Guidelines

Internet of Things (IoT) Cyber Security Guide

In consultation with:

SG:D
EMPOWERING POSSIBILITIES

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CSA SINGAPORE

IMDA IoT Cyber Security Guide
Version 1, Mar 2020

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Contents

This Guide is a living document which is subject to review and revision periodically.

Guides are informative documents and voluntary in nature except when it is made mandatory by a regulatory authority. It can also be reference in contracts as mandatory requirements. Users are advised to assess the suitability of this guide for their intended use.

Compliance with this guide does not exempt users from any legal obligations.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE LIABLE FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT THE PRACTICE OR IMPLEMENTATION OF THIS GUIDE MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY CONTRIBUTORS OF THIS DOCUMENT OR ANY THIRD PARTY.

AS OF THE DATE OF THE ISSUANCE OF THE PUBLIC CONSULTATION OF THIS GUIDE, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS GUIDE. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELATED STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF PATENT RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE GUIDE IF REQUIRED.

IMDA IoT Cyber Security Guide

1 Introduction

The Internet of Things (IoT) brings together the physical environment and a wide range of objects such that they can interact with one another seamlessly through the use of Information and Communication (ICT) systems. It encompasses many supporting technologies such as sensing and control technologies, networking technology, information technology and software technology. Together, all these technologies enable sensors, actuators, middleware, data and communication networks, and applications, to interconnect to form an IoT ecosystem.

The significance of the economic impact of IoT is well-documented and increasingly being felt, with the increasing adoption of IoT solutions among consumers, enterprises and governments. Examples include connected wearables, smart homes, smart buildings, connected vehicles, video surveillance and analytics.

As people and devices become more connected, issues relating to the safeguarding of data and management of cyber security threats become increasingly important. IoT devices can collect significant amounts of information about their users and their environment, including personally identifiable, commercially confidential and/or sensitive data. For example, wearables can track an individual's steps, heart rate and sleep patterns while commercial sensors and actuators may expose enterprise control systems to the risk of data exfiltration, or even worse attacks. Measures will need to be taken to protect this large and growing volume of sensors and sensitive data.

Unfortunately, early IoT devices have several vulnerabilities which may be easily exploited, making them easy targets for cyber security attacks. For instance, compromised devices can be controlled by a botnet and be made to participate in Distributed Denial-of-Service (DDoS) attacks on other organisations.

Security has been consistently ranked as the top concern inhibiting user adoption. On the other hand, industry has provided feedback that conforming to existing standards not designed with IoT in mind, is time-consuming, costly and impractical for the dynamic and evolving technologies and applications of IoT.

Protecting organisations and individuals from rising cyber threats is a national priority as well as an area of economic opportunity. It is integral to ensuring that Singapore remains cyber secure in a digital economy, with a set of trusted infrastructure to support our Smart Nation initiatives.

Similar to any system, an IoT system is as secure as its weakest link. It is thus important to ensure that proper security considerations and measures are put in place for both the implementation and operational stages of the deployment of any IoT system. This document aims to provide guidance to users and enterprises when procuring, deploying and operating IoT devices/systems, while enabling solution providers to verify the security posture of their solutions, by providing practical guidelines that include baseline recommendations, foundational concepts and checklists. A risk-based and system-oriented approach is taken to identify and mitigate threats to IoT solutions. Enterprise users and their vendors are guided to work together to secure their IoT systems over their lifecycles.

2 Scope

This document serves as a practical guide for enterprise users (and their vendors) that intend to deploy IoT solutions, providing baseline recommendations[1], foundational concepts and checklists, which focus on the security aspects for the acquisition, development, operations and maintenance of IoT systems.

It focuses primarily on system-level recommendations and builds on the concepts introduced in ITSC TR 64: "Guidelines for IoT security for smart nation" and provides further details on the implementation of IoT security through case studies.

This guide can be used by:

1. IoT developers who want to design, develop and deploy secure IoT products and systems. Examples of developers include solution architects, programmers, manufacturers and system integrators.
2. IoT providers who need to roll-out, configure, operate, maintain and de-commission IoT systems securely. Examples of providers include network operators, platform providers, data analysts and service delivery managers.
3. IoT users who want to procure and interact with IoT systems. For system interactions, IoT users can by either human or software agents.

