CIA Triad

1. Confidentiality

Confidentiality is about protecting data from unauthorized access and disclosure. It ensures that only authorized individuals, systems, or processes can view or use sensitive information.

- **Goal:** To maintain privacy and secrecy.
- **Threats:** Unauthorized access, data breaches, snooping, theft, and human error (e.g., sending an email to the wrong person).
- **Examples of Security Controls:**
    - **Encryption:** Scrambling data so that it's unreadable to anyone without the correct decryption key. This is used for data at rest (stored on a hard drive) and in transit (sent over a network).
    - **Access Control:** Restricting access to information based on roles and permissions. This includes passwords, multi-factor authentication (MFA), and user access controls.
    - **Data Classification:** Labeling data based on its sensitivity (e.g., public, internal, confidential, top secret) to apply appropriate security measures.

Common Confidentiality Threats and Concerns

- **Data Breaches**: This is the most direct way confidentiality is compromised. Data breaches happen when an attacker gains unauthorized access to a system and steals sensitive data. This can occur through exploiting a software vulnerability, using stolen credentials, or leveraging misconfigured systems. The stolen data can include everything from personally identifiable information (PII) like names and addresses to financial records, trade secrets, and intellectual property.
- **Social Engineering**: Attackers often exploit human psychology to bypass security controls. Techniques like **phishing** and **pretexting** trick people into revealing confidential information, such as passwords or company data. A user might receive a fraudulent email that appears to be from their boss, asking for a sensitive file, and by sending it, they compromise confidentiality.

- **Insider Threats**: A significant concern is a breach of trust from within an organization. An insider threat can be a current or former employee, contractor, or partner. Whether acting maliciously or through negligence, they can expose sensitive information. For example, a disgruntled employee might intentionally leak customer data, while a careless one might accidentally email a confidential document to the wrong person.
- **Weak Access Control**: Failing to implement strong access controls directly undermines confidentiality. If a system doesn't properly restrict who can view or modify data, unauthorized users may gain access. This can include using weak passwords, not enforcing multi-factor authentication (MFA), or granting excessive privileges to employees (violating the principle of least privilege).
- **Lack of Encryption**: When data isn't encrypted, it's vulnerable to anyone who can intercept it. For example, if a user sends confidential information over an unencrypted Wi-Fi network, an attacker can perform a **man-in-the-middle (MitM) attack** to eavesdrop on the communication and steal the data. Similarly, if sensitive data is stored on a hard drive without encryption, it's at risk if the device is lost or stolen.

2. Integrity

Integrity is the assurance that information is accurate, consistent, and trustworthy throughout its entire lifecycle. It prevents unauthorized modification or destruction of data.

- **Goal:** To prevent unauthorized changes to data.
- **Threats:** Unauthorized modifications, data corruption, tampering, and malicious insider activity.
- **Examples of Security Controls:**
    - **Hashing and Checksums:** Creating a unique "fingerprint" of data. If the data is altered in any way, the hash will change, indicating that its integrity has been compromised.
    - **Digital Signatures:** Verifying the authenticity of a document or message and confirming that it has not been tampered with since it was signed.
    - **Access Controls:** Restricting who can make changes to data. This is often done by giving users different levels of access, such as "read-only" or "read-write."

- **Version Control:** Keeping track of changes to files, allowing you to restore a previous, unaltered version if needed.

Common Threats to Data Integrity

Threats to data integrity can come from both malicious and accidental sources.

1. **Malware and Ransomware:** Malicious software can be designed to corrupt, alter, or delete data. **Ransomware** is a prime example, as it encrypts a victim's files, rendering them unusable until a ransom is paid. This directly attacks data integrity by changing its state and making it unreliable.
2. **SQL Injection Attacks:** An attacker can insert malicious SQL code into a web form. If the website is not properly secured, this code can execute commands on the back-end database, allowing the attacker to **modify or delete data** directly. For instance, an attacker could use this technique to change prices in an e-commerce database or alter financial records.
3. **Insider Threats:** This can be either a malicious or negligent employee. A malicious insider might intentionally alter data for personal gain or to sabotage the company. A negligent insider could accidentally delete or modify critical files, which can also compromise data integrity.
4. **Human Error:** One of the most common threats to data integrity is simple human error. Mistakes like incorrect data entry, accidentally deleting a file, or misconfiguring a system can corrupt data and lead to serious problems.
5. **Physical and Environmental Damage:** Events like power outages, hard drive crashes, or natural disasters can physically damage hardware, leading to data corruption and loss. Without proper backups and redundancy, the data's integrity can be permanently lost.

3. Availability

Availability ensures that information and resources are accessible to authorized users when they need them. This means that systems, networks, and data must be reliable and operational.

- **Goal:** To ensure timely and reliable access.
- **Threats:** Denial-of-Service (DoS) attacks, hardware or software failures, power outages, and natural disasters.
- **Examples of Security Controls:**

- **Redundancy:** Having backup systems and components so that if one fails, another can take over immediately. This includes redundant servers, power supplies, and network connections.
- **Disaster Recovery and Business Continuity Plans:** Having a plan in place to restore operations and data quickly after a major incident.
- **Regular Backups:** Creating copies of data so it can be restored in case of corruption or loss.
- **System Maintenance:** Regularly updating software and hardware, as well as monitoring systems to prevent outages.

