use of a trusted third party (TTP) to confirm the authenticity and correctness of a message or transaction.



Attack surface and Attack trees.

Attack surface

The attack surface is the total set of points where an unauthorized user (attacker) can try to enter or extract data from a system.

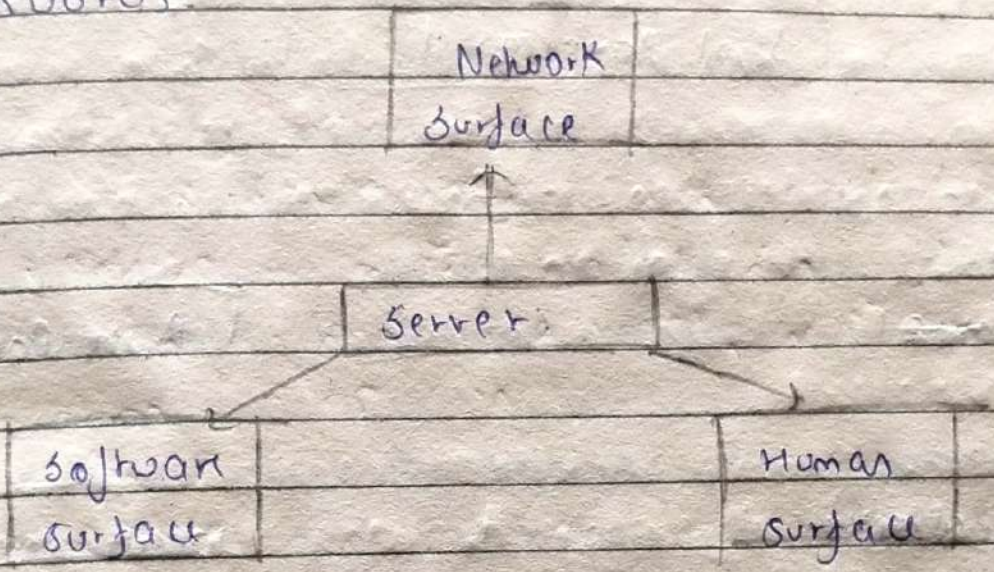
It defines how large and exposed the system is to potential attacks.

Components of Attack surface:

1. Network Attack Surface :- Open ports, protocols, services exposed.

2. Software Attack surface :- Applications, APIs, code vulnerabilities.

3. Human attack surface :- Users, social engineering, weak passwords.



Attack trees.

An attack tree is a diagram that represent the different ways an attacker can achelve a malicious goal.

Root node :- Represents the attacker's main objective (eg, "Steal sensitive data").

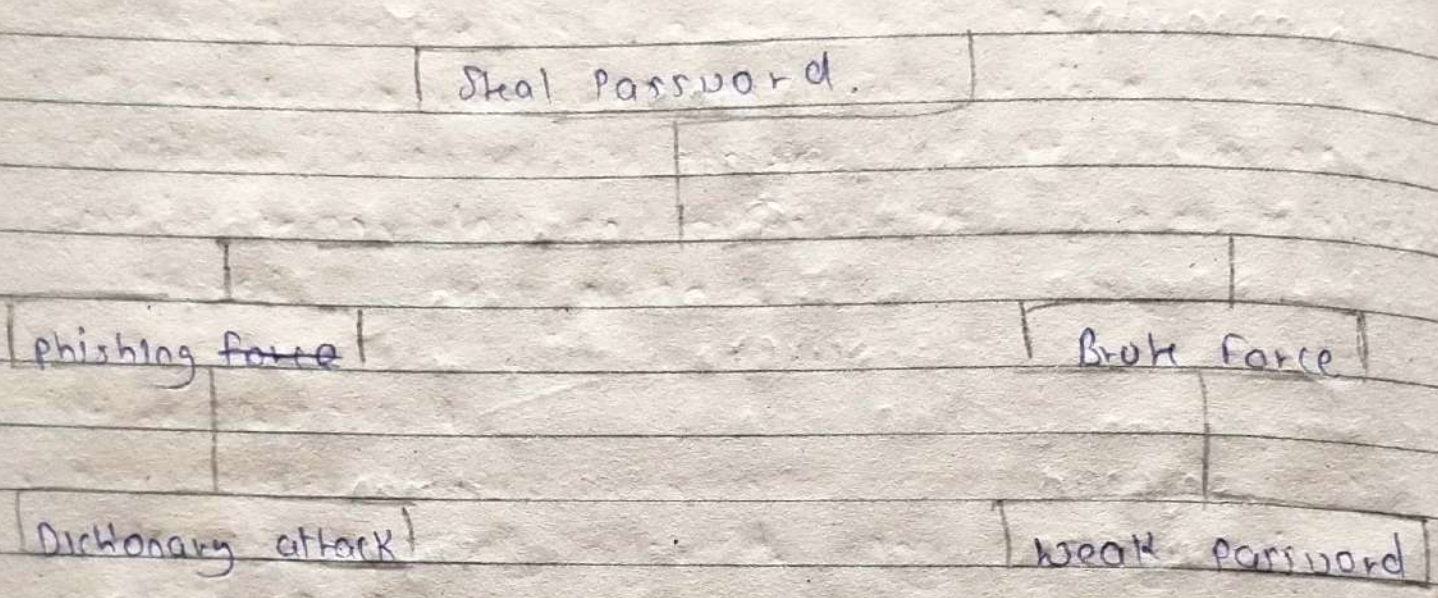
Branches / child Nodes :- Different possible attack methods.