With respect to the lifecycles of IoT systems, IoT developers are mainly involved in the implementation phase, which covers the design, develop, deploy, integrate and test stages, while IoT providers are involved in the operational phase, which covers the operate, support, maintain, upgrade and retire stages. IoT users could be involved in both the implementation and operational phases. It should be noted that multiple cycles of implementation and operation phases could take place with the introduction of new features over the entire life-span of an IoT system.

Figure 1 depicts the two areas of focus of this document with respect to ITU's Information Security Management Framework as defined in ITU-T X.1052.

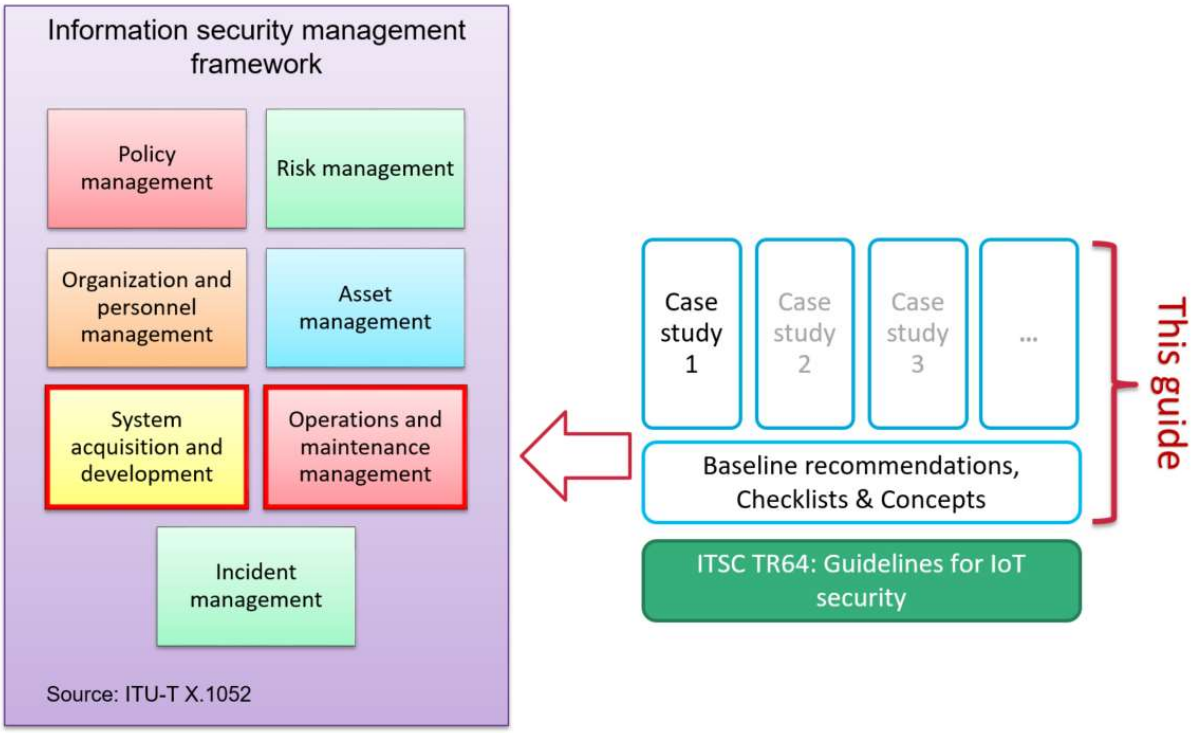

Figure 1: Overview of scope

[1] This guide does not cover areas on privacy. Guidelines on privacy are available on the website of Personal Data Protection Commission (PDPC) at https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines.

3 References

In this document, reference has been made to the following standards. Where versions are not indicated, reference shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

[1] Cloud Security Alliance IoT Controls Framework

[2] ENISA Baseline security recommendations for IoT

[3] ETSI TS 103 645 cyber security for consumer IoT

[4] GSMA IoT security guidelines for endpoint ecosystems

[5] IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

[6] ITSC TR 64 : 2018 Guidelines for IoT security for smart nation

[7] Online Trust Alliance – IoT trust framework

[8] OWASP – https://www.owasp.org/index.php/Application_Threat_Modeling

4 Terms and definitions

Access Control	Functions, which include identification, authentication, authorisation and accountability.
Authentication	Act of confirming the identity of an entity.
Authorisation	Act of specifying the access permissions to a resource.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes. [ITSC TR 64]
Denial of service (DoS)	Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users. [ITSC TR 64]
Identification	Act of stating the identity of an entity.
Internet of Things (IoT)	System of physical and virtual entities that are connected with one another, allowing interaction anytime, anywhere. [ITSC TR 64]

