

UNIT 6

Securing IoT Systems

(3 Hours) — Internet of Things (CACS460)

⚠ Please Note

These notes were prepared quickly and **may contain errors or omissions**. Please cross-check important definitions, formulas, code and diagrams with your textbook, class notes and the official TU syllabus before relying on them in exams.

6.1 IoT Security Challenges

IoT devices connect the digital and physical worlds, so a security failure can mean stolen data *and* physical harm (unsafe machines, unlocked doors, tampered medical devices). Security is harder in IoT than in ordinary IT because of the scale and nature of devices.

Main Challenges

Challenge	Explanation
Resource constraints	Low CPU, memory and battery limit strong cryptography and security software.
Weak/default credentials	Devices ship with default passwords (admin/admin) that users never change.
Lack of updates and patching	No secure update mechanism; devices stay vulnerable for years; vendors stop support.
Large scale and heterogeneity	Millions of devices with different hardware, OS and protocols; difficult to manage uniformly.
Insecure communication	Unencrypted protocols (plain HTTP/MQTT/Telnet); weak or no authentication.
Physical exposure	Devices are deployed in the field and can be stolen, opened or tampered with (side-channel, firmware extraction).
Privacy concerns	Constant collection of personal data (location, health, habits) with unclear consent.
Insecure cloud, APIs and apps	Weak access control or exposed endpoints leak data of many users.
Lack of standards and regulation	Manufacturers focus on cost and speed to market rather than security.
Supply-chain risks	Compromised components, firmware or third-party libraries.

Common Attacks on IoT

Attack	Description	Example
Botnet / DDoS	Many compromised devices flood a target with traffic	Mirai botnet (2016) used cameras and routers with default passwords
Eavesdropping / sniffing	Capturing unencrypted traffic	Reading sensor data on open WiFi
Man-in-the-middle	Attacker sits between device and server, reading/altering messages	Fake gateway or rogue access point
Spoofing / impersonation	Pretending to be a legitimate device or server	Fake sensor injecting false readings
Replay attack	Re-sending captured valid messages	Replaying a recorded “unlock” command
Firmware tampering	Installing malicious firmware	Unsigned update accepted by device
Physical / side-channel attack	Attacking the hardware directly (debug port, power analysis)	Dumping keys from flash memory
Denial of service / battery drain	Exhausting device resources	Constant wake-up requests drain battery
Ransomware and data theft	Locking or stealing device/cloud data	Smart-home or hospital device lock-out

Note: Mirai is a widely cited real example of IoT insecurity. If you cite it in an exam, mention it exploited default credentials.

The CIA Triad in IoT

- **Confidentiality:** only authorised parties can read the data (encryption, access control).
- **Integrity:** data and firmware cannot be modified without detection (hashes, digital signatures, MACs).
- **Availability:** devices and services remain usable when needed (redundancy, DDoS protection).

Additional IoT goals: **authentication, authorization, non-repudiation, privacy and safety.**