·Nodes may combine using AND/OR :

AND :- All conditions must be satisfied.

OR :- Any one condition is enough

Ex of attack tree (for stealing password):



A Model of Network Security

A network security model defines how communication between two parties can be made secure, even in the presence of attackers.
It provides a structured framework for ensuring confidentiality, integrity, authentication, and availability of information.

~~Def~~ The model consists of the following components:-

1. Sender (A) :- Originates the message (plaintext).

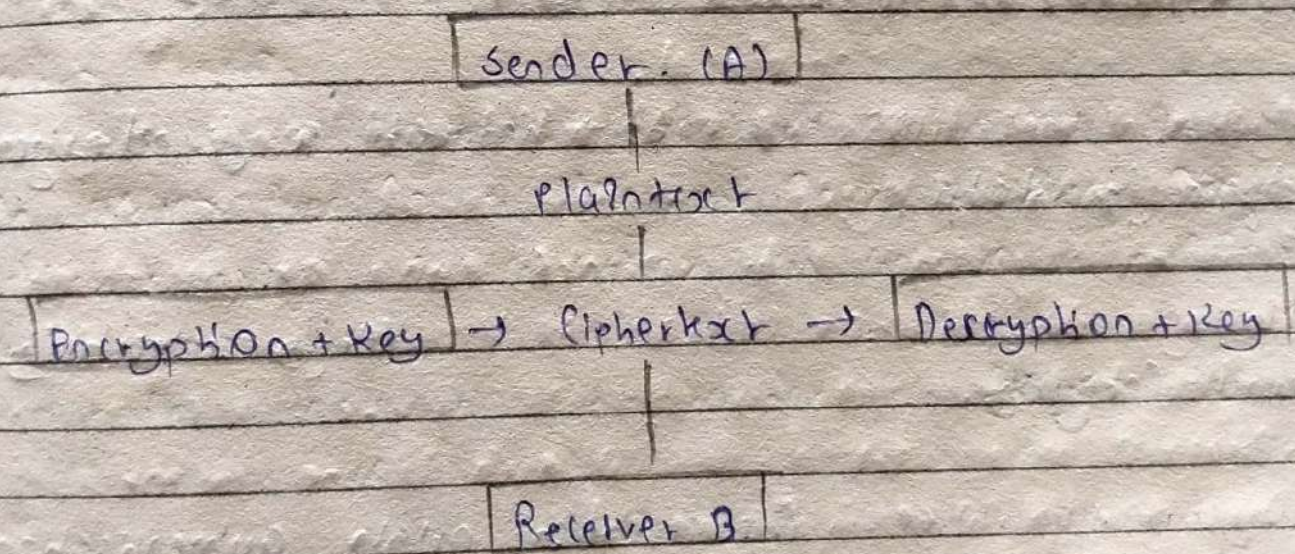
2. Encryption Algorithm :- Converts plaintext into unreadable ciphertext using a Key.

