Networks and Security Systems – Lecture 08 Notes

1. Introduction to IoT

The Internet of Things (IoT) refers to interconnected physical devices equipped with sensors, software, and network interfaces. These devices collect, transmit, and sometimes act upon data. IoT spans consumer (smart home), industrial (IIoT), healthcare, transport, and more.

Key characteristics:

- Sensor-based data collection
- Actuator-driven responses
- Embedded computing
- Network connectivity
- Cloud integration for analytics, ML, and long-term storage

2. IoT Hardware and Devices

2.1 Sensors and Actuators

- **Sensors:** temperature, pressure, motion, GPS, etc.
- **Actuators:** motors, relays, LEDs, signals.

2.2 Device Types

- **Custom-built devices:** industrial machines, ruggedised controllers.
- **Developer kits:** Arduino, ESP32, Raspberry Pi; good for prototyping.

2.3 Microcontrollers

Small computers with CPU, memory and GPIO pins for sensor/actuator interaction. Low-power, ideal for simple repetitive tasks.

2.4 Single-board Computers (SBCs)

More powerful boards running full operating systems, enabling complex processing (e.g., edge analytics).

3. IoT Architecture

3.1 Four-Layer IoT Architecture

1. **Perception Layer:** sensors, actuators.
2. **Network Layer:** connectivity (Wi-Fi, Zigbee, Ethernet).
3. **Processing Layer:** cloud or edge computing, data analysis.
4. **Application Layer:** smart home apps, industrial dashboards, etc.

3.2 Four-Stage IoT Architecture Model

- **Devices** produce data.
- **Internet Gateways** handle initial data routing and preprocessing.
- **Edge Computing** performs near-device processing for low latency.
- **Cloud** enables storage, large-scale analytics, AI/ML, and dashboards.

4. IoT Connectivity

4.1 Wired

- Ethernet, coaxial, fibre, powerline.
- Pros: secure (physical access needed), stable.
- Cons: installation limitations, distance constraints.

4.2 Wireless

- **Wi-Fi:** high bandwidth.
- **Cellular (4G/5G):** long-range, mobility.
- **Bluetooth/BLE:** ultra low-power.
- **Zigbee:** mesh networking for smart homes.
- **LoRaWAN:** long-range, low-power.

4.3 Spectrum Types

- **Licensed:** less interference (e.g., telecom bands).
- **Unlicensed:** free, more interference (e.g., 2.4 GHz).

5. IoT Security

5.1 IoT Security Challenges

Device-level vulnerabilities:

- Weak/default passwords
- No secure update mechanism
- Physical tampering
- Outdated components

Network-level threats:

- MITM attacks
- Weak wireless protocols
- Poor segmentation

Data privacy risks:

- Sensitive data exposure

- Tampering without integrity checks

Scalability issues:

- Managing millions of heterogeneous devices
- Patch/orchestration complexity

6. IoT Security Best Practices

1. **Secure Device Design:** TPM, secure boot, minimal services.
2. **Authentication & Access Control:** MFA, device identity, least privilege.
3. **Secure Communication:** TLS/DTLS, lightweight crypto (ECC).
4. **Monitoring & Updates:** signed firmware, automation.
5. **Network Security:** segmentation, IDS/IPS, firewall rules.

OWASP IoT Top 10

Highlights: weak passwords, insecure services, insecure update mechanisms, data exposure, outdated components, poor privacy, insecure defaults.

7. Cloud Security

7.1 Cloud Models

- **IaaS:** customer manages OS/apps.
- **PaaS:** customer deploys apps only.
- **SaaS:** provider manages everything except data.

7.2 Deployment Models

Public, Private, Hybrid, Multi-cloud.

8. Cloud Security Challenges

- Misconfigurations (main cause of breaches)
- Insecure APIs
- Account hijacking
- Insider threats
- Data sovereignty/compliance
- Multi-tenancy security concerns
- Supply chain risks and vendor lock-in

9. Cloud Security Best Practices

Identity & Access Management (IAM)

- MFA, RBAC, least privilege

- Regular permission reviews
- Dedicated service accounts
- SSO

Data Security

- Encryption (AES-256, TLS 1.2+)
- Key management (AWS KMS, Azure Key Vault)
- Backups and DLP
- Data classification

Network Security

- VPCs, security groups, segmentation
- WAF, DDoS protection

Configuration & Monitoring

- IaC (Terraform, CloudFormation)
- SIEM
- Cloud-native security tools
- Automated compliance checks

Container & Serverless Security

- Image scanning
- Secrets management
- Runtime monitoring

10. Convergence of IoT and Cloud

IoT and cloud form a deeply interconnected ecosystem. Integration challenges include:

- Extended attack surface
- Multi-point data flow security
- Scale/automation demands

Solutions:

- Zero-trust architecture
- Security orchestration/automation
- Edge security processing

11. Emerging Trends

- AI-driven anomaly detection

- Quantum threats to encryption
- 5G-driven device density challenges
- Stronger IoT regulations (e.g., device baseline security)

12. Case Studies

Mirai Botnet (2016): exploited default credentials → DDoS attacks.
Capital One (2019): WAF misconfiguration + SSRF → major data breach.
St. Jude Medical Devices (2017): vulnerabilities in pacemakers → potential life-threatening misuse.