TECHNICAL CODE

INTERNET OF THINGS - DEVICE SECURITY REQUIREMENTS

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

MCMC MTSFB TC GXXX:2023

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact, Cyber 663000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : (+603) 8680 9950
Fax : (+603) 8680 9940
Email : admin@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Internet of Things Security Sub Working Group supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB), constitute by representatives from the following organisations:

Celcom Axiata Berhad

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

SIRIM Berhad

Telekom Malaysia Berhad

Universiti Kuala Lumpur

Foreword

This technical code for Internet of Things - Application Security Requirements ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INTERNET OF THINGS - DEVICE SECURITY REQUIREMENTS

0. Introduction

Devices are the endpoints of the Internet of Things (IoT) ecosystem. Data from IoT Analytics State of IoT report 2022 show that there are 12.2 billion active connected endpoints. The quantities are expected to grow and to be predicted in 2025, there will be approximatively 27 billion connected IoT devices.

1. Scope

This Technical Code provides the IoT device security requirements covering the endpoint and gateway areas illustrated in Figure 1 which is based on the IoT high level reference model stated in MCMC MTSFB TC G013.

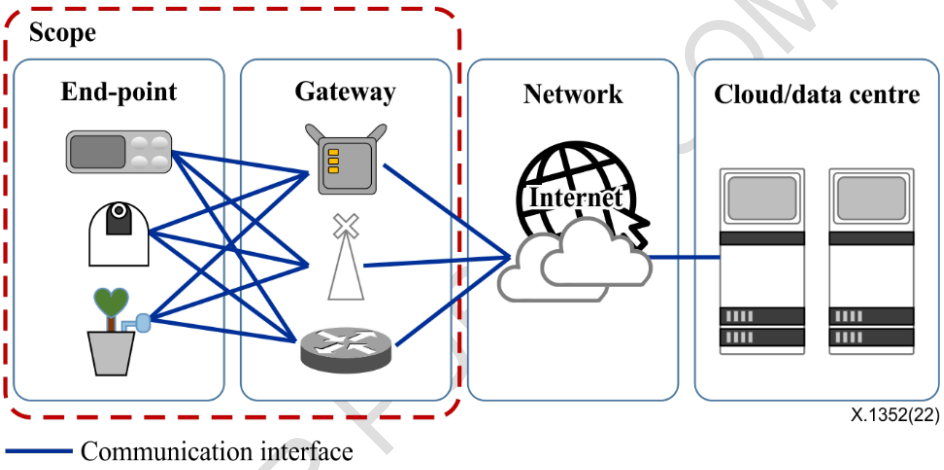

Figure 1. Scope of security requirements

Five (5) security dimensions applicable under this scope are:

a) authentication;

b) cryptography;

c) data security;

d) device platform security; and

e) physical security.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

Recommendation ITU-T X.1352, *Security requirements for Internet of things devices and gateways*

Recommendation ITU-T X.1361, *Security framework for the Internet of things based on the gateway model*

Recommendation ITU-T Y.4100, *Common requirements of the Internet of things*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

API	Application Programming Interface
CoAP	Constrained Application Protocol
DoS	Denial of Service
FTP	File Transfer Protocol
I/O	Input/Output
ID	Identifier
IoT	Internet of Things
JTAG	Joint Test Action Group
LwM2M	Lightweight Machine-to-Machine
MCU	Microcontroller Unit
MQTT	Message Queuing Telemetry Transport
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
SD	Secure Digital
SNMP	Simple Network Management Protocol
SSA	Shoulder-Surfing Attack
ST-D	Security Threat - Device

ST-G	Security Threat - Gateway
SWD	Serial Wire Debug
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver/Transmitter
UID	Unique Identifier
UPnP	Universal Plug and Play
USB	Universal Serial Bus

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Internet of Things (IoT) devices

An IoT device and gateway are commonly composed of a Microcontroller Unit (MCU), communication module, memory modules and Input/Output (I/O) peripherals.

A secure element exists as a form of hardware or software. In an MCU, there are firmware, physical interfaces and memory. In this context, the software with an Operating System (OS) can be replaced by firmware.

The communication module requires cryptography for data security on transmission. Data in flash memories is stored securely for authentication, cryptography and data confidentiality/integrity.

