INTERNATIONAL STANDARD

ISO/IEC 27400

First edition
2022-06

Cybersecurity — IoT security and privacy — Guidelines

Cybersécurité — Sécurité et protection de la vie privée pour l'IoT — Lignes directrices

Reference number
ISO/IEC 27400:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Information security is a major concern of any information and communication technology (ICT) system and Internet of Things (IoT) systems are no exception. IoT systems present particular challenges for information security in that they are highly distributed and involve a large number of diverse entities. This implies that there are a very large attack surface and a significant challenge for the information security management system (ISMS) to apply and maintain appropriate security controls across the whole system.

Privacy or personally identifiable information (PII) protection is a significant concern for some types of IoT systems. Where an IoT system acquires or uses PII, it is usually the case that there are laws and regulations that apply to the acquisition, storage and processing of PII. Even where regulations are not a concern, the handling of PII by an IoT system remains a reputational and trust concern for the organizations involved, for example, if the PII is stolen or is misused, potentially causing some form of harm to the people identified by the information.

Security and privacy controls in this document are developed for stakeholders in an IoT system environment, so as to be utilized by each IoT stakeholder, throughout the IoT system life cycle.

Cybersecurity — IoT security and privacy — Guidelines

1 Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924, ISO/IEC 27000, ISO/IEC 29100, ISO 31000 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.5]

3.2
cloud service
one or more capabilities offered via *cloud computing* (3.1) invoked using a defined interface

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.8]

3.3
IoT device
entity of an IoT system that interacts and communicates with the physical world through sensing or actuating

3.4
IoT device developer
entity that creates an assembled final IoT device

Note 1 to entry: “final” in this definition means the stage of delivery to the IoT service developer in the assemble process.

3.5
IoT platform
infrastructure that enables the deployment, management and operation of IoT devices

3.6
IoT system
system providing functionalities of Internet of Things

Note 1 to entry: IoT system is inclusive of IoT devices, IoT gateways, sensors, and actuators.

Note 2 to entry: In the context of this document, this also includes applications and backend that support IoT solutions.

3.7
IoT solution
seamlessly integrated bundle of technologies, potentially including sensors, gateways and actuators

Note 1 to entry: These can solve a specific problem or need or they can be used to build additional functionality in other none IoT solutions

3.8
ecosystem
infrastructure and services based on a network of organizations and stakeholders

Note 1 to entry: Organizations can include public bodies.

[SOURCE: ISO/IEC TS 27570:2021, 3.8]

4 Abbreviated terms

ASD	Application and Service Domain
CRM	Customer Relationship Management
DoS	Denial of Service
IC	Integrated Circuit
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ITS	Intelligent Traffic System
OMD	Operations and Management Domain
OTA	Over The Air
PED	Physical Entity Domain
PII	Personally Identifiable Information
RAID	Resource Access and Interchange Domain
SCD	Sensing and Controlling Domain
UD	User Domain
Wi-Fi	Wireless Fidelity

5 IoT concepts

5.1 General

This clause provides a brief introduction to IoT concepts and reference models which are useful in the context of security and privacy. Detailed information on these topics is provided in ISO/IEC 30141.

5.2 Characteristics of IoT systems

The applications of IoT systems are diverse, making it impractical to define a generally applicable set of characteristics for every IoT system. As a practical way to describing characteristics of IoT systems, "common characteristics" and "specific characteristics for application areas" can be identified.

IoT systems share following common characteristics.

- IoT systems include IoT devices, which is specific hardware and software equipment which is used in conjunction with or attached to physical things or materials.
- IoT devices are connected to networks and have the ability to transmit and receive data. Wired as well as wireless networks can be used.
- IoT devices usually have sensing capabilities, e.g. for detecting environment states or movements.
- IoT devices can have actuating capabilities, e.g. receiving controlling data in order to initiate physical actions.
- IoT systems include IoT applications in order to process data from IoT devices, to generate and send controlling data, and to enable integration with other systems.
- IoT systems include operational components which allows the setup and operation of IoT devices and applications.
- IoT systems support human or digital users (for further information refer to ISO/IEC 30141).

Depending in which area or for which purpose IoT systems are used there are specific requirements. See the following list of examples.

- For consumer IoT systems pricing is very sensitive, which makes low cost for manufacturing and operating IoT devices important. Depending on the data processed, data privacy can also be very important.
- Industrial IoT systems can replace or be used in conjunction with an industrial plant and control systems and therefore, be subject to similar requirements such as high availability or safety. Safety of process utilizing IoT systems may depend on the security characteristics of an IoT device.
- IoT systems used in vehicles are used in the context of reliability or safety relevant functionalities. Whereas in the reliability related use case privacy requirements can be important to consider, a safety use case can impose high integrity and availability requirements.

For further information and discussion of specific use cases for IoT systems, refer to ISO/IEC TR 22417:2017.

IoT service providers often use cloud infrastructure to implement their services. Especially when using public cloud services, this allows low initial cost and great scalability.

An IoT service provider should ensure as a consumer of a cloud service that the cloud service has adequate security controls in place. These controls, often also in combination with additional controls at the IoT service provider's side, should fully address the security and privacy requirements of the IoT users (e.g. regarding protection of PII), for which the IoT service provider is in a supplier role.

For further guidance on supplier relationships in cloud services refer to ISO/IEC 27036-4, for guidance on security controls for cloud services based on ISO/IEC 27002 refer to ISO/IEC 27017, and further guidance on PII protection in public cloud is provided in ISO/IEC 27018.

5.3 Stakeholders of IoT systems

5.3.1 General

In order to be able to implement security and privacy for an IoT system, it is important to know the stakeholders of the system. Depending on their role, they are either setting the level of security and privacy required for the system based on their risk appetite, or they contribute to effective controls for achieving these requirements.

ISO/IEC 30141 defines three types of roles: IoT service provider, IoT service developer and IoT users. It also defines a number of subroles and activities, some of them relate to security and privacy.

In 5.3, the common stakeholders relevant for most IoT systems are introduced.

5.3.2 IoT service provider

An IoT service provider manages and operates the services of an IoT system which are offered to the IoT users.

Common services provided by IoT service providers include connectivity services, data collection and management services as well as management service for IoT-related assets such as IoT devices.

The IoT service needs to match the IoT user's needs and is dependent on a specific use case or a relevant IoT ecosystem.

IoT service providers need to understand the functional and non-functional requirements of IoT users for services provided, and to satisfy IoT users with the services, particularly in terms of security and privacy.

In order to achieve this, IoT service providers also need to fully understand any relevant threat vectors in order to be able to perform a risk assessment and to select effective risk treatment options.

For specific controls which have to be considered by an IoT service provider, refer to the controls given in Clause 7 which have "IoT service provider" as the indicated audience.

5.3.3 IoT service developer

IoT service developers are responsible for the design, implementation and integration of IoT services.

IoT service developers can be further specialized, e.g. by taking on the role as architect for IoT solutions or platforms, as designer and or implementer for IoT applications, as designer or implementer for IoT devices.

In each role, IoT service developers should follow best practices for design and development, e.g. adhering to security and privacy by design principles or using secure software development life cycles.

One of the subroles of IoT service developers is IoT device developer. It does engineer and produce specific hardware equipment to be used in IoT systems, in particular IoT devices.

IoT devices can either be operated and used directly by an IoT user or by an IoT service provider, and the technically same device can be used in various different IoT use cases. It is important for an IoT device developer to consider the security and privacy requirements of potential usage scenarios for the device in the design phase, in order to be able to offer devices which have the right set of functionality and features to fulfil their customers' need.

IoT service developers need to understand and consider the security and privacy expectations and requirements of the IoT service providers as well as of IoT users, so that necessary controls are selected to ensure adequate treatment of risks of the IoT system.

For more information regarding controls which have to be considered by IoT service developers, refer to the controls given in Clause 7 which have "IoT service developer" as an indicated audience.