5 Abbreviations and acronyms

AAA	Authentication, Authorisation, Accounting
ABAC	Attribute-Based Access Control
APN	Access Point Name
CIA	Confidentiality, Integrity, Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	De-Militarised Zone
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
ENISA	European Network and Information Security
ETSI	European Telecommunications Standards Institute
HTTP	HyperText Transfer Protocol
IoT	Internet of Things
ISG-CERT	Info-communications Singapore Computer Emergency Response Team
IT	Information Technology
ITSC	Information Technology Standards Committee (Singapore Standards)
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JTAG	Joint Test Action Group
MFA	Multi-Factor Authentication
MQTT	Message Queueing Telemetry Transport
NIST	National Institute of Standards and Technology

OT	Operational Technology
OTA	Over-The-Air
PDPC	Personal Data Protection Commission of Singapore
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
SingCERT	Singapore Computer Emergency Response Team
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOP	Target Of Protection
TPM	Trusted Platform Module
TR	Technical Reference
TS	Technical Specification
UDP	User Datagram Protocol
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

6 Baseline recommendations for the implementation phase

6.1 Introduction

Section 6 provides a set of baseline security recommendations for IoT users and IoT developers during the implementation phase.

The recommendations cover four fundamental IoT security design principles (refer to Annex A for more details):

1. Secure by defaults
2. Rigour in defence
3. Accountability
4. Resiliency

Individual products are used to implement a system and the system operates in the context of an organisation's processes, policies and people. The increasing levels of integration, from product to system and finally organisation require additional considerations, as the overall security posture is only as strong as its weakest links. Together, the recommendations are fundamental to safeguarding the IoT system systematically and over its lifecycle.

While the baseline recommendations provided in this document are common across a majority of IoT systems, the IoT users and IoT developers need to determine the appropriateness of the recommendations for the intended systems/solutions, based on the business needs and relevant regulatory requirements.

6.2 Principle 1: Secure by defaults

6.2.1 Employ strong cryptography [2]

Strong cryptographic capabilities are the fundamental building blocks used to ensure the security of data transactions, including authentication and sensing data exchange between IoT devices. Examples of the usage of cryptographic capabilities include digital signatures and encryption.

Recommendation: Industry accepted cryptographic techniques and best practices shall be applied appropriately and adequately on for the IoT system. Examples of best practices include:

- use of approved algorithms
- sufficient key length
- use of approved random number generator(s)
- recommended crypto-period
- recommended entropy sources
- use of updatable cryptography

6.2.2 Protect impactful data [1], [3]

Impactful data of the IoT system can refer to keys, credentials, codes/firmware, personal data, inputs/commands and sensing data, etc. Access to impactful data should require assurance and/or verification that it originates from authentic sources, and be protected from tampering, modification and/or disclosure to unauthorised parties.

Recommendation: Impactful data shall be checked for authenticity, and protected from disclosure and modifications by unauthorised parties. All sensitive communications to/from IoT devices shall be encrypted.

6.3 Principle 2: Rigour in defence

6.3.1 Conduct threat modelling [8]

Threat modelling provides a systematic approach, which helps to identify the system assets, the security needs of the system assets and the possible threats to these system assets so that the limited available resources can be focused on what needs to be protected. Threat modelling[2] helps to minimise the exposed attack surfaces and mitigates the remaining vulnerabilities.

Recommendation: Threat modelling should be conducted at the start of the implementation phase, and account for the intended usage of IoT devices within the defined operating environments.

6.3.2 Establish Root-of-Trust [4], [5]

Root-of-Trust provides a tamper protected module that stores and protects the keys of the devices so as to establish a firm foundation for other security mechanisms to build upon, hence achieving higher assurance of security through a chain of trust.

Recommendation: Root-of-Trust should be established and utilised by key system components, such as IoT gateways and IoT platforms, as they may host sensitive data and execute impactful operations. For example, Root-of-Trust can be based on a Trusted Platform Module (TPM) chip embedded in the device, or a virtual secure element integrated within the device's software.

