Introduction to Cyber Security: Concepts and Threat Awareness

1. What is Cyber Security? (CIA Triad)

Cyber security is the practice of protecting systems, networks, applications, and data from digital attacks. The foundation of cyber security is the **CIA Triad**, which consists of **Confidentiality, Integrity, and Availability**.

Confidentiality

Confidentiality ensures that sensitive data is accessed **only by authorized users**.

Real-world examples:

- **Banking:** Your ATM PIN and net banking password must remain private.
- **Social Media:** Only you should be able to read your private WhatsApp chats.

If confidentiality is broken, attackers can steal personal data, passwords, or financial information.

Integrity

Integrity ensures that data is **accurate and not altered** without permission.

Real-world examples:

- **Banking:** The amount transferred should not change during a transaction.
- **Online exams:** Marks should not be modified by unauthorized users.

If integrity is compromised, attackers can manipulate records, leading to fraud or misinformation.

Availability

Availability ensures that systems and data are **accessible when needed**.

Real-world examples:

- **Banking apps:** Should be accessible 24/7.
- **Social media:** Platforms like Instagram should not crash due to attacks.

Denial-of-Service (DoS) attacks aim to break availability.

2. Types of Attackers

Script Kiddies

- Beginners who use ready-made hacking tools.
- Motivated by curiosity or fun.
- Cause damage without deep knowledge.

Insiders

- Employees or trusted users misusing access.
- Very dangerous because they already have permissions.
- Example: An employee leaking customer data.

Hacktivists

- Attack systems for political or social reasons.
- Example: Defacing government websites.

Nation-State Actors

- Government-sponsored attackers.
- Highly skilled and well-funded.
- Target critical infrastructure like power grids and defense systems.

---

3. Common Attack Surfaces

An **attack surface** is any point where an attacker can try to enter a system.

Web Applications

- Login pages, forms, URLs
- Vulnerable to SQL Injection, XSS

Mobile Applications

- Insecure storage of data
- Weak authentication

APIs

- Expose data between services
- Broken authentication can leak data

Networks

- Wi-Fi, routers, firewalls
- Can be attacked using sniffing or man-in-the-middle attacks

Cloud Infrastructure

- Misconfigured cloud storage
- Publicly exposed databases

---

4. OWASP Top 10 (Why They Are Dangerous)

OWASP Top 10 lists the **most critical web application vulnerabilities**.

Some key ones include:

- **Broken Access Control:** Users access data they shouldn't.
- **Injection Attacks:** Malicious input alters database queries.
- **Security Misconfiguration:** Default passwords, open ports.
- **Cryptographic Failures:** Weak encryption exposing sensitive data.

These vulnerabilities are dangerous because they allow attackers to **steal data, take control of systems, or crash services**.

---

5. Mapping Daily-Used Applications to Attack Surfaces

Application	Possible Attack Surfaces
Email -	Phishing, malware, weak passwords
WhatsApp -	Account takeover, data interception
Banking Apps	Credential theft, insecure APIs
Social Media	Fake links, session hijacking

---

6. Data Flow Explanation

Typical data flow:

User → Application → Server → Database

Example (Banking App):

1. User enters login details
2. App sends data to server
3. Server verifies credentials
4. Database stores user information
5. Response is sent back to user

---

7. Where Attacks Can Happen

- **User Side:** Phishing, malware
- **Application:** Input validation flaws
- **Network:** Packet sniffing, MITM attacks
- **Server:** Weak authentication
- **Database:** SQL injection, data leaks

---

8. Summary

Cyber security is essential to protect modern digital systems from attackers. The CIA triad helps ensure data is private, correct, and accessible. Different attackers have different motivations and skill levels, making defense complex. Applications expose multiple attack surfaces, and vulnerabilities like those listed in OWASP Top 10 show how small mistakes can lead to serious breaches. Understanding how data flows and where attacks occur builds strong awareness and helps in designing secure systems.