5.3.4 IoT user

An IoT user is the end user of an IoT service and can be categorized into human user and digital user. Human user is an individual who uses the IoT service. Digital user is a non-human user of the IoT service; it can be an automated service acting on behalf of a human user.

In the case of human user, he/she can be either represented by an individual, for example, in the case of consumer level IoT systems, or by an organization, e.g. in the case of industrial IoT systems.

In any case, the IoT user does directly set or at least does influence the functional and non-functional requirements for an IoT system or an IoT service.

It is in the core interest of the IoT user that an IoT system or IoT service can be used without introducing unacceptable risks in the area of security and privacy.

The level of security and privacy required to be provided in a IoT system or service is mainly driven by expectations or risk considerations done by IoT users. However, IoT users may often be unaware of the security implications of the technologies.

For any use case a profound understanding of the IoT users and of their needs and requirements is crucial.

In order to be able to treat IoT related risks adequately, there are also controls an IoT user should consider and implement. For more information regarding these controls, refer to the controls given in Clause 7 which has "IoT User" as an indicated audience.

5.4 IoT ecosystem

Dependencies among IoT service providers, IoT service developers and IoT users in the context of security and privacy in an IoT system can be described as an ecosystem, an analogy to the concept in ecology. The dependencies in security and privacy in IoT include:

a) products and services supplier relationships;

b) provision of measures by other entities within the ecosystem necessary in implementing security and privacy controls (see Clause 7); and

c) potential externality of consequences in conceivable risk scenarios not contained within an entity (see Clause 6), e.g. failure in implementing a control by an IoT service provider or an IoT service developer giving rise to security and privacy risk of IoT users.

Furthermore, there are concerns about adverse effects on other organizations beyond the impact between stakeholders assumed in a single IoT system, such as cyber attacks against external organizations and countries that exploit vulnerable IoT systems and devices. These adverse effects need to be addressed in an expanded ecosystem that includes the entities potentially affected, and responsible organizations should implement controls (Clause 7) addressing them.

5.5 IoT service life cycles

An IoT service introduces various life cycles, which can be mapped to the stakeholders of an IoT system.

More specifically, an IoT service is:

a) developed by an IoT service developer and IoT device developer(s);

b) provided by an IoT service provider, and

c) used by IoT users.

Processes of these stakeholders form a set of interdependent life cycles of device development, service development, service provision and use of the service. Figure 1 shows these life cycles of IoT service and the relationships among them.

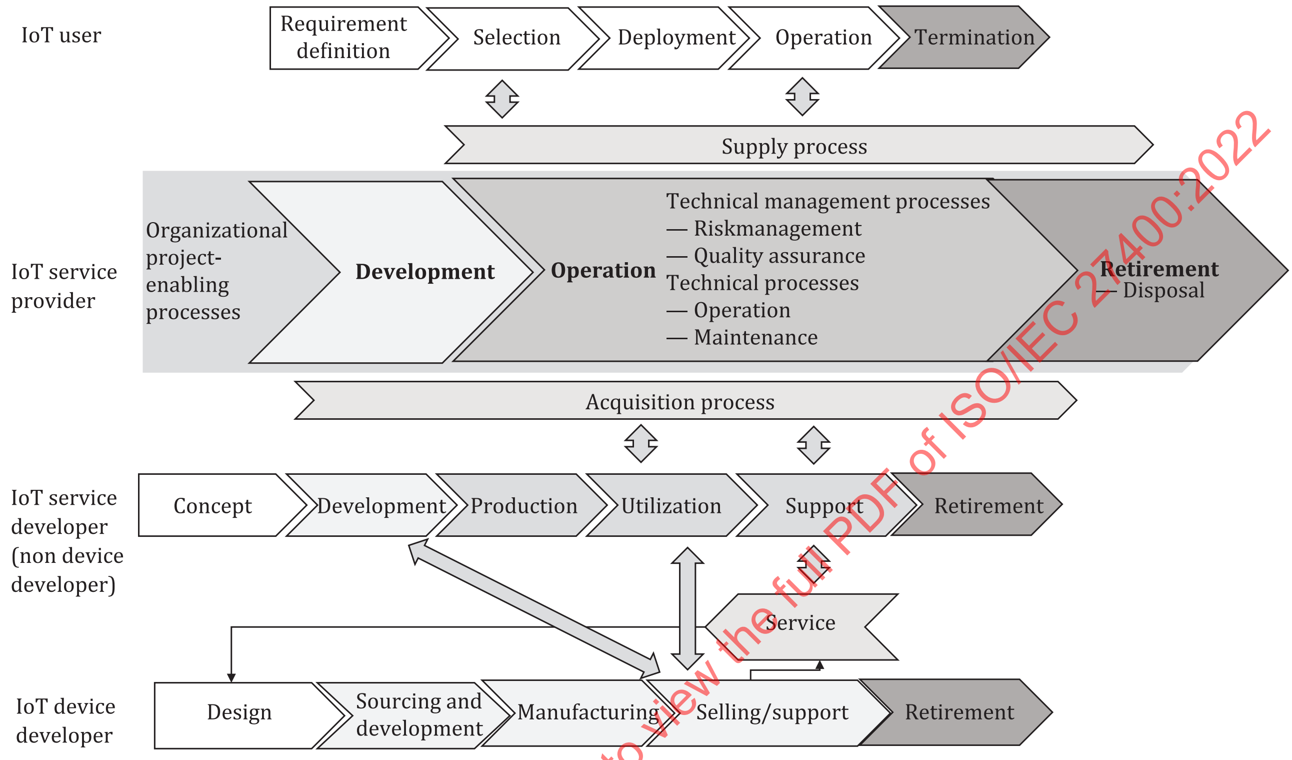

Figure 1 — IoT service life cycles

In the life cycle of the IoT device, the IoT device developer designs, develops, manufactures, sells to and supports the IoT service developers, the IoT service providers or the IoT users. At retirement of the device, the IoT device developer terminates supporting the IoT device. Security and privacy requirements are considered in design and development of the IoT device, and implemented as features of the IoT device, e.g.

d) user authentication and access control mechanisms of the device;

e) physical security feature such as secure case; and

f) device software and firmware updating mechanism and operation.

During supplier relationships, information of these features is provided to and used by the IoT service developers and the IoT service providers at relevant stages of their life cycles. An IoT device developer should ensure that adequate and updated device information including security related information is available to all relevant stakeholders.

The IoT service developer designs, develops, produces, and supports the IoT system that enables the IoT service. At retirement, the IoT service developer terminates supporting the IoT system. Based on requirements for an IoT service driven by the needs of the assumed users of the service, security and privacy requirements are considered in design and development of the IoT system, and implemented as features of the IoT system, e.g.

g) user authentication and access control mechanisms of the service;

h) protection against malware;

i) redundancy of components and network;

j) software updating mechanism and operation; and

k) functions and procedures for system operations.

Information of these features is provided to and used by the IoT service providers at relevant stages of its life cycle and they need to be aligned with the security features of the used IoT devices.

The IoT service provider develops the operation and operates the IoT service acquired from the IoT service developer. At retirement, the IoT service provider terminates provision of the service. The activities of these phases of the life cycle, i.e. development, operation and retirement, are implementation of system life cycle processes given in ISO/IEC 15288 including but not limited to:

l) acquisition process;

m) supply process;

n) organizational project enabling processes;

o) technical management processes;

    1) risk management process;

    2) quality assurance process;

p) technical processes;

    3) operation process;

    4) maintenance process; and

    5) disposal process.

Among these processes, the risk management process and the quality assurance process are key to security and privacy in the IoT service. In the risk management process, security and privacy risks are assessed and treated by applying the features of the IoT devices and the IoT system and implementing secure operations. Through the quality assurance process, the IoT system and software are ensured to be excluding vulnerabilities and malicious components, and to have necessary safety functions that ensure availability of the IoT system along with other safety aspects.

