Towards a certification scheme for IoT security evaluation

Workshop paper on Industrial Automation and Control Systems (IACS)

Raman Barakat[1], Faruk Catal[2], Sascha Hackel[3], Axel Rennoch [4], Martin A. Schneider [5]

Abstract: Many European and international standardization bodies and industrial organizations do provide more or less detailed specification catalogues addressing IoT product security requirements, test cases and evaluation methods. In this contribution, a dedicated set of relevant standards, guides and recommendations which recently have been recognized by the European Union Agency for Cybersecurity (ENISA) will be introduced. Special attention is given to their contribution for the security evaluation process and the product quality itself, including the level of details regarding their suitability for test definition and execution.

Keywords: IoT, security, evaluation, testing, certification.

1 Introduction

Caused by the massive usage of IoT products and lots of attacks on such products, e.g. by the worm Mirai [Ant17], a strong request for the evaluation and certification of significant security aspects is being discussed. Various organizations have published standards that provide requirements for the evaluation and testing of IoT products. It is important to understand the different approaches and possibilities of these standards.

The remainder of this paper is organized as follows: Section 2 provides a brief description of standards and what they are intended for. Section 3 proposes an initial classification of these standards and assigns them to the pairs product (requirements) and (assessment of the) process but also product design and product quality.

[1] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, ramon.barakat@fokus.fraunhofer.de
[2] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, faruk.catal@fokus.fraunhofer.de
[3] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, sascha.hackel@fokus.fraunhofer.de
[4] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, axel.rennoch@fokus.fraunhofer.de, https://orcid.org/0000-0003-3419-298X
[5] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, martin.schneider@fokus.fraunhofer.de, https://orcid.org/0000-0002-8864-6492

2 Overview of considered standards

The following list is a selection of standards for further discussion. The documents have been identified by ENISA's Stakeholder Cybersecurity Certification Group (SCCG) [Eni21] as relevant for the development of a cybersecurity certification scheme for IoT products.

2.1 IEC 62443 Industrial communication networks - IT security for networks and systems

IEC 62443:2018 is a series of standards that describes security aspects of industrial products. Part 4 of this standard series addresses the cybersecurity for industrial automation and control systems (IACS). IEC 62443-4 defines secure development lifecycle (SDL) requirements related to cybersecurity for products intended for use in the IACS and provides guidance on how to meet these requirements. These requirements can be applied to new or existing processes and cover the entire lifecycle, including developing, maintaining and retiring hardware, software or firmware.

2.1.1 IEC 62443-4-1 Secure product development lifecycle requirements

Part 4-1 of IEC 62443 specifies generic SDL process for IoT products. The covered lifecycle phases include security requirements definition, secure design, secure implementation, including coding guidelines, verification and validation, defect management, patch management and product end-of-life. Each requirement is supported with a rationale and supplemental guidance that supports the implementation of the requirement. An annex provides an example of possible metrics to measure the effectiveness of the implementation of the security requirements in a specific process.

2.1.2 IEC 62443-4-2 Technical security requirements for IACS components

In contrast to Part 4-1 of 62443, Part 4-2 specifies technical security requirements for the product itself. The standard provides detailed component requirements (CRs) associated with the seven foundational requirements (FRs) that are described in Part 1-1 of the 62443 standard series and include defining the requirements for control system capability security levels and their components. These seven foundational requirements (FRs) are

- identification and authentication control (IAC),
- use control (UC),
- system integrity (SI),
- data confidentiality (DC),
- restricted data flow (RDF),
- timely response to events (TRE), and

- resource availability (RA).

These FRs are the basis for defining four security capability levels where the lowest level would imply minimal security capabilities, preventing systems from unauthorized disclosure of information via eavesdropping and casual exposure, and the highest level means that components are resistant against information disclosure in case sophisticated methods are actively applied by an adversary with specific IACS knowledge and sufficient resources. In addition to the FRs the document also specifiers specific requirements for software applications (SAR), embedded devices (EDR), host devices (HDR) and network devices (NDR). Defining security capability levels for the control system component is the goal and objective of this document as opposed to targeted and achieved security levels.

2.2 ISO/IEC 11889 Trusted Platform Module

ISO/IEC 11889:2015 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. TPM meeting the requirements may enable establishing trust in platform scenarios involving security and privacy. TPMs require hardware protections to provide three roots of trust: storage, measurement, and reporting. Basing TPM roots of trust in hardware is an improvement over software-based solutions whose protections are vulnerable to malicious software. The architecture defines a TPM that is a component that receives commands and returns responses. By sending commands to a TPM and processing the responses, security benefits accrue for the platform as a whole. The root of trust for storage consists primarily of creating, managing and protecting cryptographic keys and other data values. Artefacts protected by or associated with encryption keys, like passwords, certificates or other credentials, can be used for authentication and many other security scenarios.

ISO/IEC 11889 consists of the following four parts:

- Part 1: Architecture
- Part 2: Structures
- Part 3: Commands
- Part 4: Supporting routines

Part 1 introduces the relevant modules while parts 2, 3 and 4 do provide some sources for the implementation of the modules using C programming language.

