1. Secure Handling and Storage of Sensitive Data in Mobile and IoT Contexts

What is Sensitive Data?

Sensitive data includes:

- Personal data (name, address, phone number)
- Authentication data (passwords, tokens)
- Location information
- Health and financial information
- Device control commands (for IoT)

Challenges in Mobile & IoT:

- **Limited resources** (less processing power, storage, etc.)
- **Wireless communication** (easily intercepted)
- **Decentralized architecture** (data flows between many devices)

Best Practices for Secure Handling:

1. **Data Encryption**:
    - Always encrypt sensitive data **at rest (storage)** and **in transit (during transfer)**.
    - Use strong algorithms like AES-256 or RSA.
2. **Secure Storage**:
    - Use **KeyStore** in Android or **Secure Enclave** in iOS for storing sensitive keys.
    - IoT devices can use **TPM (Trusted Platform Module)** or secure elements.
3. **Authentication and Access Control**:
    - Use **multi-factor authentication (MFA)** for users and devices.

- Role-based access for apps or users.

4. **Secure APIs**:
    - Ensure APIs used in IoT/Mobile apps are authenticated and encrypted (HTTPS with SSL/TLS).
5. **Data Minimization**:
    - Store only necessary data. If you don't need it, **don't collect it**.
6. **Remote Wipe**:
    - Allow users or admins to wipe data remotely in case of theft or compromise.

2. IoT and Mobile Threat Landscape

Common Threats:

Type of Threat	Description
Data Leakage	Apps unintentionally or maliciously leaking sensitive data
Unsecured Communications	Data sent over unencrypted channels can be intercepted
Malware	Mobile and IoT malware can steal data or control devices
Unauthorized Access	Weak passwords or default credentials exploited
Physical Attacks	Devices stolen or tampered with
Botnets	IoT devices used in large-scale attacks (e.g., Mirai Botnet)

IoT-specific Threats:

- **Firmware vulnerabilities**
- **Default credentials left unchanged**

- **Lack of updates/patching mechanisms**
- **Poor physical security (like open USB ports)**

Mobile-specific Threats:

- **Fake apps** in app stores
- **Jailbreaking/rooting risks**
- **App permissions misuse**
- **Spyware & Adware**

3. Analysis of Common Threats and Attacks Targeting IoT and Mobile Environments

Threat Analysis Includes:

- **Identifying attack vectors**: How the attacker can get in
- **Understanding the target**: What the attacker wants
- **Tools used by attackers**: E.g., sniffers, fake apps, exploits

Common Attacks:

Environment	Common Attacks
IoT	- Firmware tampering- Botnet recruitment- DoS attacks- Side-channel attacks
Mobile	- Phishing through SMS or apps- Credential stealing malware- Keyloggers- App repackaging

4. Vulnerability Assessment and Risk Management in IoT and Mobile Security

Vulnerability Assessment Steps:

1. **Asset Identification**: Know what you're protecting (devices, data, services)
2. **Threat Identification**: Understand who/what could harm the system
3. **Vulnerability Scanning**: Use tools like **Nessus**, **Mobile Security Framework (MobSF)**, **Shodan** for IoT
4. **Penetration Testing**: Try to exploit vulnerabilities safely
5. **Reporting**: Document findings and rank them by severity

Risk Management Process:

1. **Risk Identification** – What could go wrong?
2. **Risk Analysis** – What is the likelihood and impact?
3. **Risk Evaluation** – Is it acceptable?
4. **Risk Treatment** – Reduce, avoid, transfer, or accept risk
5. **Monitoring & Review** – Continuously check and update

Security Tools

- **MobSF** – Analyze APK files (static/dynamic testing)
- **Burp Suite** – Intercept and modify traffic
- **Wireshark** – Analyze packets
- **Shodan** – Find vulnerable IoT devices