International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1352

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things (IoT) security

Security requirements for Internet of things devices and gateways

Recommendation ITU-T X.1352

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	**X.1350–X.1369**
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1352

Security requirements for Internet of things devices and gateways

Summary

Recommendation ITU-T X.1352 establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security, based on the IoT reference model specified in Recommendation ITU-T Y.4100 and the IoT security framework in Recommendation ITU-T X.1361.

The authentication dimension includes user authentication, secure use of authentication credentials and device authentication. The cryptography dimension includes the use of secure cryptography, secure key management and secure random number generation. The data security dimension includes secure transmission and storage, information flow control, secure session management and personally identifiable information (PII) management. The device platform security dimension includes five elements: software security; secure update; security management; logging; and timestamp. Likewise, the physical security dimension includes a secure physical interface and tamper-proofing.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1352	2022-09-02	17	11.1002/1000/14990

Keywords

Authentication, cryptography, data security, device platform security, IoT device and gateway security, IoT gateway, IoT security evaluation, physical security.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1352

Security requirements for Internet of things devices and gateways

1 Scope

This Recommendation establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security. These security requirements are based on the IoT reference model specified in [ITU-T Y.4100] and on the IoT security framework specified in [ITU-T X.1361].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.1254]: Provision of assurance of the claimed identity of an entity.

3.1.2 capability [b-ISO 16100-1]: Set of functions and services with a set of criteria for evaluating the performance of a capability provider.

3.1.3 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.4 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.5 cryptographic-quality random number [b-ITU-T X.667]: A random number or pseudo-random number generated by a mechanism, which ensures sufficient spread of repeatedly generated values to be acceptable for use in cryptographic work (and is used in such work).

3.1.6 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.

3.1.7 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.9 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.10 patch management [ITU-T X.1361]: Process which encompassing acquiring, testing, and installing multiple patches to information systems.

NOTE – Vulnerability management capability could be considered.

3.1.11 personally identifiable information (PII) [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.12 physical security [b-ITU-T X.800]: The measures used to provide physical protection of resources against deliberate and accidental threats.

3.1.13 secure configuration [ITU-T X.1361]: Process by which network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

3.1.14 security gateway [ITU-T X.1361]: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy in the IoT environment.

NOTE – The term is sometimes referred to a gateway. The definition is adapted from [b-ISO/IEC 27033-1].

3.1.15 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.16 vulnerability [b-ISO/IEC 27000]: Weakness of an asset or control that can be exploited by one or more threats.

3.1.17 vulnerability management [ITU-T X.1361]: Process that consists of identifying, classifying, remediating, and mitigating vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security dimension: A set of security measures designed to address a particular aspect of security.

3.2.2 device platform security: A security set for firmware and its updated capability and management of third party software together with audit capability on an Internet of things device and gateway.

NOTE – Firmware is replaced by software on an operating system depending on the hardware capability.

3.2.3 obfuscation: Effect of an operation performed on the program code or application data that results in the applications being hidden or obscured in some way without affecting the output of the code.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CoAP	Constrained Application Protocol

DoS	Denial of Service
F/W	Firmware
FTP	File Transfer Protocol
H/W	Hardware
ID	Identifier
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IPS	Intrusion Prevention System
LwM2M	Lightweight Machine to Machine
MAC	Media Access Control
MCU	Microcontroller Unit
MQTT	Message Queuing Telemetry Transport
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
S/W	Software
SD	Secure Digital
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSA	Shoulder-Surfing Attack
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

5 Conventions

This Recommendation uses the following conventions:

The auxiliary verb "should" indicates a requirement that is recommended, but which is not absolutely required.

The auxiliary verb "shall" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

In the body of this Recommendation, the auxiliary verb "can" sometimes appears, in which case it is to be interpreted as "is able to".

The appearance of the auxiliary verb "should" in Appendix I has no normative intent.

6 Overview

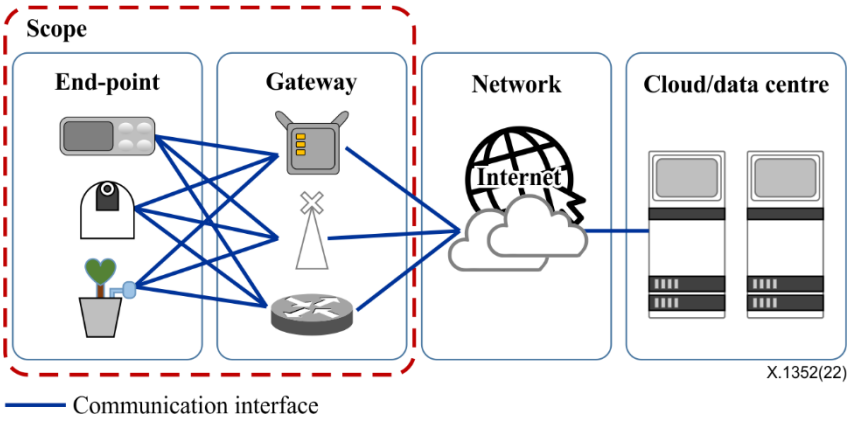

Figure 1 – Scope of security requirements

Based on the security capabilities proposed in [ITU-T X.1361] and [ITU-T Y.4100], and as discussed in Appendix II, security requirements to address the challenges and threats of IoT devices and gateways (excluding network systems and platforms) are specified for five security dimensions, namely: authentication; cryptography; data security; device platform security; and physical security.

