## Vulnerability, Threat, Control

Vulnerability : is a weakness in the security system, procedure, design or implementation that might be exploited to cause harm / loss.

Threat: to computer system is a set of circumstances that has a potential to cause loss / harm.

Control: is an action, device, procedure or technique that removes or reduces vulnerability.

* Threat → blocked by control of vulnerability

eg: 1) Online Zoom Calls

Threats: 1) Zoombombing 2) Inappropriate or malicious chats
3) Recording w/o consent

Vulnerability: 1) Publically accessible meeting links
2) Unrestricted permissions 3) weak pass.

Controls: 1) Block chatting & recording permission 2) Waiting-room feature 3) password-protected meetings

## 2) Bank Transaction

### Attack, Mechanism, Service (information security)

Security Attack: any action that compromises the security of info

Security Mechanism: mech. designed to detect, prevent or recover (dpr) from a security attack.

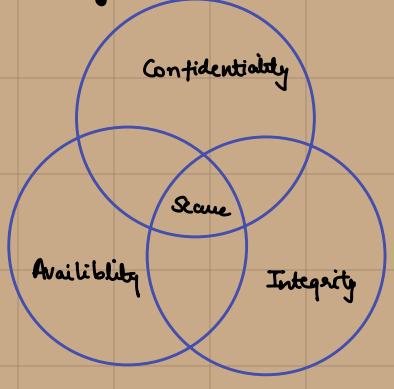
Security Service: A service that enhances security of data processing systems & info transfers. (use one or more security mech.

eg: Attack: Phishing e-mail Mech: e-mail filter + OTP

Service: Authentication

### Security Goals

> They define what we want security to achieve (end-goals) or the main things we want to protect in info systems.



## Confidentiality :

1) ensures comp related assets are accessed only by auth. parties
2) access refers to reading, viewing, printing or knowing that a particular asset exists
3) also known as secrecy / privacy

## Integrity :

1) It means that assets can be modified only by auth parties in authorized ways.
2) Integrity of an item is preserved if it is -
   precise, accurate, unmodified, modified in correct ways - by authorized parties using auth. processes, consistent, meaningful, & usable.

## Availibility :

1) applies to both data and data processing
2) A data item, service or system is available if
   - there is timely response to our request
   - fair to all ie no bias towards requesters
   - fault tolerant
   - controlled concurrency, deadlock management & exclusive access as req.

## Security Attacks → by function

1. Interruption : attack on availability, confidentiality
   - resources should be acc. when needed
   - data destroyed & not retrievable ↳ no access
   - ↳ system/data is destroyed, damaged or made unavailable

2. Interception: attack on confidentiality
   - ↳ an authorized party gains access to data

3. Modification : attack on integrity
   - ↳ unauthorized party changes data in unauth. ways

4. Fabrication: attack on authenticity → genuine user/data accept
   - ↳ unauthorized party inserts false data, info into system

