Cybersecurity

Definition

Cybersecurity is the practice of protecting computer systems, networks, devices, and data from digital attacks, damage, or unauthorized access, using technologies, processes, and policies to ensure **confidentiality**, **integrity**, and **availability** of information. It involves defending against threats such as malware, phishing, and ransomware to prevent data theft, financial loss, and operational disruption for individuals and organizations.

Key areas of cybersecurity include network security, application security, information security, and operational security, focusing on defense, detection, and response to threats.

Core Principles and Goals

- **Confidentiality:** Ensuring sensitive data is accessed only by authorized parties.
- **Integrity:** Protecting data from unauthorized alteration or destruction.
- **Availability:** Making sure systems and data are accessible when needed.

1 Confidentiality

Confidentiality ensures that information is accessible only to those authorized to have access [?]. It prevents the unauthorized disclosure of sensitive data.

Goal: Keep data secret and private.

Protection Methods: Encryption, access controls (usernames and passwords), and secure storage [?].

Real-World Example (Banking): When you log in to your online bank account, the system uses encryption to ensure that your financial details (account balances and transaction history) are transmitted securely and are only visible to you and authorized bank staff [?]. Unauthorized access to this information would be a breach of confidentiality.

Real-World Example (Social Media): Direct messages (DMs) on platforms such as Instagram or Twitter are designed to be confidential and visible only to the sender and the recipient [?]. A breach would occur if a third party could read private conversations without authorization.

2 Integrity

Integrity ensures the accuracy, completeness, and reliability of information and systems [?]. It prevents unauthorized or accidental modification of data.

Goal: Maintain the trustworthiness and correctness of data.

Protection Methods: Hashing, digital signatures, version control, and access logs [?].

Real-World Example (Banking): When money is transferred between accounts, the bank's system ensures that the correct amount is debited from one account and credited to another without alteration [?]. If a hacker could change the transaction amount during the transfer, it would be a breach of integrity.

Real-World Example (Social Media): When a user uploads a photo on Facebook, integrity ensures that the image seen by others is exactly the same as the one uploaded and has not been modified by an attacker or system error [?].

3 Availability

Availability ensures that information and systems are accessible to authorized users whenever required [?]. It guarantees reliable and timely access to data and services.

Goal: Ensure systems and data are operational and accessible.

Protection Methods: Redundant systems and backups, disaster recovery plans, load balancing, and denial-of-service (DoS) attack prevention [?].

Real-World Example (Banking): Banks ensure that online banking portals and ATM services are available 24/7 [?]. A power failure or cyberattack that prevents customers from accessing their accounts would be a breach of availability.

Real-World Example (Social Media): During major events, platforms like X (formerly Twitter) handle large volumes of traffic while remaining available [?]. A major server failure that makes the platform unreachable would be a breach of availability.

Cyber Threat Actors

Cyber threat actors can be categorized based on their motivation, skill level, and available resources. They range from unskilled individuals seeking thrills to highly organized, state-sponsored groups conducting sophisticated cyber operations.

4 Types of Cyber Attackers

4.1 Script Kiddies

Script kiddies are individuals with limited technical expertise who use pre-written scripts and tools developed by others to carry out cyberattacks.

Motivation: They are often driven by boredom, curiosity, or the desire to impress others and gain recognition.

Impact: Despite their low skill level, they can cause significant disruption, such as website defacement or Distributed Denial-of-Service (DDoS) attacks, particularly against poorly secured systems.

4.2 Insiders

Insiders are individuals who have legitimate access to an organization's systems and data, such as employees, former employees, contractors, or business partners.

Motivation: Their actions may be intentional (financial gain, revenge, or espionage) or unintentional (carelessness or human error).

Impact: Insiders are especially dangerous because they can bypass external security controls and have direct knowledge of internal systems and sensitive data.

4.3 Hacktivists

Hacktivists are attackers driven by social, political, or ideological objectives.

Motivation: They seek to promote a cause, expose perceived wrongdoing, or damage the reputation of targeted organizations.

Impact: Their activities commonly include website defacement, data leaks (doxxing), and DDoS attacks to gain public attention.

4.4 Nation-State Actors

Nation-state actors are highly skilled and well-funded cyber groups sponsored by governments.

Motivation: They pursue political or strategic objectives such as cyber espionage, intellectual property theft, economic advantage, and disruption of critical infrastructure.

Impact: They use advanced techniques, including zero-day exploits and long-term stealthy attacks known as Advanced Persistent Threats (APTs), making them extremely difficult to detect.