The authentication dimension consists of user authentication, secure use of authentication credentials and device authentication.

The cryptography dimension includes the use of a secure cryptographic algorithms, secure key management, and secure random number generation.

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

For the device platform security dimension, there are five items: software (S/W) security; secure update; security management; logging; and timestamp.

Likewise, for the physical security dimension, a secure physical interface and defence against tampering have been specified.

Figure 2 shows the targets for security dimensions in an IoT device and gateway. An IoT device and gateway are commonly composed of a microcontroller unit (MCU), communication module, memory and in/out ports. A secure element exists as a form of hardware (H/W) or S/W. In an MCU, there are firmware (F/W), physical interfaces and memory. Here, S/W with an operating system (OS) can be replaced by F/W. 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 H/W interfaces shall be removed or switched off.

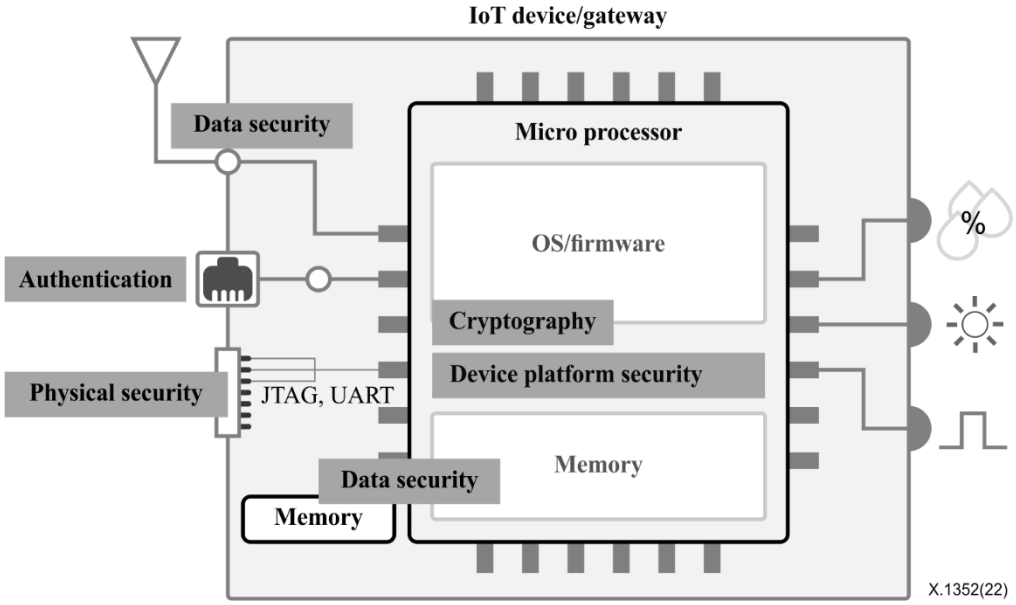

Figure 2 – Example for applied security dimensions on IoT devices and gateways

7 Security threats/vulnerabilities to IoT devices and gateways

Security threats/vulnerabilities to IoT devices and gateways, which may make them possible targets for cyber-attacks, are described in clauses 7.1 and 7.2. Security threats to gateways include threats to IoT devices.

7.1 Security threats/vulnerabilities to IoT devices

Device-specific threats/vulnerabilities include the following.

– ST-D-1: Authentication bypass: An unauthorized 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: Unauthorized device connection: A device is exposed to any unauthorized device, or its data such as user data can be transmitted to any unauthorized device.

– 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 unauthorized 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: User session hijacking: An attacker may gain unauthorized access to a genuine user account whose session is 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 unauthorized/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 S/W: 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.
– 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: Unauthorized physical access: A device is exposed to unauthorized physical access and unintended changes in its configuration.

7.2 Security threats/vulnerabilities to IoT gateways

Gateway-specific threats/vulnerabilities include the following.

– ST-G-1: Untrusted data transmission: An untrusted data transmission may cause a device to malfunction or malicious code to be distributed.
– ST-G-2: Denial of service (DoS) or distributed DoS: A DoS attack may cause a device to lose its availability.

8 Security requirements

This Recommendation specifies security requirements for IoT devices and gateways based on the five security dimensions defined in clause 6 and a set of security requirements is formed based on the provisions of the threat model and specific functional properties of IoT, etc. The security capability is based on [ITU-T X.1361], as discussed in Appendix II.

8.1 Authentication

The authentication dimension consists of user authentication, secure use of authentication credentials, and device authentication.

8.1.1 User authentication

The factory default password shall be changed (AU-1-1).

– A password shall be set up at the time of initial authentication or when change is required after initial authentication.

– Ensure that a password differs from the initial or previous value.

A user shall first be identified and authenticated when security management or sensitive data are accessed (AU-1-2).

– On accessing security management, such as setup of an IoT device, user account or privilege, the user shall be identified and authenticated.

– Users with privileged access to security management or sensitive data shall be managed separately from normal users.

