Security Concepts:

Information security has 3 major goals - CIA Triad

Confidentiality

- Protects information from unauthorized access

Concerns:

1. Snooping:
    a. As the name suggests, Accessing information that is left out in the open.
    ★ *Can be avoided by maintaining clean desk space and closing the files or hiding confidential information when they are leaving somewhere.*
2. Dumpster diving:
    a. As the name suggests they doesn't wander around office like snooping instead look at garbage or recycle bin to find any sensitive information/documents
    ★ *It can be protected using paper shredder / Shredding*
3. Eavesdropping:
    a. Physical: Attacker can place themselves as server in an open place or anywhere which helps him in eavesdropping
    ★ *Can be avoided by discussing sensitive information in restricted areas like Office buildings etc.*
4. Wiretapping also known as electronic eavesdropping:
    a. Occurs when an attacker gains access to the network and monitors data being sent to and fro.
    ★ *Can be protected by following encryption standards when data is sent over network*
5. Social Engineering:
    a. Attacker uses psychological tricks to persuade employee to give it or give access to information
    ★ *Can be protected by Education and Training protects against social engineering*

Integrity:

Protects information from unauthorized changes

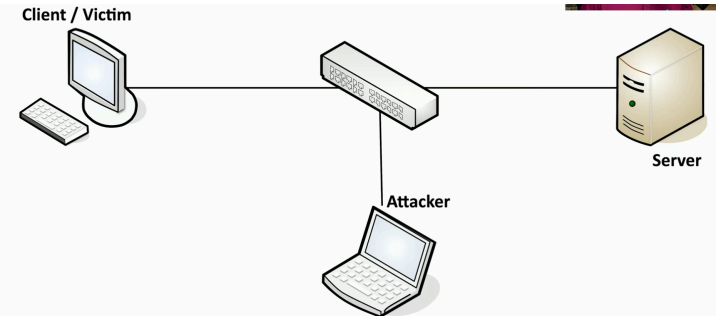
Concerns

1. Unauthorized Modification:
    a. Attackers make changes without permission (can be internal=employees or external)
    ★ Follow the principle of least privilege.
2. Impersonation Attack:
    a. Attackers pretend to be someone(legit) than who they actually are.
    ★ Strong education is the way to avoid it.

    Impersonation can be electronic and can be called as MITM
3. Man in the middle attack(MITM):
    a. When an attacker is displaced in the middle of a communication session.
    b. Attacker intercepts network traffic as a user is logging into a system and then pretends to be that user. They sit in the middle of the communication, relaying information between the user and the system while monitoring everything that's occurring.
    c. They try to steal the password of the user and later use it to log into the system.
    ★ Encryption can prevent MITM
4. Replay attack:
    a. Attackers eavesdrop on logins and reuse the captured credentials

    Detailed Explanation: attacker needs the access to network data which will reuse it and send it the original destination pretending it to be coming from the original sender. For this process they perform Physical Network Tap to watch the traffic, ARP poisoning to redirect the traffic or put malware on the victim's computer to gather information going across the network.

    Let's understand this with a story



The client sends a hashed username and password to the server but the attacker places himself in order to sniff the traffic and gain hashed username and password, later he replays the attack by sending the same hashed username and password to the server which validates and gives access to the attacker. This is called Pass the hash

★ Encryption prevents Replay attacks along with encryption maintaining timestamps or session IDs that created new hash passwords after the session expires

Availability:

Ensures that information and systems remain available to authorized users when needed.

Concerns:

1. Denial-of-service attacks:
    a. When a malicious individual bombards a system with an overwhelming amount of traffic.
    b. The idea to is to send so many requests to a server that it is unable to answer any requests from legitimate users
    ★ Firewalls block unauthorized connections to protect against Denial of Service attacks. And partnering with internet service providers to block the malicious ips

2. Power outages:
    a. Increased demand can overwhelm the power grid, natural disasters can disrupt service and other factors can cause power outages that disrupt access to systems.
    ★ Having redundant power sources and back-up generators protect against power outages

3. Hardware failures:
    a. Failure of servers, hard drives, network gear etc
    b. Redundant components protect against hardware failure
    ★ Building systems that have a built-in redundancy, so that if one component fails, the other will take over
4. Destruction of equipment:
    a. Sometimes equipment is just outright destroyed. This may be the result of intentional or accidental physical damage, or it may be the result of a larger disaster, such as a fire or a hurricane.
    ★ Protect against small scale destruction with redundant systems.
    ★ Against larger scale disasters, have backup data centers in remote locations or in the cloud.
5. Service outages:
    a. Service outage may occur due to programming errors, failure of underlying equipment, and many more reasons
    ★ Building systems that are resilient in the fact of errors and hardware failures protect against service outages

Authentication & Authorization

Access Control Process

1. Identification:

   Identification involves making a claim of identity (Can be false)

★ Electronic identification commonly uses usernames

2. Authentication

   Authentication requires proving a claim of identity

★ Electronic authentication commonly uses passwords

3. Authorization

   Authorization ensures that an action is allowed

★ Electronic authorization commonly takes the form of access control lists

Access Control Lists also provides

4. Accounting functionality

   Accounting allows to track and maintain logs of user activity

★ Can track systems and web browsing history; Resources used by that specific user : Login time, data sent and received, logout time etc

Authentication + Authorization + Accounting = AAA

Password Security:

Controls you can implement when setting password requirements:

- Password length requirements set a minimum number of characters.
- Password complexity requirements describe the types of characters that must be included.
- Password expiration requirements
- Force password changes
- Password history requirements
- Cannot use previously used passwords

Every organization should make it easy for users to change their passwords, however, be careful of the password reset process as it may provide an opportunity for attackers to take advantage through unauthorized password reset.

Password Managers: They facilitate the use of strong and unique password (suggested passwords)

- Secured password vaults often protected by biometric mechanisms (ex=fingerprints)
- Facilitates the use of strong, unique passwords
- Stores passwords

MFA-Multi Factor Authentication

3 types of authentication factors

1. Something you know: 1st factor of Authentication
    - Passwords, Pins
2. Something you are: 2nd factor of Authentication
    - Biometric Security Mechanisms
    - Fingerprints
    - Voice
3. Something you have :3rd factor of authentication
    - Software and Hardware Tokens

Note: Passwords combined with security questions are NOT multi factor authentication. Passwords and security questions are both something you know

Single Sign-On (SSO)

Shares authenticated sessions across systems

Organizations create SSO solutions within their organizations to avoid users repeatedly authenticating

Non-repudiation:

- Prevents someone from denying the truth
    - Physical signatures can provide non-repudiation on contracts, receipts etc
    - Digital signatures use encryption to provide non-repudiation
    - Other methods can be biometric security controls, Video-surveillance etc

Privacy

Organization Privacy Concerns

1. Protecting our own data
2. Educating on users on how they can protect their own personal information
3. Protecting data collected by our organizations

2 Types of Private Information

Personally-Identifiable Information (PII)

- Any information that can be tied back to a specific individual

Protected Health Information (PHI)

- Health care records - Regulated by HIPAA

Reasonable expectation of privacy

Many laws that govern whether information must be protected are based upon whether the person disclosing the information had a reasonable expectation of privacy

- If you upload a YouTube video, you do not have a expectation of privacy
- You do have some expectation of privacy for private electronic communications such as: email, instant chats etc
- You do not have a reasonable expectation of privacy when sharing PII with an organization
- You do not have a reasonable expectation of privacy when using employer resources