Privacy & Security in IoT: Standards & Challenges

Capacity Building Workshop on Spectrum Aspects of Internet of Things (IoT)

(Vertical Industries)

Sao Tomé

Attlee M. GAMUNDANI

17 October 2023

Agenda

- Introduction to Privacy & Security
- Role of Privacy in IoT
- Security Challenges in IoT
- Security Standards & Guidelines
- ITU Recommendations

Practical Activity (50 mins): Analysing Current IoT Market Trends

Learning Outcomes

- Understand the importance of privacy and security in IoT.
- Familiarise with security standards and guidelines.
- Know the intricacies of licensing, spectrum, and roaming for IoT.
- Understand the complexities of data management in IoT.
- Recognise the challenges and implications of IoT product liability.

Key Issues

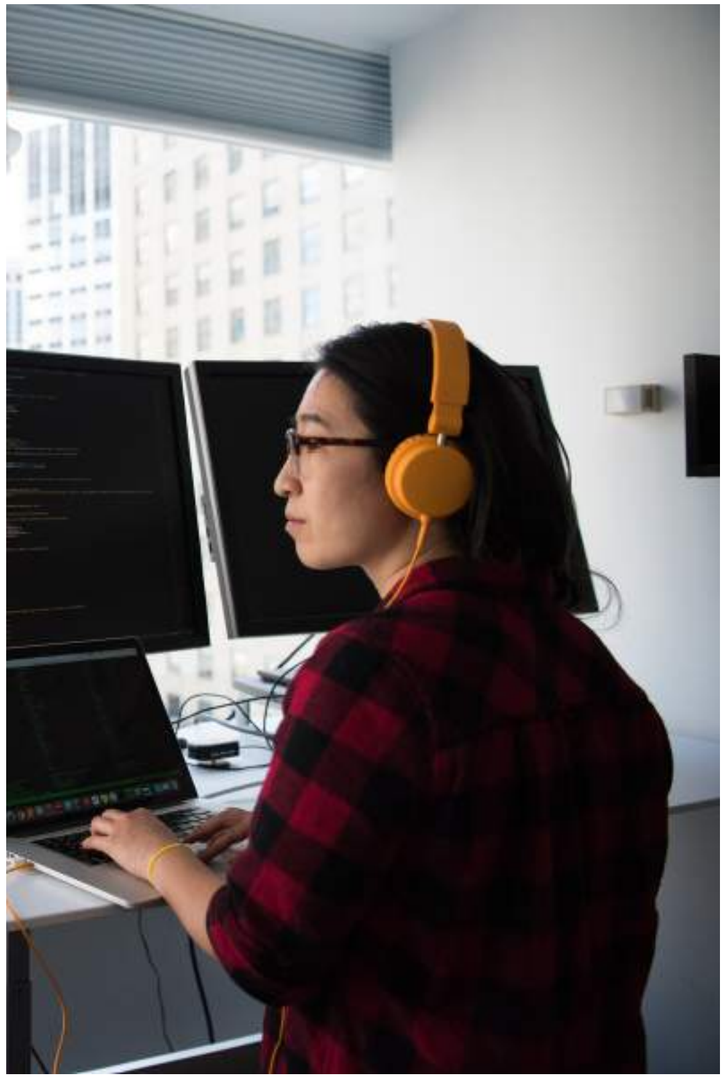
- Security, Privacy, and Trust
- Privacy means different things to different people.
- Privacy is no longer a local notion but trans-border data exchange and distributed data processing call for minimum international privacy measures.
- ITU (under the ICT Security Standards Roadmap), and others (European Commission under its Digital Agenda for Europe, the United States Federal Trade Commission) are looking at these issues

Introduction to Privacy & Security

- Definition of Privacy & Security
- Importance in the Digital Age
- Brief on ITU's role in setting standards

Privacy and Security in IoT

- **Personal Data**:
  - Collection, storage, and use in IoT.
- **Security Threats**:
  - Device vulnerabilities, and unauthorised data access.
- **Mitigation Measures**:
  - Data encryption, secure booting.
- **Reference:**
  - Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.



Role of Privacy in IoT

- IoT devices as data collectors
- Importance of user consent in data collection
- Impact on individual's rights and autonomy
- **Reference:** ITU's Y.4806 "Security capabilities supporting the safety of the Internet of Things"

Security Challenges in IoT

Security Challenges in IoT

1. Device Diversity & Interoperability
2. Massive Volume of Devices
3. Limited Computational Resources in Devices
4. Lifecycle Management of Devices
5. Data Integrity & Confidentiality

Security Challenges in IoT...

6. Lack of User Awareness & Education
    a. Physical Access & Tampering
    b. Firmware & Software Vulnerabilities
    c. Network Vulnerabilities
    d. Emerging Threats & Zero-Day Exploits

Introduction to Security Standards & Guidelines

A revisit to the IoT Definition

Internet of Things [b-ITU-T Y.4000]:

- A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

- **NOTE 1** – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, **whilst ensuring that security and privacy requirements are fulfilled.**

- **NOTE 2** – From a broader perspective, the IoT can be perceived as **a vision with technological and societal implications**.

Introduction to Security Standards & Guidelines

- The importance of standardised security measures
- Role of standards in ensuring interoperability and trustworthiness
- Organisations involved in setting IoT standards (ITU)

Security Standards and Guidelines

- **Protocols:**
  - Secure MQTT, and DTLS for CoAP.
- **Guidelines:**
  - Regular software updates, and user authentication.
- **Industry Standards:**
  - OWASP's Top Ten IoT Vulnerabilities.
- **Reference:**
  - Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

Technology Standards to Projects and Development Initiatives

- SG-17 - Security and privacy protection aspects of IoT
- Security
- **SG2 Question 3/2** - securing information and communication networks; best practices for developing a culture of cybersecurity
- **Output 3.1 on building confidence and security in the use of ICTs:** Regional initiatives on building confidence in use of tel/IC

ITU Recommendations for IoT Privacy

- Y.4806: "Security capabilities supporting safety of the Internet of Things"
  - Frameworks for secure IoT
  - Approaches to handle threats and vulnerabilities
- Y.4552/X.1373: "Framework of device lifecycle security management"
  - Security management across the IoT device lifecycle

ITU Recommendations for IoT Security

- Y.2060: "Overview of the Internet of Things"
  - General overview, potential security implications
- X.1361: "Secure application services based on the Internet of Things"
  - Guidelines for providing secure application services
- Y.4401/X.5091: "Functional architecture of IoT for network security"
  - Architectural framework for ensuring security

Introduction to IoT Regulations

- **Definition:**
  - Set of rules governing the development, deployment, and management of IoT devices.
- **Importance:**
  - Ensuring security, privacy, and interoperability in the expanding IoT ecosystem.
- **Reference:**
  - Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30.

Conclusion

- Importance of aligning IoT development with ITU recommendations
- Urgency in addressing privacy & security challenges
- Emphasis on multi-stakeholder collaboration

Practical Activity

Practical Activity (15 mins): Analysing Current IoT Market Trends.

Thank You for your attention