The number of authentication attempts shall be limited (AU-1-3).

– An IoT device may be vulnerable to brute force attacks if repeated authentication attempts are allowed. Thus, it shall offer a function for appropriately responding to continuous authentication attempts.

– This function can be provided using one of the following methods:

  a) limiting the number of authentication attempts to lock the account or deactivate the authentication function for a certain period of time (limiting the number of authentication attempts to five or fewer and deactivating the authentication function for at least 5 min is recommended);

  b) exceeding the specified number of authentication attempts is regarded as unauthorized network traffic and the user is added to the autoblock list (limiting the number of authentication attempts to 10 or fewer is recommended);

  c) application of a completely automated public Turing test to tell computers and humans apart (CAPTCHA).

The pre-installed password of the device should be unique (AU-1-4).

A function to manage user accounts and privileges should be provided (AU-1-5).

– It should be possible to manage all user accounts (including the administrator account) used on an IoT device, e.g., for 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 functions of the IoT device and assign privileges accordingly.

The principle of least privilege should be applied to all user accounts (AU-1-6).

– Role-based privileges should be assigned to all user accounts.

Concurrent access to the administrator account should be restricted (AU-1-7).

– Concurrent access of management services should be limited to the same administrator account and provide a function to disconnect previous access or limit new access attempts.

A secure password in terms of length, cycle and complexity should be provided (AU-1-8).

– IoT devices should provide a function for the user to set a secure password considering the length, cycle and complexity.

8.1.2 Secure use of credentials

Hard-coded credentials should be not used (AU-2-1).

– Password (PIN, secret, etc.) should be neither hard coded nor stored in plain text.

During authentication by password the password should be masked (AU-2-2).

– If a password is displayed in plain text, it may be vulnerable to an SSA. Thus, to prevent such a display on password entry, the component characters of the password should be masked, e.g., using asterisks ("*").

No specific feedback for authentication failure should be provided (AU-2-3).

8.1.3 Device authentication

The unique identifier (UID) of each H/W device shall be retained (AU-3-1). See Table 1.

– The IoT device shall have an identifier (ID) that is unique and fixed.

Table 1 – UID of IoT devices

ID	Description
Media access control (MAC) address	Unique identifier assigned to the network interface for communication at the data link layer of the network segment (48 bit).
International mobile equipment identity (IMEI), international mobile terminal authentication number	Unique number for smartphones. Assigned by the manufacturer on cell phone release. Consists of 15 digits in all, including: an approval code (eight digits); model serial number (six digits); and a verification number (one digit)

Devices should be mutually authenticated before sensitive data is transmitted or the devices are interconnected for control purposes (AU-3-2).

– 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).

8.2 Cryptography

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

– Cryptographic algorithms to protect against side-channel attacks should be used.

Cryptographic keys shall be securely managed throughout their entire lifecycle (CR-1-2).

– Keys should be generated, updated, distributed, used, stored and destroyed in a secure way.

A random number should be generated within an algorithm with proven randomness (CR-1-3).

8.3 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.

8.3.1 Secure transmission and storage

Data transmitted shall be encrypted (DS-1-1).

– Data transmitted shall be encrypted using a secure cryptographic algorithm (see CR-1-1).

A secure mode should be applied when a data or control channel is created (DS-1-2).

– 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.

Data stored in devices shall be encrypted (DS-1-3).

– Data storage devices shall be encrypted using a secure cryptographic algorithm (see CR-1-1).

Deleted data shall not be restored (DS-1-4).

– If it is necessary to scrap, update or replace the device, a deletion capability (e.g., factory initialization) shall be provided so that data cannot be recovered.

8.3.2 Information flow control

Unauthorized network traffic should not be allowed (DS-2-1).

8.3.3 Secure session management

The session should be terminated after idle time-outs (DS-3-1).

– If accessing again after session termination, re-authentication should be conducted.

The session ID should be an unpredictable value (DS-3-2).

– 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.

8.3.4 PII management

PII should be securely managed in the key lifecycle (DS-4-1).

– PII should be gathered, used, stored, and destroyed in a secure way.

8.4 Device platform security

In the device platform security dimension, there are five items: S/W security; secure update; security management; logging; and timestamp.

8.4.1 Software security

Secure coding should be applied (PL-1-1).

– S/W should be designed and implemented with consideration of security.

Known security vulnerabilities shall be checked and removed (PL-1-2).

– If the S/W was developed using protocols, libraries, an application programming interface (API), packages or open sources containing known security vulnerabilities, the F/W and OS may also have them.

– The public domain of known security vulnerabilities (e.g., [b-CVE]) shall be used to check the security vulnerabilities of the device and remove them.

Obfuscation should be applied (PL-1-3).

– 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.

An integrity verification function for configuration parameters and executable codes should be supported (PL-1-4).

– 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.

8.4.2 Secure update

The update shall be conducted by authorized users (PL-2-1).

The rollback function should be supported if the update fails (PL-2-2).

Integrity and authentication should be checked prior to an update (PL-2-3).

– Authentication should be done against the user performing the update, integrity checks should be done against the update server address, both should be checked against the update file.
– The authenticity of a user can be confirmed by re-authenticating the user immediately prior to the update procedure.
– An authorized user can check the integrity of the update server address by visual inspection.
– Checking the integrity and authenticity of update files can be done by verifying a cryptographic digital signature.