3. Ciphertext :- Transmitted securely across the network.

4. Opponent (Attacker) :- Attempts to intercept or alter data.

5. Decryption Algorithm :- At the receiver side, converts ciphertexts back to plaintext using a Key.

6. Receiver (B) :- Gets the original secure message.



*Attacker may try to intercept / modify ciphertext in transmit

Rajshree
PAGE NO.:
DATE:

Content Integrity.

Content Integrity means ensuring that the data or message content remains unaltered and accurate during storage, processing, or transmission.
It guarantees that information received is exactly the same as what was sent, with no modification, deletion, or insertion by unauthorized parties.

How it works.

Integrity is usually enforced using cryptographic techniques such as:-

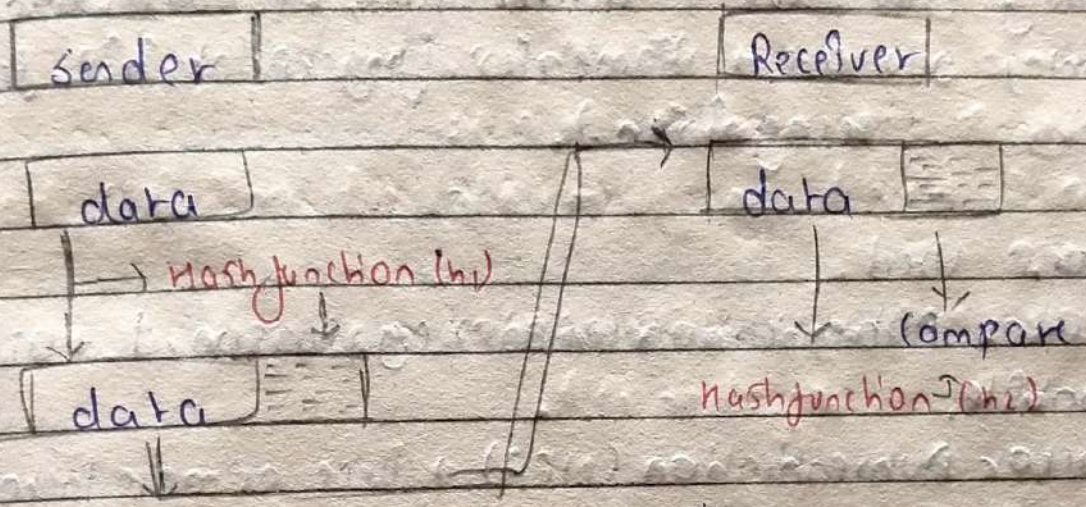
- Hash functions (MD5, SHA-256) → Generate a fixed-size digest for data.
- Message Authentication Codes (MACs) :- Verify authenticity and integrity.
- Digital signatures :- Ensure both origin authentication and content integrity.

Applications.

- Emails → Prevents tampering of message body and attachments.

- Banking transactions → Ensures no one modifies transaction amount / details.

- Software distribution → Verifies that downloaded software is not altered by malware.



If $h_1 = h_2$ → Integrity Maintained
If $h_1 \neq h_2$ → Integrity violated

Strong Authentication

Authentication ensures that a user, system, or entity is truly who/what it claims to be.
Strong Authentication refers to the use of two or more independent authentication factors to provide higher security than simple password-based authentication. It protects against identity theft, unauthorized access,

and replay attacks.

Authentication factors.

Strong authentication usually combines at least two of the following:

1. Something you know → Password, PIN, security questions
2. Something you have → Smart card, OTP token, mobile devic
3. Something you are → Biometrics (fingerprint, iris, face recognition).