Access through physical interfaces like a Universal Asynchronous Receiver/Transmitter (UART) also demands user authentication. Unused hardware interfaces shall be removed or switched off.

Figure 2 illustrate the five (5) security dimensions applicable to IoT device and gateway.

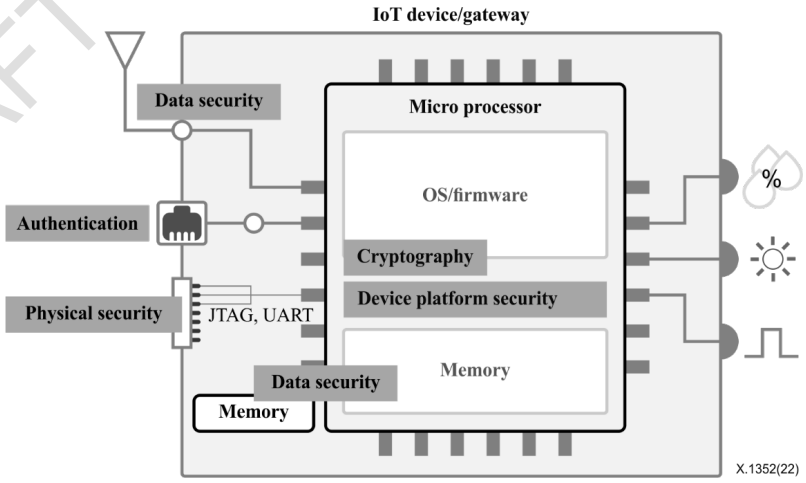

Figure 2. Example for applied security dimensions on IoT devices and gateways

4.1.1 Sensors and actuators

Sensor functions as input devices that gather information about their environment and its context, which will be subsequently processed. In contrast, actuators serve as output units, they act based on the processed information and executing decisions. In most IoT deployments, sensors and actuators are not only found standalone, but also integrated into embedded systems.

Sensors and actuators are the fundamental elements of IoT which may be connected to the cloud backend through gateways to have the data coming from the sensors processed, in order to make a decision.

4.1.2 Gateway

An IoT gateway is a physical device or software program that serves as the connection point between the cloud and controllers, sensors as well as intelligent devices. All data moving between IoT devices, and the cloud passes through an IoT gateway, which can be either a dedicated hardware appliance or software program. An IoT gateway might also be referred to as an intelligent gateway.

An IoT gateway acts as a network router, routing data between IoT devices and the cloud. Early on, most gateway devices only sent traffic in one direction: from the IoT devices to the cloud. Now, it's common for a gateway device to handle both inbound and outbound traffic.

4.2 Internet of Things (IoT) high level reference model

The IoT high level reference model defined in MCMC MTSFB TC G013, includes the following four (4) main layers (see Figure 3).

a) Device layer represents an object that has a specific identifier, with sensors and/or actuators.

b) Network layer represents the communication capabilities.

c) Service and application support layer represent the cloud platform, backend and services.

d) Application layer represents use cases.