Through the supply process, information related to security and privacy in the use of the IoT service and software updates are provided to the IoT user.

The IoT user chooses an IoT service that meets its service and functional requirements along with security and privacy requirements. Information related to security and privacy is provided by the IoT service provider and the IoT device developer, and are examined by the IoT user at this stage. After purchasing the IoT service, the IoT user applies software and firmware updates and uses other information provided by the IoT service provider and the IoT device developer to keep the level of security and privacy during the operation till the decommissioning of the IoT device.

It should be noted that security and privacy issues can occur due to lack of consistency among life cycles of the stakeholders. As an example, the IoT service providers should be aware of the possibility that support period of a specific IoT device terminates during the operation of the IoT service, or the IoT device developer or other IoT service developer cease to exist in the market, while the IoT users continue to use the IoT device whether aware or not of the termination.

5.6 Domain based reference model

IoT reference models presented in ISO/IEC 30141 provide views of the IoT systems. One of the reference models is the domain based reference model which is a framework of functions constituting the IoT system and its operations. Figure 2 is derived from ISO/IEC 30141:2018, Figure 13. The IoT user, the

IoT service provider and the IoT service developer are added in this figure to show relevance of these stakeholders to the IoT domains.

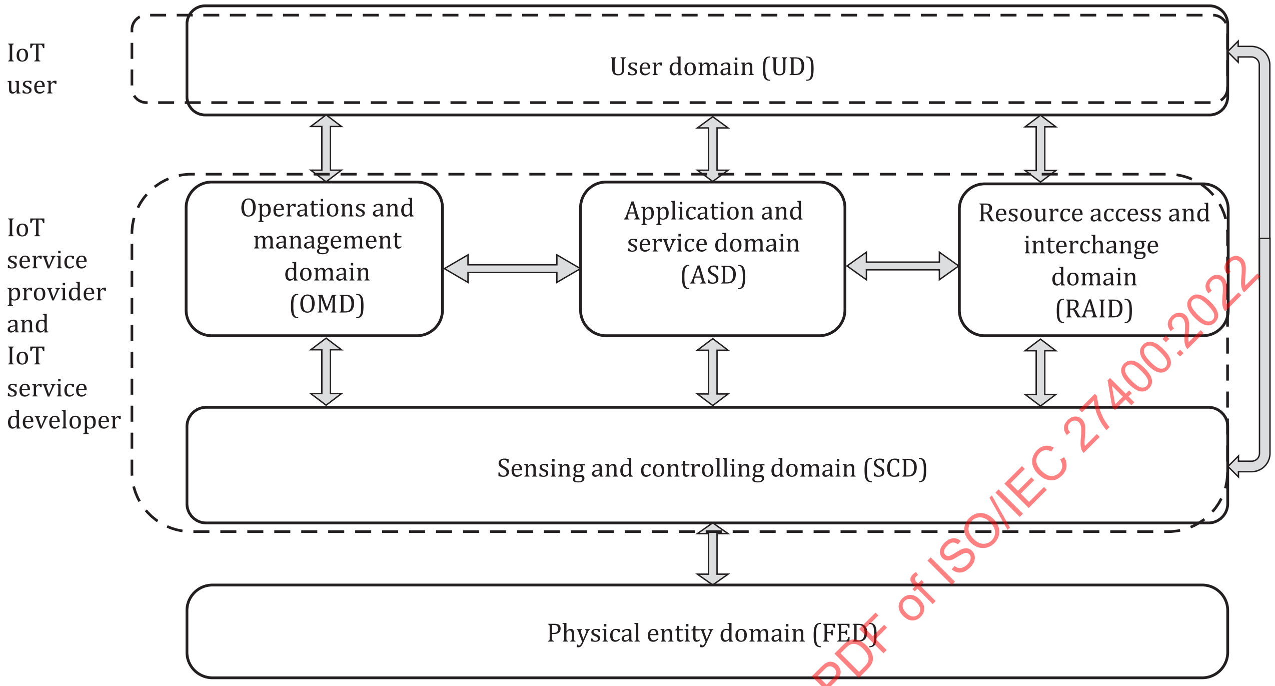
IoT user
User domain (UD)
IoT service provider and IoT service developer
Operations and management domain (OMD)
Application and service domain (ASD)
Resource access and interchange domain (RAID)
Sensing and controlling domain (SCD)
Physical entity domain (FED)

Figure 2 — Domain based reference model

Figure 2 shows the following IoT domains:

— the User Domain (UD) includes human and digital users;

— the Physical Entity Domain (PED) includes the physical entities in an IoT system;

— the Sensing and Controlling Domain (SCD) includes IoT devices and IoT gateways;

— the Operations and Management Domain (OMD) includes the operation support system and the business support system;

— the Resource Access and Interchange Domain (RAID) provides mechanisms by which external entities can access the capabilities of the IoT systems; and

— Application and Service Domain (ASD) includes the applications and services offered by the IoT service providers.

The domain-based reference model provides the overall structure of the elements of an IoT system for considering IoT security and privacy. The risk sources can be identified in relation to the IoT domains (see 6.2). Each of the security and privacy controls can be related to one or more IoT domains (see Clause 7).

6 Risk sources for IoT systems

6.1 General

This clause provides guidance and information on IoT specific factors and inputs which need to be considered when identifying risk sources for IoT systems.

Based on identified risk sources, risk management for IoT systems should be done by using the approaches and methods which have been standardised.

Information on these approaches or methods is already covered by other International Standards, in particular:

- ISO 31000, giving generic guidelines on risk management;
- ISO/IEC 27005, giving information security specific guifdelines for risk management;
- IEC 62443 (all parts), giving guidance in the domain of industrial automation and control systems;
- ISO/IEC 29134, giving guidelines on privacy impact assessment.

Where adoption of an information security management system is required, following International Standards are relevant as well:

- ISO/IEC 27001, providing requirements for information security management systems;
- ISO/IEC 27701, providing extended requirements to the information security management systems requirements for privacy information management.

There are IoT specific risk sources which need to be considered for the risk assessment of IoT systems, which are further detailed in 6.2.

6.2 Risk sources

6.2.1 General

A risk source is an element which alone or in combination has the intrinsic potential to give rise to risk (see definition of risk source in ISO/IEC 31000). When identifying risk scenarios and risks in an IoT system, application or service, relevant risk sources to be contained in the risk scenarios should be identified thoroughly. Please see Annex A: IoT monitoring camera sample risk scenario for a detailed walkthrough to performing a risk assessment. There are varied categories of risk sources including but not limited to:

a) vulnerability of the IoT system, application or service;

b) lack of knowledge and skills of persons who have roles in the provision or use of the IoT system, application or service;

c) human error of persons who have roles in the provision or use of the IoT system, application or service;

d) existence of persons who have malicious intent of attacking the IoT system, application or service;

e) quality of the IoT system, application or service and components of them;

f) existence of external systems and devices that can be abused in generating attacks on the IoT system, application or service;

g) existence of natural phenomena, e.g. lightning, flood and earthquake; and

h) lack of the organizational governance within the stakeholders of the IoT systems.

6.2.2 provides sample risk sources for each of the IoT system domains, 6.2.3 lists risk sources originating from outside the IoT domains, and 6.2.4 discusses privacy related risk sources.

6.2.2 Sample risk sources related to IoT domains

6.2.2.1 Sensing and controlling domain

Following is a list of risk sources which should be considered in the sensing and controlling domain.

- Software and firmware of an IoT device or an IoT gateway has technical vulnerabilities.