Attack Surface and Attack Vectors

5 What is an Attack Surface?

An **attack surface** is the total set of all possible locations such as systems, applications, devices, users, and processes that an attacker can target to compromise an organization's environment. These represent the potential "holes" that attackers can exploit to gain unauthorized access.

6 Difference Between Attack Surface and Attack Vector

6.1 Attack Surface

An attack surface includes every possible entry point into a system or network that an attacker might exploit. These entry points may be physical or digital and exist across multiple layers of an organization's technology.

Examples of Attack Surface Components:

- **Servers and Workstations:** Desktops, laptops, and cloud servers that store or process sensitive data.
- **Applications:** Internal and external software such as web applications, mobile apps, and third-party services.
- **Endpoints:** Devices such as smartphones, tablets, printers, and IoT devices.
- **Network Infrastructure:** Routers, switches, firewalls, and communication channels.
- **Processes:** APIs, cloud services, and internal workflows.
- **Users:** Employees, contractors, partners, and customers with access to systems.

6.2 Attack Vector

An **attack vector** is the specific method or technique an attacker uses to exploit a weakness within the attack surface.

Common Attack Vectors:

- Phishing emails
- Unpatched software
- Social engineering
- Malware (viruses, worms, ransomware)
- Brute-force attacks

7 Types of Attack Surfaces

7.1 Internal Attack Surface

The internal attack surface includes all systems, devices, and applications inside an organization's private network.

Components:

- Servers, workstations, and internal applications
- Mobile devices, desktops, and laptops
- Internal databases and sensitive resources
- Privileged user accounts

Common Risks:

- Poor access control configuration
- Insider misuse
- Lateral movement by attackers

7.2 External Attack Surface

The external attack surface consists of systems accessible via the internet.

Key Components:

- Web applications and portals
- Internet-facing APIs
- DNS configurations and external servers
- Open ports

Common Risks:

- Misconfigured cloud storage
- Unpatched web applications
- Shadow IT or abandoned assets

7.3 Digital Attack Surface

The digital attack surface includes all online properties and third-party platforms associated with an organization.

- Social media, websites, and blogs
- SaaS platforms and third-party services
- Customer engagement and marketing tools

7.4 Physical Attack Surface

This includes physical devices and infrastructure.

- Data centers, servers, and networking equipment
- IoT devices, printers, and routers
- Laptops, tablets, and mobile phones

Common Risks:

- Theft of devices
- Physical tampering
- Lack of physical security controls

7.5 Cloud and Hybrid Attack Surface

This includes cloud-hosted and hybrid IT environments.

- Cloud services and workloads
- Containers, microservices, and serverless functions
- IAM and API configurations

Challenges:

- Misconfigured cloud resources
- Excessive IAM privileges
- Lack of uniform security policies

7.6 Human Attack Surface

The human attack surface consists of all people who interact with the organization's systems.

- Employees, contractors, partners, and customers

Common Risks:

- Phishing and social engineering
- Weak passwords
- Lack of security awareness

Major Digital Attack Surfaces

8 Web Applications

Web applications are primary targets because they are directly exposed to the internet. Vulnerabilities in application code, poor configuration, and weak input validation can be exploited by attackers.

Examples: E-commerce websites, content management systems (CMS), and online banking portals.

Common Vulnerabilities:

- **Injection Flaws:** SQL, NoSQL, or command injection attacks that allow attackers to send malicious data to an interpreter.
- **Cross-Site Scripting (XSS):** Injection of malicious scripts into trusted websites.
- **Insecure Deserialization:** Improper handling of serialized data that can result in remote code execution.

9 Mobile Applications

Mobile applications have unique attack surfaces including local data storage and communication with backend APIs.

Examples: Banking apps, fitness trackers, and social media applications.

Common Vulnerabilities:

- **Insecure Data Storage:** Storing sensitive data without proper encryption.
- **Broken Cryptography:** Use of weak or improperly implemented encryption algorithms.
- **Insecure Communication:** Sending data over unencrypted channels such as HTTP instead of HTTPS.

10 APIs (Application Programming Interfaces)

APIs connect applications, services, and mobile apps, making them a valuable target for attackers.

Examples: APIs used by mobile apps, third-party services, and microservice architectures.

Common Vulnerabilities:

- **Broken Object Level Authorization (BOLA):** Accessing unauthorized data objects.
- **Excessive Data Exposure:** APIs returning more information than required.
- **Lack of Rate Limiting:** Allowing attackers to overwhelm services with excessive requests.

