Towards Cybersecurity Act: A Survey on IoT Evaluation Frameworks

Maxime Puys, Jean-Pierre Krimm and Raphaël Collado

Université Grenoble Alpes, CEA, LETI, DSYS, Grenoble F-38000, France
Email: firstname.name@cea.fr

***Abstract*—On the 7^{th} of June 2019, the Cybersecurity Act was adopted by the European Union. Its objectives are twofold: the adoption of the permanent mandate of ENISA and the definition of a European cybersecurity certification framework, which is essential for strengthening the security of Europe's digital market. Delivered certificates according to this scheme will be mutually recognized among European countries. The regulation defines three certification levels with increasing requirements. Among them, the "basic level" which typically targets non-critical, consumer objects (e.g.,smart-home or "gadget" IoT). Yet, various evaluation and certification schemes related to the IoT already exist prior to the adoption of the Cybersecurity Act. Thus, discussions are being carried on at the moment of redaction in order to either choose an existing scheme or to design a unified scheme based on existing ones. In this paper, we focus on the basic level, and assemble a survey on existing evaluation and certification schemes for consumer IoT and compare them based on various criteria. Then, we propose a unified evaluation scheme for the basic level driven by Bureau Veritas, based on existing schemes.**

***Keywords*–Cybersecurity Act; Internet of Things; IoT; certification; evaluation scheme; smart-home.**

I. INTRODUCTION

On the 7^{th} of June 2019, the Cybersecurity Act has officially been adopted by the European Union. Its objectives are twofold: the adoption of the permanent mandate of the European Union Agency for Cybersecurity (ENISA), the European Union Agency for Cybersecurity, and the definition of a European cybersecurity certification framework, which is essential for strengthening the security of Europe's digital market. Delivered certificates according to this scheme will be mutually recognized among European countries. Cybersecurity certification is the attestation of the conformance and robustness of a product made by a third party evaluator, according to a scheme describing the security needs of the users, and taking into account technological developments. The adoption of the Cybersecurity Act will both encourage the use of certification and recognition of certificates issued by one Member State throughout the EU, thereby contributing to the security of the single market. The regulation defines three certification levels with increasing requirements:

- The basic level which typically targets non-critical, consumer objects (e.g.,smart-home or "gadget" IoT);
- The substantial level that targets the median risk (e.g.,cloud computing or non-critical industrial IoT);
- The high level that targets critical solutions where there is a risk of attacks by actors with significant skills and resources (e.g.,vehicles, critical industry or medical devices, etc.).

Yet, various evaluation and certification schemes related to the IoT already exist prior to the adoption of the Cybersecurity Act, with companies proposing evaluation services according to these schemes. Thus, discussions are being carried on at the moment of redaction in order to either choose an existing scheme or to design a unified scheme based on existing ones.

a) Contributions:: In this paper, Bureau Veritas (BV) and CEA-Leti teamed up to focus on the "basic" level, targeting consumer IoT such as cameras, toys, or other "smart-devices". We assemble a survey on existing evaluation and certification schemes for consumer IoT and compare them based on various criteria. Then, we propose a unified evaluation scheme for the basic level driven by Bureau Veritas, based on existing schemes. The objectives of this unified scheme are twofold: (i) be a candidate for official certification scheme for the basic level; and (ii) maintain compliance with existing schemes to allow certification companies to maintain their services independently of the chosen scheme.

b) Outline:: The rest of the paper is organized as follows. Section II will present and compare existing schemes. Section III will then define our unified evaluation scheme. Finally, Section IV will introduce related works on IoT certification surveys and Section V will conclude.

II. COMPARISON OF EXISTING EVALUATION FRAMEWORKS

In this section, we propose to analyze and compare existing referential frameworks dealing with cybersecurity of consumer directed IoT devices. These evaluation schemes are candidates to become the one chosen within the Cybersecurity Act. However, it appears that theses documents have been redacted with sometimes quite different purposes and target specific audience. Moreover, their structure can vary significantly. We first propose to compare them on various criteria, such as:

a) Type of document: This describes the main purpose of the document, such as evaluation/certification or good practices. Evaluation and certification seek to ensure the compliance of the device with a predefined list of requirements. They are usually performed by a third party when the development is finished and prior to a public release. Depending on the type of evaluation, they can include compliance against functional requirements to ensure the device only does what it claims to do; but also robustness evaluation assessing the strength and

 ISBN: 978-1-61208-821-1

the robustness of a device against cybersecurity threats. On the other hand, good practices aim at being applied during the development.

b) Targeted audience: This defines who the document is destined to. This criterion is generally linked to the type of document described above. That is, a certification scheme is usually for "conformity assessment bodies" (CAB). They are third parties conducting the evaluation of a product. However, an evaluation scheme may be applied by developers during development within continuous integration. Good practices are generally directed to developers, testers, Chief Information Security Officers (CISO), or Chief Technical Officers (CTO).