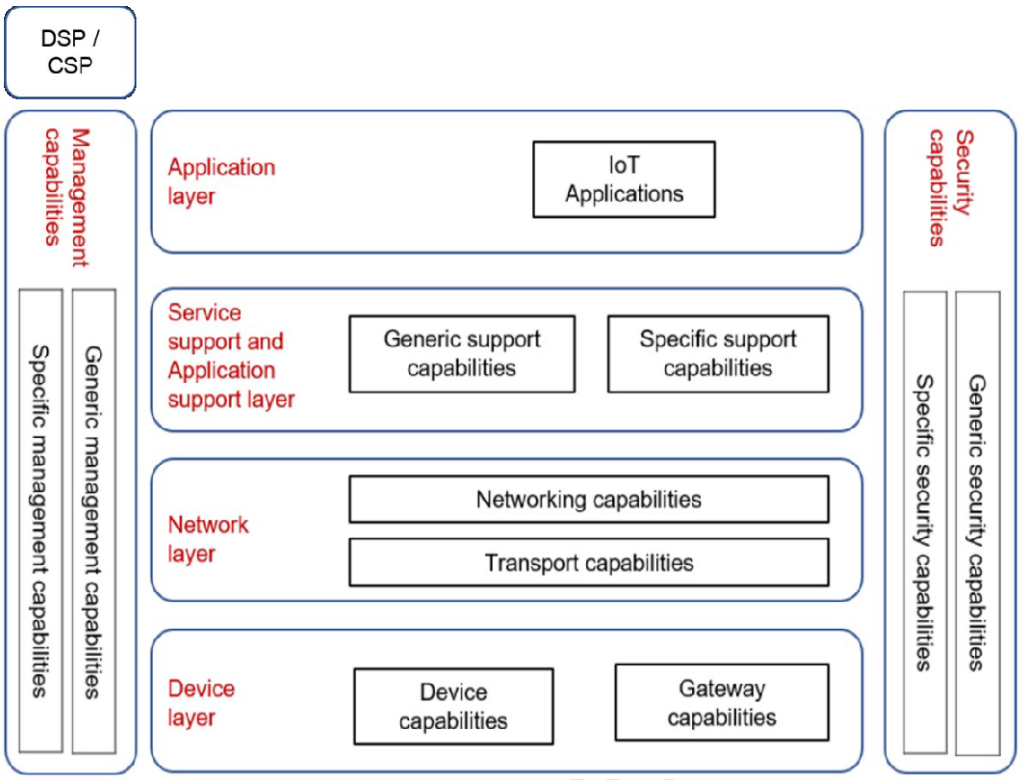

Figure 3. IoT high level reference model

5. Internet of Things (IoT) device security threats

Security threats/vulnerabilities to IoT sensors/devices and gateways, which may make them possible targets for cyber-attacks, are described in 5.1 and 5.2. Security threats to gateways include threats to IoT devices.

Security threats/vulnerabilities to IoT sensors/devices

Device-specific threats/vulnerabilities include the following:

Table 1. IoT device security threats

Code	Security threats/vulnerabilities	Descriptions
ST-D-1	Authentication bypass	An unauthorised user gains access to a device, and is also able to access critical data, including user data and configuration files stored in the device.
ST-D-2	Unauthorised device connection	A device is exposed to any unauthorised device, or its data such as user data can be transmitted to any unauthorised device.

Table 1. IoT device security threats *(continued)*

Code	Security threats/vulnerabilities	Descriptions
ST-D-3	Excessive privilege	Giving excessive privilege or unnecessary privilege allows an attacker to be able to access all acceptable operations and controlled data including the user data of a device.
ST-D-4	Unrestricted repeated authentication attempts	An unauthorised user who repeats authentication attempts may gain access to a genuine user account.
ST-D-5	Error due to concurrent access	A concurrent access from multiple administrator accounts may cause uncoordinated changes in the configuration of critical functionalities.
ST-D-6	Authentication information exposure and guessing	When authentication information such as a password is hard coded or stored in plain text, or when an authentication password or Personal Identification Number (PIN) is exposed in plain text (also known as a Shoulder-Surfing Attack (SSA)), the authentication information may be exposed to or guessed by an attacker.
ST-D-7	Weak password	An attacker may obtain an unsecured combination, e.g., involving a default or weak password, that may allow the attacker to pose as a genuine user.
ST-D-8	Weak encryption key/random number	An insufficient cryptographic key or predictable “random” number may not be able to protect critical data.
ST-D-9	Weak cryptographic algorithm	An attacker may predict key data or discover the plain text of an encrypted message (ciphertext) by analysing traffic that uses a weak cryptographic algorithm.
ST-D-10	Absence of input validation	An absence of input validation may cause a device to malfunction.
ST-D-11	Data exposure and data manipulation	Critical data, such as user data, device configuration and cryptographic keys, that is transmitted via or stored on a device may be exposed to, exploited or manipulated by an attacker.
ST-D-12	Session hijacking	An attacker may gain unauthorised access to a device which session was closed abnormally or exploit valid sessions of multiple devices that use the same cryptographic key.
ST-D-13	Unsafe update	An intended update file is not downloadable or a manipulated update file whose source is unauthorised/unauthenticated may be executable.
ST-D-14	Update failure	An error that occurred during an update may cause abnormal device operation.
ST-D-15	Integrity error	An unintended manipulation of executable codes or configuration values may cause a device to malfunction.
ST-D-16	Malicious Software	Code that has unintended functions may be used with a malicious purpose.
ST-D-17	Residual memory information exploitation	The cryptographic key, password and sensitive data used for cryptological operations, authentications and data transmissions remain in the memory and may be exploited.
ST-D-18	Unintended change in critical configurations	An absence of device security controls may cause unintended changes in critical configurations and unsafe service deliveries.
ST-D-19	Unsafe error response	An absence of appropriate detection of and response to errors and malicious behaviour of a device may cause unsafe service deliveries.
ST-D-20	Unsafe development	Potential security vulnerabilities may originate from the design and implementation of a device, and an assessment of and response to them during the testing process may be absent or inappropriate.

