Fundamentals of Cyber Security and Attack Surfaces

1. Introduction to Cyber Security

Cybersecurity is a practice meant to protect computer systems, networks, and data from digital threats. It focuses on protecting sensitive information, preventing unauthorized access, and ensuring the reliable operation of systems.

2. The CIA Triad

Confidentiality: Ensures data is accessible to authorized persons only. Examples include encrypted banking data and private social media messages.

Integrity: Ensures accuracy of data and prevents unauthorized changes. Examples include bank statement records and academic transcripts.

Availability: Ensures that systems and data are accessible when they are needed. Examples include online services, ATMs, and cloud platforms.

3. Categories of Cyber Attackers

- Script Kiddies: Unsophisticated individuals with little technical capability who use readily available tools.
- Insiders: Employees or trusted persons who abuse their authorized access.
- Hacktivists: Actors driven by political or social causes.
- Nation-State Actors: Government-supported groups conducting cyber espionage or offensive operations.

4. Attack Surface

An attack surface refers to the total collection of all potential entry points through which an adversary may exploit a system. An increased attack surface translates to an increased risk of compromise.

5. Common Attack Surfaces

- Web applications
- Mobile applications
- APIs
- Networks (e.g., Wi-Fi, routers)
- Cloud infrastructure

6. OWASP Top 10

The OWASP Top 10 is an internationally accepted list of the most critical web application security risks. It is designed to help developers and organizations recognize and mitigate common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), broken authentication, and insecure configurations.

7. Mapping Daily Applications to Attack Surfaces

- Email: Phishing attacks, malware attachments, and credential theft.
- Messaging applications: Account takeovers and malicious links.
- Banking applications: Man-in-the-middle attacks, insecure APIs, and mobile malware.

8. Data Flow in Applications

The typical data flow originates from user input, is processed by the application, sent to the server, stored or retrieved from the database, and finally returned to the user as a response.

9. Potential Attack Points in the Data Flow

- User level: Phishing and malware
- Application level: Cross-site scripting and insecure storage
- Network level: Man-in-the-middle attacks
- Server level: Misconfigurations
- Database level: SQL injection

10. Conclusion

A well-rounded understanding of the fundamentals of cyber security, attack surfaces, and common vulnerabilities is crucial to building secure systems. This foundational knowledge allows early identification of risks and efficient protection of sensitive data.