8.4.3 Security management

Unnecessary services should be disabled (PL-3-1).

– 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.

Remote management should be done in a reliable environment (PL-3-2).

A secure third party library should be applied (PL-3-3).

– The third party library and module used for development should be the latest version, without any known security vulnerabilities or defects.

A self-test should be provided (PL-3-4).

– A self-test function for detecting errors of the main H/W and S/W when an IoT device is started (powered up) or after it is started should be provided.

8.4.4 Logging

Logging should be generated for security-related events (PL-4-1).

– The logging should be implemented, and it should be possible to detect and trace any abnormal device behaviour.

A secure logging mechanism should be provided (PL-4-2).

– To provide against its loss and unauthorized changes (including deletion), there should be a mechanism for protecting a log.

8.4.5 Timestamp

A reliable timestamp should be provided (PL-5-1).

8.5 Physical security

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

8.5.1 Secure physical interface

Any unnecessary external interface should be deactivated (PH-1-1).

– 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 to prevent unauthorized access.

Unauthorized access to the internal interface shall be prevented (PH-1-2).

– 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 unauthorized access.

8.5.2 Tamper-proofing

A detection and response function to unauthorized physical manipulation should be supported (e.g., tamper-evident seals, locks, tamper response, zeroization switches and alarms) (PH-2-1).

Annex A

Mapping list between Internet of things security requirements and security threats/vulnerabilities

(This annex forms an integral part of this Recommendation.)

The IoT security requirements are listed and described in clause 8 and security threats/vulnerabilities are specified in clause 7. The mapping of IoT security requirements to security threats/vulnerabilities is shown in Table A.1.

Table A.1 – The mapping list of IoT security requirements and security threats/vulnerabilities

Requirement number	Requirement dimension	Requirement description	Security Threats/vulnerabilities
AU-1-1	Authentication	The factory default password shall be changed.	ST-D-6
AU-1-2	Authentication	A user shall first be identified and authenticated when security management or sensitive data are accessed.	ST-D-1
AU-1-3	Authentication	The number of authentication attempts shall be limited.	ST-D-4 ST-D-5
AU-1-4	Authentication	The pre-installed password of the device should be unique.	ST-D-1
AU-1-5	Authentication	A function to manage function for user accounts and privileges should be provided.	ST-D-3
AU-1-6	Authentication	The principle of least privilege should be applied to all user accounts.	ST-D-3
AU-1-7	Authentication	Concurrent access to the administrator account should be restricted.	ST-D-1
AU-1-8	Authentication	A secure password in terms of length, cycle and complexity should be provided.	ST-D-7
AU-2-1	Authentication	Hard-coded credentials should be not used.	ST-D-6
AU-2-2	Authentication	During authentication by password the password should be masked.	ST-D-6
AU-2-3	Authentication	No specific feedback for authentication failure should be provided.	ST-D-6
AU-3-1	Authentication	The unique ID of each hardware device should be retained.	ST-D-2
AU-3-2	Authentication	Devices should be mutually authenticated before sensitive data is transmitted or controlled before interconnection.	ST-D-2
CR-1-1	Cryptography	Secure encryption algorithms shall be used when data is transmitted or stored.	ST-D-8 ST-D-9

Table A.1 – The mapping list of IoT security requirements and security threats/vulnerabilities

Requirement number	Requirement dimension	Requirement description	Security Threats/vulnerabilities
CR-1-2	Cryptography	Cryptographic keys shall be securely managed throughout their entire lifecycle.	ST-D-8
CR-1-3	Cryptography	A random number should be generated within an algorithm with proven randomness.	ST-D-8
DS-1-1	Data security	Data transmitted shall be encrypted.	ST-D-11
DS-1-2	Data security	A secure mode should be applied when a data or control channel is created.	ST-D-11
DS-1-3	Data security	Data stored in device shall be encrypted.	ST-D-11
DS-1-4	Data security	Deleted data shall not be restored.	ST-D-17
DS-2-1	Data security	Unauthorized network traffic should not be allowed.	ST-G-1
DS-3-1	Data security	A session should be terminated after idle time-outs.	ST-D-12
DS-3-2	Data security	The session ID should be an unpredictable value.	ST-D-12
DS-4-1	Data security	PII should be securely managed in the key lifecycle.	ST-D-11
PL-1-1	Device platform security	Secure coding should be applied.	ST-D-10 ST-D-20 ST-D-23 ST-D-24
PL-1-2	Device platform security	Known security vulnerabilities shall be checked and removed.	ST-D-16 ST-D-21
PL-1-3	Device platform security	Obfuscation should be applied.	ST-D-16
PL-1-4	Device platform security	An integrity verification function for configuration parameters and executable codes should be supported.	ST-D-15
PL-2-1	Device platform security	An update shall be conducted by an authorized user.	ST-D-13
PL-2-2	Device platform security	A rollback function should be supported if an update fails.	ST-D-14
PL-2-3	Device platform security	Integrity and authentication should be checked prior to the update.	ST-D-15
PL-3-1	Device platform security	Unnecessary services should be disabled.	ST-D-16
PL-3-2	Device platform security	Remote management should be done in a reliable environment.	ST-D-18
PL-3-3	Device platform security	A secure third party library should be applied.	ST-D-22