Table 1. IoT device security threats *(continued)*

Code	Security threats/vulnerabilities	Descriptions
ST-D-21	Vulnerable OS	Device functionalities may be compromised or bypassed in a vulnerable OS environment.
ST-D-22	Vulnerable third-party modules or libraries	Vulnerable third-party modules or libraries may allow an attacker to call those at risk.
ST-D-23	Unsecured sensitive information record in system log	Sensitive information recorded in a system log may be exposed to and exploited by an attacker.
ST-D-24	Critical information exposure through debugging	Critical information may be exposed to and exploited by an attacker through log generation and debugging when a device is released and distributed.
ST-D-25	Unauthorised physical access	A device is exposed to unauthorised physical access and unintended changes in its configuration.
ST-D-26	Device capture	Refers to a device being physically compromised within device lifecycle (manufacturing, distribution, installation and post-installation) or having its keys lost.
ST-D-27	Impersonating of sensor/device	This attack happens when an attacker successfully masquerades as the identity of a legitimate sensor/device.
ST-D-28	Replay attack	This attack happens when attacker intercepting and recording a legitimate communication between device and gateway, and successfully gained legitimate response by replaying the recorded communication.
ST-D-29	Untrusted data transmission	An untrusted data transmission may cause a device to malfunction or malicious code to be distributed.

5.1 Security threats to IoT gateways

Gateway-specific threats/vulnerabilities include the following:

Table 2. IoT gateways security threats

Code	Security threats/vulnerabilities	Descriptions
ST-G-1	Denial of Service (DoS) attack	The DoS attack causes a target to significantly slow down or, ideally, stop the services it provides by exhausting the target's memory and/or computing capacity. Targets are kept busy responding to the illegitimate traffic that attackers are sending. The wireless sensor network is particularly vulnerable to DoS attacks due to its features of an open medium, dynamic changing topology, and the lack of a clear line of defence. DoS attacks are a growing problem in networks today. Many of the defence techniques developed for fixed wired network are not applicable to mobile network environments.
ST-G-2	Unauthorised access	Unauthorised access to a gateway can cause the disclosure of sensitive information, data modification, DoS and illicit use of resources. For example, once an attacker has accessed a gateway, monitoring of the now unencrypted data can result in usernames, passwords, location information and secure configuration data being compromised.

Table 2. IoT gateways security threats *(concluded)*

Code	Security threats/vulnerabilities	Descriptions
ST-G-3	Rogue gateway	A rogue wireless access point may deliberately and covertly be installed in order to grant easy access to a perpetrator on the network either locally or remotely. A perpetrator (known as an 'evil twin') could replace an existing wireless access point with one on which they have full configuration and monitoring access or even configure a rogue wireless access point, with similar settings, but with a higher power ratio necessary to overcome the legitimate wireless access point's signal. Once a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be gathered.

6. Security requirements

Based on the security capabilities proposed in ITU-T X.1361 and ITU-T Y.4100, the security requirements to address the challenges and threats of IoT devices and gateways (excluding network systems and platforms) are specified for five (5) security dimensions, namely:

6.1 Authentication

The authentication in IoT devices comprise of the following:

6.1.1 User authentication

Table 3. User authentication security requirements

Code	Controls	Descriptions
AU-1-1	Password shall be changed timely.	At the initial authentication, a password must be created or changed. Ensure that the password is distinct from the initial or previous value.
AU-1-2	A user shall first be identified and authenticated when security management or sensitive data are accessed.	The user must be identified and authenticated when attempting to access security management, such as configuring an IoT device, user account, or privilege. Users with privileged access to security management or sensitive data must be managed independently of regular users.
AU-1-3	The number of authentication attempts shall be limited.	An IoT device may be vulnerable to brute force attacks if repeated authentication attempts are permitted. As a result, it must include a feature for appropriately responding to continuous authentication attempts. This function can be provided using one of the following methods: limiting the number of authentications attempts to lock the account or deactivate the authentication function for a certain period of time.
AU-1-4	Unique pre-installed password.	The pre-installed password of the device should be unique.
AU-1-5	A function to manage user accounts and privileges should be provided.	All user accounts (including the administrator account) used on an IoT device should be manageable, including their addition and removal, as well as privilege assignment. If a role-based access control model is used, clearly specify the access privileges for all IoT device functions and assign them accordingly.

