IoT
Security Best Practice Guidelines

January 2020

hkpc 生產力局

HKCERT

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC) reserve the right to amend the document from time to time without prior notice.

While we have made every attempt to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader’s own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Licence

Table of Contents

1. Executive Summary

The adoption of Internet of Things (IoT) technology is a growing trend in various sectors. Startups, small and medium-sized enterprises (SMEs), and other enterprises have started adopting IoT technology to create business values for their products and bring about new customer experience. As focus remains on the functions and features that IoT technology brings, not many people fully understand the accompanying potential security risks.

This document aims to facilitate developers to incorporate IoT security best practices early at the design stage. And, it provides verification checklists for developers to perform self-verification on their IoT solutions in order to raise the security awareness of IoT technology.

An IoT architecture model is proposed to illustrate the composition of IoT solutions. It consists of four layers, namely the perception layer, network layer, management layer, and application layer. IoT-related security issues, best practices and verification items are discussed pertinent to each layer and presented in tables for ease of reference.

This document enables developers to first be aware of various security issues raised at each layer; second, to understand the associated best practices while developing IoT solutions; and, finally, to conduct self-verification to verify their IoT solutions according to the verification checklists. In the long run, it is hoped that developers would incorporate IoT security into their development cycles.

2. Introduction

2.1 Overview

Put simply, the Internet of Things (IoT) technology uses network connectivity (e.g. Internet) to interconnect various physical devices to collect, exchange, process, and react to the data around the physical world. It ushers a new era of innovation and business opportunities that yields benefits in terms of efficiency, business growth, and quality of life.

However, new cyber security threats also arise from IoT technology as attackers from time to time have been seeking to exploit vulnerabilities in IoT devices. One famous DDoS attack from infected IoT devices was the Mirai Botnet which brought down the domain registration services provider, Dyn, in October 2016.

To better preserve IoT security, developers are encouraged to get involved and adopt the best practices at the early stage of product design. Besides, developers should go through the self-verification checklists to verify the security level at the testing stage.

2.2 Objectives

The objectives of this document are as follows:

- To raise the security awareness of IoT technology;
- To give developers a basic understanding on common security issues with IoT solutions;
- To facilitate developers to incorporate IoT security best practices at the design stage; and
- To provide verification checklists for developers to perform self-verification on their IoT solutions.

2.3. Scope

The scope of this document mainly focuses on common security issues that HKCERT has observed with regard to IoT solutions, as well as proposes feasible and essential best practices for improving the IoT security. As the scope is not aimed at providing a holistic security framework on IoT security, this document cannot be served as a bulletproof security baseline. Yet, it serves the purpose of attaining a certain level of security controls that would reduce common security risks.

2.4. Target audience

The target audience of this document is developers, who take part in the following areas:

- IoT hardware design
- IoT software / firmware development
- Use of wireless technologies
- IT related infrastructure supporting IoT solutions
- IT application development supporting IoT solutions
- Mobile app development supporting IoT solutions
- IoT architecture and solution development

Besides, this document may also benefit other audiences including:

- Business drivers who are sourcing for different IoT solutions
- Business owners who adopt IoT technology in businesses
- Academics who teach topics related to IoT technology (e.g. STEM education)
- General public who are users of IoT related solutions

3. Methodology

This study was carried out in five stages.

1. Scope definition
   The scope definition involves defining the scope, objectives, target audience, key elements of the document and the study.

2. Desktop research
   The desktop research involves identifying existing publications and information on the topics related to the objectives of the study, which will serve as supporting materials for analysis and formulation of the best practice guidelines. The list of reference publications can be referred in the Appendix.

3. IoT security testing
   The IoT security testing involves identifying the common IoT security issues from the security tests on various technologies used in IoT solutions.

4. Analysis and development
   Analysis and development stage involves analysing the results collected from the desktop research and IoT security tests. Common security issues were then identified and categorised into a proposed IoT architecture model for formulating the best practice guidelines.

5. Report write-up and validation
   The report write-up and validation stage involves synthesising related information to form the report structure. The report was validated according to the publication policy.

4. IoT Security Best Practice Guidelines

4.1 IoT Architectural Model

Layered Structure of IoT solution

In general, several layers composite a complete IoT solution. It can be depicted in the below model with a basic four-layer architecture which shows cross-cutting security across all layers (see figure 1).

