

CLICK FOR VIDEO (LINK) :

[HTTPS://DRIVE.GOOGLE.COM/FILE](https://drive.google.com/file/d/IJQX6UI6HA2COG78INKDME9V-XG4DD2LW/view?usp=drive_link)
[/D/IJQX6UI6HA2COG78INKDME9V-](https://drive.google.com/file/d/IJQX6UI6HA2COG78INKDME9V-XG4DD2LW/view?usp=drive_link)
[XG4DD2LW/VIEW?USP=DRIVE LINK](https://drive.google.com/file/d/IJQX6UI6HA2COG78INKDME9V-XG4DD2LW/view?usp=drive_link)

MODEL OF NETWORK SECURITY - ATTACKS, SERVICES & MECHANISMS



CNS ISE I

-PARSHWA HERWADE (22510064)

Model of Network Security - Attacks, Services & Mechanisms

- Introduction to Network Security
- Model of Network Security
- Classification of Security Attacks
- Passive Attacks
- Active Attacks
- Security Services (as per ISO X.800)
- Security Mechanisms
- Mapping - Attacks, Services, and Mechanisms
- Conclusion
- References

Introduction to Network Security

- Network security = protecting data & resources in communication.
- Deals with preventing, detecting, and responding to security threats.
- Key objectives (CIA Triad):

1. Confidentiality → Prevent unauthorized disclosure.

2. Integrity → Ensure data is accurate and unaltered.

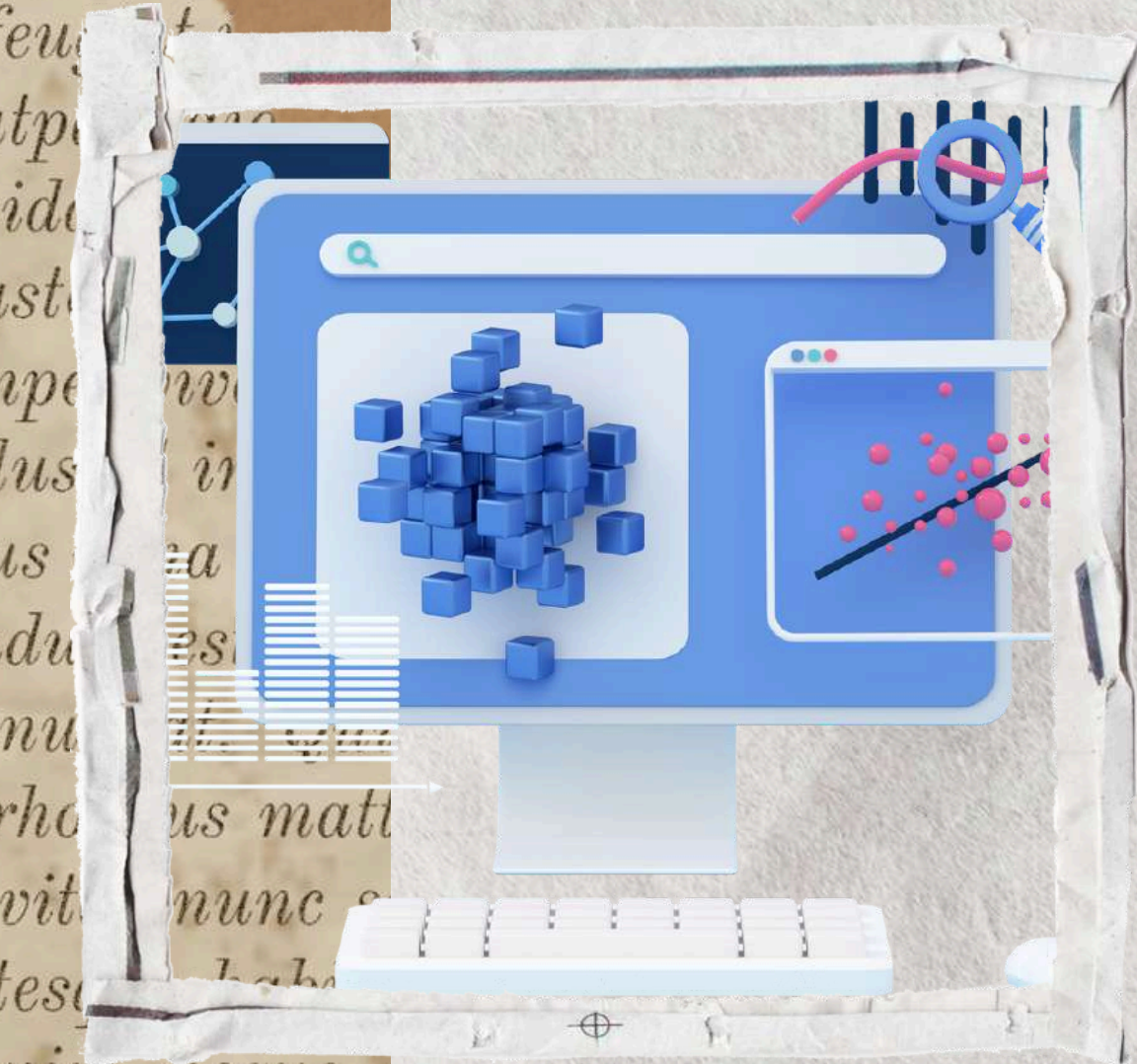
3. Availability → Ensure systems and services are accessible.