## Active vs Passive Threats

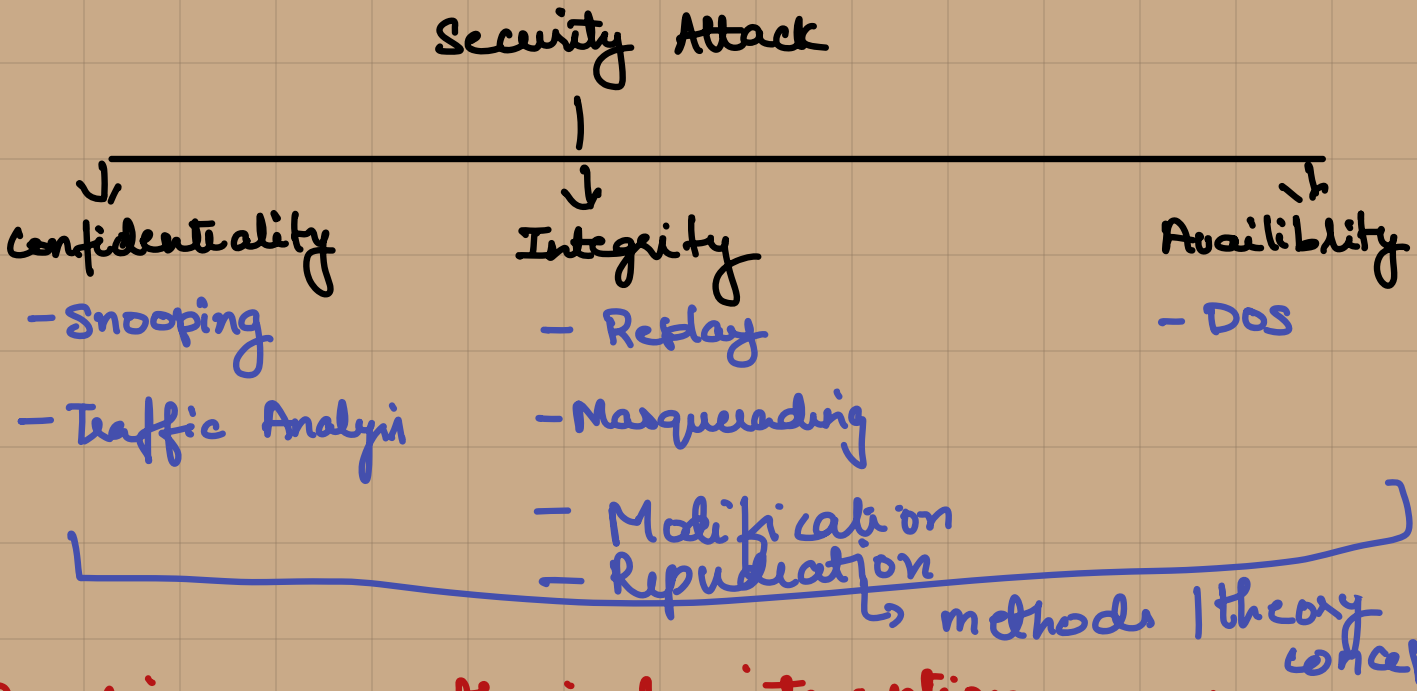
↑ Integrity Avail., Authen., Acc.

- ↳ attacker modifies, disrupts or injects data (Active)
- ↳ attacker only observes/monitors comm/data w/o alteration

↓ Confidentiality

→ detn., cfg, appn.

Attacks → Cryptanalytic : exploit math weakness of crypto algos
→ non : threats to security goals (CIA)




→ Snooping : unauthorized interception of data.
passive attack
eg: Eavesdropping, MITM

→ Traffic Analysis: even if messages are encrypted attackers study metadata (who talks to whom, how often, when) to infer info.
eg: Traffic Analysis attack
→ passive

→ Modification: unauthorized altering of data stored.

→ Active attack

eg: MITM + Data tampering + Malware

→ **Masquerading:** (impersonation) attackers try to act as a legitimate source

→ Active attack.

eg: Brute + Spoofing + Phishing + Session Hijacking

→ **Replaying** : capturing valid data & resending it later to gain unauth access + data.

↓ authenticity

→ Active attack

eg: Replay Attack + Session Hijack

→ **Repudiation:** a user denies performing an action

↓ accountability

→ Active attack

eg: Non-repudiation

→ Denial of Service : Overloading a system so that legitimate users can't access

→ Active

eg : DOS + Malware

🔐 Attacks with Security Mechanism Controls

1. Eavesdropping

* Definition: Secretly listening to communication/data in transit.

* Applications: Sniffing credentials on open Wi-Fi.

* Category: Interception → Snooping.

* Active/Passive: Passive.

* CIA Affected: Confidentiality.

* Controls (Mechanisms):

  * Encipherment (Encryption): Encrypt traffic with TLS, VPN, WPA3 Wi-Fi.

  * Authentication Exchange: Ensure both parties authenticate before session (e.g., TLS handshake).

  * Routing Control: Force data through trusted routes, avoid untrusted relays.

2. Traffic Analysis Attack

* Definition: Observing communication patterns (metadata) instead of content.

* Applications: Inferring command servers or user relationships.

* Category: Interception → Traffic analysis.

* Active/Passive: Passive.

* CIA Affected: Confidentiality.

* Controls (Mechanisms):

    * Traffic Padding: Add dummy traffic to hide patterns.

    * Encipherment: Encrypt headers and metadata where possible (VPNs hide real endpoints).

    * Routing Control: Use onion routing (Tor) to obscure paths.

3. Replay Attack

* Definition: Capturing valid data and retransmitting later.

* Applications: Replaying login tokens, bank transfers.