c) Structure of the document: A complete cybersecurity certification process is generally defined as presented in Figure 1. From a set of assets to protect, hypotheses (for instance on the environment), threats originating from threats origins, security objectives are obtained. Theses objectives can be seen as generic counter-measures regarding threats. For instance, if a threat is "Configuration alteration", a matching security objective could be "Secure authentication on administration interface". Then security objectives are derived on security requirements, which are more technical and related to the target of evaluation. Regarding to the objective "Secure authentication on administration interface", a requirement could be "Use two-factor authentication". Finally, security requirements are derived in technical requirements which are completely related to the programming language or framework used by the product. In parallel, security requirements are derived into tests procedures, detailing how CAB must conduct evaluation. This criterion defines which part of this structure are covered by the scheme.

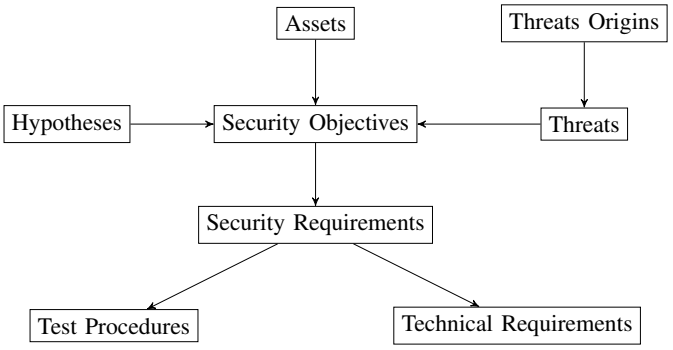

Figure 1. Structure of certification schemes

d) Split in different security levels: This criterion defines if the scheme proposes different security levels providing increasing security level and adding more security requirements to cope with. These security levels are internal to the framework and should not be mistaken with the basic, substantial and high of the Cybersecurity Act.

e) Technical perimeter: This explains how widely the scheme covers in terms of technical cybersecurity topics (network, system, cryptography, etc).

f) Level of accuracy of the requirements: This shows how precise are the requirements provided by the scheme. That is, if they stay quite generic or become quite technical.

g) Support from the community/industry: This criterion details how much the scheme is supported by either the scientific community or industry. This is a subjective criterion based on the variety of authors and members if the scheme belongs to an alliance.

We focus on five IoT evaluation schemes, known to be the best contenders for the basic level of the Cybersecurity Act, namely: ETSI, CTIA, OWASP, Eurosmart, IoT-SF. We first describe briefly every one, then we propose a summary table given the criteria we defined earlier.

h) ETSI-EN-303-645 (version 2.1.0, 2020-04): ETSI is a European standards organization based in France. In May 2018, they release the first version of TS-103-645, later officialized as EN-303-645 [1], a list of good practices in order to increase the cybersecurity of consumer IoT devices. This document is based on a "Code of Practice for Consumer IoT Security" proposed by the UK government. Destined to vendors, it is organized as a list a security objectives mixed with requirements. No separation in levels is provided. It covers a wide perimeter, going from passwords to communications, with system integrity and personal data. Requirements stay at a generic level. ETSI involves more than 850 members, drawn from 65 countries, including major universities.

i) CTIA Cybersecurity Certification Test Plan for IoT Devices (version 1.0.1, 2018-10): CTIA represents the United States wireless communications industry. In August 2018, they released the initial version of their certification plan for IoT devices [2]. Clearly destined to CAB, it is separated in three levels with increasing security features. It is not obvious if all three levels would fit in the "basic" Cybersecurity Act, given the fact that level three implies advanced security features such as two-factor authentication or secure boot. It is structured as a list of generic requirements along with test procedures, test prerequisites and test cases. The technical perimeter is wide.

j) OWASP IoT Top Ten (version 2018): The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. In 2018, OWASP released their Internet of Things Top 10 [3], a list of good practice. Destined to vendors, it is a list of 10 security objectives representing the 10 main kinds of vulnerabilities targeting IoT devices. It is not divided into levels but covers a wide range of topics. This list stays at a very low level of accuracy, only proposing security objectives. However, OWASP is widely known to propose a very technical set of coding rules to avoid most of the vulnerabilities. Yet, the IoT Top 10 document does not refer directly to them. OWASP has many members both from academic and industry across the world.

k) Eurosmart IoT Device Certification Scheme (version 2019-05-16): Eurosmart is a European organization based in Brussels. Their members are mainly working in hardware security (semiconductor and secure-elements) or in high-security software and include major companies and research laboratories. In April 2019, they released an initial version of their certification scheme [4] designed for CAB, however, the writing process still seems ongoing. According to published documents, they aim to cover the whole certification procedures from assets to CAB tests. Yet at the moment of redaction, they cover risk analysis (from assets to security

