IoT Security – Designing India Standard

A K Upadhyaya, Scientist G, STQC
Member LITD17, Convener LITD17 P5

The current scenario

- IOT devices have penetrated deep into our society
- Approximately 7.62 billion population but there may be 20 billion IoT devices by 2022 (Source: internet)
  - CCTV
  - Traffic Lights
  - Temperature Sensors
  - Light Sensors
  - Wearables
  - ⋮

The current scenario

- Smart Cities, Houses, Buildings
- Railways
- Banks
- Highways
- Ministries
- Home Appliances
- Residence/ Societies
- ISO/IEC TR 22417:2017 IoT use cases:
  - Identifies 14 context of use; 25 use cases

The problem

- Focus was on Functionality
- The issue is:
  - Security
  - Privacy

Approach to Security & Privacy

- Define Architecture
- Identify components
- Identify stakeholders
- Define lifecycle

Approach to Security & Privacy

- Identify risks w.r.t.
  - Components
  - Stakeholders
  - Lifecycle
- Identify Security & Privacy Controls with respect to the identified risks

ISO/ IEC 27400 does this

ISO/ IEC 27400: 2022

- Provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.
- IoT Architecture (Based on ISO/IEC 30141: 2018)
- Risk sources
- Security and Privacy Controls

Challenges of ISO/ IEC 27400

- Addresses to all components of IoT echo system (different components, stakeholders, lifecycles)
- Generic
  - Not all controls applicable to each IOT component
    - IoT Device; IoT Gateway; Communications Network; Applications etc.
- Missing
  - Measurable checkpoints for security controls
  - Security levels

Other standards

- ETSI EN 303 645 V2.1.1 (2020-06)
  - Cyber Security for Consumer Internet of Things: Baseline Requirements
- ISO/IEC FDIS 27402: 2023
  - Cybersecurity — IoT security and privacy — Device baseline requirements

ISO/IEC FDIS 27402: 2023

- This Standard provides basline security requirements for IoT devices.
- It proposes that further security requirements can be added for different verticals as per their needs.

International Scenario

IoT Security Assurance Framework by IoTSF

- Launched on 23/09/2015
  - Good Documentation (Freely Available)
  - Assurance Questionnaire (Available for Members)
  - Community Driven
    - Risk Assessment
    - Assurance Class (0 to 4)
    - Assessment

International Scenario

OWASP

- OWASP ASVS 4.0.3 Appendix C
  - 3 Levels
    - L1 (14 Requirements)
    - L2 (24 Requirements)
    - L3 (34 Requirements)
- OWASP ISVS Version 1.0, 22 January 2021
  - 5 category of requirements
  - 3 Levels
  - Each levels have different number of requirements under the 5 categories.

International Scenario

- NISTIR 8228 (June 2019)
  - identifies three high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices
- ETSI EN 303645 V2.1.1 (2020-06)

Need for BIS Standard

- ISO Standard did not provide measurable checkpoints & security levels
- Assessment Methodology not available in the international standard

Draft BIS standard provides both

The Draft BIS Standard on IoT Security & Privacy

- Aligned with ISO/ IEC 27400
- Have used IoTSF requirements also to bring granularity

Controls and Requirements

- Security and Privacy Controls
- Assurance Levels
- Security and Privacy Requirements
- Mapping with Requirements from other international bodies (OWASP, IoTSF)

Features

- Currently only for IoT devices
- Later other components will be covered
- Security requirements against security controls have been identified
- Risk based
  - Risks to IoT device security listed
  - Risks are mapped to the security requirements
  - For implementation of security controls Security requirements must be satisfied

Security Levels

- 3 levels have been proposed-L0; L1; L2
- Each level addresses one set of risks
- But an IoT device may not exactly fall with one particular level
- So an user may select his/ her own set of risks applicable to the device
- And define own level- L0+; L1+
- L0+ and L1+ are not unique!
  - There may be many variants of L0+ & L1+
- Mapping with 3 levels of OWASP and 5 Levels of IoTSF also given

Methodology

- Independent Testing
- Code Review
- Witness Testing
- Demonstration
- Process Audit

Important issues

- Hardware Interfaces
- Cryptography
- Secure Boot- Root of trust
- Secure update
- Data at Rest; Data in transit
- Protocols

Trust is bigger issue

Secure supply chain

Assessment and Evaluation

- Compliance Process
  - Identify risks
  - Assign Assurance Level
  - Perform Assessment for corresponding requirements to the Assurance level

MeitY is the nodal ministry and may bring notification for compliance to the National standard

Challenges

- Incomplete information
- Client reluctant in sharing information
  - Proprietary issues
- Front ending team not competent
- Difficulty in obtaining cooperation from SoC provider/ developer/ other stakeholder

Contribution by Industry

- BIS committees are representatives from Industry and Industry associations also
- Anybody wishes to contribute towards National/ International Standards may contact BIS
- More participation is encouraged
- A Lot has to be done in IoT
  - Other components
  - New risks
  - Emerging technologies
  - Refinements
  - Relevant to industry and currency with the international developments

Thank You

akupadhyay@stqc.gov.in