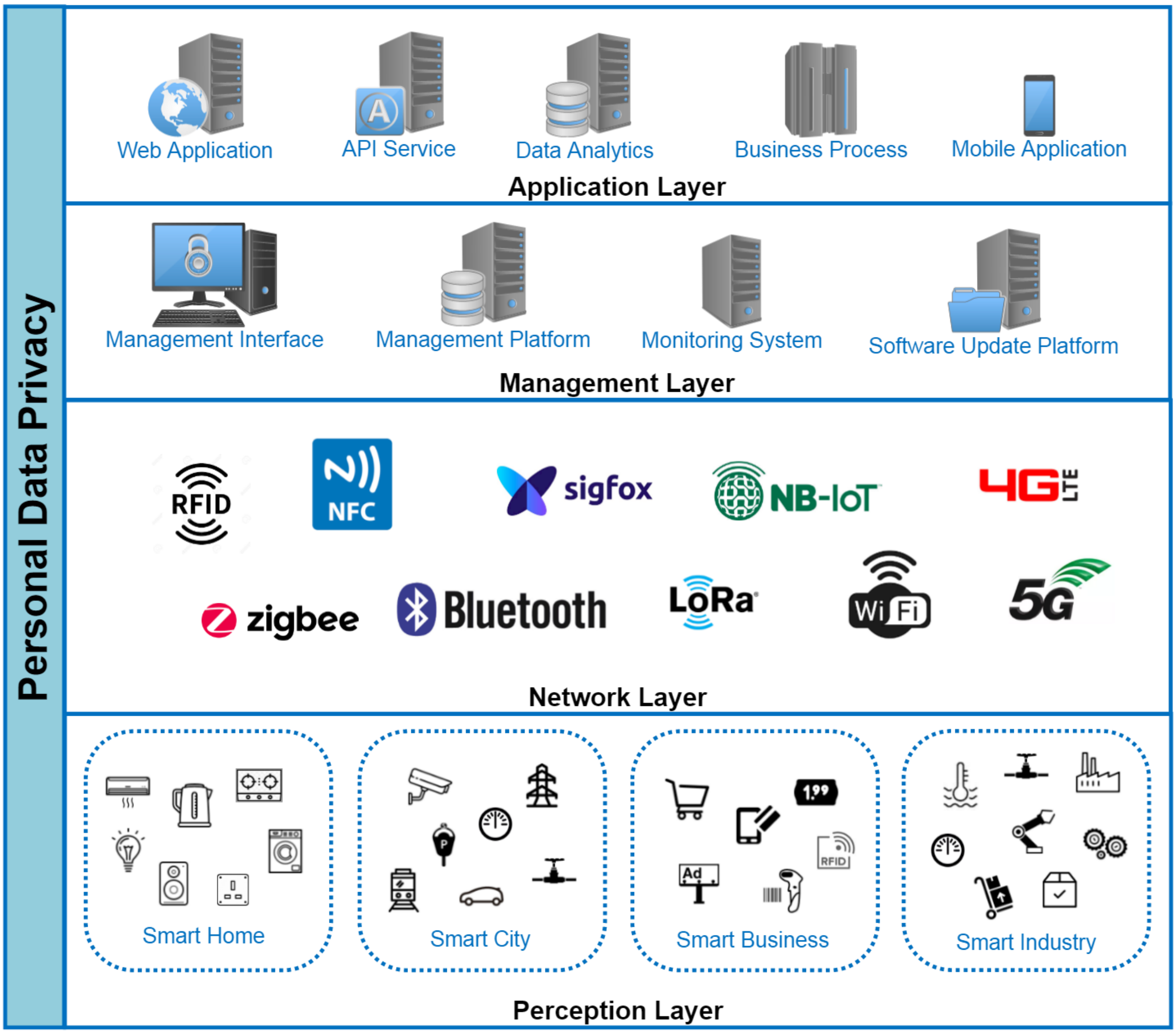

Figure 1: IoT Layered Architecture Model

Application Layer

Application layer is responsible for delivering application services. In general, this layer consists of web application, API service, data analytics, business process and mobile application. Users mainly interact with this layer through the web application and mobile application. This layer also handles all application data processing, analytics, and storage. Some IoT solutions may also integrate with their corporate IT infrastructure for other business workflow processes, big data and AI modelling.

Management Layer

Management layer is used for managing the IoT services. In general, this layer consists of management platform, monitoring system and software update platform. IoT solution providers interact with this layer through the management interface to manage the lifecycle of the IoT devices. For example, this layer manages the provision, deployment, monitoring, software update, and disposal of IoT devices.