6.2 IoT System's Security Practices

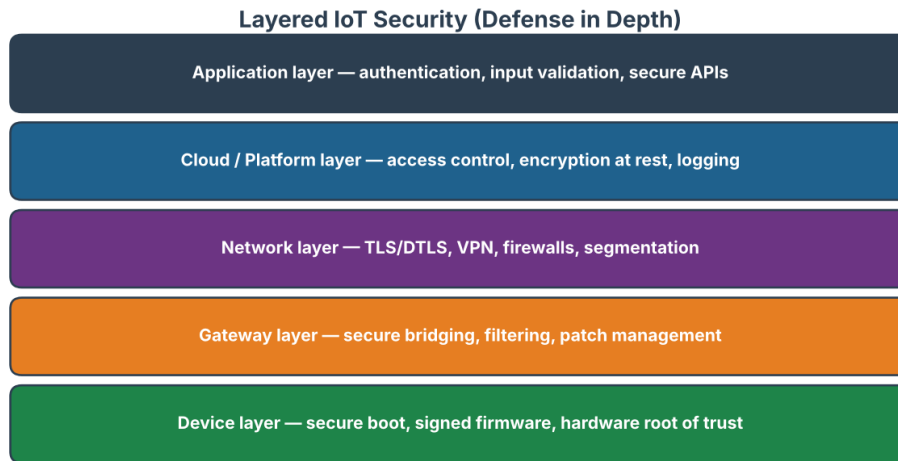


Figure 6.1 — Layered (defence in depth) IoT security

Device Security

- **Change default credentials;** use unique per-device passwords or certificates.
- **Secure boot and signed firmware:** the device only runs code verified by the manufacturer's key.
- **Secure over-the-air (OTA) updates** with signature checking and rollback protection.
- Disable unused ports/services (Telnet, debug UART/JTAG); apply the **principle of least privilege**.
- Use hardware security: TPM, secure element, trusted execution environment (TEE) to store keys.
- Tamper-resistant enclosures and encrypted storage for sensitive devices.

Communication and Network Security

- Encrypt data in transit with **TLS** (TCP) or **DTLS** (UDP); use MQTT over TLS (port 8883) and CoAP over DTLS.
- Use WPA2/WPA3 for WiFi, and VPN or secure tunnels for remote access.
- **Network segmentation:** put IoT devices in a separate VLAN so a compromised bulb cannot reach the office PCs.
- Firewalls and **intrusion detection/prevention systems (IDS/IPS)**; allow-list only the destinations a device needs.
- Protect against replay with timestamps, nonces and sequence numbers.

Authentication and Access Control

- Mutual authentication of device and server using **X.509 certificates** or pre-shared keys.
- Users: strong passwords, **multi-factor authentication (MFA)**, role-based access control (RBAC).
- APIs: OAuth 2.0 / token-based authentication with expiry and scopes.
- Unique device identity and registration (**device provisioning**) with the ability to revoke a stolen device.

Data Security and Privacy

- Encrypt data **at rest** (AES-256) and in transit; manage keys securely (key management service).
- **Data minimisation:** collect only what is needed; anonymise or pseudonymise personal data.
- Follow privacy rules and laws (e.g., GDPR principles; local data-protection laws) and obtain user consent.
- Secure backups; define retention and deletion policy.

Cloud and Application Security

- Secure APIs: validate input, rate limit, avoid exposing admin interfaces to the Internet.
- Regular vulnerability scanning, penetration testing and dependency updates.
- Logging, monitoring and alerts (SIEM) to detect anomalies; incident response plan.

Lifecycle and Management Practices

- **Security by design:** consider threats from the first design step (threat modelling) instead of adding security later.
- Maintain an inventory of devices; monitor and patch regularly.
- Plan the end-of-life: secure decommissioning, wiping data and revoking credentials.
- Follow standards and guidelines: **OWASP IoT Top 10**, NIST IoT guidance, ETSI EN 303 645, IEC 62443 (industrial).

Threat	Countermeasure
Default passwords / botnets	Unique credentials, forced password change, disable Telnet
Sniffing and MITM	TLS/DTLS, certificate validation, VPN
Malicious firmware	Secure boot, signed OTA updates

Threat	Countermeasure
Replay and spoofing	Nonces, timestamps, mutual authentication
Lateral movement	Network segmentation, firewall rules, least privilege
Physical tampering	Tamper-resistant hardware, encrypted flash, disable debug ports
Data leakage	Encryption at rest, access control, data minimisation

Example 6.1 — Securing a smart-home door lock

List four measures to secure a WiFi smart door lock that is controlled from a phone app and cloud service.

Solution

1. **Authentication:** unique device certificate/key and user login with MFA for the app.
2. **Encryption:** TLS for all traffic between lock, cloud and phone; certificates validated.
3. **Replay protection:** every unlock command carries a nonce/timestamp and expires in seconds.
4. **Secure updates and hardening:** signed OTA firmware, no default PIN, debug ports disabled, lockout after repeated failed attempts, audit log of events.

Key Takeaways

- ✓ Challenges: constrained devices, default passwords, no patching, huge scale, insecure communication, privacy and physical access.
- ✓ Know major attacks: botnet/DDoS (Mirai), sniffing, MITM, spoofing, replay, firmware tampering, physical attacks.
- ✓ Aim for confidentiality, integrity, availability plus authentication, authorization and privacy.
- ✓ Practices: unique credentials, secure boot, signed OTA updates, TLS/DTLS, segmentation, MFA, encryption, monitoring.
- ✓ Security must be designed in from the start and maintained throughout the device lifecycle.

— End of Unit 6 —