Security & Reliability

1. IoT Security Problems & Threats

- **Problems in IoT Security**
  - Devices often have **limited resources** (low CPU, memory, battery) → harder to implement strong encryption.
  - Large **attack surface**: sensors, gateways, cloud, mobile apps.
  - Many devices ship with **default passwords** and weak authentication.
  - **Lack of regular updates** → devices stay vulnerable.
- **Common Threats**
  - **Eavesdropping**: attacker listens to unencrypted communication.
  - **Spoofing**: fake device pretends to be real.
  - **Malware injection**: inserting malicious code.
  - **DDoS attacks**: hijacked IoT devices flood a target server.

2. Elements of IoT Security

- **Confidentiality** → Protect data (encryption).
- **Integrity** → Prevent tampering (hash, signatures).
- **Authentication** → Verify devices/users (certificates, tokens).
- **Authorization** → Define what devices can do.
- **Availability** → Ensure system is always online (DoS protection).

3. IoT Security Challenges

- **Heterogeneity**: Devices use different OS, hardware, and protocols.
- **Scalability**: Millions of devices → key management is hard.
- **Update Mechanism**: Pushing OTA securely is complex.
- **Physical Security**: Attackers can access hardware directly (JTAG, UART).
- **Cost vs Security**: Manufacturers often cut costs and ignore security.

4. IoT Security Tomography

- Analogy: like **medical tomography** (layer-by-layer scan).
- Looks at IoT security in **layers**:
    - **Perception layer** (sensors, actuators) → threats: cloning, fake sensors.
    - **Network layer** (routers, protocols) → threats: sniffing, MITM attacks.
    - **Application layer** (cloud, apps) → threats: weak APIs, data leaks.
- Helps in identifying **vulnerabilities at each layer**.

5. Layer Attacker Model

- Explains which **attackers operate at which layer**:
    - **Device layer attackers**: tamper sensors/actuators physically.
    - **Network layer attackers**: sniff data, inject packets.
    - **Application layer attackers**: exploit cloud APIs, steal data.
- Helps design **layer-wise defense mechanisms** (e.g., encryption at network, authentication at app layer).

Summary

- IoT devices are highly vulnerable due to limited resources, large scale, and poor updates.
- Security must be designed with **CIA triad (Confidentiality, Integrity, Availability)** + **Authentication & Authorization**.
- Protection should be done **layer by layer** (perception → network → application).
- Key practical defenses: **TLS, strong keys, OTA updates, watchdog timers, secure bootloaders, hardware security modules**.