Security Goals and Attacks

Cryptography and Network Security Notes

1 Security Goals

In information security, the three main goals are **Confidentiality**, **Integrity**, and **Availability** — collectively known as the **CIA Triad**. These goals form the foundation of all security mechanisms.

1.1 Confidentiality

Definition: Confidentiality ensures that information is accessible only to authorized users and is protected from unauthorized access or disclosure.

Explanation:

- Protects data from being exposed to unauthorized entities.
- Applies to both storage and transmission of data.
- Prevents data leakage during communication.

Examples:

- Military: concealment of sensitive information.
- Banking: customer account secrecy.
- Industry: protection from competitors.

Mechanisms to Achieve Confidentiality:

- **Encryption (Encipherment)** – Converts readable data into unreadable form.
- **Access Control** – Restricts who can view data.
- **Authentication** – Confirms the identity of users.

1.2 Integrity

Definition: Integrity ensures that data is accurate, complete, and can only be modified by authorized entities through authorized mechanisms.

Explanation:

- Protects against unauthorized modification or deletion.
- Maintains trustworthiness of data during storage or transmission.
- Violations can be malicious or accidental (e.g., power failure).

Examples:

- Bank account updates during deposits or withdrawals.

Mechanisms:

- Cryptographic Hash Functions (SHA, MD5)
- Digital Signatures
- Checksums / Error-detection codes
- Audit Logs

1.3 Availability

Definition: Availability ensures that authorized users have continuous access to information and resources when required.

Explanation:

- Even if data is secure, it's useless if not accessible.
- Ensures reliability and accessibility despite system failures or attacks.

Examples:

- Banking services must be available for customer transactions.

Mechanisms:

- Redundancy and Backups
- Load Balancing
- Firewalls and Intrusion Prevention Systems
- Disaster Recovery Plans

2 Attacks

The CIA goals can be threatened by various **security attacks**. Attacks are actions that compromise the confidentiality, integrity, or availability of information systems.

2.1 Attacks Threatening Confidentiality

2.1.1 Snooping (Eavesdropping)

Unauthorized interception or access to data. **Example:** Intercepting a file transfer over the Internet. **Countermeasure:** Use encryption to make intercepted data unreadable.

2.1.2 Traffic Analysis

Even if data is encrypted, attackers can analyze communication patterns. **Example:** Observing frequent messages between a company and a supplier. **Countermeasure:** Use anonymization or dummy traffic.

2.2 Attacks Threatening Integrity

2.2.1 Modification

Attacker intercepts and alters messages to benefit themselves. **Example:** Changing a bank transaction to redirect funds. **Countermeasure:** Use message authentication codes (MACs) or digital signatures.

2.2.2 Masquerading (Spoofing)

Attacker impersonates another user or entity. **Example:** Fake websites or stolen credentials. **Countermeasure:** Strong authentication, digital certificates.

2.2.3 Replaying

Attacker captures a valid message and reuses it later. **Example:** Replaying a valid bank transfer to gain multiple payments. **Countermeasure:** Use timestamps, nonces, or session tokens.

2.2.4 Repudiation

One party denies having sent or received a message. **Example:** Customer denies sending a payment request. **Countermeasure:** Digital signatures and transaction logs.

2.3 Attacks Threatening Availability

2.3.1 Denial of Service (DoS)

Attackers overload or block system resources to make services unavailable. **Examples:**

- Flooding a server with bogus requests.
- Intercepting or deleting server responses.

Countermeasures:

- Firewalls and Filtering
- Rate Limiting
- Distributed Architectures (CDNs)

3 Passive vs Active Attacks

Category	Goal	Examples	Characteristics
Passive Attack	Obtain information without modification	Snooping, Traffic Analysis	Difficult to detect, prevented by encryption
Active Attack	Modify or disrupt data/system	Modification, Spoofing, Replay, Repudiation, DoS	Easier to detect, harder to prevent

4 Security Services and Mechanisms

Security services and mechanisms are defined by the **ITU-T X.800** standard. They work together to achieve the goals of **Confidentiality, Integrity, and Availability (CIA)** and to defend against security attacks.

4.1 Security Services

A **security service** is a process or communication service that enhances the security of data processing systems and information transfer. ITU-T (X.800) defines five main security services.

4.1.1 Data Confidentiality

Goal: Protect data from unauthorized disclosure (snooping and traffic analysis).
Description:

- Ensures that data is accessible only to authorized users.
- Applies to both entire messages and specific parts.
- Protects against traffic analysis by concealing communication patterns.

Mechanisms Used: Encipherment, Traffic Padding, Routing Control.
Example: Encrypting banking transactions so that third parties cannot read or infer communication.

4.1.2 Data Integrity

Goal: Protect data from unauthorized modification, insertion, deletion, or replay.
Description:

- Ensures that received data is exactly as sent.
- Detects accidental or malicious modifications during transmission.