- Provides foundation for trust in digital communication.
- Implemented through security services & mechanisms.
- Without network security, attackers can eavesdrop, modify, or block data.
- Data in transit (over networks like Internet).
- Data at rest (stored in systems/servers).
- Security is not just technical → it also includes policies, procedures, and controls.
- Acts as a bridge between cryptography (mathematical techniques) and network protocols (practical communication).



Model of Network Security

- A generic model describes how security is applied to communication:
- Sender: Generates the message.
- Security Transformation: Message is encrypted, signed, or authenticated.
- Channel: Insecure medium (Internet) where attackers may interfere.
- Opponent: Tries to intercept, modify, or block the message.
- Receiver: Applies decryption/verification to retrieve original message.
- Trusted Third Party: Provides certificates, key management, or authentication support.
- Flow:
 - Sender → [Encryption/Signature] → Channel (Attacker present) → [Decryption/Verification] → Receiver



Classification of Security Attacks

- Security attacks = any action compromising information security.
- Two broad categories:

I. Passive Attacks:

- Attempt to read/observe communication without altering it.
- Goal: Obtain confidential information.
- Examples: Eavesdropping, traffic analysis.

2. Active Attacks:

- Attempt to modify, fabricate, or disrupt communication.
- Goal: Affect system integrity/availability.
- Examples: Masquerade, Replay, Modification, DoS.

- Key Difference:
- Passive = Silent & Undetectable.
- Active = Disruptive & Detectable.



Passive Attacks

- Definition: Attacks that only monitor or read communication without affecting system resources.

- Types:

I. Release of Message Contents: Attacker reads emails, chats, or confidential files.

2. Traffic Analysis: Even if encrypted, attackers analyze frequency, size, and patterns of communication.

- Features:

- Do not alter the communication.
- Extremely hard to detect (no traces left).
- Prevention is critical → encryption and traffic padding are common defenses.



Active Attacks

- Definition: Attacks that involve modification, disruption, or fabrication of communication.
- Types:
 - a. Masquerade → Attacker pretends to be an authorized entity.
 - b. Replay Attack → Attacker captures data and retransmits it later to gain unauthorized access.
 - c. Modification of Messages → Data altered during transmission.
Example: changing bank account numbers in transactions.
 - d. Denial of Service (DoS) → Flooding the network or system, making services unavailable.
- Features:
 - Easier to detect than passive attacks (cause visible disruption).
 - Require prevention, detection, and recovery mechanisms (firewalls, IDS, authentication).



Security Services (ISO X.800)

- Security services = essential functions that protect information and communication.

1. Authentication → Ensures the identity of sender/receiver (e.g., digital certificates, login systems).
2. Access Control → Restricts unauthorized users from accessing resources (firewalls, permissions).
3. Data Confidentiality → Protects data from unauthorized disclosure (encryption, VPN).
4. Data Integrity → Ensures data is not modified during transmission (hashing, MAC).
5. Non-Repudiation → Prevents denial of sending/receiving a message (digital signatures).
6. Availability → Ensures services remain accessible (redundancy, backups, DoS protection).

