# **48. Security Fundamentals**

## **Key Security Concepts**

### **Why Security?**

What is the purpose/goal of security in an enterprise?

* The principles of the **CIA Triad** form the foundation of security:
  + **Confidentiality**
    - Only **authorized users** should be able to access data.
    - Some information/data is **public** and can be accessed by anyone.
    - Some information/data is **secret** and should only be accessed by specific people.
  + **Integrity**
    - Data should not be **tampered with** (modified) by unauthorized users.
    - Data should be **correct and authentic**.
  + **Availability**
    - The **network/security** should be operational and accessible to **authorized users**.

Attackers can threaten the **confidentiality, integrity, and availability** of an enterprise’s systems and information.

## **Vulnerability, Exploit, Threat, Mitigation**

* A **vulnerability** is any potential weakness that can compromise the **CIA** of a system/information.  
  + A potential weakness isn’t a problem on its own.
* An **exploit** is something that can potentially be used to take advantage of a vulnerability.  
  + Something that can *potentially* be used as an exploit isn’t a problem on its own.
* A **threat** is the potential of a **vulnerability** to be exploited.  
  + A hacker exploiting a vulnerability in your system is a **threat**.
* A **mitigation technique** is something that can protect against threats.  
  + Should be implemented everywhere a vulnerability can be exploited:
    - Client Devices
    - Servers, Switches, Routers, Firewalls

💡 **No system is perfectly secure!**

## **Common Attacks**

### **1. DoS (Denial of Service) Attacks**

* DoS attacks threaten the **availability** of the system.
* One common DoS attack is the **TCP SYN Flood**:  
  + **TCP Three-Way Handshake:** SYN | SYN-ACK | ACK
  + The attacker sends countless **TCP SYN** messages to the target.
  + The target sends a **SYN-ACK** message in response to each SYN it receives.
  + The attacker never replies with the final **ACK**.
  + The incomplete connections **fill up** the target’s **TCP connection table**.
  + The attacker continues sending SYN messages, preventing legitimate TCP connections.
* In a **DDoS (Distributed Denial of Service) Attack**, the attacker infects many computers with malware and uses them to initiate a DoS attack.  
  + This group of infected computers is called a **botnet**.

### **2. Spoofing Attacks**

* **Spoofing** an address means using a **fake source address** (IP or MAC).
* Numerous attacks involve spoofing; it’s not a single kind of attack.
* Example: **DHCP Exhaustion Attack**
  + The attacker uses **spoofed MAC addresses** to flood **DHCP Discover** messages.
  + The target server’s **DHCP pool** becomes full, causing **Denial-of-Service**.

### **3. Reflection / Amplification Attacks**

* In a **Reflection Attack**, the attacker sends traffic to a **reflector** and spoofs the **source IP** as the target’s IP.
* The **reflector** (e.g., a **DNS server**) sends replies to the target.
* A **Reflection Attack** becomes an **Amplification Attack** when a small request triggers **a large response**, overwhelming the target.

### **4. Man-in-the-Middle (MITM) Attacks**

* The attacker **intercepts** communications between two parties to **eavesdrop** or **modify** traffic.
* Example: **ARP Spoofing (ARP Poisoning)**
  + The attacker sends a **fake ARP reply**, associating their MAC address with the target IP.
  + The victim’s traffic is now sent to the attacker, who can **read or modify** the data before forwarding it.
  + This compromises **confidentiality** and **integrity**.

### **5. Reconnaissance Attacks**

* Not direct attacks but used to **gather information** about a target for a future attack.
* Examples:
  + **nslookup** to learn a site’s IP address.
  + **WHOIS query** to find email addresses, phone numbers, and physical addresses.

### **6. Malware**

* **Malware (Malicious Software)** refers to harmful programs that infect computers.
* Types:
  + **Viruses** infect other software (host program) and spread when shared.
  + **Worms** spread independently and congest networks.
  + **Trojan Horses** disguise as legitimate software to trick users into installation.

### **7. Social Engineering Attacks**

* Target the **most vulnerable** part of a system: **people**!
* Examples:
  + **Phishing**: Fake emails trick users into revealing credentials.
    - **Spear Phishing**: Targeted at specific employees.
    - **Whaling**: Targets high-profile individuals.
  + **Vishing (Voice Phishing)**: Over the phone.
  + **Smishing (SMS Phishing)**: Using text messages.
  + **Watering Hole Attack**: Infecting sites frequently visited by the victim.
  + **Tailgating Attack**: Gaining access to a secured area by following an authorized person.

### **8. Password-Related Attacks**

* Systems rely on **username/password** combinations for authentication.
* Attack Methods:
  + **Guessing**
  + **Dictionary Attack**: Using common words/passwords.
  + **Brute Force Attack**: Trying all possible combinations.
* Strong passwords should have:
  + At **least 8 characters** (preferably more).
  + A mix of **uppercase, lowercase, numbers, and special characters**.
  + Should be **changed regularly**.

## **Multi-Factor Authentication (MFA)**

* MFA involves providing more than just a **username/password** to prove identity.
* Requires **two** of the following (**Two-Factor Authentication - 2FA**):
  + **Something You Know**: Password, PIN, etc.
  + **Something You Have**: Phone notification, security badge, etc.
  + **Something You Are**: Biometrics (face scan, fingerprint, retina scan, etc.).
* **Increases security**: Even if an attacker learns the password, they can't log in without the second factor.

## **Digital Certificates**

* **Digital Certificates** verify the identity of a certificate holder.
* Used for **website authentication** to ensure legitimacy.
* Entities request a **Certificate Signing Request (CSR)** from a **Certificate Authority (CA)**.

## **Controlling and Monitoring Users with AAA**

* **AAA (Triple-A)** stands for **Authentication, Authorization, and Accounting**.
* It controls and monitors users of a system.
* Components:
  + **Authentication**: Verifying a user's identity (e.g., logging in).
  + **Authorization**: Determining what a user is allowed to do.
  + **Accounting**: Tracking user activities for security and auditing purposes.