- Software and firmware of an IoT device or an IoT gateway has no or insecure updating mechanism.
- An IoT device or an IoT gateway has no or weak security function, e.g. weak authentication function, encryption and redundancy.
- An IoT device or an IoT gateway can be configured in an insecure way.
- An IoT device or an IoT gateway does not have a level of quality that ensures continued operation in a durable period.
- A developer of an IoT device or an IoT gateway does not have the capabilities required to develop a secure IoT device or an IoT gateway.
- A developer of an IoT device or an IoT gateway does not have the capabilities to implement quality that ensures continued operation in a durable period.
- An IoT device or an IoT gateway is located at a site not protected by physically secure facility.
- An IoT device or an IoT gateway is located at a site where no personnel are stationed.
- An IoT device or an IoT gateway operates under influence of weather and other environmental conditions.
- An IoT device or an IoT gateway is produced through ICT supply chain.

6.2.2.2 Operations and management domain

Following is a list of risk sources which should be considered in the operations and management domain.

- An IoT service provider does not have the capabilities required to operate the IoT system securely.
- Documented procedure for operation of an IoT system or service has vulnerabilities.
- Documented procedure for operation of an IoT system or service is not followed by a system operator.
- An administrator or an operator of an IoT system or service makes mistake in the operation.
- An administrator or an operator of an IoT system or service has malicious intent.
- An IoT service provider lacks awareness on privacy while using CRM (customer relationship management).

Risk sources in this domain likely affect the integrity and availability of sensor data or actor instructions.

Integrity issues or unauthorized changes of such data might be difficult to detect – as an example, changed sensor calibration data might still lead to senseful sensor data, but which might not reflect reality.

6.2.2.3 Application and service domain

Following is a list of risk sources which should be considered in the application and service domain.

- An IoT service developer does not have capabilities to develop a secure IoT application and service.
- An IoT service developer does not have the capabilities to implement quality that ensures continued operation in a durable period.
- Established methodology is not followed in the development of a system, application or service.
- A developer of an IoT system, application or service makes errors in the development.

- An IoT system, application or service has vulnerabilities.
- A developer of a system, application or service has malicious intent.

6.2.2.4 Resource access and interchange domain

Following is a list of risk sources which should be considered in the resource access and interchange domain.

- An IoT system, application or service has no or weak security function, e.g. weak authentication and authorization function or access control.
- An IoT system, application or service does not have a level of quality that ensures continued operation in durable period.
- An IoT service developer does not have capabilities to design and apply secure settings for an IoT system, application or service.

Risk sources in this domain likely affect the integrity and availability of sensor data or actor instructions.

Incidents caused by risk source of this domain might also be difficult to detect – as an example, sensor data from the wrong sensor which is of the same type than the correct sensor is very likely still in a valid range.

6.2.2.5 User domain

Following is a list of risk sources which should be considered in the user domain.

- An IoT user is not aware of the risks in security and privacy in the use of an IoT device and an IoT service.
- An IoT user does not have capabilities to choose secure IoT device or IoT service.
- An IoT user does not have capabilities to securely setup and operate an IoT device and an IoT service.
- An IoT user does not know the contact point that provides support for the secure use of IoT device or IoT service.
- An IoT user lacks knowledge of technical vulnerabilities.
- An IoT user does not know when the period of support ended for the IoT device and/or the IoT services.

Incidents caused by risk source of this domain can also be difficult to detect – e.g. since wrong sensor data might still be in a valid range and no immediate impact might be visible to the user.

Following is a privacy risk source which should be considered in IoT user domain:

- IoT user lacks knowledge and awareness on privacy by design framework.

6.2.3 Risk sources from outside the IoT domains

Following is a list of risk sources that can be identified in the areas external to an IoT system. 6.2.2 provides sample risk sources for each of the IoT system domains, and in 6.2.3 other sample risk sources originating from outside the IoT system domains are given.

- There exist persons with malicious intent who attack, intrude into or abuse the IoT system, application or service.
- There exist vulnerable systems and devices on the internet and other networks that can be abused to generate attacks on the IoT system, application or service.

- There exist natural phenomena, e.g. lightning, flood and earthquake, which can compromise operations of IoT system, application or service.
- Availability of IoT system, application or service depends upon availability of electric power and other utilities supply.
- Availability of IoT system, application or service depends upon availability of network services.
- The complexity of the ICT ecosystem may lead to a privacy breach.

6.2.4 Privacy related risk sources

Privacy is a key concern for the IoT-enabled products and services across verticals. While new business and service models are being designed in different domains using data recorded by IoT sensors and data derived from IoT services, it is also bringing up concerns about protection of user's privacy.

Many IoT services tend to focus on the need to simplify IoT user responsibilities, placing those responsibilities on IoT device developers and IoT service providers. The user might find it difficult to understand the architecture of these IoT products and services, and what data the IoT sensors are collecting about them, because that details of captured data are either not shared explicitly by the device manufacturers and service providers or the users may be lacking awareness that they should know the operational know-how of the IoT device and IoT service to a certain extent for their personal benefit.

As IoT enabled services to become popular, the gradual overlap of IoT devices and services with our daily routine will also result in increased concerns of user privacy if it is not addressed right from the design phase. This is because the capability of IoT devices to talk to each other (M2M Machine to Machine communication) and the technical capability of sharing contextual data between these devices and third parties can aid in profiling of users and gauging user behaviour by data aggregation, re-identification and analytic methods, for business benefits that might happen without the knowledge or consent of the user. As IoT devices are almost always online, these can leave a trail of data on the internet. Such data can be accumulated to create a digital footprint of the devices and the device owners. Cookie invasion of IoT devices can also cause privacy breaches.

For example, a digital impression of our daily life can be created by monitoring smart devices at home, tracking the location of our smart cars, monitoring our health parameters from smart health devices or by tracking our conversations using the smart devices meant for some other use. The spatial and temporal aspects of the IoT products and services can assist in aggregation of specific data that can help to infer various traits of the users. The smart products and services can be interconnected and interdependent, as in smart cities, where the home security system can feed data and alerts to the city surveillance system maintained by the city police or government, the smart refrigerator can order food from online grocery on behalf of the owner, or the smart health monitoring system can send health data from the smart wearable health monitoring device to the health insurer. The IoT service interfaces can make the contextual data usage opaque to ordinary people who may leave the IoT devices on default settings without any fine-tuning for privacy conservation, ultimately leading to privacy breaches.

These design faults from IoT service developers and IoT service providers, and lack of cognizance or inability of the IoT users can lead to misuse of personally identifiable information and privacy invasion leading to mistrust and disrepute of the smart devices and services. Privacy should be considered as a key enabler to realize the potential of the IoT technology in tandem with other trust-enablers like security, safety, reliability and resilience. These together form the foundation of a trustworthy connected world of 'things'.

7 Security and privacy controls

7.1 Security controls

7.1.1 General

Security controls are recommended here for IoT systems. These are intended for the IoT service provider, IoT service developer and IoT user.

These controls are intended to be used in conjunction with others, without being limited to IoT specific controls. For example, these can be utilized in combination with the controls in ISO/IEC 27002.

For the description of the controls a common format is used:

Control XX – Specified Control, where XX stands for a serial number, which is introduced for easy reference to the control.

Purpose – explains the purpose of the controls.

Audience – names the stakeholders which are involved and should be informed about the control. Refer to 5.3 for a list of the relevant stakeholders.

IoT domain – lists the domains the control relates to, based on domain based reference model introduced in 5.6.

Guidance – provides guidance information for the implementation of the control.

7.1.2 Security controls for IoT service developer and IoT service provider

7.1.2.1 Policy for IoT security

Control-01

A policy for IoT security should be defined, approved by management, published, communicated to relevant personnel and relevant external parties and reviewed at planned intervals or if significant changes occur.

NOTE The concept of personnel includes the organization’s members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.

Purpose

To provide management direction and support for IoT security within the IoT service developer or the IoT service provider in accordance with business requirements, expectations of stakeholders.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The IoT service provider or the IoT service developer should define its policy for IoT security demonstrating management commitment to IoT security.

The policy for IoT security should address requirements identified through understanding:

a) organizational responsibilities in the provision of IoT services;

b) internal and external stakeholders and their expectations; and

c) risk environments.

