Cybersecurity

Practice of ensuring the confidntiality, integrity and availability of data by securing the assets and data from unauthorised access or criminal exploitation.

CIA Triad

- **Confidentiality**- Keeping sensitive information private, accessible only to those who are authorised to see it.

  Authentication process like MFA, file permissions, access control mechanisms, encryption to prevent data from unauthorised access.

- **Integrity-** The data should remain accurate and complete, it shouldn't be altered without permission.

  Hashing, checksums, digital signatures are used to check the data is unaltered and accurate. These are required to detect any unauthorised changes and responding to potential threats quickly.

- **Availability-** The data should be available at all times to legitimate users when required.This means keeping systems, networks, and devices up and running.

Examples

- **Banking-** Online banking apps requiring 2FA to log in to their account- **confidentiality.**Reviewing account balances, statements, regular updates to transactions- ensures **integrity** and has a customer helpline number incase of any discrepancies. Customers can login to their accounts whenever required and can connect to customer care at all times- be it day or night- **Availability** of data at all times.

- **Organisation**- Encrypting employee records to prevent unauthorised access- **Confidentiality.** Hashing to check those records are unaltered over time- **Integrity.** Data is available to those who require it to fulfill their job- **Availability.**

- **Social Media**- Requiring a password and OTP to logon to your account- **Confidentiality.** Viewing your content that it is unaltered or reporting incase of any changes in the account to protect the account-**Integrity.** People can login to their accounts whenever required and can report issues at any time- **Availability.**

Threat Actor

Any person or group who presents a security Risk.

Types of Attackers

- **Cybercriminals-** This is the most common type of threat actor. Their attacks are intended to steal data for financial gain. Sometimes they will make that data inaccessible to the victim until they pay a hefty ransom, otherwise known as ransomware. Working alone or in a group, their primary motivation is money.

- **Hacktivists-** threat actors are driven by political, social, or ideological causes. Hacktivists are not primarily motivated by money but rather by a need to publicize an organization's misdeeds or to be a part of a political or social movement. They may target organizations, websites, or systems to promote their beliefs or make a statement.

- **State-sponsored Actors-** These are government-backed entities that conduct cyber espionage, sabotage, or other offensive activities to advance their nation's interests. They often possess advanced capabilities and significant resources.

- **Insiders-** Insiders are individuals within a business. They misuse their close access to systems, data, or information for personal gain, espionage, or sabotage. An insider can be an employee, third-party contractor, or partner who wants to get at organizational data and/or compromise key processes.

- **Script Kiddies-** These are typically inexperienced individuals who use existing hacking tools and techniques without a deep understanding of the underlying technology. They may engage in cyberattacks for fun or to impress others.

- **Organized Crime Groups-** Criminal organizations may use cyberattacks as part of their broader criminal activities, such as drug trafficking or money laundering.

- **Terrorist Groups-** Some terrorist organizations may use cyber-attacks as a means of furthering their goals, disrupting services, or causing fear. Terrorist organizations are also a type of threat actor when they indulge in cyber-terrorism for propaganda and for political, ideological, and financial purposes.

Attack Surface

An attack surface is the sum of all possible points (digital, physical, or human) where an unauthorized user can try to enter or extract data from an organization.

Types

1. **Digital Attack Surface**: All software, systems, and connections on a network.
    - Examples: Websites, APIs, cloud services, applications, servers, code repositories, network ports, wireless connections, and even forgotten shadow IT.
    - Risks: Code vulnerabilities, misconfigurations, outdated software, weak authentication.
2. **Physical Attack Surface**: Tangible assets an attacker can physically touch or access.
    - Examples: Laptops, servers, USB drives, mobile devices, routers, and even improperly discarded hardware.
    - Risks: Theft, physical break-ins, data left on insecure devices.
3. **Human/Social Engineering Attack Surface**: Weaknesses in people that attackers exploit.
    - Examples: Employees falling for phishing, pretexting, baiting, or vishing (voice phishing) to reveal credentials or install malware.
    - Risks: Insider threats, successful social engineering, compromised credentials.
4. **Internal Attack Surface:** Parts of the network not exposed to the internet, but accessible from within.
    - Examples: Internal servers, workstations, private cloud deployments, and internal applications.
    - Risks: Lateral movement by attackers who breach the perimeter.
5. **External Attack Surface**: Internet-facing assets visible from the outside.
    - Examples: Public-facing websites, web services, and third-party platforms.
    - Risks: Direct attacks from the internet.
6. **Cloud & Hybrid Attack Surface**: Assets in cloud environments, adding complexity.
    - Examples: SaaS applications, public/private cloud deployments, and interconnected services.
    - Risks: Misconfigured cloud settings, third-party integrations.