* Category: Modification / Fabrication → Replay.

* Active/Passive: Active.

* CIA Affected: Integrity, Authenticity.

* Controls (Mechanisms):

    * Authentication Exchange: Use challenge-response with nonces/OTPs.

    * Data Integrity Mechanisms: Use hashes + timestamps to detect replays.

    * Digital Signature: Sign messages so they can’t be reused later without invalidating freshness.

4. Non-repudiation Attack (Repudiation)

* Definition: A party denies sending/receiving a message or action.

* Applications: A user denies an online purchase.

* Category: Fabrication / Accountability.

* Active/Passive: Active.

* CIA Affected: Non-repudiation, Authenticity.

* Controls (Mechanisms):

    * Digital Signature: Bind sender identity to message, cannot be denied later.

    * Notarization: Trusted third party timestamps/verifies transactions.

    * Data Integrity Mechanisms: Audit logs with cryptographic hashes.

5. Man-in-the-Middle (MITM) Attack

* Definition: Attacker intercepts & alters communication.

* Applications: TLS stripping on public Wi-Fi.

* Category: Interception + Modification.

* Active/Passive: Active.

* CIA Affected: Confidentiality, Integrity, Authenticity.

* Controls (Mechanisms):

    * Encipherment: End-to-end encryption prevents unauthorized reading.

    * Digital Signature: Certificates bind servers to their identity.

    * Authentication Exchange: Mutual authentication prevents fake endpoints.

    * Routing Control: Avoid malicious relays/nodes.

6. Data Tampering

* Definition: Unauthorized modification of data.

* Applications: Changing grades, altering firmware.

* Category: Modification.

* Active/Passive: Active.

* CIA Affected: Integrity (primary).

* Controls (Mechanisms):

    * Data Integrity Mechanisms: Hashes, checksums, MACs to detect changes.

    * Digital Signature: Verifies authenticity of unmodified data (e.g., signed firmware).

    * Notarization: Third party confirms data version/time.

7. Denial of Service (DoS)

* Definition: Overloading/disrupting resources.

* Applications: SYN floods, HTTP floods.

* Category: Interruption.

* Active/Passive: Active.

* CIA Affected: Availability.

* Controls (Mechanisms):

    * Routing Control: Redirect or balance load through alternate routes.

    * Traffic Padding: Sometimes used to absorb volume fluctuations.

    * Authentication Exchange: Prevent illegitimate clients from consuming resources.

8. Brute Force Attack

* Definition: Repeated trial of credentials/keys.

* Applications: Password/PIN cracking.

* Category: Masquerading (auth bypass).

* Active/Passive: Active.

* CIA Affected: Confidentiality, Authentication.

* Controls (Mechanisms):

    * Authentication Exchange: MFA, challenge-response protocols.

    * Encipherment: Strong encryption with large keyspace to resist brute force.

    * Data Integrity Mechanisms: Account lockout logs ensure failed attempts are tracked.

9. Zero-day Exploit

* Definition: Attack exploiting an unknown vulnerability.

* Applications: Worms or targeted remote exploits.

* Category: Multi-category (interception, modification, interruption).

* Active/Passive: Active.

* CIA Affected: C, I, A.

* Controls (Mechanisms):

    * Encipherment: Limits data theft even if exploit succeeds.

    * Routing Control: Isolate vulnerable systems to limit lateral spread.

    * Data Integrity Mechanisms: Detect tampered binaries or injected code.

10. Phishing & Social Engineering

* Definition: Deceiving users into revealing information or actions.

* Applications: Fake login forms, vishing calls.

* Category: Masquerading (Impersonation).

* Active/Passive: Active.

* CIA Affected: Confidentiality, Authentication.

* Controls (Mechanisms):

    * Authentication Exchange: MFA protects even if passwords are stolen.

    * Digital Signature: Emails signed (S/MIME, DKIM) to prove authenticity.

    * Notarization: Verified brand identities in messages.

11. Spoofing

* Definition: Forging identity data (IP, email, caller ID).

* Applications: Email spoofing, IP spoofing in DDoS.

* Category: Fabrication → Masquerading.

* Active/Passive: Active.

* CIA Affected: Authenticity, Integrity.

* Controls (Mechanisms):

    * Digital Signature: Signed data validates real sender.

    * Authentication Exchange: Mutual verification of endpoints.

