Cyber Security Basics and Attack Surface

CIA Triad in Cyber Security

The CIA Triad is a core framework in information security that helps organizations protect data and maintain secure, reliable systems.

- Three principles: Confidentiality, Integrity, Availability
- Guides policies for protecting sensitive information
- Ensures data is secure, accurate, and accessible

1.Confidentiality

Confidentiality ensures that sensitive data is accessible only to authorized individuals or systems. Its purpose is to prevent unauthorized viewing, access, or misuse of private information.

Example:

Bank Passwords , Personal emails

2.Integrity

Integrity ensures that data remains accurate, authentic, and unaltered during storage or transmission. Any unauthorized modification or corruption compromises the reliability of data.

Example:

Bank Balance Should not change wrongly

3.Availability

Availability ensures that systems, networks, and data are accessible to authorized users whenever needed. Disruptions can halt operations and cause major losses.

Example:

Banking Apps should be available 24/7

Types of Cyber Attackers

1.Script Kiddies

Script kiddies are beginners who use ready-made tools and scripts to perform cyber attacks without deep technical knowledge.

2.Insider Attackers

Insider attackers are employees or trusted people who misuse their authorized access to steal or damage data.

3.Hacktivists

Hacktivists carry out cyber attacks to support political, social, or ideological causes.

4.Nation-State Attackers

Nation-state attackers are government-sponsored hackers who target other countries for espionage or cyber warfare.

Attack Surface in Cyber Security

Attack surface refers to all the possible entry points through which an attacker can access or attack a system.

Common Attack Surfaces Include:

- Web applications
- Mobile applications
- APIs
- Networks (Wi-Fi, routers)

- Cloud infrastructure

Example:

A login page of a banking application is an attack surface because attackers can try to steal user credentials.

Attack Surface in Cyber Security

OWASP Top 10 overview

OWASP Top 10 is a list published by OWASP that identifies the most common and critical security vulnerabilities found in web applications.

Some common OWASP Top 10 vulnerabilities are:

1. SQL Injection:

Attackers can manipulate database queries to access or modify data.

2.Broken Authentication:

Weak login systems allow attackers to take over accounts.

3.Cross-Site Scripting (XSS):

Malicious scripts are injected into web pages.

4.Security Misconfiguration:

Improper security settings expose applications to attacks.

5.Sensitive Data Exposure:

Confidential data is not properly protected.

Importance of OWASP Top 10:

OWASP Top 10 helps developers and organizations understand common security risks and improve the security of their applications.

Data Flow in an Application

Data flow describes how information moves from the user to the application, then to the server, and finally to the database.

Typical data flow:

User → Application → Server → Database

Interpretation:

- User: The user enters data such as username or password.
- Application: The application sends the user data to the server.
- Server: The server processes the request and checks permissions.
- Database: The database stores or retrieves the required data.

Possible Attack Points

- During login, attackers may try to steal passwords.
- While data is transmitted, attackers may intercept the data.
- If the database is not secure, attackers may steal sensitive information.

Example:

In a banking application, user login details travel from the mobile app to the bank server and then to the database. If any part is insecure, attackers can exploit it.