Secure IoT through Framework Design and Deployment considerations

Ratnakar Gandhe
IOT Penetration

1. Smart home
2. Wearables
3. Smart City
4. Smart grids
5. Industrial internet
6. Connected car
7. Connected Health
8. Smart Retail
9. Smart Supply Chain
10. Smart Farming
Secure IoT  
Vulnerability of Connected Devices and Systems

Hackers Remotely Kill a Jeep on the Highway—Uconnect Vulnerability
Secure IoT Vulnerability of Connected Devices and Systems
Secure IoT Standards, Guidelines and Recommendations

- oneM2M
- GSMA
- 3GPP
- ETSI
- OASIS
- NIST
- OWASP
- IOTSF
- ISO
- IETF

50+ Worldwide organisations
100+ documents

Disclaimers
Secure IoT Product and Solutions

Contributing Factors

- Framework
- Secure by Design
- Architecture
- Threat Modelling
- Best Practices

Stakeholders
- Manufacturers
- Service Providers
- System Integrators
- Developers
- Customers
Framework  Security key issues and supply chain of trust

Key Issues

- **Management governance**
  Responsible for product security/information privacy

- **Engineered for Security**
  Hardware and software take care security threats

- **Fit for purpose cryptography**
  Authentication/Authorization/Key Management

- **Secure network Framework and application**
  Secure apps, web I/F & server software

- **Secure production processes and supply chain**
  Manufacturing, delivery and installation

- **Secure for customer**
  Configuration control, software updates, VDS and life cycle mgmt.

Supply of product/solutions components from variety of sources need to be under consideration (Electronics/Mechanical/Web, mobile apps)
Risk based process

Context is important: Find risk appetite
Each application differs, driven by use case and operating environment

Risk analysis of the product/Solution in target environment
(Risk register, CIA triad)

Determine compliance class
(Security objectives, Product environment)

Compliance requirement mapping for the class
(Mandatory, Advisory)

Compliance Class

<table>
<thead>
<tr>
<th>Class</th>
<th>Security Objective (CIA triad)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 0</td>
<td>Confidentiality: Basic</td>
</tr>
<tr>
<td></td>
<td>Integrity: Basic</td>
</tr>
<tr>
<td></td>
<td>Availability: Basic</td>
</tr>
<tr>
<td>Class 1</td>
<td>Confidentiality: Basic</td>
</tr>
<tr>
<td></td>
<td>Integrity: Medium</td>
</tr>
<tr>
<td></td>
<td>Availability: Medium</td>
</tr>
<tr>
<td>Class 2</td>
<td>Confidentiality: Medium</td>
</tr>
<tr>
<td></td>
<td>Integrity: Medium</td>
</tr>
<tr>
<td></td>
<td>Availability: High</td>
</tr>
<tr>
<td>Class 3</td>
<td>Confidentiality: High</td>
</tr>
<tr>
<td></td>
<td>Integrity: Medium</td>
</tr>
<tr>
<td></td>
<td>Availability: High</td>
</tr>
<tr>
<td>Class 4</td>
<td>Confidentiality: High</td>
</tr>
<tr>
<td></td>
<td>Integrity: High</td>
</tr>
<tr>
<td></td>
<td>Availability: High</td>
</tr>
</tbody>
</table>

Little discernible impact to organisation, person

• Basic: Public info, Minor impact and disruption
• Medium: Personal sensitive info, limited impact
• High: Personal sensitive info, high impact

Source: IOTSF-IoT-Security compliance Framework release 2.0
Framework **Security Requirements compliance**

### Compliance requirements from System and business point of view

- Business Security Processes, Policies and Responsibilities
- Device Hardware & Physical Security
- Device Software
- Device Operating System
- Device Wired and Wireless Interfaces
- Authentication and Authorization
- Encryption and Key Management for Hardware
- Web User Interface
- Mobile Application
- Privacy: Data protection, regulatory compliance
- Cloud and Network Elements
- Secure Supply Chain and Production
- Configuration
- Device Ownership Transfer
Framework Requirements compliance samples