The policy for IoT security should contain statements regarding:

1) definition of IoT security;

2) organizational objectives of IoT security;

3) roles and responsibilities for IoT security within the organization (see 5.3).

The policy for IoT security should address information security and other aspects which include quality of the IoT service that are relevant to IoT security and can cause IoT security incidents. The policy for IoT security should also consider the consequences of incidents that affect safety of the internal and external stakeholders.

7.1.2.2 Organization of IoT security

Control-02

Roles and responsibilities for security of IoT should be defined and allocated.

Purpose

To establish and maintain a management framework to initiate and control the implementation and operation of IoT security within the IoT service provider or the IoT service developer.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management.

Guidance

Allocation of roles and responsibilities for security of IoT should be done in accordance with the policy for IoT security (see 7.1.2.1).

Subroles of IoT service provider and IoT service developer (see 5.3.2 and 5.3.3) should be allocated with IoT security roles and responsibilities.

The IoT security roles and responsibilities should include but not limited to those for:

a) risk management activities (see Clause 6);

b) designing security measures for the IoT systems, devices and services;

c) implementing and operating the security measures in the development and operation of the IoT systems, devices and services;

d) managing supplier relationships;

e) awareness, education and training programs; and

f) incident management program.

Roles and responsibilities should be documented, disseminated within the organization and reviewed and updated as necessary.

7.1.2.3 Asset management

Control-03

Information, IoT devices and systems and their functions and operations to be protected should be identified.

Purpose

To identify assets of IoT devices and systems for designing appropriate protecting measures.

Audience: IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

IoT service providers need to identify the assets related to the life cycle of the IoT service and document their importance. The life cycle of the IoT service should include creation, processing, storage, transmission, deletion, destruction. Documents related to the identified assets should be saved in a dedicated or existing inventory as needed.

Inventory of assets should be accurate, up to date, consistent.

The assets in the life cycle of IoT devices and systems may include the followings:

a) software and firmware implemented on IoT devices and systems;

b) factory-set properties for initial use of IoT devices and systems;

c) sensed data and controlling data;

d) communicated data from/to IoT devices and systems.

Implement an IoT device management to manage IoT device configurations and to always have knowledge to which physical assets IoT devices are paired.

7.1.2.4 Equipment and assets located outside physical secured areas

Control-04

Specific security measures should be applied to IoT equipment and assets which are located or operated outside physical secured areas.

Purpose

To prevent loss, damage, theft or compromise of IoT devices and interruption to the operation of IoT services.

Audience: IoT service provider.

IoT domain: Operations and Management.

Guidance

When IoT devices are located outside the premises of the IoT service provider, the following guidance should be considered to address associated risks.

a) Ensure adequate physical protection of sensors and actuators. Cases of sensors and actuators placed in public areas should provide adequate resistance against opening to protect sensors and actuators from theft, destruction or manipulation.

b) Ensure that locations of sensors and actuators are regularly checked, e.g. in the context of asset management activities.

c) If only limited physical protection of IoT devices is possible, any users of the devices (e.g. consumers of sensor values) should be made aware of the limited trust level the devices provide.

d) Ensure sensitive information, such as cryptographic key material, is adequately protected from unauthorized disclosure or modification, using hardware based secure storage or similar techniques.

7.1.2.5 Secure disposal or re-use of equipment

Control-05

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose

To prevent information leakage and malicious use of the IoT device and other equipment of the IoT system at its disposal or re-use.

Audience: IoT service provider.

IoT domain: Operations and Management or Sensing and Controlling.

Guidance

Storage media should be physically destroyed, or information stored in the media should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable before disposal or re-use.

Disposal or re-use of IoT devices incur risks that software code or data are retrieved, analysed, modified and abused. Consequences of insecure disposal or re-use can be identity theft, unauthorized transaction, attacks on the IoT system, infringement of license terms and other incidents that affect the IoT users, IoT service developers, IoT service providers and other entities.

7.1.2.6 Learning from security incidents

Control-06

Knowledge gained from analysing and resolving IoT security incidents should be used to reduce the likelihood or impact of future incidents.

Purpose

To reduce negative effects of incidents in the provision and use of IoT services.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The source of knowledge can be internal or external.

a) When an incident handling by the IoT service developer or IoT service provider is closed, the causes and consequences of the incident are identified.

b) When an IoT security incident is reported by external authority, its relevance to the IoT system and service is examined and identified.

Based on the knowledge, IoT service developer and IoT service provider should modify as necessary:

c) risk assessment, e.g. identification of risk sources and evaluation of risk;

d) risk treatment, e.g. applied controls and their implementation; or

e) incident management processes.

For example, knowledge of:

- newly announced software vulnerability can affect security measures of the IoT service (c);

- an attack on the IoT system can require modified or additional implementation of a control (d); or
- an operational issue can indicate need for changing incident management process across IoT service provider and IoT users (e).

Other information

ISO/IEC 27035 (all parts) provides guidelines for information security incident management, including lessons learnt, which are generic and applicable to all organizations. Guidance of this subclause highlights the aspects of lessons learnt relevant to IoT services.

7.1.2.7 Secure IoT system engineering principles

Control-07

Principles for engineering secure IoT systems that address designing and implementation of security functions, defence in depth and hardening of systems and software should be applied to the development of IoT systems.

Purpose

To ensure that security is designed and implemented in the development of IoT systems.

Audience: IoT service developer.

IoT domain: Application and Service, Sensing and Controlling or Resource Access and Interchange.

Guidance

The IoT service developer should have principles for engineering secure IoT systems.

The principles should require risk identification of IoT system considering the consequences that can affect the IoT users, the IoT service providers and other external entities on the network.

The risk identification should take different aspects of the IoT system into consideration. Examples of those aspects are:

a) interfaces between the IoT system and external entities through networks;

b) internal fraud in system operation and maintenance;

c) quality issues of products and services acquired from external entities;

d) physical access to the IoT system and devices;

e) changes in environmental conditions; and

f) manufacturing processes for installing critical data, e.g. firmware, cryptographic keys and certificates.

The principles should address the following areas of security measures to be considered in the IoT system development:

g) security functions;

h) hardening requirements of the system and software;

i) requirements for defence in depth, i.e. layered design of security functions; and

j) functions for monitoring and logging.

The principles should be applied to the development of IoT systems with the following security design concepts:

k) Secure by default: this concept covers guidelines to choose the most secure options that are available during procurement and configuration, for example:

- minimizing attack surfaces;
- using a secure supply chain;
- using standards, best practices and reuse validated codes;
- system hardening and operating with least privilege;
- reducing exposure time.

l) Rigour in defence: this concept covers guidelines to ensure care and completeness in architecting the system, for example:

- defence in depth (multilayer);
- defence in breadth (variety), protecting uniformly;
- compartmentalization of system (e.g. network segmentation);
- using encapsulation to manage access to functions;
- monitoring, detection and reporting of anomalies, including the use of honey pots;
- vulnerability assessment and pen testing;
- using a secure engineering approach;
- secure system life cycle;
- patch diligently.

m) Accountability: this concept covers guidelines to ensure care in granting and monitoring access to assets during operation. It also includes responsibility for reporting and mitigating known vulnerabilities, for example:

- connecting carefully and deliberately;
- ensuring the segregation of duties;
- establishing and protecting audit trails;
- practicing transparency (e.g. vendor disclosure, breach disclosure).

n) Resiliency: this concept covers guidelines to ensure ability to resist or recover from a security incident, for example:

- designing for redundancy;
- managing availability;
- assumption of breach;
- failing securely (e.g. loss of devices or connectivity);
- managing vulnerability;
- backup and recovery;
- testing for scale.

7.1.2.8 Secure development environment and procedures

Control-08

Secure development environment and procedures should be applied to the development of IoT systems.

Purpose

To avoid introduction of insecurity to IoT systems during development.

Audience: IoT service developer.

IoT domain: Operations and Management, Application and Service or Sensing and Controlling.

Guidance

A development environment includes people, processes, technology and facilities associated with a system development.