6.3.3 Employ secure transport protocols [2]

Transport protocols are used to transfer data within and between systems. It is thus important to ensure that secure versions of transport protocols are properly configured, protecting data in transit effectively.

Recommendation: Proven transport protocols[3] shall be employed with security controls properly activated, wherever possible. Examples of security controls of proven transport protocols include:

- use of TLS for TCP payloads
- use of DTLS for UDP payloads
- use TLS when using MQTT
- disable non-authenticated Bluetooth pairing procedures

6.4 Principle 3: Accountability

6.4.1 Enforce proper access controls [2], [5]

Access to system resources shall be controlled and managed throughout its lifecycles, minimising opportunities for malicious actors. Default passwords and weak passwords are the most commonly exploited vulnerabilities. The use of Multi-Factor Authentication (MFA) provides a higher assurance of the identity of initiators, enhances accountability and mitigates against mistakes.

Recommendation: Proper access controls, both cyber and physical, for devices, networks and data shall be enforced. Fundamental access controls include:

- Replacement of all default passwords
- Enforcement of strong passwords as specified in section 7.2.1
- Enforcement of multi-factor authentication (MFA) for impactful remote operations
- Securing physical access to devices and their service ports

6.4.2 Provide audit trails [1]

Intentional misuse, bypassing restrictions and misconfigurations are still potential risks even with the proper implementation of access control measures. It is thus important to have audit trails.

[2] A threat modelling checklist is provided as a reference in section 8 of this document

[3] The latest versions of transport protocols should be employed, whenever possible.

Recommendation: All attempts to access sensitive data and altering system resources shall be properly monitored and logged.

6.5 Principle 4: Resiliency

6.5.1 Guard against resource exhaustion [2]

IoT systems are vulnerable to resource exhaustion attacks. Attackers and compromised devices can send requests continuously to IoT devices/networks/systems to deplete its resources and impact systems' availability.

Recommendation: The system should employ mechanisms to protect against malicious attacks such as DDoS. Examples include:

- Monitor system/device resources are sufficient to sustain services.
- Detect resource exhaustion for early intervention.
- Specific control over resource-intensive software.
- Enforce power consumption thresholds on IoT devices.
- Limit number of concurrent sessions.
- Operate with excess capacity.

7 Baseline recommendations for operational phase

7.1 Introduction

Section 7 provides a set of baseline security recommendations for IoT users and IoT providers during the operational phase.

The recommendations are organised according to the same four fundamental IoT security design principles used in section 6.

While the baseline recommendations provided in this document are common across a majority of IoT systems, the IoT users and IoT providers need to determine the appropriateness of the recommendations for the intended systems/solutions, based on the business needs and relevant regulatory requirements.

7.2 Principle 1: Secure by defaults

7.2.1 Use strong credentials [2], [5]

Weak credentials, e.g., user identifications and passwords are consistently been placed as top vulnerability, which are subjected to brute-force attacks.

Recommendation: Default credentials shall be avoided, and strong passwords shall be used throughout the system. Password complexity (strength) should adhere to the published international best practices if regulatory requirement is not available. Minimally, passwords should consist of 8 or more characters comprising a combination of letters and numbers. It is also encouraged that symbols and upper-case characters be used to enhance password strength. Multi-factor authentication should be enabled, whenever possible, for access to impactful data and operations.

7.3 Principle 2: Rigour in defence

7.3.1 Segment IoT and enterprise networks [2], [5]

A single compromised device can be the attack vector into your enterprise systems.

Recommendation: Network segmentation should be employed so that IoT devices belonging to different networks can be properly segmented from one another and also from other corporate enterprise systems and networks. Firewalls and malware mitigation solutions should be implemented to protect each network whenever possible.

7.4 Principle 3: Accountability

7.4.1 Establish proper device management [5]

All connected devices are potentially exposed to malicious actors, and may be exploited, allowing cyberattacks to compromise the whole IoT system. Stolen devices can be tampered with, reverse-engineered and used against the IoT system. Outdated and unpatched firmware/software can contain known vulnerabilities that malicious actors can exploit. Hence, proper management of connected devices is critical to ensure the security of the whole system.