Business Security Processes, Policies and Responsibilities

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Compliance Class and Applicability</th>
<th>Primary Keyword</th>
<th>Secondary Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>The product’s processor system has an irrevocable hardware Secure Boot process.</td>
<td>M for Class 1 and above</td>
<td>System</td>
<td>Hardware</td>
</tr>
<tr>
<td>The product’s processor system has an irrevocable “Trusted Root Hardware Secure Boot”.</td>
<td>M for Class 2 and above</td>
<td>System</td>
<td>Hardware</td>
</tr>
<tr>
<td>The product’s processor system has a measured irrevocable hardware Secure Boot process.</td>
<td>M for Class 3 and above</td>
<td>System</td>
<td>Hardware</td>
</tr>
<tr>
<td>The Secure Boot process is enabled by default.</td>
<td>M for Class 1 and above</td>
<td>System</td>
<td>Hardware</td>
</tr>
<tr>
<td>Any debug interface (for example, I/O ports such as JTAG) only communicates with authorised and authenticated entities on the production devices.</td>
<td>M for Class 1 and above</td>
<td>System</td>
<td>Hardware</td>
</tr>
</tbody>
</table>

Device Hardware & Physical Security

Source: IOTSF-IoT-Security compliance Framework release 2.0
Architecture  Hub based architecture

Stakeholders
- CxO, IoT purchase
  - Informed decision
- IT department
  - Security focused IoT device management
- Developers, OEM
  - IoT management and security needs

Classes
1. Fully controlled/connected
2. Partially controlled/connected
3. Information sharing

Hub’s 3 main Features
1. Network Management and Security tools
2. Connecting devices securely
3. Lifecycle management

**Hub feature 1: Network Management and security tools**

- **Local IoT Network**
  - Hub act as gateway separating Local IoT-Business/Networks
  - Minimize attack surface, address threat vectors

- **Separation of testing, staging and live System**
  - Separate test and staging furcation – New device may lower the security
  - Manage device setup and connection

- **Firewall and Gateways**
  - To protect network and data flow
  - Enable segmentation, routing and traffic monitoring

**Network Management and security tools**

- Local IoT Network
- Separation of Testing, staging and Live system
- Firewall and Gateways
Hub feature 2: Connecting Devices Securely

- **Authentication and Authorization**
  - Device Identity Management
  - Managing privileges
  - Black or whitelisting
  - Validating software/Hardware updates

- **Secure Boot**
  - Secure/Trusted/Measured boot for authorized software
  - Alerts if hub has been tempered for privileges, actions

- **Root of Trust**
  - Have industry standard cryptography
  - Have hardware Root of trust
  - Manage private and public root of trust
  - Detect malicious software

- **Connecting Devices Securely**
  - Authentication and authorization
  - Secure Boot
  - Root of Trust
**Hub feature 3: Life Cycle Management**

**Life Cycle Management**

- Monitor and Audit
  - Monitor and audit devices and traffic in IoT ecosystem
  - Central repository of information
  - Notification, Alerts, Status updates, Report

- Update and Patch
  - To protect against threat and security vulnerability
  - Schedule updates, maintain reports
  - Code signing to verify

- Manage Device Identity and End of Life
  - Assigning device ID
  - Managing manufacturer end of sale
  - Change of ownership
  - Permissions and revoking authorization
**Why hub based architecture**

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Hub Architecture</th>
<th>Tree Network</th>
<th>Hub-and-Spoke / Star</th>
<th>Mesh</th>
<th>Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized network management tool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hybrid network sub-architectures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct communication with management tool (not through unneeded nodes or pathways)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information must be shared in a hierarchical manner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network management tool is resilient to device and network disruptions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In the event of management point failure, networks and devices can continue functioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central management and information aggregation point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management tool supports IoT device identity, access and authorization resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management tool supports minimization of attack surface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated device for network and IoT device management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hub Architecture characteristics for IoT ecosystem**

- **Centralized management**
  - Focal point in a network, IoT lifecycle management, monitor traffic, RoT
- **Software update and patch**
  - Protect devices without update capabilities
- **Security compliance**
  - Act as firewall, log and reporting, status repository
- **Troubleshooting**