2.3 ISO/IEC 27402 (committee draft)

The ISO/IEC committee draft (CD) 27402 Cybersecurity — IoT security and privacy — Device baseline requirements standard is intended to specify a security baseline or platform for ‘IoT devices’ [things] supporting information security and privacy controls. Examples of baseline [information security] requirements cover the following topics:

- Unique device identifier that should be immutable and verifiable
- Factory reset functionalitiy
- Delete all user data information' functionaility
- Protection of data
- Patching/updating capability for firmware and software)

It is anticipated that additional security controls will be required and may be defined in further standards for specific applications (e.g., medical things). Currently, the standard is at 1st committee draft stage.

2.4 GP Security Evaluation Standard for IoT Platforms (SESIP)

The Security Evaluation Standard for IoT Platforms (SESIP) provided by GlobalPlatform Inc. (GP) is designed specifically for the IoT platforms and platform parts on which IoT products are based. SESIP provides a common and optimized approach for evaluating the security of connected products that meets the specific compliance, security, privacy and scalability challenges of the evolving IoT ecosystem. SESIP follows all mandatory aspects of ISO 15408 Common Criteria standard. Based on "Mapping" documents, the SESIP Certificate is reusable in another certification schemes by composition of certified parts, and reuse of certification across different evaluations.

2.5 ETSI TC CYBER series

Within ETSI TC CYBER, experts are working on "Cyber Security for consumer Internet of Things". Basic requirements have been published in ETSI EN 303 645. Starting from this baseline, the experts are currently defining related test cases and assessment criteria.

2.5.1 ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements

The ETSI EN 303 645 standard specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services.

In addition to the requirements, it provides basic guidance through examples and explanatory text on how to implement these requirements.

2.5.2 ETSI TS 103 701 (draft)

The ETSI TS 103 701 document specifies test scenarios for assessing consumer IoT products against the provisions of EN 303 645. It is to set out mandatory and recommended assessments, guidance and examples to support their implementation. The document

targeting testing labs and certification bodies that provide assurance on the security of relevant products. It is additionally targeting manufacturers that wish to carry out a self-assessment. The assurance schemes that this document is used in and their outcomes are out of scope. The proposed document also does not set out detailed testing protocols. However, the proposed document is intended as input to a future EU common cybersecurity certification scheme as proposed in the Cybersecurity Act.

3 Classification

3.1 Common Criteria

In order to find a classification and relevant approach for the comparison of standards, we first provide a brief introduction of the international concept of Common Criteria (CC) for security evaluation [Iso17]. The Common Criteria standard provides a generic catalogue for both the security functional requirements (SFR) of the product under consideration, i.e., the target of evaluation (TOE), and a systematic approach for the evaluation facility to address the relevant steps and documentation for the assurance of the desired evaluation level. The SFRs have been ordered in eleven main classes, e.g. for the product audit functions, cryptographic support, identification and authentication facilities or the protection of the access to the TOE. The CC also introduces the concept of Protection Profiles (PP), addressing a category of products (e.g., firewalls) that cover the specific SFRs of such product groups. Evaluators of the security product or protection profile are requested to check security assurance requirements (SAR) that in most cases cover six assurance classes, including lifecycle, development aspects (e.g., product architecture and specification), testing and vulnerability analysis. The Common Criteria Quick Reference Card [RD18] provides a comprehensive overview of the CC systematic.

Due to the broad scope and generic systematic of the Common Criteria we use them for classifying the documents introduced in Section 2, i.e., to distinguish requirements related to the product itself and the assurance process.

3.2 Classification of considered documents

In this section, the scope of the selected documents has been considered w.r.t. to the main two requirement groups proposed by the CC, i.e., if the contents include SFRs for the product and SARs for the assessment of the evaluation process. Furthermore, it has been checked if the documents support the design and contribute to the testing of the product quality.

IEC 62443-4-1 focus on the design aspects for the target industrial security product. It provides development guidance to ensure an advanced development process for some secure target product. The content is on a general level and can be described as a best

practice guide without much detail on functionality and evaluation aspects. As part of the product lifecycle, the document contains details on security verification and validation testing. However, they have been provided on a high level and do not contain concrete test scenarios. W.r.t. certification schemes, the contents of the document can contribute to the aspects of the assessment process (ADV, ALC, ATE).

IEC 62443-4-2 provides a very detailed list of industrial security product requirements. It can be stated that this document considers all SFR classes from the CC. However, the ordering and naming of the requirements in this document differ from the generic requirements from the CC. It should be noted that the product requirements have been related to security levels 0 to 4. In contrast, the CC introduce evaluation assurance levels (EAL) related to the depth of the evaluation process that range from 1 to 7.

ISO/IEC 11889 provides a detailed specification for a trusted platform module, including many recommended specific technical details for the target product. Parts 2 to 4 represent a reference implementation for the required functionality. In this sense, the standard also pre-defines some design and implementation aspects that can be regarded as prerequisites for the product evaluation in addition to true SFRs. The details within the multi-part standard provide many design recommendations but no scenarios for quality testing.