11 Networks

Traditional network infrastructure forms a major attack surface that supports communication between systems.

Examples: Routers, switches, firewalls, Wi-Fi access points, and VPN gateways.

Common Vulnerabilities:

- **Misconfigurations:** Open ports, default passwords, and weak firewall rules.
- **Vulnerable Protocols:** Use of insecure protocols such as FTP or Telnet.
- **Lack of Segmentation:** Allowing attackers to move freely across network segments.

12 Cloud Infrastructure

Cloud platforms such as AWS, Azure, and GCP introduce new attack surfaces due to shared responsibility and configuration complexity.

Examples: S3 buckets, EC2 instances, Azure Blob storage, and Kubernetes clusters.

Common Vulnerabilities:

- **Misconfigured Storage:** Publicly accessible cloud storage without proper access controls.
- **Improper IAM:** Excessive privileges granted to users or service accounts.
- **Insecure APIs:** Weak protection of cloud management interfaces.

13 OWASP Top 10 (2025) Web Application Vulnerabilities

The **OWASP Top 10** lists the most critical web application security risks, which are dangerous because they are frequently exploited and can lead to severe consequences such as data breaches, unauthorized system access, and financial losses. Here's why each is dangerous:

- **A01:2025 - Broken Access Control:** Users access data or functions beyond their authorization (e.g., viewing other users' accounts), leading to unauthorized data disclosure or modification.
- **A02:2025 - Security Misconfiguration:** Default settings, exposed services, or incomplete setups (like open cloud storage) create easy entry points for attackers.

- **A03:2025 - Software Supply Chain Failures:** Compromised or outdated third-party components (libraries, frameworks) introduce vulnerabilities into your application.
- **A04:2025 - Cryptographic Failures:** Weak encryption or poor key management leaves sensitive data exposed, both in transit and at rest.
- **A05:2025 - Injection:** Untrusted data used as commands (SQL, OS, LDAP) can be manipulated to execute malicious code.
- **A06:2025 - Insecure Design:** Flaws in the fundamental architecture or design, often from lack of threat modeling, allow vulnerabilities to exist before coding.
- **A07:2025 - Authentication Failures:** Weak login, session management, or MFA bypasses allow attackers to impersonate legitimate users.
- **A08:2025 - Software or Data Integrity Failures:** Attackers can modify code or data (e.g., insecure updates, unsigned plugins) to achieve malicious goals.
- **A09:2025 - Security Logging & Alerting Failures:** Insufficient logging and alerting means breaches go undetected and attackers can operate longer.
- **A10:2025 - Mishandling of Exceptional Conditions:** Poor error handling reveals sensitive system details, while not managing unexpected states can cause crashes or security gaps.

Attack Surfaces and Threats in Digital Applications

14 Email Applications

The primary attack surface in email systems is the user and the email content itself.

Attack Surfaces:

- User interface
- Email content (links and attachments)
- User credentials
- Third-party integrations
- Mail servers

Possible Attacks and Threats:

- **Phishing and Spear Phishing:** Fraudulent emails used to steal sensitive information or distribute malware.

- **Malware Delivery:** Viruses, ransomware, and Trojans sent through attachments or links.
- **Business Email Compromise (BEC):** Impersonation of executives to trick employees into transferring money or sensitive data.
- **Account Takeover:** Unauthorized access to an email account to spy on data or conduct further attacks.

15 WhatsApp and Similar Messaging Applications

These applications have multiple attack surfaces despite using end-to-end encryption.

Attack Surfaces:

- Network communication (metadata)
- User input fields
- Local data storage
- Third-party libraries
- Device operating system

Possible Attacks and Threats:

- **Man-in-the-Middle (MitM) Attacks:** Interception of network traffic on unsecured Wi-Fi networks.
- **Malware via Links or Files:** Malicious links or files causing device compromise.
- **Social Engineering:** Tricking users into installing fake or modified applications.
- **Unauthorized Data Access:** Exploiting vulnerabilities to access cached or temporary data.

16 Mobile Banking Applications

Mobile banking apps handle highly sensitive data and have complex attack surfaces.

Attack Surfaces:

- APIs and backend services
- Client-side application code

- Local data storage and communication channels
- Authentication systems
- Third-party SDKs

Possible Attacks and Threats:

- **Banking Trojans and Malware**
- **Insecure APIs**
- **Weak Authentication and Session Management**
- **Reverse Engineering and App Tampering**
- **Phishing and Smishing**

Data Flow in a Typical Web Application

Data flow in a typical web application follows a logical sequence from the user's browser to the server and database, allowing for interactions and information retrieval.