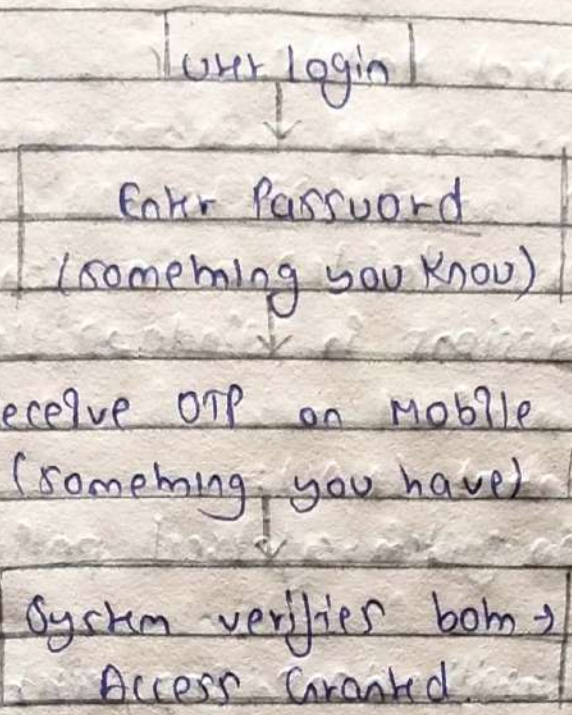
Techniques Used.

- Two-factor Authentication (2FA) → e.g., password + OTP sent to mobile
- Multi-factor Authentication (MFA) → Three or more factors combined.
- Digital Certificates / PKI → To validate identity using cryptographic keys.
- Biometric systems → fingerprints, retina, or facial verificatio

Benefits

- Prevents unauthorized access even if one factor (like password) is compromised.
- provides stronger defense against phishing, brute-force, and credential theft.
- Widely used in banking, e-commerce, VPNs, and cloud applications.

Example:- Strong Authentication with Two Factors



Access Controls:-

Access Control is the security mechanism that restricts or grant access to resources (files, systems, networks) only to ~~auth~~ authorized users.
It ensure confidentiality, Integrity, and availability of Information by preventing misuse or unauthorized operations.

Goal of Access Control.

- Ensure only legitimate users access sensitive data.
- Define what actions (read, write, modify, delete, execute) are allowed.

•Protect systems from insider and outsider threats.

Types of Access Control Models.

1. Discretionary Access Control (DAC):
   - Owner of a resource decides who can access it.
   - Example: File permissions in Windows/Linux.

2. Mandatory Access Control (MAC):
   - Access is based on system-enforced policies, not user choice.
   - Example: Military classifications (Top Secret, Secret, Confidential).

3. Role-Based Access Control (RBAC):
   - Access is based on user's role within an organization.
   - Example: An "admin" has higher privileges than a "Guest".

4. Attribute-Based Access Control (ABAC):
   - Access is determined by attributes (user, resource, environment).
   - Example: "Only employees with ID and office login can access at work hours."

Access Control Mechanisms.

- Authentication: Verify the identity of the user.
- Authorization: Grant permissions to access specific resources.
- Audit/Accounting: Monitor and record user activity for accountability

Rajshree
PAGE NO:
DATE:

Applications

- Protecting databases, cloud services, and enterprise networks
- Restricting access to financial transactions.
- Preventing unauthorized software or malware execution.

Wireless security

Wireless security refers to measures and protocols used to protect wireless networks (Wi-Fi, bluetooth, mobile networks, etc.) from unauthorized access, data theft, and attacks.

Since wireless signals travel through open air, they are more vulnerable than wired networks.

Threats in Wireless Networks

Eavesdropping : Attackers capture wireless signals to steal information.

Unauthorized Access :- Hackers connect to Wi-Fi without permission.

Man-in-the-Middle Attack (MITM) : Attacker intercepts and alters communication between two parties.

Denial of service (DoS) :- Flooding wireless signals to disrupt services.

Rogue Access Points :- Fake Wi-Fi hotspots tricking users into connecting.

Security mechanisms

1. Authentication:
   - Verifies user identity before granting access.
   - Example: WPA2 - Enterprise with RADIUS server.