The ISO/IEC 27402 (committee draft) includes both recommendations for the device manufacturer regarding some steps in the development process (e.g., risk assessment) and product declarations (e.g., security features and vulnerability disclosure). Additionally, it provides concrete requirements for the security product itself (e.g., secure storage, reset function). This understanding from the scope of the CC provides a relatively small selection towards ten SFRs (FIA, FMT, FDP, FPR, FTA, FAU) and three SARs (ADV, ASE/AVA).

GP SESIP focusses on IoT Platforms and is an adaptation of the CC for IoT platforms, and therefore addresses both SFRs and SARs. Furthermore, the document introduces five assurance levels defined by the scope of SARs. In this understanding, the document shares similarities to a product-specific protection profile as known from the CC. Due to this generic approach, the document does not provide concrete design decisions or test objectives.

ETSI EN 303 645 addresses requirements for the security product itself (storage of security parameters, secure communication, removal of user data) but also assurance requirements (software update process). It is possible to find relationships both to SFRs, e.g., password rules to FMT_MSA.2 (Secure security attributes), and to SARs, e.g., ALC_CMC (software integrity).

ETSI TS 103 701 (draft) focusses on the assessment of requirements listed in ETSI EN 303 645. In this sense, it repeats the SFRs and SARs. However, it also addresses the definition of concrete tests using an informal description of test purposes, test actions and conditions for the assignment of verdicts. Therefore, the document provides also a

refinement of the original requirements, e.g., Provision 5.3-7 on cryptography methods has been refined w.r.t. the details "not to be known to be vulnerable" (e.g., deprecated or inappropriate for the intended product lifetime).

Table 1 provides a summary of the contents of the selected documents. Some documents address several aspects, "X" stands for *covered*, "(X)" for *partially addressed*. The main focus of the documents has been identified using I (industry), C (consumer), S (system), D (device) and is emphasised using the grey colour of the corresponding field. The column "level" indicates if the document includes some grouping of product requirements (security level, SL), evaluation assurance levels (EAL) or categorizes selected requirements as *optional (o*). The number of requirements or tests has been given in the last column to get an idea of the volume of the documents (ISO 11889 does not include dedicated requirements but a specification of a reference implementation).

	TOE	Product	Assess Process	Design	Quality Test	Level	#req
IEC 62443-4-1	I S		(X)	(X)	(X)	-	48
IEC 62443-4-2	I S	X		(X)		SL	88
ISO/IEC 11889	S	X		X		-	N/A
ISO/IEC 27402	D	(X)	(X)			-	13
GP SESIP	S	X	(X)	X		EAL	53
ETSI EN 303645	C D	X	X			o	67
ETSI TS 103701	C D	(X)	X		X		109

Tab. 1: Content classification of selected standards

4 Conclusion

Currently, multiple aspects of IoT certification approaches are under discussion in various working groups of standardization bodies and industrial associations. The technical viewpoints differ due to the various stakeholders in the organisations and interest groups. It appears very important to understand the differences, e.g., if "security levels" are proposed, since they may refer to product requirements or are related to the evaluation process. However, there is still a need for harmonization and common strategies towards a security certification scheme for IoT products.

In summary, it can be noted that most documents address technical requirements for the security product itself, and many are also considering assurance requirements. Concrete test case specifications to be used for quality evaluation are rare. Therefore, we like to mention that further documents by ETSI on the Test specification for foundational Security IoT-Profile [Ets21] have recently been released that include formalized test purpose specifications for IoT.

Acknowledgements

This contribution has been partly supported by the European commission H2020-EU.2.1.1, Grant agreement ID: 952684: https://cordis.europa.eu/project/id/952684.

Bibliography

[Iso17] ISO15408 Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. April 2017.

[Eni21] Enisa Stakeholder Cybersecurity certification group. Report on Draft URWP Consultation, January 2021.

[Ets21] ETSI TS 103 701, draft V0.0.7, CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements, March 2021.

[Ets20] ETSI EN 303 645. V2.1.1, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements, June 2020

[Ets21] ETSI TS 103 646 V1.1.1 (2021-01) Methods for Testing and Specification (MTS); Test Specification for foundational Security IoT-Profile

[GP20] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP) – Public Release v1.0. March 2020

[Iec19a] IEC 62443-4-1. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements, February 2019.

[Iec19b] IEC 62443-4-2. Security for industrial automation and control systems – Part 4-2: Technical Security Requirements for IACS Components, February 2019.

[Iso20a] ISO/IEC 11889-1. Information technology - Trusted Platform Module Library - Part 1: Architecture

[Iso20a] ISO/IEC 1st CD 27402. Cybersecurity – IoT Security and Privacy- Device baseline requirements, November 2020

[Ant17] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In 26th {USENIX} security symposium ({USENIX} Security 17) (pp. 1093-1110).

[RD18] Rennoch, A., deMeer, J.: Common Criteria Quick Reference Card, http://www.school-of-technology.de/resources/ccQRC.pdf.