16.1 Data Flow Sequence

Data Flow: User → Application → Server → Database

16.2 Stages of the Data Flow Process

User Interaction: A user initiates an action through the client-side application (e.g., filling out a form or clicking a link) on their device such as a web browser or mobile app. The application gathers the input and formats it into an HTTP request.

Application (Client-side): The user's application processes the input and sends the HTTP request across the internet to the server.

Server (Web/Application Server): The request arrives at the server, which validates and interprets it. The application logic running on the server determines what data is needed and how to process the request.

Database: The server communicates with the database using commands such as SQL queries to store, retrieve, update, or delete data as required by the user's request.

Reverse Flow (Response): The database sends the results back to the server. The server formats the response and sends it back to the client application, which displays the final result to the user.

Attack Surfaces in the Data Flow

Attacks can occur at virtually any stage of this process.

16.3 User / Client Side

Cross-Site Scripting (XSS): An attacker can inject malicious scripts into a website, which then execute in the victim's browser [?]. This allows attackers to steal sensitive information such as session cookies or login credentials.

Man-in-the-Browser (MitB): Malware running on the user's device can intercept or modify data before it is sent to the server.

16.4 During Transmission (User to Server)

Man-in-the-Middle (MitM) Attacks: If the connection is not encrypted (i.e., not using HTTPS), an attacker can intercept, read, or modify data while it travels across the network [?].

16.5 Server Side

SQL Injection (SQLi): An attacker manipulates user input to interfere with database queries [?]. This can allow unauthorized viewing, modification, or deletion of data, and even full database control.

Authentication/Authorization Bypass: Attackers exploit flaws in authentication systems to gain unauthorized access or elevate privileges [?].

Denial of Service (DoS/DDoS): Attackers overload the server with excessive requests, making it slow or unavailable to legitimate users [?].

Insecure Server Configuration: Misconfigured servers may expose sensitive files, services, or introduce additional vulnerabilities.

16.6 Database

Data Exfiltration: If attackers gain database access (often via SQL injection), they can steal complete datasets.

Privilege Escalation: Attackers with limited database access may exploit vulnerabilities to gain higher administrative privileges.

17 Security Mitigation Measures

Robust security measures such as input validation, parameterized queries, HTTPS encryption, and regular security audits are crucial for mitigating these risks. The OWASP Top Ten project provides extensive documentation on the most critical web application security risks and recommended countermeasures.

Overall Summary – Cybersecurity, Attacks, and Data Flow

Cybersecurity is the practice of protecting digital systems, applications, and data from cyber attacks. The main goal of cybersecurity is to maintain the three core principles known as the CIA triad: **Confidentiality**, **Integrity**, and **Availability**. Confidentiality ensures that sensitive information such as passwords, bank details, and personal messages is accessible only to authorized users. Integrity ensures that data is not altered or tampered with by attackers, while availability ensures that systems such as banking applications, email services, and social media platforms remain accessible whenever users need them.

Different types of cyber attackers exist based on their skills, motivations, and resources. Script kiddies use pre-built hacking tools with limited technical knowledge. Insiders misuse their authorized access to steal or leak information. Hacktivists conduct attacks to promote political or social causes. Nation-state attackers are highly skilled groups sponsored by governments to spy on or disrupt other nations.

Every digital system has an **attack surface**, which includes all possible entry points that attackers may try to exploit. These include web applications, mobile applications, APIs, networks, and cloud servers. As systems become more connected, their attack surfaces grow larger and more complex.

The **OWASP Top 10** highlights the most critical web application security risks, such as broken access control, weak authentication, insecure system design, outdated or vulnerable software, and poor monitoring. These weaknesses are dangerous because they allow attackers to steal sensitive data, take control of systems, or remain undetected.

Daily-use applications such as email, WhatsApp, and mobile banking rely on mobile apps, web servers, APIs, and databases. Data flows from the user to the application, then to the server, and finally to the database, before returning to the user. At each stage of this flow, attackers may attempt to compromise the system by infecting user devices, intercepting network traffic, exploiting applications, attacking servers, or stealing data from databases.

Conclusion

Cybersecurity is about protecting data and systems at every level, from the user's device to backend servers. Understanding attackers, attack surfaces, vulnerabilities, and data flow enables organizations to design secure systems and effectively defend against cyber threats.