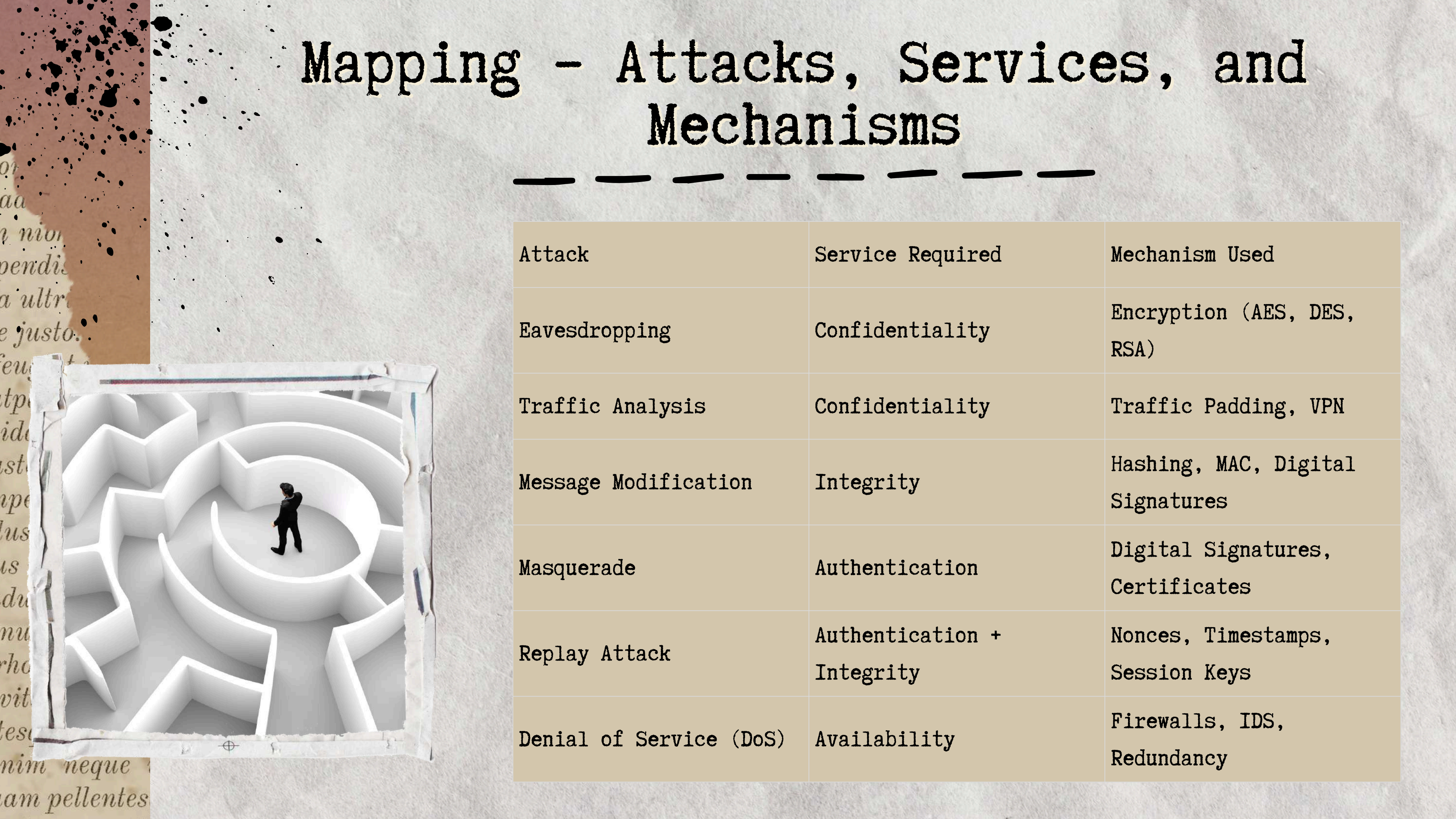
Security Mechanisms

- Security mechanisms are the tools/techniques that implement security services.
- Examples:
 - Encipherment → Encrypting messages to ensure confidentiality.
 - Digital Signatures → Authentication, integrity, and non-repudiation.
 - Access Control Mechanisms → Passwords, biometrics, firewalls, role-based access.
 - Data Integrity Mechanisms → Hash functions (SHA, MD5), Message Authentication Codes (MAC).
 - Authentication Exchange → Challenge-response protocols, digital certificates.
 - Traffic Padding → Inserting dummy data to disguise communication patterns.
 - Routing Control → Secure routing paths to prevent interception.
 - Notarization → Involving a trusted third party to verify communication.



Mapping - Attacks, Services, and Mechanisms

Attack	Service Required	Mechanism Used
Eavesdropping	Confidentiality	Encryption (AES, DES, RSA)
Traffic Analysis	Confidentiality	Traffic Padding, VPN
Message Modification	Integrity	Hashing, MAC, Digital Signatures
Masquerade	Authentication	Digital Signatures, Certificates
Replay Attack	Authentication + Integrity	Nonces, Timestamps, Session Keys
Denial of Service (DoS)	Availability	Firewalls, IDS, Redundancy




Conclusion

- The Network Security Model explains the relationship between:
- Attacks → Passive (eavesdropping) & Active (modification, DoS).
- Services → Confidentiality, Authentication, Integrity, Availability, Non-repudiation.
- Mechanisms → Encryption, signatures, access control, firewalls.
- Key Point: Security is not achieved by one mechanism alone → it requires a layered defense strategy.
- Strong cryptography + secure protocols + monitoring = robust protection against threats.

References

- William Stallings - Cryptography and Network Security: Principles and Practice.
- Behrouz A. Forouzan - Cryptography and Network Security.
- ISO X.800 Security Architecture Standard.





Thank you