Network Layer

Network layer is responsible for network connectivity for IoT devices, network devices, and servers. This layer handles data transmission between IoT devices, mobile phones that runs over the mobile application and backend servers. This layer involves different network technologies including short range device to device wireless connectivity (e.g. RFID, NFC, zigbee, Bluetooth, etc.), long range device to carrier gateway wireless connectivity (e.g. Sigfox, NB-IoT, LoRa, etc.), wireless Internet connectivity (e.g. WiFi) and cellular network connectivity (e.g. 4G and 5G).

Perception Layer

Perception layer is the physical layer where IoT devices reside. IoT devices interact with the physical world through different sensors to collect different physical measurements (e.g. temperature, air quality, speed, humidity, pressure, flow, movement, electricity, etc.). IoT devices would also have some sort of kinetic interaction with the physical world through actuator, motors, robotics, etc. Depending on the capability of IoT devices, some IoT devices may not be capable of supporting Internet Protocol (IP) to connect the Internet directly. In this case, IoT gateways are used to act as the network bridge between the IoT devices and the Internet.

Personal Data Privacy

The personal data privacy cuts across all the above four layers. It covers various security issues arising from each layer and the necessary solutions to mitigate the risks.

4.2 Best Practices and Verification Checklists

4.2.1 Personal Data Privacy

The following best practices are applicable to all layers.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.1.1 Personal Data Privacy Security	➢ For handling of personal data, security protections are critical. Failure to comply with related regulations on personal data privacy could result in legal liability.	✓ The solution should observe the Personal Data (Privacy) Ordinance[1] in collection, retention, use and security of personal data. ✓ The solution should provide clear explanation to end users on its policy and practice in handling all personal data throughout the data processing lifecycle (i.e. privacy policy), such as what kinds of personal data will be collected, the purposes of collection, the potential transferees of the personal data and the security measures adopted to protect the personal data. ✓ The solution should protect the personal data collected by taking all reasonably practicable security measures, such as using encryption at	□ Personal data is collected, retained, used and protected in compliance with the Personal Data (Privacy) Ordinance. □ Clear privacy policy is communicated to end-users. □ All reasonably practicable security measures have been implemented to protect personal data, including encryption of personal data at rest and in transit. □ Collection and retention of personal data is minimised. Only de-identified or anonymised data is stored if applicable. □ End users' consent is obtained for data collected beyond what is

[1] Personal Data (Privacy) Ordinance (https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html)

		rest and in transit, and other IoT security best practices recommended in this Guideline. ✓ The solution should minimise the collection and retention of personal data, and should only store and process de-identified or anonymised data if applicable. ✓ The solution should seek end users' consent for data collected beyond what is needed for proper operations of the device. ✓ The solution should seek end users' consent if personal data is to be used for purposes unrelated to the original core functions of the device, or for purposes not specified in its privacy policy communicated to end users. ✓ The solution should destroy or anonymise personal data when the data is no longer necessary for achieving the purposes communicated to or consented by end users. Note: The developer or business user of the device may make reference to ISO/IEC	needed for proper operations of the device. □ End users' consent is obtained before using personal data for purposes unrelated to the original core functions of the device, or for purposes not specified in its privacy policy communicated to end-users. □ Personal data that is no longer necessary is destroyed or anonymised.

		27701:2019 for security techniques for privacy information management[2].	

4.2.2 Application Layer

The following best practices are applicable to application layer.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.2.1 Authentication Security	➢ Authentication plays an important role in application security. Without authentication, your application will not be able to determine on the provision of application functionality and the authorisation of data access. As such, role-based access control is necessary to provide granular control on data access for each user. ➢ Other security measures, such as strong passwords, account lockout, two-factor authentication, etc., are essential to prevent account hijacking and identity theft. ➢ Default usernames and passwords can be obtained easily on the Internet. Changing them after setup can reduce the risk of unauthorised access.	✓ The solution should adopt strong password where authentication is needed. ✓ The solution should include role-based access control for multi-user environments. ✓ The solution should implement two-factor authentication where possible. ✓ The solution should provide secured password recovery mechanisms. ✓ The solution should support password expiration enforcement and periodic password change policy.	□ The solution only accepts strong password (e.g. at least 8 characters containing uppercase letters, lowercase letters, numbers and characters) where authentication is needed. □ Role-based access control is supported for multi-user environments. □ Two-factor authentication is supported (e.g. use of mobile authenticator, SMS verification). □ Password recovery mechanism is available and requires verification through registered email and/or mobile SMS verification code.