Table 3. User authentication security requirements *(continued)*

Code	Controls	Descriptions
AU-1-6	Least privilege.	The principle of least privilege should be applied to all user accounts.
AU-1-7	Concurrent access to the administrator account should be restricted.	Concurrent access to management services should be limited to the same administrator account, and a function to disconnect previous access or limit new access attempts should be provided.
AU-1-8	A secure password complexity should be provided.	IoT devices should allow the user to set a secure password that takes into account; length, character variations, and avoid repetitive and sequence characters.
AU-1-9	Certificate-based authentication	Using digital certificates is a more secure method for verifying the identity of a device and establishing a secure connection. However, it requires more complex implementation and operation compared to password-based authentication, which may not suit to all business use cases.
AU-1-10	Certificate lifecycle management	Carefully manage digital certificates and provide a secure and reliable means to update a digital certificate and its certificate chain on a device before it expires. Additionally, a certificate used to identify a device should be unique and only used to identify that one device to prevent reuse of the certificate across multiple devices.

6.1.2 Secure use of authentication credentials

Table 4. Authentication credentials security requirements

Code	Controls	Descriptions
AU-2-1	Hard-coded credentials should not be used.	Password should be neither hard coded nor stored in plain text.
AU-2-2	During authentication by password the password should be masked.	If a password is displayed in plain text, it may be vulnerable to an SSA.
AU-2-3	Error handling.	No specific feedback for authentication failure should be provided.

6.1.3 Device authentication

Table 5. Device authentication security requirements

Code	Controls	Descriptions
AU-3-1	The Unique Identifier (UID) of each hardware device shall be retained.	The IoT device shall have an Identifier (ID) that is unique and fixed.

Table 5. Device authentication security requirements *(continued)*

Code	Controls	Descriptions
AU-3-2	Mutual authentication.	Devices should be mutually authenticated before sensitive data is transmitted or the devices are interconnected for control purposes. Mutual authentication examples are as follows: a) use of a private key based on the public key encryption method; b) use of security attributes (UID, key, etc.) and security chips; c) application of Transport Layer Security (TLS) (or datagram TLS) to the light communication protocol, i.e., Constrained Application Protocol (CoAP), Lightweight Machine-to-Machine (LwM2M) protocol, or Message Queuing Telemetry Transport (MQTT).

6.2 Cryptography

If it is difficult to use general cryptographic algorithms due to limited memory and storage capacity, suitable cryptography algorithms shall be used.

Table 6. Cryptography requirements

Code	Controls	Descriptions
CR-1-1	Industry standard cryptography.	Cryptographic algorithms to protect against side-channel attacks should be used. Ensure cryptographic key methodology generates sufficient randomness.
CR-1-2	Key management.	Cryptographic keys shall be securely managed throughout their entire lifecycle. Keys should be generated, updated, distributed, used, stored and destroyed in a secure way.
CR-1-3	Unique cryptographic keys.	To prevent compromise, it is best to use each cryptographic key for only one purpose. For example, data encryption keys should be used exclusively for encrypted data, while keys used to secure passwords should be different. Do not mix keys or key pairs between uses for encryption and authentication. Each key should have a unique use, including the unique key for each IoT device.

6.3 Data security

The data security dimension is composed of transmission data protection and data protection in rest, information flow control, secure session management and PII protection.

6.3.1 Secure transmission and storage

Table 7. Transmission and storage security requirements

Code	Controls	Descriptions
DS-1-1	Data transmitted shall be encrypted.	Data transmitted shall be encrypted using a secure cryptographic algorithm (see CR-1-1).
DS-1-2	A secure mode should be applied when a data or control channel is created.	When data is transmitted, a security protocol should be used, ensuring the confidentiality and integrity of the transmitted data, as well as authenticating source and destination parties.