Architecture Support security principles and Threat modeling

Hub architecture support to treat STRIDE* threat model

<table>
<thead>
<tr>
<th>Threat</th>
<th>Threat example</th>
<th>Treatment</th>
<th>Architecture (Hub) to support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Address Resolution Protocol (ARP) used to redirect traffic</td>
<td>Update and patch device to prevent vulnerability</td>
<td>Authentication &amp; Authorization, Update and Patch</td>
</tr>
<tr>
<td>Tempering</td>
<td>Tampering software to modify permissions, install spyware</td>
<td>Secure boot and update by trusted resources</td>
<td>Secure boot, Monitor and audit</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Sensor data modified in transit to cloud services</td>
<td>Secure identity of devices and users. PKI to manage and revoke certificates, RoT</td>
<td>Authentication &amp; Authorisation, Roots of Trust (RoT)</td>
</tr>
<tr>
<td>Information Disclosure (Data Breach)</td>
<td>Diagnostics information containing Enterprise information</td>
<td>Traffic monitoring and management, separate IoT/business network</td>
<td>Local IoT network, Gateway and firewalls</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Using exploits in a device to execute DoS or DDoS attack on another IoT device</td>
<td>Traffic monitoring on IoT network, Gateway and firewall to monitor and block traffic</td>
<td>Local IoT network, Monitor and Audit, update and patch</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>Unauthorized access of a cloud service provider to get on the IT/IoT network</td>
<td>Separation of IoT and business network</td>
<td>Local IoT network, Authentication and authorization, Monitor and Audit</td>
</tr>
</tbody>
</table>

*Based on IoT deployment may use other models: PASTA, NIST, ISO 27000, OWASP

Security risk in IoT implementation and security principles

- **Three Key principles**
  1. Confidentiality
  2. Integrity
  3. Availability

- **Connecting device to IoT network**
  1. Data need to be private, audited and trusted
  2. Timely arrival of data
  3. Access or control of device
  4. Updating
  5. Ownership management

- **Who (hub) provides**
  - Trust management
  - Layered security
  - Network access/revoke
  - Safe to make data transparent (M&C)
  - Enterprise data info, criticality and safety

** Source: IoTSF “Make it safe to connect: Establishing principles for Internet of Things Security” IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
Secure by Design **Code of practice/Security mindset**

### Stakeholders Responsible for implementation

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manufacture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT Service Providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Application Developers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retailers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Guiding principles

1. To reduce burden: consumer/Supply chain
2. Transparency: what security mechanism
3. Measurability: Effectiveness
4. Facilitating Dialogue: Share best practices
5. Resilience: Business continuity, fall back mechanism

- **Monitor System telemetry data**
- **Make it easy for consumers to delete personal data**
- **Make installation and maintenance of devices easy**
- **Validate input data**
- **Securely store credentials and security-sensitive data**
- **Ensure that personal data is protected**
- **Ensure software integrity**
- **Minimise exposed attack surfaces**
- **Communicate securely**
- **No default password**
- **Implement a vulnerability disclosure policy**
- **Keep software updated**
- **Monitor System telemetry data**
Case study **Smart Building Energy Management (Hub based)**

Building management with energy efficient operations, fault detection, operational scenario and schedules.

IoT Hub/ Gateway with following features

- Secure boot
- Device Identity Management
- Managing privileges
- Black or whitelisting
- Validating software/Hardware updates
- Routing and traffic monitoring
- Notification, Alerts, Status updates, Report
Case study **Smart Parking with Hub Features** (Distributed Hub)

Allows drivers to access parking quickly and efficiently. Enables real-time monitoring and management of available parking space, maximizing parking occupancy.

**IoT Hub/Gateway**

- IoT Hub Gateway function distributed.
- Security Management is part of video analytics server.

www.mindteck.com
Case study **Secure by design : Hardware and system level**

- **Concentrated solar power plant mirror controller with modified WiMax protocol**

Secure and reliable communication hardware with
  - 802.16 phy
  - Modified WiMax for security breach
  - Protocol on FPGA to achieve the high speed of 26 Mbps
  - Frequency diversity: Software Defined Radio to operate single hardware in 800MHz to 6 GHz
References


• Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices [https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm](https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm)


• The CEO's Guide to Securing the Internet of Things [https://www.business.att.com/content/dam/attbusiness/reports/exploringiotsecurity.pdf](https://www.business.att.com/content/dam/attbusiness/reports/exploringiotsecurity.pdf)


• IoTSF Compliance Framework, Compliance Checklist and Vulnerability Disclosure Guidelines can be found [https://iotsecurityfoundation.org/best-practice-guidelines](https://iotsecurityfoundation.org/best-practice-guidelines)

Confidentiality and **Disclaimer Notice**

This document contains confidential information of Mindteck which is provided for the sole purpose of permitting the recipient to evaluate the capabilities submitted herewith. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information: which was known to the recipient prior to receipt of such information from Mindteck, or becomes publicly known through no fault of recipient, or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Mindteck.

This publication is produced by Mindteck for private circulation among selected constituents. It is for informational purposes only. While every effort is made to ensure the information given is accurate, Mindteck will not accept any responsibility for loss or damage to any person resulting from reliance on information presented herein.

All trademarks, trade names, service marks, service names, and images mentioned herein belong to their respective owners, even if not clearly identified.
Thank You