Recommendation: Proper management of devices, including firmware/software updates and patches, shall be established. An inventory of connected devices, software and firmware versions[4] should be kept and up-to-date patches should be applied throughout the "Operational" lifecycle stage. Access controls, including for physical access to IoT devices, should be strictly enforced. IoT users and IoT providers should subscribe to notifications and advisories issued by IMDA's ISG-CERT and Cyber Security Agency (Singapore)'s SINGCERT, as appropriate, to be apprised of newly discovered vulnerabilities and threats to IoT and ICT systems.

7.5 Principle 4: Resilience

7.5.1 Recover from attacks [5]

IoT systems will be targeted for attacks, especially if the asset is valuable enough. A determined attacker will find a way to compromise the system as more sophisticated attacking tools are developed. There is therefore a need to be prepared to fail safely and recover from it, especially when the compromise of an IoT system can affect the safety of humans or facilities.

Recommendation: Regular backups of system data (include settings) as well as regular disaster recovery exercises for systems shall be conducted.

7.5.2 Conduct periodic assessments [7]

An IoT system can be a dynamic and complex system. As threats are always evolving, periodic penetration testing and/or vulnerability assessment is required to mitigate security risks.

Recommendation: Penetration testing and/or vulnerability assessments of the IoT system should be conducted periodically. Threat modelling should be conducted as part of vulnerability assessments.

[4] IoT users and IoT providers may be dependent on IoT developers to provide patches for new vulnerabilities in a timely manner.

8 Threat modelling checklist

This section provides a suggested checklist for threat modelling. The checklist can be used to guide the threat modelling process and ensure that it is conducted properly and systematically. While STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) is the model used to help analyse and find threats to the system. It should be noted that other methodologies exist and might be more appropriate for specific use cases.

Please refer to the case study in annex B for an illustration of the application of the threat modelling checklist.

ID	Threat modelling checklist	Y / N	Supporting materials
1	Identify the potential target(s) to be protected a. Define its boundaries and the external systems (including users) that it needs to interact with b. Decompose the target(s) into its subcomponents c. Identify data flows within the target(s), and inputs and outputs from external systems d. Identify sensitive data and where they are handled (at rest, in transit, in use) e. Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (**CIA triad**)) for subcomponents and data flows f. Identify hardware, software and protocols in use		
2	Define the security problem a. Identify system accessibility • Identify attack surfaces • Determine operating environments • Determine system / device lifecycles and supply chain b. Identify system susceptibility (aka vulnerabilities) • Determine known vulnerabilities • Enumerate threats to attack surfaces (using Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (**STRIDE**) as a guide) • Enumerate threats to operating environments (using STRIDE as a guide) • Enumerate threats to stages of system / device lifecycles and supply chain (using STRIDE as a guide) c. State any assumptions		
3	Conduct risk assessment • Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets • Assess attacker capabilities required to realise the threats • Assess the likelihood of the risk • Prioritise the risks for mitigation, including other considerations (e.g. monetary, safety, social and usability impacts)		
4	Determine the security objectives • State the security objectives. For example, OT systems emphasize safety, where system integrity takes precedence over data confidentiality		

ID	Threat modelling checklist	Y / N	Supporting materials
5	Define the security requirements • State the necessary requirements to address the identified security objectives without going into their specific implementation		
6	Design and implement the capabilities		
7	Validate and verify that the capabilities address the security requirements adequately		

9 Vendor disclosure checklist

This section provides a non-exhaustive list of security questions that enterprise solution vendors can use for self-disclosure. It identifies the possible important security capabilities/services that vendors should focus on and also, allows users to better evaluate and compare the security aspects of the IoT solutions/systems proposed by different vendors. Thus, this checklist facilitates communication, enables fair comparisons of security across IoT solutions and promotes the implementation of better security. Notwithstanding the described uses of the checklist, it should be noted that the checklist is only a template of common security considerations. Users are required to determine the appropriateness and applicability of the checklist items so as to add on, remove, and/or adjust them according to the uses and businesses' needs.

Please refer to the case study in annex B for an illustration of the application of the vendor disclosure checklist.