2. Encryption:-
   - Protects data transmitted over wireless networks.
   - Protocols.
     - WEP (Wired Equivalent Privacy):- Weak, outdated.
     - WPA (Wi-Fi Protected Access):- Improved over WEP.
     - WPA2/WPA3: Strong encryption using AES.

3. Access Control:
   - Restricts network access using MAC address filtering, role-based policies.

4. VPN (Virtual Private Network):-
   - Creates a secure tunnel for communication over public Wi-Fi.

5. Intrusion Detecting Systems (IDS):-
   - Monitors wireless traffic for suspicious activities.

Best Practices.
- Use WPA3 encryption for Wi-Fi.

- Change default SSID and router passwords.
- Disable open networks (no password).
- Regularly update router firmware.
- Use firewalls & VPNs for extra protection.

Honey pots

A honeypots is a decoy system or resource intentionally set up to attract attackers.
It appears as a vulnerable target but is isolated and monitored.
Purpose:- to detect, deflect, or study hacking attempts.

Types of Honey pots.

1. Production Honeypots
- Deployed inside an organization's network.
- Help detect and divert real-time attacks.
- Simple to maintain, less complex.

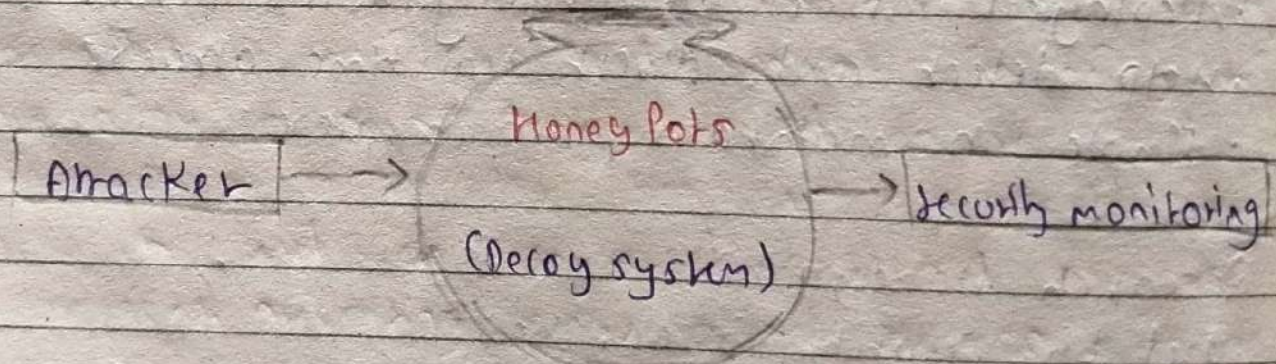
2. Research Honeypots
- Used by security researchers.
- Collect information about attackers techniques, tools, and motives.
- More complex, for long-term monitoring.

Working Principle.

- Attackers interacts with honeypot (thinking it is real)
- security team monitors activity to:-
  - identifying attack patterns.
  - discover new vulnerabilities.
  - Strengthen defenses of real systems.

Advantages

- Early detection of attacks.
- Provides insight into attacker behavior.
- Diverts attackers from real assets.
- Helps in developing better intrusion detection / Prevention systems.



Proxy Servers and Anonymizers

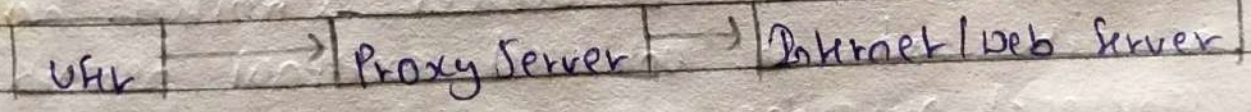
Proxy Server

A proxy server acts as an intermediary between a client and the Internet. When a client requests a web resource, the request is first sent to the proxy server, which then forwards it to the destination server. The response is also routed back through the proxy.

- Functions:
  - Improves security by hiding the client's IP address.
  - Provides caching to improve performance.
  - Enforces network policies (filtering, blocking, logging).

- Examples: An organization using a proxy to restrict employees from accessing social media websites.