[2] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (https://www.iso.org/standard/71670.html)

Security Aspects	Security Issues	Best Practices	Verification Checklists
		✓ The solution should enforce mandatory default password change at initial setup stage. ✓ The solution should provide an option for changing privileged account username. ✓ The solution should support account lockout mechanism to prevent against brute force attack. ✓ The solution should have proper measures (e.g. CAPTCHA) to prevent account lockout DoS attack.	□ User is mandated to perform password change in case of password expiration. □ User is mandated to change default password at initial setup stage. □ Users have the option to change privileged account username to reduce security risks. □ Account is locked out when multiple incorrect password attempts were logged. □ Login requires CAPTCHA verification to prevent automated attacks.
4.2.2.2 Web Application Security	➢ Web application is considered a major attack surface that requires the implementation of effective security measures. Many web application standards have already been well-established. As such, it is advised to reference and check against those well-established web application security standards to ensure web application security.	✓ The web application should be checked against well-established web security standards. ✓ The web application should require user authentication (refer to the row “Authentication Security” for details). ✓ The web application should enable session timeout.	□ The web application is checked not vulnerable to common web application vulnerabilities (e.g. OWASP[3] Top 10 including cross-site scripting (XSS), SQL injection and Cross-site request forgery (CSRF), etc.). □ The web application requires user login for user authentication.

[3] OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

Security Aspects	Security Issues	Best Practices	Verification Checklists
	➢ Other security measures, such as session timeout, input validation, encryption, digital certificate authenticity, etc., are essential to web application security. ➢ As web attack tactics are ever-changing, using web application firewall is an effective way to protect the web application with up-to-date ruleset addressing web application vulnerabilities.	✓ All data input of web application should be validated before processing. ✓ The web application should use encryption to protect transmitted information. ✓ The web application should be protected by web application firewall.	□ The web application automatically logs out the user after the session has been idled for a period of time. □ The web application denies the input that contains invalid or malformed data (e.g. data generated by fuzzing tool). □ The web application uses encrypted HTTPS protocol only. □ The web application is protected by web application firewall (WAF) software component or network-based WAF.
4.2.2.3 Application Programming Interface (API) Security	➢ API service is supported by a backend web server that is subject to the same security risk as web application does. Web application standards also apply to API services. ➢ Many web application standards have already been well-established. As such, it is advised to make reference to and check against those well-established web application security standards to ensure web application security.	✓ The API service should be checked against well-established web security standards. ✓ The API service should require authentication prior to processing other service requests. ✓ The API service should respond to authenticated request only (refer to the row "Authentication Security" for details).	□ The web application is checked not vulnerable to common web application vulnerabilities (e.g. OWASP[4] Top 10 API Security including broken authentication, injection and rate limiting, etc.). □ All unauthenticated requests are denied by the API service.

[4] OWASP Top 10 API Security (https://www.owasp.org/index.php/OWASP_API_Security_Project)