Mechanisms Used: Cryptographic Hash Functions, MACs, Digital Signatures.
Example: Verifying software files using hash values.

4.1.3 Authentication

Goal: Confirm the identity of communicating entities.
Description:

- Ensures sender and receiver are genuine.
- Prevents impersonation or masquerading.

Types of Authentication:

- **Peer Entity Authentication:** For connection-oriented systems.
- **Data Origin Authentication:** For connectionless systems.

Mechanisms Used: Encipherment, Digital Signature, Authentication Exchange.
Example: Secure website login using valid credentials.

4.1.4 Nonrepudiation

Goal: Prevent sender or receiver from denying participation.
Description:

- Provides proof of origin and delivery.
- Ensures accountability and prevents false denial.

Types:

- Nonrepudiation of Origin
- Nonrepudiation of Delivery

Mechanisms Used: Digital Signatures, Notarization.
Example: Digitally signed emails that verify the sender.

4.1.5 Access Control

Goal: Prevent unauthorized use of resources.
Description:

- Ensures only authorized users can perform actions like reading or modifying data.
- Implements authentication and authorization.

Mechanisms Used: Passwords, PINs, Access Control Lists (ACL), Authentication Systems.
Example: Only administrators can change system configurations.

4.2 Security Mechanisms

A **security mechanism** is a method or tool used to implement one or more security services. They are divided into **specific mechanisms** and **pervasive mechanisms.**

4.2.1 Encipherment

Purpose: Protect confidentiality. **Description:** Converts plaintext into ciphertext using cryptographic algorithms (symmetric/asymmetric). **Example:** AES encryption.

4.2.2 Data Integrity Mechanism

Purpose: Ensure data has not been altered. **Description:** Adds a check value (hash or MAC) for verification. **Example:** File checksum comparison.

4.2.3 Digital Signature

Purpose: Provide authentication, integrity, and nonrepudiation. **Description:** Sender signs data using a private key; receiver verifies with the public key. **Example:** Signed PDF or email.

4.2.4 Authentication Exchange

Purpose: Prove identities of communicating parties. **Description:** Entities exchange credentials to verify each other. **Example:** SSL/TLS client-server authentication.

4.2.5 Traffic Padding

Purpose: Protect against traffic analysis. **Description:** Adds fake data packets to disguise traffic patterns. **Example:** Padding messages to uniform size.

4.2.6 Routing Control

Purpose: Avoid interception by controlling message paths. **Example:** VPN routing or secure tunnels.

4.2.7 Notarization

Purpose: Prevent repudiation by involving a trusted third party. **Example:** Digital time-stamping services.

4.2.8 Access Control Mechanism

Purpose: Enforce access policies. **Example:** Role-based access control, password systems.

Relation Between Services and Mechanisms

Service	Primary Mechanisms Used
Data Confidentiality	Encipherment, Traffic Padding, Routing Control
Data Integrity	Data Integrity Mechanism, Digital Signature
Authentication	Encipherment, Digital Signature, Authentication Exchange
Nonrepudiation	Digital Signature, Notarization
Access Control	Access Control Mechanisms, Authentication

5 Techniques

Mechanisms describe **what to do**; techniques describe **how to do it.** Two key techniques implement security mechanisms: **Cryptography** and **Steganography.**

5.1 Cryptography

Definition: The science and art of transforming messages to make them secure and immune to attacks. Ensures confidentiality, integrity, and authentication.

5.1.1 Symmetric-Key Encipherment

- Uses a single shared secret key for both encryption and decryption.
- Fast and efficient but requires secure key exchange.

Example: AES, DES, 3DES.

5.1.2 Asymmetric-Key Encipherment

- Uses two keys: public and private.
- Public key encrypts, private key decrypts.
- Used for encryption, key exchange, and digital signatures.

Example: RSA, ECC.

5.1.3 Hashing

- Converts input data into a fixed-length digest.
- Used for integrity verification and password storage.
- One-way function: cannot reverse the hash.

Example: SHA-256, MD5.

5.2 Steganography

Definition: Technique of hiding the existence of a message within another medium. **Cryptography hides content; Steganography hides existence.**

5.2.1 Historical Uses

- Hidden writing on wax tablets or invisible ink.
- Null ciphers and microdots.

5.2.2 Modern Uses

- **Text Cover:** Hide binary data using spaces or text patterns.
- **Image Cover (LSB Method):** Hide bits in least significant pixels.
- **Audio/Video Cover:** Embed data in sound or video frames (e.g., watermarking).

Comparison: Cryptography vs Steganography

Aspect	**Cryptography**	**Steganography**
Purpose	Conceals message content	Conceals message existence
Visibility	Message is visible but unreadable	Message is invisible within a medium
Technique	Encryption using keys	Hiding in text, image, or audio
Example	Encrypted email	Hidden data in an image