The IoT service developer should assess risks in individual IoT system development efforts and establish secure development environments considering:

a) personnel working in the environment;

b) applied development methodologies and software and data handling processes;

c) use of outsourced products and services;

d) physical and network environment; and

e) coexistence with other development and operational efforts.

The IoT service developer should determine development environment and associated procedures to mitigate the risks. The procedures should be disseminated to individuals involved in the development efforts.

Secure software development procedures should be applied to IoT software development. Methodologies supporting the procedures, not limited to those for IoT applications, include those addressing:

f) secure software development life cycle;

g) threat modelling; and

h) secure coding.

Secure software development procedures can be facilitated by tools for integrated development environment and secure coding supporting the implementation of the methodologies.

7.1.2.9 Security of IoT systems in support of safety

Control-09

Security principles in support of safety should be applied to the development of IoT systems.

Purpose

To support safety in IoT systems.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

In an IoT system, security events and controls can affect safety of the IoT system, e.g.:

a) incorrect or corrupted control data can cause malfunctioning of the IoT system;

b) security attack can cause safety function of the IoT system being inoperable; and

c) implementation of a security control can affect performance of the IoT system and its safety functions.

The IoT service developer should consider hazards in the IoT system that can affect operation of the IoT system and its safety functions as possible consequences of security events.

The IoT service developer should also consider impacts of implemented security controls upon operation of the IoT system and its safety functions.

Other information

There is a case that "safety" is prioritized over "security". This can be covered by the standards in ISO/IEC JTC 1/SC 41.

7.1.2.10 Security in connecting varied IoT devices

Control-10

An IoT system should be designed and implemented to ensure and maintain security in connecting varied IoT devices.

Purpose

To maintain security of IoT system in connecting varied IoT devices including those not necessarily verified by the IoT service developer or the IoT service provider.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The IoT service developer and the IoT service provider design and implement an IoT system and require the IoT devices to meet defined specifications. The IoT devices are tested as components of the IoT system.

There is possibility that the IoT devices not yet tested as components of the IoT system are adopted. This is possible because testing all of the new models of supported devices can be impracticable. Or, IoT users, as consumers, can choose the devices available at market.

The IoT service developer and the IoT service provider should design and implement secure IoT system which is prepared for the situation. The IoT system can have the following capabilities as necessary:

a) selectively connect the IoT device using a whitelist; or

b) where applicable, obtain the specifications of the device, e.g. name of provider, model, year of production, conformance to relevant standard and use of best practices, when negotiating with the device for connection, and determine if the connection request is accepted or rejected, or confine the scope of function, service or information to be made available.

7.1.2.11 Verification of IoT devices and systems design

Control-11

Design and implementation of IoT devices and IoT systems should be verified.

Purpose

To ensure security and safety of the IoT device and IoT system.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

An IoT system is composed of IoT devices and other equipment. In the case where the IoT service developer or the IoT service provider acquires and integrates the IoT devices to build the IoT system, it should verify that the IoT devices and integrated IoT system function as intended.

The IoT service developer and the IoT service provider should:

a) identify the IoT devices, functions and interfaces that need to be verified;

b) plan verification testing; and

c) perform the testing.

7.1.2.12 Monitoring and logging

Control-12

States, events and network traffic of IoT devices and systems should be monitored and logged.

Purpose

To detect and trace abnormalities and incidents of IoT devices and systems.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management.

Guidance

Monitoring and logging should be designed and implemented addressing the following aspects:

a) functions and operations for monitoring and logging the states, events and network traffic of IoT systems and devices including sensors and actuators;

b) functions and processes to analyse the logs;

c) systems, human and organizational response triggered by detected abnormalities and incidents.

States, events and communications to be monitored and logged can include those of:

d) security;

- user authentication;
- location of IoT devices;
- changes to the IoT system configurations;
- network traffic;
- processors and memory usage;
- indication of attacks and unauthorized accesses;
- malfunction;

- values which exceed normal ranges of sensing and actuating data;
- values which indicate any unauthorized or unintended manipulation of sensing and actuating data; and

e) reliability;

- outage of IoT device or system; and
- environmental conditions, e.g. temperature and moisture.

If an IoT device is able to self-locate its position, this should be used to monitor unintended transfer of the device.

Available resources for computing, storage and communication should be considered, and various needs for monitoring and logging should be prioritized when designing the functions for monitoring and logging. It should be noted that there are IoT devices which have limited resources and functions and not feasible for self-monitoring and logging. For these devices, monitoring and logging need be designed to be performed on servers or network nodes of the IoT system.

Logs of an IoT system can be collected in a logging system to facilitate management and operations. IoT devices located off-premises of IoT service provider can be vulnerable in maintaining the logs.

Clocks should be synchronized within an IoT system to allow consistent analysis.

Ensure adequate monitoring of IoT sensors, IoT actuators and other equipment is in place to early detect outages, malfunctions or values which exceed normal ranges indicating any unauthorized or unintended access as well as manipulations of sensed of actuating data.

Include IoT Elements in logging and monitoring activities to early identify any suspicious behaviour of IoT elements. This should include indications of unauthorized access as well as manipulations of sensor or actor data.

7.1.2.13 Protection of logs

Control-13

Logs for IoT devices and systems should be protected from leakage, destruction and unintended alteration.

Purpose

To ensure the capability and reliability of logging.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management.

Guidance

Protection of the logs for IoT devices and systems should be designed and implemented. Measures to protect the logs can include:

a) access control of the log file;

b) access control of the device or system handling the log;

c) physical access control of the facility housing the log media;

d) enforcement of procedures for handling the logs;

e) redundant configuration of the log;

f) detection of destruction or alteration of the log, e.g. use of hashed values;

g) encryption of the log;

h) entries in the log with timestamps; and

i) logs that should only be “read-only” for all except for the system process.

7.1.2.14 Use of suitable networks for the IoT systems

Control-14

Applied network and communication technologies for IoT and systems should meet the needs of communication function, capacity and security, and of function and performance of IoT devices.

Purpose

To use the network that meets security, performance and other needs of the IoT system.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management, Application and Service or Resource Access and Interchange.

Guidance

The IoT service developer and the IoT service provider should identify security, performance and other needs for the network. The needs can be those related to:

a) geographical locations of the IoT devices and system;

b) mobility of the IoT devices;

c) performance and functional restrictions of IoT devices to be connected;

d) confidentiality and integrity of information in transit;

e) availability of the communication; and

f) bandwidth of the network.

To meet the identified needs, the IoT service developer and the IoT service provider should consider to:

g) choose adequate communication devices and services considering, e.g. service area, requirement for wireless communication, and bandwidth;

h) apply encryption for transmitted information; and

i) use gateway communication device to support IoT device with limited functions.

7.1.2.15 Secure settings and configurations in delivery of IoT devices and services

Control-15

IoT devices and services should be delivered with secure settings and configurations.

Purpose

To ensure security of IoT devices and services in delivery.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The initial settings and configurations of IoT devices and services should be designed to contribute to the security of IoT users.

According to the features of the IoT device or service, relevant settings and configurations can be:

a) versions and patches of software;

b) open ports and network services; and

c) access restriction to the functions and data of the service.

If the IoT device or service requires the IoT user to enter a password, its initial value should be unique to the device or unique to the user of the service. The initial value should be securely informed to the IoT user.

7.1.2.16 User and device authentication

Control-16

Authentication function of users and IoT devices for accessing IoT systems and services should be implemented and applied.

Purpose

To protect information, IoT devices, systems and services from unauthorized access and other security breaches.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

Needs for authenticating the IoT users and IoT devices should be identified considering the operation of the IoT service and associated security risks. The needs can include those for authenticating:

a) a human user for accessing the IoT device, system or service; and

b) an IoT device for connecting to the IoT system.