Security Aspects	Security Issues	Best Practices	Verification Checklists
	➢ Other security measures, such as session timeout, input validation, encryption, digital certificate authenticity, etc., are essential to web application security. ➢ As web attack tactics are ever-changing, using web application firewall is an effective way to protect the API service with up-to-date ruleset addressing web application vulnerabilities.	✓ The API service should enable session timeout. ✓ The API service should perform input data validation for all input data. ✓ The API service should use encrypted connection protocols. ✓ The API service should deploy valid TLS server certificate signed by trusted certificate authority such that API clients can verify the authenticity of the API service. ✓ The API service should use rate limiting to slow down volumetric attack attempts. ✓ The API service should be protected by web application firewall.	□ Authentication is required by the API service prior to accepting other service requests. □ The API service asks for re-authentication after the session has been idled for a period of time. □ The API service denies requests that contain invalid or malformed data (e.g. data generated by fuzzing tool). □ The API service accepts encrypted connection protocols (e.g. HTTPS) only. □ The web server which hosts the API service uses valid TLS server certificate signed by trusted certificate authority. □ The API service has defined the maximum number of requests to be accepted per second and per source IP address and blocked access exceeding this limit. □ The API service is protected by web application firewall (WAF) software component or network-based WAF.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.2.4 Mobile Application Security	➢ Mobile application often involves user data collection, processing and visualisation. But there is a risk of mobile phone being lost or stolen that poses security risk of information disclosure. ➢ Security measures, such as encryption, secure storage, two-factor authentication, etc., are essential to protect the sensitive data stored by mobile applications.	✓ The mobile application should store sensitive data (e.g. personal data, user credentials, cryptographic keys, etc.) to system credential storage facilities. ✓ The mobile application should implement mobile supported two-factor authentication (e.g Face recognition, Fingerprint, etc.) to further protect sensitive data collected and stored by mobile applications. ✓ The mobile application should use encrypted communications with backend cloud applications or IoT devices.	□ No sensitive data is stored outside application containers or system credential storage facilities. □ Two-factor authentication is required for accessing sensitive data in the mobile application. □ The communications from mobile applications to backend cloud applications or IoT devices are encrypted.
4.2.2.5 Cloud Data Security	➢ It is common to build IoT solution with cloud database or cloud storage platform. Since the cloud database and cloud data store is directly accessible through the Internet, it may pose higher risk of data breach due to cyber attack. ➢ Although many cloud service providers provide various data protection features to address the data security on cloud, the adoption of the features are often neglected, which may pose	✓ The solution should protect the data on cloud using encryption at rest and in transit. ✓ In using data encryption on cloud, the solution should adopt encryption key management to manage the whole lifecycle of encryption key operations (e.g. key generation, key storage, key usage, key rotation, key revocation and key destruction). ✓ For IoT solution that processes highly sensitive or requires higher security	□ Data is encrypted at rest and in transit. □ In using data encryption on cloud, the solution adopts key management in whole lifecycle of encryption key operations (e.g. key generation, key storage, key usage, key rotation, key revocation and key destruction). □ For IoT solution that processes highly sensitive or requires higher security assurance of data encryption on cloud, Hardware Security Module

Security Aspects	Security Issues	Best Practices	Verification Checklists
	higher risk of sensitive information disclosure.	assurance of data encryption on cloud, FIPS 140-2 certified [5] cryptographic module (e.g. Hardware Security Module) should be used to protect encryption keys throughout the lifecycle of encryption key operations.	(HSM) is used to protect all encryption key operations.

4.2.3 Management Layer

The following best practices are applicable to management layer.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.3.1 Vulnerability Management	➢ Every software may contain security vulnerabilities that need to be fixed and patched from time to time. The same issue applies to software and firmware running on IoT devices. Vulnerability management is essential to manage the entire process of vulnerabilities discovery, risk assessment, fixing and patch deployment during the lifecycle of IoT products. ➢ Since attackers may compromise software source or delivery mechanism to inject malware into delivered software / firmware / patch files,	✓ Manufacturers or developers should devise vulnerability management and disclosure policies for the IoT products. ✓ Manufacturers or developers should provide security patches to fix the device vulnerabilities within a reasonable timeframe. ✓ The device management platform should provide the automatic software / firmware / patch deployment capabilities.	□ Manufacturers or developers provide an official channel (e.g. product website) for the disclosure of device vulnerabilities and related information. □ Manufacturers or developers provide an official channel (e.g. product website) for the security patch software. □ Users can validate the authenticity of the software / firmware / patch files by verifying digital signature or file checksum.

[5] FIPS 140-2 Security Requirements for Cryptographic Modules (https://csrc.nist.gov/publications/detail/fips/140/2/final)

Security Aspects	Security Issues	Best Practices	Verification Checklists
	proper validation of integrity of delivered items is required.	✓ All software / firmware / patch files should be signed or provided with file checksum such that users can validate the authenticity of the files.	□ Software / firmware / patch can be deployed to connected device through the device management platform.
4.2.3.2 Device Management	➢ Managing IoT devices with unique identifiers can prevent invalid or illegitimate IoT devices from affecting the security of IoT solutions. ➢ Since IoT devices may not be kept updated in a timely manner and the old version may be still in use, device asset information is essential to assess the scope of impact on vulnerability management. ➢ IoT solution usually involves data collection from IoT devices, analysis of data and producing insights into business decision making. It is essential to ensure the integrity of IoT devices and avoid tampering the source of data collection.	✓ The device management platform should have the capabilities of managing and tracking connected devices through unique identifiers. ✓ The device management platform should provide device asset information including device models and firmware versions. ✓ The device management platform should validate the integrity of device root of trust boot process status, monitor abnormal behaviour of IoT devices and quarantine devices if there is any anomaly with IoT device integrity.	□ Individual device can be identified with unique identifier. □ Individual device can be tracked on the device management platform. □ Device model and firmware version can be checked on the device management platform. □ When anomaly with IoT device integrity is detected, individual device can be quarantined from the device management platform.
4.2.3.3 Data and Event Monitoring	➢ Unlike IT system, IoT devices often lack data and event monitoring. ➢ On-going security monitoring helps maintain the security status of IoT	✓ Audit logs and security event logs should be monitored. ✓ The solution should define all security relevant events.	□ Audit logs and security event logs are being monitored. □ Security relevant events, such as elevation of privilege attempts;