Common Availability Threats

- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**: These are the most direct attacks on availability. Attackers flood a server or network with an overwhelming amount of traffic, making it impossible for legitimate users to access the service. A DDoS attack uses a network of compromised devices (a **botnet**) to launch the attack, making it harder to block the source.
- **Ransomware**: While ransomware is often seen as a confidentiality threat because it encrypts files, it's also a primary concern for availability. The core goal of a ransomware attack is to make data and systems completely unavailable until a ransom is paid. This can bring an entire company's operations to a halt, affecting everything from manufacturing to healthcare services.
- **Hardware and Software Failures**: Availability isn't just about malicious attacks. Hardware failures, like a hard drive crashing or a server rack losing power, can take critical systems offline. Similarly, software bugs, misconfigurations, and outdated systems can cause unexpected crashes or performance issues, making services unavailable.
- **Natural Disasters and Environmental Issues**: Events like floods, fires, or power outages can physically damage data centers or disrupt network connectivity. Without a robust **disaster recovery plan** and off-site backups, an organization's systems may become completely unavailable.

AAA Triad

1. Authentication

Authentication is the process of verifying a user's identity. It answers the question, "Are you who you say you are?" Before a user can access a system or network, they must prove their identity.

- **Methods:** This is typically done using one or more of the following:
    - **Something you know:** A password, PIN, or passphrase.
    - **Something you have:** A physical token, smart card, or mobile phone.
    - **Something you are:** Biometric data like a fingerprint or facial scan.
    - **Somewhere you are:** Location data or IP based
- **Example:** When you enter your username and password to log in to your email, you are authenticating yourself.

---

2. Authorization

Authorization determines what an authenticated user is allowed to do. It answers the question, "What are you permitted to do now that we know who you are?" Once a user's identity is verified, the system checks their permissions to decide which resources they can access and what actions they can perform.

- **Principle of Least Privilege:** A core concept in authorization is the principle of least privilege, which states that users should only have the minimum level of access required to perform their job duties.
- **Example:** After logging in, a regular employee might only be able to view certain files, while a manager may have the authority to edit or delete them.

---

3. Accounting

Accounting (sometimes called auditing) is the process of logging and tracking a user's activity while they are connected to a system. It answers the question, "What did you do?" This provides a detailed audit trail that can be used for security monitoring, troubleshooting, and forensics.

- **Information Recorded:** Accounting logs can include information such as:
    - The time and duration of the user's session.
    - The specific files or resources they accessed.
    - The commands or actions they performed.
- **Example:** A log file might show that a specific user accessed a sensitive database at 2:00 PM and downloaded a financial report. This information can be used to investigate a potential data breach or ensure compliance with security policies.

Attack Vectors

1. Malware Attacks 🦠

Malware, short for "malicious software," is a broad category of attacks that use harmful software to infiltrate systems. Once a system is infected, the malware can disrupt operations, steal data, or gain unauthorized access.

- **Ransomware:** This type of malware encrypts a victim's files or system and demands a ransom payment to restore access. It's one of the most financially damaging attacks today.
- **Viruses:** These attach themselves to a legitimate program and require a user's action (like opening a file) to spread and execute their malicious code.
- **Worms:** Unlike viruses, worms are self-replicating and can spread across networks without any human interaction, often exploiting software vulnerabilities.
- **Trojans:** Named after the Trojan Horse, this malware disguises itself as a useful or harmless program to trick a user into installing it. Once inside, it can create a "backdoor" for a hacker to access the system.
- **Spyware:** This software secretly monitors a user's activity and gathers sensitive information, such as passwords, banking details, and browsing history, to send back to the attacker.

---

2. Social Engineering Attacks 🎭

Social engineering is a manipulation technique that exploits human psychology to trick people into giving up confidential information or performing actions they shouldn't. It's often the first step in a larger cyberattack.

- **Phishing:** The most common form of social engineering. An attacker sends fraudulent emails or messages that appear to be from a trusted source (like a bank or a co-worker) to trick victims into revealing personal information or clicking a malicious link.
- **Spear Phishing:** A highly targeted form of phishing that focuses on a specific individual or organization. Attackers often research their target to make the message more convincing.

- **Baiting:** An attacker uses a tempting lure, like a "free movie download" or a USB drive left in a public place, to entice a victim into an action that installs malware or gives up data.
- **Pretexting:** This involves creating a fabricated scenario or "pretext" to gain trust and extract information. For example, an attacker might pretend to be an IT support person needing your password to "fix" a technical problem.

---

3. Denial-of-Service (DoS) Attacks 💥

The goal of a DoS attack is to make a service or website unavailable to its intended users by overwhelming it with excessive traffic. This can slow down or crash a server.

- **Distributed Denial-of-Service (DDoS):** A more powerful and common version of a DoS attack. Instead of using a single source, a DDoS attack uses a network of compromised computers (a **botnet**) to flood the target with traffic from multiple locations, making it much harder to block.

---

4. Injection Attacks 💉

Injection attacks involve injecting malicious code into a program or system to execute commands, alter data, or gain unauthorized access.

- **SQL Injection (SQLi):** An attacker inserts malicious SQL code into a web form field. If the website is vulnerable, the code can be executed by the database, allowing the attacker to steal, modify, or delete data.

---

5. Man-in-the-Middle (MitM) Attacks 🤫

A MitM attack occurs when an attacker intercepts and relays communication between two parties who believe they are communicating directly with each other. This allows the attacker to eavesdrop on, or even alter, the data being exchanged.

- **Wi-Fi Eavesdropping:** A common MitM attack where a hacker creates a fake public Wi-Fi hotspot. When a user connects, the attacker can intercept all their network traffic, including sensitive information like login credentials and credit card numbers.