Table A.1 – The mapping list of IoT security requirements and security threats/vulnerabilities

Requirement number	Requirement dimension	Requirement description	Security Threats/vulnerabilities
PL-3-4	Device platform security	A self-test should be provided.	ST-D-19
PL-4-1	Device platform security	Logging should be generated for security-related events.	ST-D-23
PL-4-2	Device platform security	A secure logging mechanism should be provided.	ST-D-23
PL-5-1	Device platform security	A reliable time stamp should be provided.	ST-D-18
PH-1-1	Physical security	Any unnecessary external interface should be deactivated.	ST-D-24 ST-D-25
PH-1-2	Physical security	Unauthorized access to the internal interface shall be prevented.	ST-D-24 ST-D-25
PH-2-1	Physical security	A function of detecting and responding to unauthorized physical manipulation should be supported (e.g., tamper-evident seals, locks, tamper response and zeroization switches and alarms).	ST-D-24 ST-D-25

Appendix I

Security capabilities for the Internet of things

(This appendix does not form an integral part of this Recommendation.)

I.1 Overview

This Recommendation addresses security requirements only and takes into account the reliability and quality of services. The security capabilities for IoT are expanded from those described in [ITU-T X.1361]. The IoT architecture should include the general capabilities listed in Table I.1.

Table I.1 – Mapping table between security requirements and security capabilities

Capabilities	Related requirements
Secure communication capability for supporting secure, trusted, and privacy-protected communication	DP-1-1, DS-1-2
Secure key management capability for supporting secure communications	CR-2-1
Secure data management capability for providing secure, trusted, and privacy-protected data management	DS-2-1, DS-1-4
Authentication capability for authenticating devices	AU-1-1, AU-1-2, AU-1-3, AU-1-4, AU-1-8
Authorization (access control) capability for authorizing devices	AU-3-1, AU-3-2
Audit capability for monitoring data access or attempts to access IoT applications in a fully transparent, traceable, and reproducible manner, based on appropriate regulations and laws	PL-4-1, PL-4-2
Secure service provision capability for providing secure, trusted, and privacy-protected service provision	DS-4-1, DS-3-2
Secure integration capability for integrating different security policies and techniques related to the various IoT functional components	–
Capability to implement secure protocols using publicly available and standardized cryptographic algorithms	CR-1-1
Capability to implement secure protocols based on lightweight cryptography	CR-1-1
Secure and robust software update capability for updating software modules or applications	PL-2-1, PL-2-2, PL-2-3
Identity management capability for IoT device/sensor, gateway, and platform/service	AU-2-1, AU-2-2, AU-2-3, DS-3-2, DS-4-1
Vulnerability scanning capability	–
Capability for monitoring data access or attempts to access IoT applications in a fully transparent, traceable, and reproducible manner	PL-4-1, PL-4-2
Hardware-based (e.g., trusted platform module) security capability to prevent occurrences of physical security risks that come with network and gateway virtualization	PH-1-1, PH-1-2, PH-2-1
Multi-path routing capability for preventing selective forwarding attacks	–
PII protection capability against PII breaches throughout the entire PII lifecycle	DS-4-1
Secure configuration capability	–
Capability using lightweight cryptography	CR-1-1

Table I.1 – Mapping table between security requirements and security capabilities

Capabilities	Related requirements
Simple encryption capability with encryption with associated mask data (EAMD) [b-ITU-T X.1362] for communicating with other entities including the gateway	–

The IoT architecture should include the cryptographic algorithm-related capabilities listed in Table I.2.

Table I.2 – Mapping table between security requirements and security capabilities for cryptographic algorithm

Capabilities	Related requirements
Capability of producing a cryptographic-quality random number for supporting key management [b-IETF RFC 4086]	CR-3-1
Periodic update capability for the cryptographic keys necessary for broadcast streams	–
Capability using standardized cryptographic algorithms	CR-1-1

The IoT architecture should include the context-related capabilities listed in Table I.3.

Table I.3 – Mapping table between security requirements and security capabilities for Context

Capabilities	Related requirements
Capability to resist side-channel attacks	–
Capability to support secure coding practices that enforce rigorous data validation input in systems and services, database applications and web services	PL-1-1, PL-1-3, PL-1-4
Capability to conduct a planned risk assessment to determine risks across operational contexts	PL-1-4

I.2 Security capabilities for sensor/device

IoT sensors/devices should include the security capabilities listed in Table I.4.