Technologies applicable for implementing required level of authentication can be:

c) for human users, use of:

- password authentication;
- hardware credential, e.g. IC card; or
- biometrics;

d) for IoT devices, use of:

- device identifier; or
- trust anchor using hardware protection means.

The authentication function should be secure:

e) Password management should be secure against unauthorized use: initial delivery and changing procedures should be secure, strong password should be enforced.

f) Authentication credential should be adequately protected against unauthorized access regardless if it is stored in IoT device or system or in transit.

7.1.2.17 Provision of software and firmware updates

Control-17

Mechanism for updating software and firmware of IoT devices and systems should be designed, implemented and operated.

Purpose

To ensure security for updating software and firmware of IoT device and IoT system.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service or Sensing and Controlling.

Guidance

In the development of IoT service, mechanism for updating software and firmware of IoT devices should be designed and implemented as a basic function.

Software and firmware updates should be provided through reliable source and route such as certified website of the IoT device developer or the IoT service provider.

The software/firmware update package should have its digital signature, signing certificates and signing certificate chain verified by the device before update process begins.

Integrity and confidentiality of cryptographic keys used for update should be securely managed and appropriately operated.

When updates are conducted over the air (OTA), the updates should be performed over encrypted communication channels.

When device cannot verify authenticity of updates itself, it should roll back to the last known good configuration that was stored on the device.

Updates using OTA should either succeed completely or fail in a recoverable manner. In addition, conducting updates should not reduce the existing security level of IoT devices and systems.

The mechanism for rolling back software and firmware should also be designed and implemented to address update failures.

There should be a mechanism to prevent unauthorized downgrade or rollback to an older version during normal operation.

7.1.2.18 Sharing vulnerability information

Control-18

Vulnerabilities of IoT devices, systems and services should be monitored and informed to the IoT users and relevant parties along with associated risks.

Purpose

To ensure relevant stakeholders are informed of vulnerabilities of IoT devices, systems and services and aware of derived risks.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

Vulnerability information should be collected, analysed and disseminated to relevant IoT stakeholders, and finally necessary measures such as firmware updates (see 7.1.2.17) shoud be taken.

The IoT service developers and the IoT service providers should have functions to:

a) investigate security incidents related to the IoT service and identify vulnerability of the IoT system or device that can cause the incidents;

b) collect vulnerability information from the IoT service developers providing components of the system, ISAC (information sharing and analysis centre) and other stakeholders;

c) analyse the impact of the obtained vulnerability information on the IoT devices / systems and services;

d) based on the results of analysis of the vulnerability and its impact on IoT users and stakeholders, determine if it needs to be informed to them.

7.1.2.19 Security measures adapted to the life cycle of IoT system and services

Control-19

Security measures of the IoT system and service should be adapted to and kept during the stages of the life cycle, including their development, operation, maintenance and destruction.

Purpose

To maintain security of IoT system and service throughout the life cycle.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management or Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

During development, security measures of the IoT system and service should be designed and implemented in accordance with the secure IoT system engineering principles (7.1.2.7) and relevant controls given in 7.1.2.8 to 7.1.2.14.

To prepare for operation, maintenance and destruction, the IoT service developer and the IoT service provider should identify relevant entities including IoT users and other IoT service developers and providers with which security information should be exchanged.

When the IoT system and service are installed and operated, secure configurations and settings should be continually enforced. It should be supported by sharing information about:

a) hardening of the IoT system and service;

b) use of secure passwords or other user credentials;

c) disclosed vulnerabilities;

d) software updates;

e) security alerts and workarounds; and

f) termination of technical support for devices and software by the vendors.

When the IoT system, service or components terminate the life cycle:

g) confidential information should be securely destroyed; and

h) the IoT users should be informed of the process to be followed at termination of the IoT system and service.

7.1.2.20 Guidance for IoT users on the proper use of IoT devices and services

Control-20

The IoT users should be provided with guidance on the proper use of IoT devices with risks and undesirable effects of IoT system and service that can be derived from improper use of IoT devices.

Purpose

To make the IoT users aware of the security risks in the use of IoT devices, and to ensure implementation of security measures.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The IoT service developers and the IoT service providers have responsibilities in security that commensurate to their respective roles in the development and provision of the IoT service. In the use of the IoT devices, some of the security measures need to be carried out by the IoT users. To support the IoT users, the IoT service developers and the IoT service providers should provide information about the risks and consequences, and guidance for proper use of IoT devices.

Risks and required actions to mitigate the risks should be informed to the IoT user before commencement of service delivery.

Risks and required actions can include those related to:

a) supported IoT devices;

b) supported versions and modification levels of software;

c) requirements for initial set-up and user registration;

d) secure use of the IoT system and service;

e) security risks caused by inappropriate use of the IoT system and device, and

f) contact point of the IoT service developer and the IoT service provider accessible during operation.

Especially changes to the settings and configurations by the IoT users should be guided with supporting information that contribute to the secure use of the device or service.

The IoT users should be guided to change the initial password. Change of initial password may be procedurally mandated where appropriate.

The guidance can include:

g) devices and configurations verified for use in the IoT system and service;

h) necessary security updates for software;

i) secure setting (such as for Wi-Fi) and configuration; and

j) criteria for qualified passwords.

Risks and consequences provided to the IoT users can include but not limited to:

k) malware infection of the IoT device;

l) leakage of the IoT user's personal information;

m) leakage of business information; and

n) malicious use of the IoT device for DoS attack.

The security information provided by the IoT service developer or the IoT service provider should be a part of the user/administrator guide of the product or service.

7.1.2.21 Determination of security roles for stakeholders

Control-21

Roles of IoT service developer, IoT service provider and other stakeholders in security of IoT system and service should be determined and agreed among relevant parties.

Purpose

To ensure security of IoT system and service that involve entities participating in the provision and use of IoT system and service.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

The roles of IoT service developer and IoT service provider in security should be determined along with their roles in IoT service provision. The IoT service developer should have security roles in developing, implementing, testing and integrating the IoT service. The IoT service provider should have security roles in managing and operating the IoT service. Subroles of the IoT service developer and the IoT service provider should be allocated with security roles as necessary.

The security roles should be communicated to relevant parties including the IoT users. The communication can be in the form of:

a) service specification provided to the IoT users; or

b) agreement between the parties in the supply chain for the IoT service.

The security role of the IoT user can be enforced in the initial set-up procedure requiring an action as confirmation of the security role.

7.1.2.22 Management of vulnerable devices

Control-22

Vulnerable IoT devices should be detected, recorded, and alerts provided to IoT users and administrators of these devices.

Purpose

To maintain IoT devices to be secure.

Audience: IoT service provider.

IoT domain: Operations and Management.

Guidance

The IoT service provider should develop and establish mechanisms for:

a) detecting and recording vulnerable IoT devices; and

b) providing alerts to the IoT users and administrators of the devices.

During operation, IoT devices should be monitored continually to detect malfunctional behaviours. Once any suspicious behaviour is detected, it should be recorded, and alert should be noticed to the IoT users and administrators.

Include IoT devices in vulnerability management processes to ensure identification and adequate handling of any vulnerability present in devices.

7.1.2.23 Management of supplier relationships in IoT security

Control-23

Specifications and supporting obligations of suppliers for information security of IoT device and IoT service should be managed by the acquiring organization based on the contracts with suppliers.

Purpose

To ensure continued provision of secure IoT device and service.

Audience: IoT service provider or IoT service developer.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

When an IoT service developer or an IoT service provider procures IoT devices and IoT services, a mechanism should be established that allow the acquiring organization to determine security specifications and controls implemented by the supplier and security controls that should be implemented by the acquiring organization. These security specifications and controls should include;

a) vulnerability management;

b) firmware updates;

c) system changes due to the specification changes of IoT devices; and

d) provision of related information to the IoT users. When developing this mechanism, appropriate management based on contracts should be conducted so that necessary information can be reliably obtained from the suppliers.

When an IoT device developer suspends supply of IoT devices or drastically changes their specifications, notice should be provided with sufficient time so that appropriate decision can be made by the acquiring organizations.