OWASP Top 10:2025

1. **A01:2025 - Broken Access Control**
2. **A02:2025 - Security Misconfiguration**
3. **A03:2025 - Software Supply Chain Failures**
4. **A04:2025 - Cryptographic Failures**
5. **A05:2025 - Injection**
6. **A06:2025 - Insecure Design**
7. **A07:2025 - Authentication Failures**
8. **A08:2025 - Software or Data Integrity Failures**
9. **A09:2025 - Security Logging and Alerting Failures**
10. **A10:2025 - Mishandling of Exceptional Conditions**

https://owasp.org/Top10/2025/

Mapping Daily Use applications to possible attack surfaces

1. Email Applications

The email attack surface is primarily focused on the inbox and the authentication process. It is the most common entry point for initial access.

- **Incoming Messages-**Phishing & Social Engineering: Malicious links or AI-generated "context-aware" scams designed to steal credentials.
- **Attachments-**Malware Delivery: Office documents, PDFs, or ZIP files containing trojans, ransomware, or spyware.
- **Authentication-**Credential Theft: Brute-force attacks or session hijacking (stealing cookies) to bypass login screens.
- **Service Integration-**Third-party Apps: Granting permissions to "Log in with Google/Outlook" on insecure websites expands your risk.

2. WhatsApp & Messaging Apps

While end-to-end encryption (E2EE) protects message content, the attack surface exists in the metadata, backups, and client-side vulnerabilities.

- Social Attack Surface (Smishing/Mishing): Receiving fraudulent links via chat. Unlike email, WhatsApp's "familiarity" makes users more likely to click.
- The "Backup" Surface: While chats are encrypted on the phone, backups to Google Drive or iCloud are often not encrypted by default unless you manually enable "End-to-end Encrypted Backups."
- Account Verification: The SMS-based OTP is a major surface for SIM Swapping or "vishing" (tricking you into sharing the code).
- Modified Clients: Using "WhatsApp Gold" or unofficial versions introduces a massive surface for data exfiltration.

3. Banking Applications
Banking apps have the highest "reward" for attackers, so their attack surface involves sophisticated device-level and backend exploits.
Digital & Technical Surfaces

- The Login Overlay: Malware (Trojans) can detect when you open a banking app and display a fake login screen on top of the real one to capture your PIN/Password.
- OTP Interception: Malware with "SMS Read" permissions can intercept your bank's 2FA codes silently.
- API Vulnerabilities: Attackers target the communication channel between the app and the bank's server (the API) to manipulate transaction data.

Network & Physical Surfaces

- Insecure Networks: Using banking apps on Public Wi-Fi opens the door to Man-in-the-Middle (MitM) attacks where traffic is intercepted.
- Local Storage: If a phone is rooted or jailbroken, other apps might be able to access the banking app's local "cache" or sensitive data stored on the device.

The Data Flow

When you perform an action (like logging into a banking app or sending an email), the data follows this path:

Step A: User → Application (The Client Side)
The user enters data (credentials, messages) into the User Interface (UI). The application validates the format locally (e.g., checking if an email has an "@" symbol) and prepares it for transmission.

Step B: Application → Server (The Transport Layer)
The application sends the data over the internet (usually via HTTPS) to the Application Programming Interface (API) endpoint on the web server. This involves DNS lookups to find the server's IP address.

Step C: Server → Database (The Storage Layer)
The server receives the request, authenticates the user's session, and processes the logic. It then creates a query (usually SQL or NoSQL) to fetch, update, or save data in the database.

Attack Surface Identification

Attackers look for "gaps" or "handoffs" between these stages. Here is where the flow is most vulnerable:

Flow Stage	Potential Attacks	Vulnerability Type
User → App	Keylogging / Screen Scrapers	**Client-Side:** Malware on the user's device records keystrokes before they are even sent.
App → Server	Man-in-the-Middle (MitM)	**Network-Side:** If encryption (TLS) is weak or absent, attackers intercept data mid-transit.
App → Server	Broken Authentication	**Session-Side:** Attackers steal "Session Cookies" to impersonate the user without needing a password.
Server Logic	DDoS / Logic Bombs	**Server-Side:** Overwhelming the server with requests or exploiting flaws in the code's business logic.
Server → DB	SQL Injection (SQLi)	**Injection-Side:** The attacker inputs malicious code into a form field that the database executes as a command.
Database	Data Exfiltration	**Storage-Side:** If the database is misconfigured or unencrypted, an attacker can dump the entire table of user records.

Summary

Above are the core cybersecurity concepts, the CIA triad which is crucial and important to maintain an organisation’s security posture. Attack surfaces which are vulnerable to different social engineering, phishing, and malware attacks. The OWASP Top 10 which lists top vulnerabilities in the present times through which security breaches occur. Mapping daily used applications to possible attack surfaces to which attacks can happen. How data flows from user to server to application and database and where can attacks happen in between those data flows.