Legend: Y – Yes, N – No, NA – Not applicable

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
1. Cryptographic support			
CK-CS-01	Do your devices and system properly utilise industry accepted cryptographic techniques and best practices? Examples of best practices include: · use of approved algorithms and their correct implementation and application · sufficient key length · use of approved random number generator(s) · recommended crypto-period · recommended entropy sources · use of updatable cryptography		
CK-CS-02	Do you employ proper key management (generation, exchange, storage, use, destruction, replacement, etc.) techniques?		
2. Security function protection			
CK-FP-01	Do you establish Root-of-Trust?		
CK-FP-02	Do you employ secure boot?		
3. Identification and authentication			
CK-IA-01	Do you employ unique, non-modifiable and verifiable identities for clients (user, device, gateway, application) and servers?		
CK-IA-02	Do you employ mutual authentication? For example, before establishing connections and after pre-defined intervals		
4. Network protection			
CK-NP-01	Do you enforce network access control? For example, ensure explicit authorisation to join a new network and/or allow remote access.		
CK-NP-02	Do you employ proven transport protocols with security controls properly activated? Examples include: · Use of TLS for TCP payloads. · Use of DTLS for UDP payloads.		
CK-NP-03	Do you employ industry best practices for secure connectivity? Examples of industry best practices: · Use of VPN or leased lines.		

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
	· Use of private mobile APNs from telecommunication operators when using a public mobile carrier network. · Use of DNS pinning to prevent DNS spoofing. · Use of traffic filtering based on type, port and destination. · Use of certificate pinning. · Employ TLS when using MQTT. · Scan for open network ports. · Use whitelisting to establish or deny connections from non-trusted sources. In addition, IETF RFC 8520 Manufacturer Usage Description (MUD) can be a standard mechanism for devices to provide this information to the network.		
CK-NP-04	Do you segregate communication channels for trusted end points from non-trusted ones? Examples include: · Use of VLAN. · Use of firewalls for DMZ. · Use of unidirectional security gateway. · Use of network segmentation or micro segmentation. · Physical isolation.		
5. Data protection			
CK-DP-01	Do you protect the confidentiality and integrity of your sensitive data? · in transit · in use · at rest		
CK-DP-02	Do you protect the authenticity and integrity of your codes and firmware? · in transit · in use · at rest		
CK-DP-03	Do you ensure the authenticity and integrity of your data (e.g. inputs, commands and sensing data)? · in transit · in use · at rest Examples include: · Validate incoming content-types. · Validate response types. · Validate the HTTP methods against authorisation credentials. · Whitelist allowable HTTP methods. · Define the acceptable character set (e.g. UTF-8). · Validate that input characters are acceptable. · Encode/escape input and output.		
CK-DP-04	Do you enforce access control to detect and prevent unauthorised data access and exfiltration, and filter your outputs?		
6. Access protection			
CK-AP-01	Do you employ mechanisms to manage and secure local and/or remote access?		

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
	Example of mechanisms include: · auto logoff. · screen lock. · delay in between login attempts and lock-out for repeated unauthorised attempts. · forced re-authorisation.		
CK-AP-02	Do you send out-of-band notifications on impactful operations and/or alerts (eg. credential reset, security update failures)?		
CK-AP-03	Do you enforce access control to prevent unauthorised access to system interfaces, system files and removable media?		
CK-AP-04	Do you employ anti-tamper mechanisms for resistance, evidence, detection and/or response?		
CK-AP-05	Do you support multi-factor authentication for impactful operations (e.g. credential reset)?		
7. Security management			
CK-MT-01	Do you employ proper user and password management? Examples include: · Enforce strong password policy. · Enforce no default passwords. · Specify password expiration. · Ensure that password recovery and reset mechanism are secure.		
CK-MT-02	Do you enforce proper access control to management functions? Examples include: · Enforce least privilege policy. · Use of attribute-based access control (ABAC) or role-based access control (RBAC). · Implement dual control for key management protection to prevent a single bad actor's compromise to the key materials. · Support granular access permissions per user and per application. · Implement separation of duties to key management system to prevent a single bad actor/administrator from compromising the system.		
CK-MT-03	Do you employ malware mitigation mechanisms? Examples include: · Ensure file integrity using cryptographic hash. · Baseline "normal" behaviour. · Detect unauthorised software. · Monitor devices and traffic flows. · Scan backup images. · Prohibit insecure bootloaders.		
CK-MT-04	Do you secure remote management of devices, including sensor gateways? Examples include: · Support secure Over-The-Air (OTA) updates of device applications and configurations. · Support software and/or firmware updates using cryptographically secure methods.		