    * Routing Control: Source address validation, SPF/DKIM for email.

12. Malware

* Definition: Malicious software (virus, worm, trojan, ransomware).
* Applications: Ransomware encrypting files, spyware stealing info.
* Category: Multi-category (interception, modification, interruption, fabrication).
* Active/Passive: Active.
* CIA Affected: C, I, A.
* Controls (Mechanisms):
    * Encipherment: Protects sensitive data from spyware.
    * Data Integrity Mechanisms: Detect altered files/processes.
    * Authentication Exchange: Prevent unauthorized installs via signed updates.
    * Digital Signature: Software signed by vendor, preventing fake apps.

13. Session Hijacking

* Definition: Stealing/taking over valid session tokens or IDs.
* Applications: Cookie theft via XSS or sniffing, session fixation.
* Category: Masquerading + Replay.
* Active/Passive: Active (theft may be passive).
* CIA Affected: Authentication, Integrity, Confidentiality.
* Controls (Mechanisms):
    * Encipherment: Encrypt cookies/tokens in transit (TLS).
    * Authentication Exchange: Re-authentication for sensitive actions.
    * Data Integrity Mechanisms: Session tokens bound to IP/device.
    * Digital Signature: Signed tokens (JWT with HMAC/RS256).

* Routing Control: Secure routing to prevent interception of tokens.

### 🔐 Security Services (What security aims to achieve)

These are the **goals/objectives** of security.

1. **Data Confidentiality**
   - Protects data from unauthorized disclosure.
   - Example: Encryption ensures only the intended recipient can read the message.
2. **Data Integrity**
   - Ensures information is not modified, deleted, or replayed without detection.
   - Sub-types:
     - **Anti-change** → Prevents unauthorized changes.
     - **Anti-replay** → Prevents attackers from re-sending old valid messages.
3. **Authentication**
   - Verifies identity and origin.
   - Sub-types:
     - **Peer Entity Authentication** → Confirms the communicating party is who they claim to be (e.g., login with OTP).
     - **Data Origin Authentication** → Ensures that the message came from the claimed source.
4. **Non-repudiation**
   - Prevents sender or receiver from denying their actions.
   - Sub-types:
     - **Proof of origin** → Sender cannot deny sending.
     - **Proof of delivery** → Receiver cannot deny receiving.
   - Example: Digital signatures.
5. **Access Control**
   - Restricts unauthorized users from accessing resources.
   - Example: Role-based access, password protection.

+ Availibliy DOS virus that delete files

### ⚙️ Security Mechanisms (How security is achieved)

These are the **tools/methods** that implement the services above.

1. **Encipherment (Encryption)** → For confidentiality.
2. **Data Integrity Mechanisms** → Hashing, checksums, MACs.
3. **Digital Signature** → For authentication, integrity, non-repudiation.
4. **Authentication Exchange** → Passwords, OTPs, challenge-response protocols.
5. **Traffic Padding** → Adding dummy data to hide actual traffic patterns (resists traffic analysis).
6. **Routing Control** → Secures routing paths to avoid compromised nodes.
7. **Notarization** → Trusted third-party confirms events (e.g., timestamping service).
8. **Access Control Mechanisms** → Firewalls, role-based access, biometrics.

Encipherment

- converting data into an unreadable format using alg Keys
- Confidentiality

- Whatsapp msg → encrypted AES → only recipient can decrypt.

2. Digital Signature
   - binds sender's identity w message
   - authentication, integrity, non-rep.

3. Data Integrity Mechanisms
   - methods like hashing, checksums, MACs to detect changes
   - integrity: data isn't accidently/maliciously modified
   - eg: downloads: SHA-256 hash

4. Authentication exchange
   - protocols to verify identity before communication.
   - authentication
   - logging in / OTP / MFA / TLS handshake

5. Traffic Padding
   - add extra (dummy) data to communication.
   - against traffic analysis attack.
   - eg: VPN sends constant "fake" packets so attacker can't see what you're browsing

6. Routing control
   - choosing secure / alternate comm. routes
   - Availibility & resists interception.

7. Notarization
   - using a TPP (trusted third party) to verify actions/ data
   - Non-Rep & authenticity
   - eg: digital timestamping

8. Access Control Meth.
   - restricting who can access resources.
     confind. & avail by blocking unauth
     RBAC, ABAC, DAC