Table I.4 – Mapping table between security requirements and security capabilities for IoT sensor/device

Capabilities	Related requirements
Key management capability	CR-2-1
Cryptographic algorithm negotiation capability	CR-1-1
Data encryption capability and, in some cases, signalling, control and management plane data to mitigate the security concerns over the confidentiality of data transmitted through wireless network	CR-1-1, DS-1-1, DS-1-2

Table I.4 – Mapping table between security requirements and security capabilities for IoT sensor/device

Capabilities	Related requirements
Data integrity capability for data transmitted through wireless network by using appropriate integrity protection scheme providing assurance that user data or signalling, control or management data has not been tampered with or altered	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Authentication capability for the origin of the data or identity of the IoT sensor/device and administrator and maintenance personnel of the sensor network	AU-1-2, AU-1-6, PL-2-1
Capability for patch management, including updating and upgrading secure software module	PL-2-1, PL-2-2, PL-2-3
Capability to implement secure protocol based on lightweight cryptography	CR-1-1
Access control capability to ensure that only authorized personnel or device is allowed access to network element, stored information, information flow, service and application	AU-1-2, AU-3-1, AU-3-2
Tamper detection or tamper prevention capability	PH-2-1
Capability to produce cryptographic-quality random number to support key management	CR-3-1
Capability to resist side-channel attack	–
Malware detection and protection capability	–
PII protection capability against PII leak	DS-4-1

IoT devices should include the security capabilities listed in Table I.5.

Table I.5 – Mapping table between security requirements and security capabilities for IoT device

Capabilities	Related requirements
Capability to verify the authenticity and integrity of software on a device using cryptographically generated digital signatures [b-ISO/IEC 9796-3]	PL-1-4
Firewall, intrusion detection, intrusion protection or deep packet inspection capability to control traffic destined to terminate at a device	DS-2-1
Capability for performing secure configurations	PL-1-4

I.3 Security capabilities for gateways

The platform/service should include the security capabilities listed in Table I.6.

Table I.6 – Mapping table between security requirements and security capabilities for gateway

Capabilities	Related requirements
Intrusion detection system (IDS)/intrusion prevention system (IPS) capability	DS-2-1
Key management capability	CR-2-1
Capability for performing secure configuration	PL-1-4
Cryptographic algorithm negotiation capability	CR1-1

Table I.6 – Mapping table between security requirements and security capabilities for gateway

Capabilities	Related requirements
Capability to encrypt data and, in some cases, signalling, control, and management plane data with IoT devices and components in the data centre to mitigate security concerns over the confidentiality of data transmitted through wireless network	CR-1-1, DS-1-1, DS-1-2
Integrity capability for data transmitted through wireless network by using appropriate integrity protection scheme providing assurances that user data or signalling, control or management data has not been tampered with or altered	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Availability capability to handle DoS attacks ranging from use of secure source coding techniques, source code analysis testing and vulnerability testing to use of network or host-based IDS/IPS	PL-1-1
Authentication capability as to the origin of the data or identity of the IoT sensor/device and administrator and maintenance personnel of the sensor network	AU-1-2, AU-1-6, PL 2-1
Access control capability to ensure that only authorized personnel or device is allowed access to network element, stored information, information flow, service and application	AU-1-2, AU-3-1, AU-3-2
IoT device accountability capability to ensure that any violation of policy will be traceable to a specific device	PL-4-1
Capability for updating secure software module	PL-2-1, PL-2-2, PL-2-3

I.4 Security capabilities for network

The network according to [b-ITU-T X.805] should include the security capabilities listed in Table I.7.

Table I.7 – Mapping table between security requirements and security capabilities for network

Items	Capabilities	Related requirements
C_NT.1 [b-ITU-T X.805]	The communication security dimension ensures that information flows only between the authorized endpoints (the information is not diverted or intercepted as it flows between these endpoints).	PL-3-1

I.5 Security capabilities for platforms/service

The platform/service should include the security capabilities listed in Table I.8.

Table I.8 – Mapping table between security requirements and security capabilities for platform/service

Capabilities	Related requirements
Capability to protect a credential for cryptographic operation, which is a set of data presented as evidence of claimed identity or entitlement	DS-2-1
Capability to change default username and password during initial setup	AU-1-1, AU-1-2
Capability to implement strong password and granular access control policy	AU-1-4, AU-1-6

Table I.8 – Mapping table between security requirements and security capabilities for platform/service

Capabilities	Related requirements
Capability to make unnecessary port unavailable	PL-3-1, PH-1-1, PH-1-2
Capability to support secure configuration, e.g., to remove unnecessary service and software	AU-1-5, PL-3-1
Capability to protect against malware infection through the use of malware protection software	PL-3-4
Capability to implement patch management policy	PL-2-1, PL-2-2, PL-2-3
Capability for vulnerability management	PL-1-1, PL-1-2
Capability for updating secure software module and application	PL-2-1, PL-2-3
Key management capability for secure message transfer between a gateway and a platform/service	CR-1-2
Capability for cryptographic algorithm negotiations for establishing secure tunnelling between the gateway and the platform/service, if there is a need for secure message transfer between the gateway and the platform/service; availability capability to handle DoS attack	AU-1-5, DS-1-1, DS-1-2
Capability for network monitoring	–
Capability for PII protection at rest	DS-4-1
Capability for application-level security to prevent application-level threats and attacks described in clause 8.4 of [ITU-T X.1361]	–
Capability to provide support for mitigating inference attack	–

Appendix II

Use cases of applying security requirements for Internet of things devices and gateways

(This appendix does not form an integral part of this Recommendation.)

Many IoT devices have security vulnerabilities and weaknesses with regard to authentication, cryptography and data protection. Moreover, most of them are vulnerable to physical interfaces and device development platforms. This appendix describes security development cases in relation to the proposed requirements.