Security Aspects	Security Issues	Best Practices	Verification Checklists
	solutions and provides timely alerts for quicker response to security incidents. ➢ Detection on event anomaly and threshold is conducive to providing early warning of potential security incidents such that necessary security measures can be taken in a timely manner. ➢ Proper access controls are required to ensure the integrity of audit logs and security event logs.	✓ The solution should monitor anomaly of relevant security events across the entire IoT solutions, including any devices; cloud services; mobile services; network or telemetry services; and storage systems. ✓ The solution should define thresholds for each type of security event and trigger alerts for investigation when the thresholds are exceeded. ✓ The solution should restrict read access of security audit logs to user group with auditor role. ✓ The solution should not provide write privileges to any security audit logs.	successful / unsuccessful firmware update events; configuration changes to IoT devices and service software; account modifications; and tamper events, are well-defined. □ Anomaly with security events are being monitored and can be identified. □ Alerts can be triggered when the defined thresholds are exceeded. □ User with auditor role has read access to security audit logs. □ No write access of security audit logs is granted to any user.

4.2.4 Network Layer

The following best practices are applicable to network layer.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.4.1 Wireless Security	➢ Since attacks can sniff wireless network traffic with radio sniffing tools, adopting encryption in wireless communications	✓ The solution should enable encryption in all wireless communications.	□ Encryption is enabled in all wireless communications.

Security Aspects	Security Issues	Best Practices	Verification Checklists
	is important to ensure data confidentiality. ➢ Due to the lack of encryption support for some IoT devices, alternative methods should be considered to prevent information disclosure from eavesdropping. ➢ Since devices may incur acceptance of any connection during the initial pairing stage, proper measures (e.g. physical interaction) can prevent interception from unauthorised remote party.	✓ If the wireless protocols are not capable of supporting encryption features by default, the solution should adopt application layer encryption. ✓ If the device computation power is not capable of supporting encryption, alternative methods such as light-weight encryption or tokenisation should be adopted to secure the content of wireless data stream. ✓ When wireless communications require initial pairing process, the solution should request physical interaction with the device or manually key in a random shared secret. ✓ During initial pairing process, the default wireless passphrase should be changed from the factory default or reset password prior to providing normal service.	□ Data is encrypted in application layer before transmission through wireless protocols without encryption features. □ Due to limited device computation power, content in wireless data stream is still secured from trivial eavesdropping with alternative encryption methods. □ User interaction is required in initial pairing process to avoid unintended pairing to unauthorised remote party. □ Default wireless passphrase is only used once during initial pairing process and enforced to be changed for proceeding to normal service.
4.2.4.2 Network Services Security	➢ Since attackers scan for any vulnerable network services over the network, reducing attack surface on the network and securing the network services minimise the security risk of network attacks.	✓ The solution should ensure all unnecessary network services are disabled. ✓ The solution should require authentication in accessing the network services.	□ No unnecessary network services are detected. □ Access is denied to network services without authentication.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.4.3 Transport Security	➢ Since Internet communications routes through public network hop may expose to eavesdropping attacks, Transport Layer Security (TLS) encryption ensures the end-to-end data confidentiality, data integrity and authentication in the course of communications over the Internet. ➢ Some IoT devices may not natively support Internet Protocols, IoT gateway can act as a firewall to enhance the network isolation and support TLS encryption for the communications over the Internet. ➢ Attackers may intercept the network transport by man-in-the-middle attack between the communications endpoints. Transport security can ensure the authenticity of communications endpoints.	✓ The solution should use Transport Layer Security (TLS) encryption for the communications between devices and the Internet. ✓ If the device does not natively support Internet Protocols, the solution should provide IoT gateway for TLS encryption communications over the Internet. ✓ The IoT gateway should act as a firewall to isolate IoT wireless network from the Internet. ✓ The application service endpoints should use valid TLS digital certificate signed by trusted certificate authority. IoT device endpoint and IoT gateway should validate the authenticity of connection endpoints with TLS digital certificate. ✓ For IoT solution that requires higher security assurance of the authenticity of each IoT device endpoint, the IoT solution should validate the authenticity of each IoT device endpoint with unique API token or unique TLS digital certificate signed by trusted certificate authority.	□ The end-to-end communications between source devices and destination Internet servers are encrypted with TLS. □ If the device does not natively support Internet Protocols, the end-to-end communications between IoT gateways and destination Internet servers are encrypted with TLS. □ The IoT gateway can block network traffic from the Internet to IoT wireless network and vice versa. □ The application service endpoints use valid TLS server certificate signed by trusted certificate authority for authenticity validation. □ Each IoT device endpoint uses unique API token or unique TLS digital certificate for authenticity validation.