Table 7. Transmission and storage security requirements *(continued)*

Code	Controls	Descriptions
DS-1-3	Data stored in devices should be encrypted.	Data storage devices shall be encrypted using a secure cryptographic algorithm (see CR-1-1).
DS-1-4	Deleted data should not be restored.	A secure erase capability is required to ensure data cannot be recovered.
DS-1-5	Secure reset recovered and scraped devices.	Perform secure data deletion prior storage of recovered devices and pre-disposal of scraped devices (see DS-1-4).

6.3.2 Information flow control

Table 8. Information flow control security requirements

Code	Controls	Descriptions
DS-2-1	Unauthorised network traffic should not be allowed.	Network segregation principle should be applied.

6.3.3 Secure session management

Table 9. Session management security requirements

Code	Controls	Descriptions
DS-3-1	The session should be terminated after idle time-outs.	If accessing again after session termination, re-authentication should be conducted.
DS-3-2	The session ID should be an unpredictable value.	A secure random number algorithm should be applied to session ID generation. During each session authentication, the session ID should be changed and used session IDs should be destroyed.

6.3.4 PII management

Table 10. PII management security requirements

Code	Controls	Descriptions
DS-4-1	Personally Identifiable Information (PII) data shall be securely managed.	PII data shall be encrypted and enforced with authentication prior access (see DS-1-2 and DS-1-3).

6.4 Device platform security

In the device platform security dimension, there are five (5) items: software security; secure update; security management; logging; and timestamp.

6.4.1 Software security

Table 11. Platform software security requirements

Code	Controls	Descriptions
PL-1-1	Secure coding should be applied.	Software should be designed and implemented with consideration of security.
PL-1-2	Known security vulnerabilities shall be checked and removed.	If the software was developed using protocols, libraries, an Application Programming Interface (API), packages or open sources containing known security vulnerabilities, the firmware and OS may also have them. The public domain of known security vulnerabilities shall be used to check the security vulnerabilities of the device and remove them.
PL-1-3	Obfuscation should be applied.	These requirements can be applied mostly to developed apps (applications), which facilitates source code restoration. Since open reverse engineering tools can be used to extract important logic or key information, an appropriate level of protection is in order.
PL-1-4	An integrity verification function for configuration parameters and executable codes should be supported.	To ensure the validity of IoT devices, the integrity of configuration parameters and executable codes should be checked for booting time, periodically in automatic mode or manually. An appropriate response is carried out in the case of integrity error.

6.4.2 Secure update

Table 12. Secure update requirements

Code	Controls	Descriptions
PL-2-1	The update shall be conducted by authorised users.	Only assigned role can perform the update. The authenticity of a user can be confirmed by re-authenticating the user immediately prior to the update procedure.
PL-2-2	The rollback function should be supported if the update fails.	To reinstate the previous security and working condition of the device.
PL-2-3	Integrity should be checked prior to an update.	Checking the integrity and authenticity of update files can be done by verifying a cryptographic digital signature

6.4.3 Security management

Table 13. Security management requirement

Code	Controls	Descriptions
PL-3-1	Unnecessary services should be disabled.	Unnecessary services (Telnet, File Transfer Protocol (FTP), Universal Plug and Play (UPnP), Simple Network Management Protocol (SNMP), etc.) should be disabled and the necessary services provided by the device should be specified.
PL-3-2	Remote management.	Remote management should be done in a reliable environment using a secure protocol.

PL-3-3	A secure third-party library should be applied.	The third-party library and module used for development should be the latest version, without any known security vulnerabilities or defects.
PL-3-4	A self-test should be provided.	A self-test function for detecting errors of the main hardware and software when an IoT device is being powered up should be provided.

6.4.4 Logging

Table 14. Logging security requirements

Code	Controls	Descriptions
PL-4-1	Logging should be generated for security-related events.	The logging should be implemented, and it should be possible to detect and trace any abnormal device behaviour.
PL-4-2	A secure logging mechanism should be provided.	The logging mechanism shall provide protection against loss and unauthorised changes. Log forwarding may be required to retain the logs at remote location.
PL-4-3	Timestamp.	Reliable timestamp source shall be provided.