II.1 Use case of authentication – Vulnerability to man in the middle attack

There is vulnerability in the authentication procedure between server and network camera. The network camera does not deny invalid certificates while TLS handshaking. An attacker steals an important key. See Figure II.1.

Countermeasures include:

– denial of invalid secure socket layer certificate;

– use hypertext transfer protocol public key pinning.

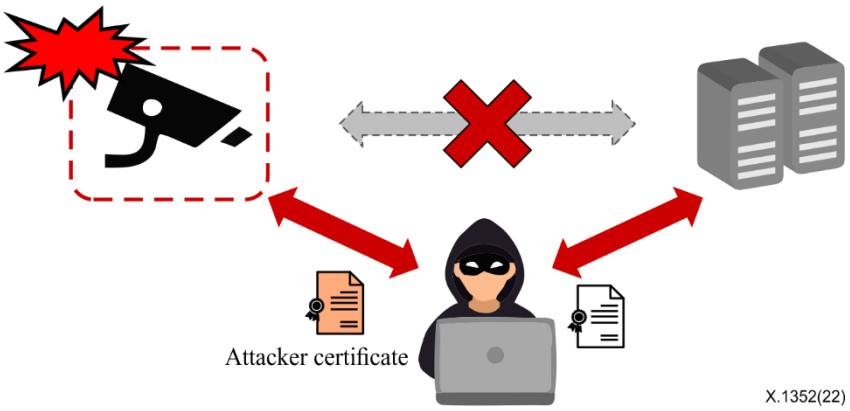

Figure II.1 – Use case of authentication

II.2 Use case of cryptography domain – Weak cryptography algorithm

See Figure II.2.

Vulnerabilities include:

– weak encryption algorithm: Base64;

– data checking methodology: secure hash algorithm 1 (SHA1).

Countermeasures include:

– a security strength higher than that of a 128-bit encryption algorithm (see [b-ISO/IEC 19790]);

– data checking methodology: SHA256 [b-ISO/IEC 10118-3].

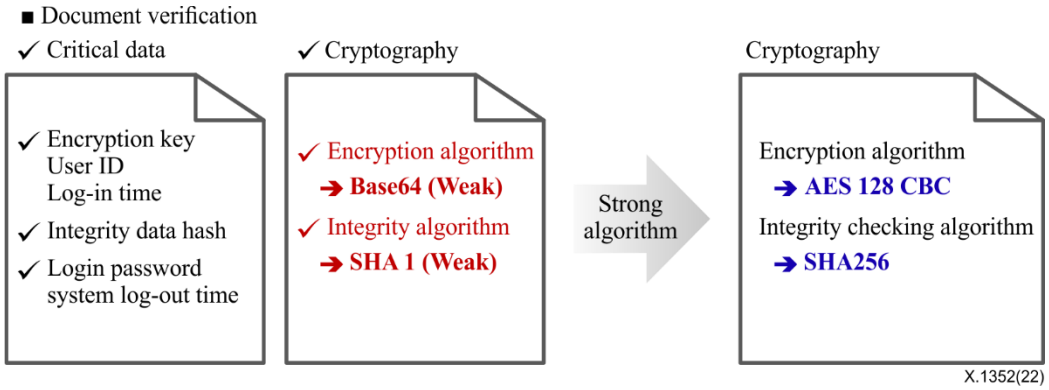

Figure II.2 –Use case of cryptography domain

II.3 Use case of data security and cryptography domain – Weak integrity checking of sending data

See Figure II.3.

Vulnerability is:

– weak integrity checking of sending data (data integrity checking methodology: cyclic redundancy check).

Countermeasures include:

– data checking methodology: SHA256 hash data [b-ISO/IEC 10118-3];

– total data splits and frame reassembled.