4.2.5 Perception layer

The following best practices are applicable to perception layer.

Security Aspects	Security Issues	Best Practices	Verification Checklists
4.2.5.1 Software / Firmware Security	➢ Since vulnerabilities may be exploited during the device lifecycle, firmware update is essential to address software issues and vulnerabilities. ➢ Since attackers may inject malware into software / firmware / patch files, proper validation of legitimate software / firmware / patch files update would prevent against malware infection through tampered update files. ➢ Since attackers may reverse engineer the firmware to extract hardcoded account credentials or passwords, it would pose serious security risk on IoT devices if the hardcoded password is disclosed publicly. ➢ Since users may often fail to change default password during initial installation and setup, default password is likely to be used by attackers to gain unauthorised access and control the device.	✓ All software / firmware / patch files should be signed or provided with file checksum such that users can validate the authenticity of the files. ✓ The device should include software / firmware update capability. ✓ The device should include security patch update capability. ✓ The device should establish the root of trust of device integrity by hardware-validated boot process with signed or encrypted software / firmware / patch files. ✓ The device should only allow the installation of signed software / firmware / patch files. ✓ The factory default or factory reset admin password should be different for each device, with the default password	□ Users can validate the authenticity of the software / firmware / patch files by verifying digital signature or file checksum. □ Users can update the device software / firmware with official software tools. □ Users can apply security patches update to fix device vulnerabilities. □ The device has hardware-validated boot process to allow booting from signed or encrypted software / firmware / patch files only. □ Users are restricted from updating unofficial or modified software / firmware to the device. □ The device manufacturer / developer confirms that the factory default or factory reset admin password is different for each device, with the

Security Aspects	Security Issues	Best Practices	Verification Checklists
		for the device being printed on the serial number label. ✓ The solution should enforce mandatory default password change at initial setup stage. ✓ The device should not contain hardcoded account credentials for any manufacturer support purpose.	default password for the device being printed on the serial number label. □ User is mandated to change default password at initial setup stage. □ The device manufacturer / developer confirms no hardcoded manufacturer support password and account credentials.
4.2.5.2 Physical Security	➢ Since attackers may exploit vulnerabilities through external interfaces or ports, disabling or limiting the capabilities of physical external interfaces or ports reduces the security risk of gaining device control locally. ➢ Since anyone can easily gain system control of the devices, debug interface disabling or applying security restriction on debug interfaces or ports reduces the security risk of system compromise due to physical intrusion.	✓ The device should disable unnecessary physical external interfaces or ports on the device. ✓ The device should restrict direct access to administrative capabilities through physical interfaces or ports. ✓ The device should disable unnecessary debug interfaces or ports. ✓ If debug interfaces or ports are required, authentication or access control should be required to restrict the access only for manufacturer support purpose.	□ No unnecessary physical external interfaces or ports exist or being enabled on the device. □ Users cannot gain administrative capabilities through physical interfaces or ports. □ Debug interfaces or ports are disabled if they are not required. □ If debug interfaces or ports are required, authentication or access control is required before granting access to system administrative capabilities.