6.5 Physical security

The physical security dimension involves securing physical interfaces and protecting IoT devices against tampering.

6.5.1 Secure physical interface

Table 15. Physical interface security requirements

Code	Controls	Descriptions
PH-1-1	Any unnecessary external interface should be deactivated.	Some of the external interfaces may be used during the development and no longer required in production. The dimensions and functions of all external interfaces (local area network, Universal Serial Bus (USB), Secure Digital (SD) card port, etc.) exposed to the outside should be specified. If necessary, access should be controlled by software to prevent unauthorised access.
PH-1-2	Unauthorised access to the internal interface shall be prevented.	The dimensions and functions of all internal interfaces (Joint Test Action Group (JTAG), Serial Wire Debug (SWD), UART, etc.) exposed to the outside shall be specified. If necessary, access control shall be conducted to prevent unauthorised access.

6.5.2 Tamper-proofing

Table 16. Tamper-proofing security requirement

Code	Controls	Descriptions
PH-2-1	Detection and response functions are required.	Unauthorised physical manipulation should be detected with the appropriate countermeasures (e.g., tamper-evident seals, locks, tamper response, zeroization switches and alarms).

Annex A
(informative)

IoT device security requirements versus IoT device security threats

A.1 User authentication

Table A.1. User authentication controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
AU-1-1	Password shall be changed timely.	ST-D-6 ST-D-7	ST-G-2
AU-1-2	A user shall first be identified and authenticated when security management or sensitive data are accessed.	ST-D-3 ST-D-6 ST-D-7 ST-D-12 ST-D-27	ST-G-2
AU-1-3	The number of authentication attempts shall be limited.	ST-D-4 ST-D-5	NA
AU-1-4	Unique pre-installed password.	ST-D-6 ST-D-7	NA
AU-1-5	A function to manage user accounts and privileges should be provided.	ST-D-3	ST-G-2
AU-1-6	Least privilege.	ST-D-3	ST-G-2
AU-1-7	Concurrent access to the administrator account should be restricted.	ST-D-5	NA
AU-1-8	A secure password complexity should be provided.	ST-D-6 ST-D-7	ST-G-2
AU-1-9	Certificate-based authentication.	ST-D-2 ST-D-7 ST-D-12 ST-D-27	ST-G-2
AU-1-10	Certificate lifecycle management.	ST-D-2 ST-D-7 ST-D-12 ST-D-27	ST-G-2

A.1.1 Secure use of authentication credentials

Table A.2. Authentication credentials controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
AU-2-1	Hard-coded credentials should not be used.	ST-D-11 ST-D-17 ST-D-20 ST-D-26	NA
AU-2-2	During authentication by password the password should be masked.	ST-D-6 ST-D-7 ST-D-8	NA
AU-2-3	Error handling.	ST-D-11 ST-D-19 ST-D-20 ST-D-24	NA

A.1.2 Device authentication

Table A.3. Device authentication controls versus threats

Code	Controls	Threats Mapping	
		ST-D-X	ST-G-X
AU-3-1	The UID of each hardware device shall be retained.	ST-D-6 ST-D-12 ST-D-27 ST-D-28 ST-D-29	NA
AU-3-2	Mutual authentication.	ST-D-2 ST-D-12 ST-D-20 ST-D-27 ST-D-28 ST-D-29	ST-G-2 ST-G-3

A.2 Cryptography

Table A.4. Cryptography controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
CR-1-1	Industry standard cryptography.	ST-D-8 ST-D-9 ST-D-13 ST-D-15 ST-D-17 ST-D-18	NA
CR-1-2	Key management.		NA
CR-1-3	Unique cryptographic keys.		NA

A.3 Data security

A.3.1 Secure transmission and storage

Table A.5. Secure transmission and storage controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-1-1	Data transmitted shall be encrypted.	ST-D-7 ST-D-11 ST-D-13 ST-D-29	NA
DS-1-2	A secure mode should be applied when a data or control channel is created.	ST-D-11 ST-D-13 ST-D-29	NA
DS-1-3	Data stored in devices should be encrypted.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2.
DS-1-4	Deleted data should not be restored.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2
DS-1-5	Secure reset recovered and scraped devices.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2