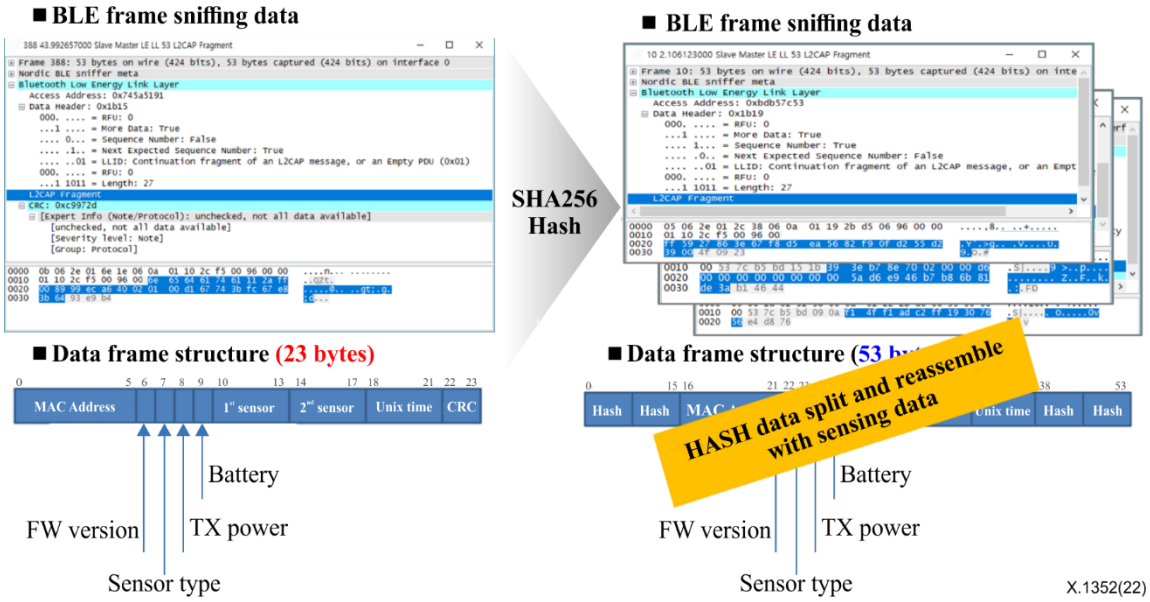

Figure II.3 – Use case of data security and cryptography domain

II.4 Use case of device platform security domain – Weak coding against exploit

See Figure II.4.

Vulnerability is:

– buffer overflow and weak API.

Countermeasure is:

– check of secure coding and proposal for elimination of weak codes by static analysis tools.

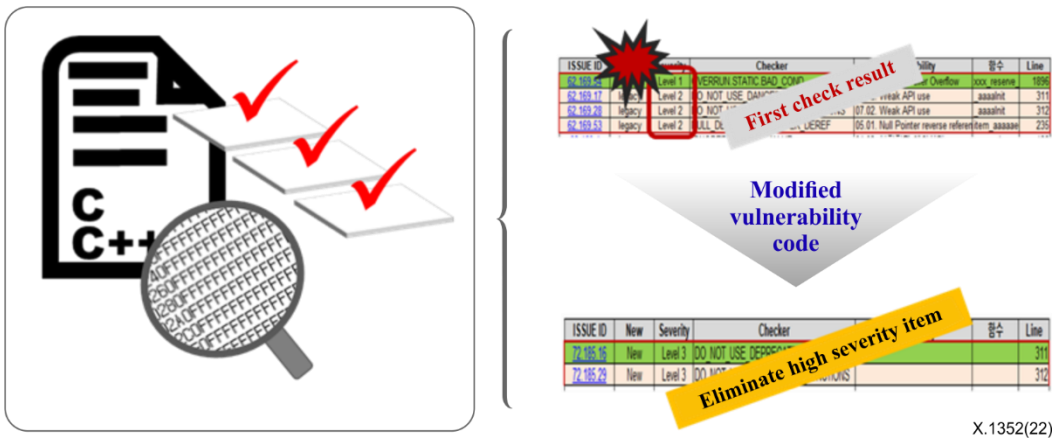

Figure II.4 – Use case of device platform security domain

II.5 Use case of physical security domain – Inner interface vulnerability in a printed circuit board

See Figure II.5.

Vulnerability is:

– JTAG port available on a mass product.

Countermeasure is:

– enablement of memory access protection in the MCU.

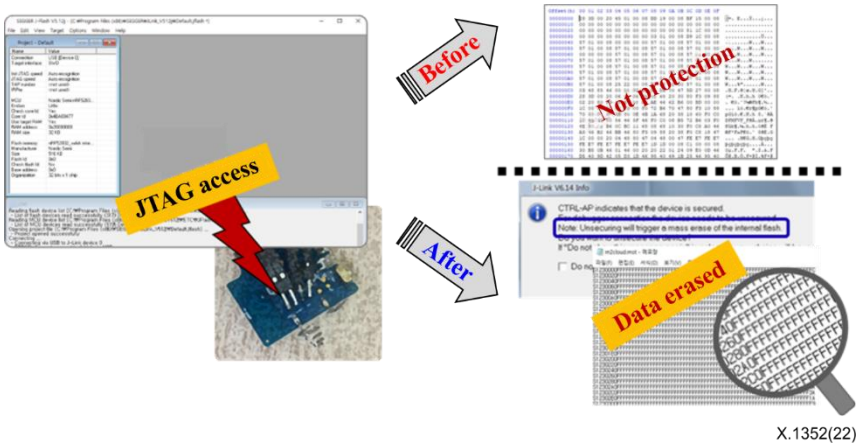

Figure II.5 – Use case of physical security domain

Bibliography

[b-ITU-T X.667] Recommendation ITU-T X.667 (2012), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework.*

[b-ITU-T X.1362] Recommendation ITU-T X.1362 (2017), *Simple encryption procedure for Internet of things (IoT) environments.*

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ISO 16100-1] ISO 16100-1:2009, *Industrial automation systems and integration – Manufacturing software capability profiling for interoperability – Part 1: Framework.*

[b-ISO/IEC 10118-3] ISO/IEC 10118-3 (2018), *IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*

[b-ISO/IEC 19790] ISO/IEC 19790 (2012), *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-ISO/IEC 9796-3] ISO/IEC 9796-3 (2006), *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness requirements for security*.

[b-CVE] Mitre Corporation (Internet). *Common vulnerabilities and exposures*. Bedford, MA: Mitre Corporation. Available [viewed 2022-10-29] at: https://cve.mitre.org/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022