ISO/IEC ~~DIS~~FDIS 27403:~~2023(E)~~

ISO/IEC JTC 1/SC 27/~~WG 4~~

~~Date: 2023-12-12~~

Secretariat: ~~ILNAS~~ DIN

Date: 2024-03-12

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

FDIS stage

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

Style Definition ...

Formatted: zzCover large

Formatted: Left: 1.5 cm, Right: 1.5 cm, Top: 1.4 cm, Bottom: 1 cm, Width: 21 cm, Height: 29.7 cm, Header distance from edge: 1.27 cm, Footer distance from edge: 1.27 cm

Formatted ...

Formatted: Cover Title_A1

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

~~Tel. + 41 22 749 01 11~~

~~Fax + 41 22 749 09 47~~

E-mail: copyright@iso.org

~~Web www.iso.org~~

Website: www.iso.org

Published in Switzerland~~.~~

Formatted: HeaderCentered

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: zzCopyright address, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: French (Switzerland)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Contents Page

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Formatted: FooterPageRomanNumber

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at ~~www.iso.org/patents and https://patents.iec.ch.~~www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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.~~www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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 and www.iec.ch/national-committees~~www.iso.org/members.html and www.iec.ch/national-committees.

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

Formatted: HeaderCentered
Formatted: English (United Kingdom)
Field Code Changed
Formatted: English (United Kingdom)
Field Code Changed
Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Introduction

Although IoT-domotics have been widely applied worldwide, many IoT-domotics devices, communication protocols and platforms are developed without sufficient security and privacy considerations, which can pose security and privacy risks. Due to the long supply chain and the large number of stakeholders involved, it is important to establish the stakeholders, identify risks during the life cycle, and put forward proposals for resolving security and privacy issues in IoT-domotics. This document provides guidelines to analyse security and privacy risks and identifies controls that should be implemented in IoT-domotics systems.

IoT-domotics have some features that differ from other forms of IoT deployment, such as non-expert users, and ad hoc architecture. This document therefore adapts the general IoT security and privacy principles to IoT-domotics~~,~~ and provides stakeholders with thorough and tailored guidelines for scenarios specific to IoT-domotics.

The target audiences of this document include IoT-domotics service providers, IoT-domotics service developers, and those who supervise or verify security and privacy for IoT-domotics.

Formatted: English (United Kingdom)

The goal of this document is to ensure that security and privacy for IoT-domotics are achieved without requiring end-users to have in-depth IT knowledge. Although this document can be used by interested end-users, they are not the target audience.

Formatted: FooterPageRomanNumber

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

1 Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT) domotics systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20924, Information technology — Internet of Things (IoT) — Vocabulary

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 29100, Information technology – Security techniques – Privacy framework

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 29100, ISO/IEC 20924 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
IoT-domotics
Internet of Things (IoT) system composed of networks, devices, services and users typically used in the domicile or as electronic wearables

Note 1 to entry: Devices are usually available to the consumer through retail purchase.

Note 2 to entry: According to ISO/IEC TR 22417:2017, 6.3, IoT-domotics denotes the private, hence highly customizable indoor area where someone lives, alone or with friends/relatives/roommates. Thus, it includes dedicated infrastructure aimed to support those individuals, such as healthcare and wellness systems, building control systems, smart metering and systems for entertainment and gaming.

3.2
entity
physical or non-physical element, which has a distinct and independent existence

Note 1 to entry: Every entity has a unique identity.

[SOURCE:Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.2].

3.3
Domains
a domain is a
major functional group of an Internet of Things (IoT) system.

Note 1 to entry: Every *entity* (3.2) in an IoT system participates in one or more domains and is said to be included or contained by that domain.

[SOURCE:Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.3].

4 Abbreviated terms

AI	artificial intelligence
App	application
AR	augmented reality
CRM	customer relationship management
DDoS	distributed denial of service
ICT	information and communication technology
IP	internet protocol
IoT	internetInternet of thingsThings
NB-IoT	narrow band internetInternet of thingsThings
PII	personally identifiable information
RF	radio frequency
TV	television
URL	uniform resource locator
USB	universal serial bus
VR	virtual reality

5 Overview

5.1 General

The security and privacy of IoT-domotics have a bearing on the normal operation of in-domicile services, the well-being of residents, and the integrity of infrastructures that are linked directly or indirectly with devices of services. Stakeholders including users, service providers, device manufacturers, network operators and industry supervisors are becoming increasingly concerned by security and privacy issues of IoT-domotics.

In comparison with other IoT solutions, IoT-domotics have specific features and concerns. It is therefore essential to adapt the general IoT security and privacy principles to IoT-domotics and provide stakeholders with thorough and tailored guidelines in specific scenarios of IoT-domotics.

The target audiences of this document include IoT-domotics service providers, IoT-domotics service developers, and those who supervise or verify security and privacy for IoT-domotics.