A.3.2 Information flow control

Table A.6. Information flow controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-2-1	Unauthorised network traffic should not be allowed.	ST-D-2 ST-D-26 ST-D-27 ST-D-29	ST-G-3

A.3.3 Secure session management

Table A.7. Secure session management controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-3-1	The session should be terminated after idle time-outs.	ST-D-12 ST-D-28	NA
DS-3-2	The session ID should be an unpredictable value.	ST-D-1 ST-D-12 ST-D-28	NA

A.3.4 PII management

Table A.8. PII management controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-4-1	PII data shall be securely managed.	ST-D-6. ST-D-11. ST-D-24.	NA

A.4 Device platform security

A.4.1 Software security

Table A.9. Platform software security controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-1-1	Secure coding should be applied.	ST-D-1 ST-D-5 ST-D-10 ST-D-12 ST-D-15 ST-D-16 ST-D-19 ST-D-20 ST-D-21 ST-D-22 ST-D-23 ST-D-24	NA
PL-1-2	Known security vulnerabilities shall be checked and removed.	ST-D-16 ST-D-21 ST-D-22	NA
PL-1-3	Obfuscation should be applied.	ST-D-15 ST-D-16	NA
PL-1-4	An integrity verification function for configuration parameters and executable codes should be supported.	ST-D-13 ST-D-14 ST-D-15 ST-D-16	NA

A.4.2 Secure update

Table A.10. Secure update controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-2-1	The update shall be conducted by authorised users.	ST-D-13 ST-D-16 ST-D-25	NA
PL-2-2	The rollback function should be supported if the update fails.	ST-D-14	NA
PL-2-3	Integrity should be checked prior to an update.	ST-D-13 ST-D-14 ST-D-16	NA

A.4.3 Security management

Table A.11. Security management controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-3-1	Unnecessary services should be disabled.	ST-D-2 ST-D-11 ST-D-22	ST-G-1
PL-3-2	Remote management.	ST-D-26	NA
PL-3-3	A secure third-party library should be applied.	ST-D-16 ST-D-22	NA
PL-3-4	A self-test should be provided.	ST-D-14 ST-D-15 ST-D-16 ST-D-26	NA

A.4.4 Logging

Table A.12. Logging controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-4-1	Logging should be generated for security-related events.	ST-D-23 ST-D-24 ST-D-25 ST-D-27 ST-D-29	ST-G-2
PL-4-2	A secure logging mechanism should be provided.		
PL-4-3	Timestamp.		

A.5 Physical security

A.5.1 Secure physical interface

Table A.13. Secure physical interface controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PH-1-1	Any unnecessary external interface should be deactivated.	ST-D-25 ST-D-26	NA
PH-1-2	Unauthorised access to the internal interface shall be prevented.	ST-D-1 ST-D-2 ST-D-25 ST-D-26	NA

A.5.2 Tamper-proofing

Table A.14. Tamper-proofing controls versus threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PH-2-1	Detection and response functions are required.	ST-D-25 ST-D-26	NA

Bibliography

[1] IoT Analytics, *State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally*
https://iot-analytics.com/number-connected-iot-devices/

Acknowledgements

Members of Internet of Things Security Sub Working Group

Prof Dr Shahrulniza Musa (Chair)	Universiti Kuala Lumpur
Dr Ahmad Shahrafidz Khalid (Vice Chair/Draft lead)	Universiti Kuala Lumpur
Mr Khairul Ekhwan Kamarudin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohd Ridhwan Mohd Salleh	Celcom Axiata Berhad
Ms Mayasarah Maslizan	CyberSecurity Malaysia
Ms Norkhadhra Nawawi	FNS (M) Sdn Bhd
Mr Hassen Abdelhamid Elberkennou	Maxis Broadband Sdn Bhd
Mr Ahmad Amzar Hanis Ahmad Zaki	SIRIM Berhad
Mr Muhamad Hasyimi Shaharuddin	Telekom Malaysia Berhad

MALAYSIAN TECHNICAL STANDARDS FORUM BHD

Malaysian Communications & Multimedia Commission (MCMC Old Building)
Off Persiaran Multimedia, Jalan Impact
63000 Cyberjaya,
Selangor Darul Ehsan

Tel: (+603) 8320 0300
Fax: (+603) 8322 0115
Website: www.mtsfb.org.my