Diagram:-



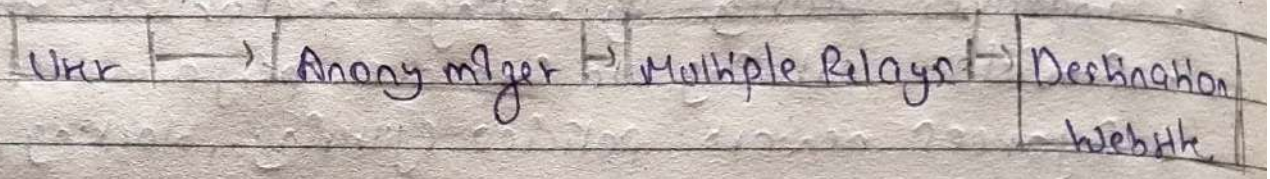
Anonymizers

An anonymizer is a special type of proxy designed to provide complete anonymity to users by making their identity and encrypting communication.

- Functions:-
  - Hides IP address to maintain user privacy.
  - Prevents tracking of online activities.
  - Used to bypass censorship and access blocked content.

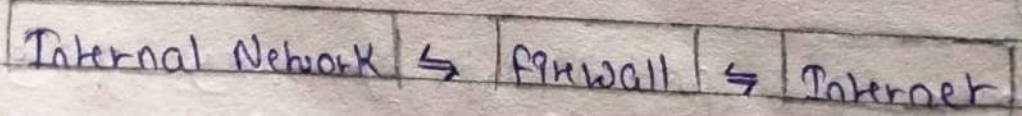
- Example: Tor network (The Onion Router) provides anonymity by routing traffic through multiple servers.

Diagram:-



Firewalls

A Firewall is a security system (hardware, software, or both) that monitors and controls incoming and outgoing network traffic based on predefined rules. It acts as a barrier between a trusted internal network and an untrusted external network (Internet), preventing unauthorized access and attacks.



Rajshree
PAGE NO.
DATE:

Types of firewalls

(a) Packet-filtering firewall
- Operates at Network layer
- Inspects packets based on IP addresses, ports, and protocol
- Simple and fast, but does not inspect packet contents.

(b) Stateful Inspection firewall
- Tracks the state of active connections
- Examines packet headers and context of communication
- More secure than simple packet filtering

(c) Proxy firewall (application-level-Gateway)
- Operates at Application layer
- Acts as an intermediary between users and services.
- Can inspect application-level data (eg. HTTP requests).
- Provides high security but slower due to deep inspection.

(d) Next-Generation firewall (NGFW)
- Combines features of traditional firewalls with intrusion prevention, deep packet inspection, and malware detection.
- Provides better protection against modern attacks.

Rajshree
PAGE NO.:
DATE:

Password cracking techniques.

1. Categories of Attacks.

- **Online attacks:** Attacker tries guesses directly against a live authentication service (e.g. SSH, web login).
  - Limited by throttling, account lockout, and network delays.
- **Offline attacks:** Attacker obtains hashed passwords (database leak) and tries guesses locally against the hash.
  - Much faster (no network latency) and can use GPUs/TPUs for massive parallelism.

2. Common Cracking Methods

- **Brute-force Attack**
  - Try every possible combination of characters until the password is found.
  - Guaranteed to succeed given enough time; complexity grows exponentially with length/charset.

- **Dictionary Attack**
  - Try words from a list (dictionary) of likely passwords (common words, leaked passwords).
  - Faster than brute force if users choose predictable passwords.

- Hybrid Attack
  - Combine dictionary words with common modifications (append numbers, replace letters with symbols).
  - Effective because users apply simple patterns (e.g. Password123!).

- Rainbow Table Attack
  - Precomputed tables of plaintext ↔ hash values to invert hash functions quickly
  - Defeated by salts (unique random values added to each password before hashing).

- Phishing & Social Engineering
  - Trick users into revealing passwords via fake pages, calls, or messages.
  - Often the simplest and most effective approach.

3. Factors that make cracking faster
- short passwords, simple patterns, and common dictionary words
- password reuse across services
- lack of salting or use of fast cryptographic hashes
- No rate limiting or account-lockout on authentication endpoints.