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
	· Support platform integrity checking, such as the measured boot mechanism or verifying the firmware integrity. · Restrict remote management to secure networks.		
8. Resiliency support			
CK-RS-01	Does your device support integrity self-test, error detection and correction for critical functions and return to a safe state?		
CK-RS-02	Do you safeguard against a compromised device from compromising the system? Examples include: · Use of Perfect Forward Secrecy (PFS) for secure communication. · Use of distinct secret keys for individual device.		
CK-RS-03	Do you employ mechanisms against failures from resource exhaustion and/or malicious attacks such as DDoS? Examples include: · Monitor to ensure that cloud resources are sufficient to sustain services. · Detect resource exhaustion, for early preventive or corrective actions · Control the execution of resource-intensive software. · Enforce power thresholds. · Limit the number of concurrent sessions. · Operate with excess capacity.		
CK-RS-04	Do you conduct regular backups of system data (including settings)?		
9. Security audit			
CK-AU-01	Do your devices and system record enough information (e.g. who does what and when) in audit logs and flag significant events? Example of events include: · User logins, logouts and unsuccessful authentication attempts. · Connection, disconnection attempts and unsuccessful connection attempts. · Unsuccessful authorisation attempts. · Access to sensitive data. · Import and export of data from removable media. · Any change in access privileges. · Creation, modification and deletion of data by user. · Impactful operations. · Remote operations. · Security update failures. · Physical access attempts where possible. · Emergency access where possible.		
CK-AU-02	Are your audit logs protected from modification, deletion, physical tampering and sensitive data disclosure?		
10. Lifecycle protection			
CK-LP-01	Have you conducted threat modelling to identify, analyse and mitigate threats to the system?		
CK-LP-02	Did you design and develop the system using a secure systems engineering approach?		

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
CK-LP-03	Do you implement and maintain the system with components from a secure supply chain, with no known unmitigated vulnerabilities?		
CK-LP-04	Do you provide, communicate and update security information (terms of service, features, guidelines, instructions and notifications, etc.), in simple language and timely manner? Examples of security information include: · Security policies. · Security updates. · Instructions for device/media sanitisation. · End-of-life notifications. · Phase out plan.		
CK-LP-05	Do you ensure that the system is hardened before the "Operational" lifecycle phase? Examples of system hardening include: · Remove all backdoors. · Remove all debug codes from the released version. · Change default configuration and disable unnecessary services. · Remove or tamper-covered JTAG, unneeded serial and ports before deployment. · Harden VM host properly, including disabling memory sharing between VM. · Remove default and hardcoded passwords.		
CK-LP-06	Do you maintain an inventory of connected devices, software and firmware versions, applied patches and updates throughout the “Operational” lifecycle stage?		
CK-LP-07	Do you conduct penetration testing and/or vulnerability assessment periodically, and before each major release?		
CK-LP-08	Do you establish proper vulnerability disclosure and management? Examples include: · Ensure the supply chain's capability to provide upgrades and patches. · Provide vulnerability disclosure and processes to track and response promptly. · Provide firmware and software patches/updates for vulnerabilities discovered, in a timely manner. · Employ proper change management processes to manage security patches or updates. · Notify and/or allow user to approve/reject updates, patches and changes to user settings, where appropriate. · Disclose minimum support period.		
CK-LP-09	Do you ensure that identities, certificates and secrets are secured throughout the lifecycle (e.g. creation, provisioning, renewal and revocation)?		
CK-LP-10	Do you sanitise devices and systems of security data and sensitive user data, before the "Reuse or Dispose" lifecycle stages?		

10 Bibliography

[1] https://cve.mitre.org/

[2] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[3] Industrial Internet of Things: volume G4 – Security framework

[4] ISO/IEC 27000 Information security management systems – Information security risk management

[5] ISO/IEC 27002 Information security management systems – Code of practice for information security controls

[6] NIST Special Publication (SP) 800-63B Digital identity guidelines – Authentication and lifecycle management

[7] Strategic principles for securing the Internet of Things (IoT) – U.S. Department of Homeland Security

[8] ITSC TR 38 : 2014 Technical Reference for sensor network for Smart Nation (public areas)

[9] ITSC TR 40 : 2015 Technical Reference for sensor networks for Smart Nation (homes)

[10] ITSC TR 47 : 2016 Technical Reference for IoT reference architecture for Smart Nation

[11] ITSC TR 50 : 2016 Technical Reference for IoT information and services interoperability for Smart Nation

[12] TS-0003 OneM2M technical specification – Security solutions