7.1.2.24 Secure disclosure of Information regarding security of IoT devices

Control-24

Information on the IoT device relevant to security of IoT services should be documented and disclosed only to the parties that require them.

Purpose

To ensure security of the IoT services that use the IoT device.

Audience: IoT device developer.

IoT domain: Sensing and Controlling.

Guidance

Information on the IoT device relevant to security of IoT services should be disclosed to the relevant IoT service developers and IoT service providers to support development and provision of security controls of the IoT services.

For planning and development of the IoT services, following information on the IoT device should be disclosed:

a) specifications including those of security functions;

b) availability of software or firmware updates; and

c) warranty period.

For operation and maintenance of the IoT services, following information on the IoT device should be disclosed:

d) newly found vulnerabilities;

e) upgrades of software or firmware; and

f) termination of manufacturing or shipment.

The information should be documented so that it can be accurately delivered. The information should be disclosed under a contract such as non-disclosure agreement to prevent its leakage to malicious third parties.

7.1.3 Security controls for IoT user

7.1.3.1 Contacts and support service

Control-25

IoT users should only choose IoT devices and IoT services that provide contact information for support service.

Purpose

To ensure security in the use of IoT device and service.

Audience: IoT user.

IoT domain: User.

Guidance

The IoT user should be able to access support services for the IoT device and IoT service that provide information and respond to queries including those related to security (7.1.2.19, 7.1.2.20, 7.1.2.22).

An IoT device or service should not be chosen if there is no information about the manufacturer or contact point for support service. The provider of such IoT device or service should not be trusted to have capability of excluding malicious code and maintain adequate security throughout the life cycle of the device or service..

7.1.3.2 Initial settings of IoT device and service

Control-26

Initial settings of IoT device and service should be applied correctly.

Purpose

To ensure secure initial settings of IoT devices and service.

Audience: IoT user.

IoT domain: User.

Guidance

Default settings of authentication information such as “factory-set ID” and “default password” for IoT devices are thought to be known to the public since the user’s manual is publicly available. The default authentication information should be reset by the IoT user. The new setting should not be the same as the original, should not be shared with other IoT device setting, and should not be easily guessable and not on the list of popular ID/password list available on the internet.

7.1.3.3 Deactivation of unused devices

Control-27

IoT devices should be deactivated and credentials revoked when they are no longer in use.

Purpose

To reduce the security risks caused by the IoT device that is no longer used.

Audience: IoT user.

IoT domain: User.

Guidance

IoT devices, that are no longer in use but are still connected to network, can be taken over and used without noticing via network by unauthorized third parties. To reduce the potential risk of abusing IoT devices, IoT devices that are no longer in use should be deactivated, e.g. turning off the device.

This control should be applied to properly implement “Termination” in the life cycle of IoT users given in 5.5.

7.1.3.4 Secure disposal or re-use of IoT device

Control-28

Data and licensed software stored in IoT device should be removed or securely overwritten prior to disposal or re-use.

Purpose

To ensure information protection in disposal or re-use of IoT devices.

Audience: IoT user.

IoT domain: User.

Guidance

Information collected and used during IoT service operation can be stored in the IoT devices. To avoid information leakage to other users and third parties, the information stored in the IoT devices should be deleted, or the IoT devices should be reset to the factory default state before disposing or reusing the IoT devices.

7.2 Privacy controls

7.2.1 General

Privacy controls are recommended here that are in the context of IoT. These are intended for the IoT service developer, IoT service provider and IoT user. These controls align with ISO/IEC 27701 for base controls on privacy information management and are distinct for IoT from the perspectives of privacy by design and privacy by default.

For the description of the controls a common format is used:

Control XX – Specified Control, where XX stands for a serial number, which is introduced for easy reference to the control.

Purpose – explains the purpose of the controls.

Audience – names the stakeholders which are involved and should be informed about the control. Refer to 5.3 for a list of the relevant stakeholders.

IoT domain – lists the domains the control relates to, based on domain based reference model introduced in 5.6.

Guidance – provides guidance information.

7.2.2 Privacy controls for IoT service developer and IoT service provider

7.2.2.1 Prevention of privacy invasive events

Control-29

Privacy enhancing capabilities should be built in the IoT devices and IoT services.

Purpose

To prevent privacy invasive events in the provision and use of IoT devices and IoT services.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

Identify sensitive data components early in the design phase. Embed privacy enhancing capabilities into the IoT device architecture and IoT service design to prevent privacy invasive events.

7.2.2.2 IoT privacy by default

Control-30

Stakeholders in an IoT system should ensure that without any IoT user interaction or intervention, the strictest privacy settings apply by default.

Purpose

To protect PII without the need of user interaction or intervention.

Audience: IoT service developer or IoT service provider.

IoT Domain: Operations and Management or Application and Service.

Guidance

Proper access control mechanism should be in-built with the device and service. The accountability of privacy protection should be on the IoT service developers and IoT service providers. A default privacy setting aims to protect PII without the need of user intervention.

Based on the privacy impact assessment, the collected PII should be determined and processed appropriately. Based on these findings, control mechanisms should be implemented to protect PII by default, and users are advised to these in a user policy or statement.

7.2.2.3 Provision of privacy notice

Control-31-1

The IoT user should be provided with a privacy notice which states personal data collected by the IoT device and IoT service and purpose of its use.

Purpose

To ensure use of personal data.

Audience: IoT service provider.

IoT domain: Operations and Management or Application and Service.

Guidance

Prior to purchase, IoT users should be provided with details of all assumed data, including PII, collected by IoT devices and services. This gives IoT users the opportunity to use the product / solution appropriately based on the data provided. It can be provided as a user contract, privacy policy, or other notification mechanism.

Control-31-2

Consent of the IoT user to the privacy notice should be obtained before collecting the personal data or changing the purpose of use.

Purpose

To ensure consented collection and use of personal data.

Audience: IoT service provider.

IoT domain: Operations and Management or Application and Service.

Guidance

End user needs to be provided a checklist that will mention the purpose, method and scope of collection, time limit, who would use this data, among others.

7.2.2.4 Verification of IoT functionality

Control-32

Independent verification of IoT device, data components and IoT service components should be supplied to provide visibility and assurance to all stakeholders that the IoT device or service is operating as per stated objectives.

Purpose

To ensure WYSIWYG (What You Sees Is What You Get) of functionalities for IoT devices and services.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

A verification based trust approach to IoT devices and data components is necessary for transparency in IoT operations. Provision for independent verification of IoT device and service provides visibility and assurance to all stakeholders that the IoT functions are operating as per stated objectives.

7.2.2.5 Consideration of IoT users

Control-33

End users' privacy requirements and concerns should be addressed in designing the IoT device and service.

Purpose

To ensure IoT users' privacy requirements and concerns are addressed in the IoT device and service and to build IoT users' trust.

Audience: IoT service developer or IoT service provider.

IoT domain: Operations and Management, Application and Service, Resource Access and Interchange or Sensing and Controlling.

Guidance

Privacy being a key requirement of end users, a 'user first' strategy in designing IoT devices and services will help to build user trust and confidence to ensure mass acceptance.

7.2.2.6 Management of IoT privacy controls

Control-34

The effectiveness of privacy controls in the IoT device and service should be reviewed, and new privacy risks be identified on a continuous basis considering the evolving privacy needs of end users and regulatory requirements.

Purpose

To justify the effectiveness of privacy controls in IoT devices and services.

Audience: IoT service provider.

IoT domain: Operations and Management.

Guidance

Implement operational and technical security and privacy controls with appropriate validation and verification of these controls on a continuous basis to ensure these controls are relevant as per the need.

7.2.2.7 Unique device identity

Control-35-1

IoT system developers (especially device developers) should use a method that uniquely identifies each IoT device to improve privacy for identifying IoT device suspected to be relevant to a cyber incident.

Purpose