Security Aspects	Security Issues	Best Practices	Verification Checklists
			□ Users cannot gain administrative capabilities through debug interfaces or ports.
4.2.5.3 Data Security	➢ Since IoT devices are more likely prone to physical tampering, proper consideration and handling of data security of the device storage are important. ➢ Since device storage can be physically extracted with the provision of proper hardware tools, sensitive data has to be encrypted at rest to ensure data confidentiality. ➢ In addition to encryption of sensitive data, proper usage and protection of encryption key are also often neglected, which may pose higher risk of sensitive information disclosure. ➢ Since devices may be recycled or re-used by other users, users should have control of performing data erasure when the device is no longer used or being disposed.	✓ Personal data, sensitive data and user credential data should be protected with encryption in device storage. ✓ Where the device hardware is capable of supporting asymmetric cryptography, each device should have a unique asymmetric key-pair securely generated at manufacture, with the private key secured within a Secure Element (if supported by the hardware), and a PKI digital certificate from the manufacturer's PKI. ✓ For device hardware that does not support asymmetric cryptography, a secret symmetric key unique per device should be securely generated at manufacture, with the private key secured within a Secure Element (if supported by the hardware). The manufacturer should securely distribute the device symmetric key to its customer as for each device supplied to that customer.	□ Personal data stored in the device storage is protected with encryption (e.g. AES-256). □ Neither personal data, sensitive data nor user credential data is stored in plain text in both internal and external storage memory. □ The device manufacturer / developer confirms a unique encryption key is generated and stored within a Secure Element (if supported by the hardware) for each device. □ Users can perform data erasure on the device such that all personal data, sensitive data and user credential data are erased. □ User can perform factory reset such that all data and user configurations are cleaned up.

Security Aspects	Security Issues	Best Practices	Verification Checklists
		✓ The device should provide the capability of erasing all personal data, sensitive data and user credential data when the device is no longer used by users or being disposed. ✓ The device should clean up all data and user configurations upon factory reset.	
4.2.5.4 Device Availability	➢ IoT devices may counter different operating conditions such as network outage, power outage, etc. that may affect the device availability. ➢ IoT devices should be able to recover automatically and resume the normal operation state in the event of different operating conditions to avoid exposure of security loopholes.	✓ The device should remain operating and locally functioning in case of loss of network connectivity. ✓ If the device requires network connectivity to function, the device should resume to an expected, operational and stable state after resumption of network connectivity automatically. ✓ The device should recover to the operating state in case of power outage.	□ The device can function locally as normal in case of loss of network connectivity or absence of network connectivity. □ If the device requires network connectivity to function, the device can resume to function normally after resumption of network connectivity automatically. □ The device can recover to normal operating state after power outage.

5. Appendix: List of Reference Publications

Publisher	Publication Name	Release Date
BSI and PETRAS	Navigating and Informing the IoT Standards Landscape - A Guide for SMEs and Start-ups https://www.bsigroup.com/en-GB/navigating-and-informing-the-iot-standards-landscape/	2019
CSA	IoT Security Controls Framework https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/	May 2019
CTIA	CTIA Cybersecurity Certification Test Plan for IoT Devices version 1.0.1 https://api.ctia.org/wp-content/uploads/2018/10/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0_1.pdf	Oct 2018
DCMS	Code of Practice for Consumer IoT Security https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security	Oct 2018
DCMS	Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards	Oct 2018
ENISA	Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot	Nov 2017
ENISA	Good Practices for Security of Internet of Things in the context of Smart Manufacturing https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot	Nov 2018
ETSI	Cyber Security for Consumer Internet of Things https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf	Feb 2019
GSMA	GSMA IoT Security Assessment CLP.17 v3.0 https://www.gsma.com/iot/iot-security-assessment/	Sep 2018
IMDA	Internet of Things (IoT) Cyber Security Guide Version 1 https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide.pdf	Jan 2019
IoTAA	Internet of Things Security Guideline V1.2 https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf	Nov 2017
IoTSF	Secure Design – Best Practice Guides Release 1.2.1 https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf	Dec 2018
IoTSF	Compliance Questionnaire Release-2.0 https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-Compliance-Questionnaire-Release-2.0-December-2018.xlsx	Dec 2018
JPCERT	IoT Security Check List https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html	Jun 2019
NIST	Consideration for Managing IoT Cybersecurity and Privacy Risks https://doi.org/10.6028/NIST.IR.8228	Jun 2019
NIST	Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://doi.org/10.6028/NIST.IR.8200	Nov 2018
OWASP	IoT Top 10 2018 https://www.owasp.org/index.php/IoT_Security_Guidance	2018
OWASP	Mobile App Security Verification Standard 1.1.3 https://mobile-security.gitbook.io/masvs/	Jan 2019