 ISBN: 978-1-61208-821-1

TABLE I. SUMMARY OF EXISTING SCHEMES

Schemes	ETSI	CTIA	OWASP	Eurosmart	IoT-SF
Type	Good practices	Certification	Good practices	Certification	Mixed
Audience	Vendors	CAB	Vendors	CAB	Vendors
Structure	Objectives Require-ments	Requirements Tests	Objectives	Complete (ongoing)	Objectives Require-ments
Levels	None	Three	None	None	Five
Perimeter	Wide	Wide	Wide	Wide	Wide
Accuracy	Generic	Generic	Low	Generic	Generic Technical
Support	World-wide	World-wide industry (mainly US)	World-wide	Sector-Specific (mainly EU)	World-wide (mainly UK)

TABLE II. MAPPING FOR FIRST BASIC LEVEL

ID	Topic	ETSI	CTIA	OWASP
1	Password management	4.1	3.2	1
2	Keeping software up to date	4.3	3.5, 3.6	4, 5
3	Securely storing sensitive data	4.4		7
4	Minimizing exposed attack surface	4.6	5.17	2, 3, 10
5	Ensuring the initial state is secure			5, 9
6	Analyzing admin. and user guides	4.2, 4.12	4.1	8
7	Third-party components management			5
(8)	Unique reference of the device			
(9)	Resistance to known vulnerabilities			10

objectives) and generic security requirements. They include a wide technical perimeter and stay a a generic level. They do not provide multiple levels of certification and according to the scheme itself, it is destined to the "substantial" level of the Cybersecurity Act.

l) IoT Security Foundation Security Compliance Framework (version 2, 2018-12): The IoT Security Foundation (IoT-SF) is composed of major companies, including almost all microchips integrators alongside major mobile network companies. Yet, smaller members and universities are mainly from UK. In 2016, they released the first version of their IoT security compliance framework [5]. Coming with a spreadsheet checklist alongside, it stands between certification and good practices as being stated as a "self-checking" framework. Destined to vendors, it is organized as a mixed list of security objectives and requirements. Five levels are introduced, based on a risk analysis to be performed on the device to assess. Depending on the importance of each security property (confidentiality, integrity, availability), the device is assigned to a minimum level. It covers a very wide perimeter, with merely all technical aspects related to security covered alongside with business, life-cycle management and governance. Interestingly, depending on the topic, requirements either stay at a generic level, or become quite technical.

Table I summarizes the criteria for all existing schemes.

III. A Unified IoT Evaluation Framework

As seen in Section II, two categories of documents are present in the current state-of-the-art. On one side, there are certification documents destined to CAB, while on the other side, there are good practice or self-assessment documents destined to vendors. It is currently (mid 2020) unclear which is preferred for the Cybersecurity Act evaluation framework, given the fact that evaluation modalities are still discussed. More precisely in the context of the basic level, it is not precised if the evaluation should be performed by CAB or vendors them-selves. According to ENISA and the European Commission during the FIC 2020 conference (Lille, 2020-01-28), such questions are likely to depend on the type of IoT device to test. In other words, there will be different evaluation schemes with different modalities for the basic level.

In this context, we propose a unified evaluation framework based on existing documents presented in Section II and driven by Bureau Veritas. Rather than providing yet another set of rules to implement, we propose a unified view detailing how existing frameworks could be mapped with each other. Thus, rather than implementing only one existing scheme, vendors and CAB can already include a global view of most of them in their process, without risking to bet on one not chosen in the end. The mapping we propose covers ETSI, CTIA, and OWASP. This choice is motivated as they seem to be the three main contenders for the final basic level of Cybersecurity Act framework, according to ongoing discussions.

A. Presentation of the Framework

The idea is to make the set-union of all topics covered in the different frameworks while pin-pointing the cross reference of related security objectives in each framework. For instance, for a common topic related to password security, we would

TABLE III. MAPPING FOR SECOND BASIC LEVEL

ID	Topic	ETSI	CTIA	OWASP
1	Password management	4.1	3.2	1
2	Keeping software up to date	4.3	**4.5, 4.6**	4, 5
3	Securely storing sensitive data	4.4		7
4	Minimizing exposed attack surface	4.6	5.17	2, 3, 10
5	Ensuring the initial state is secure			5, 9
6	Analyzing admin. and user guides	4.2, 4.12	4.1	8
7	Third-party components management			5
(8)	Unique reference of the device			
(9)	Resistance to known vulnerabilities			10
10	**Authentication and access-control**		**4.3, 4.4**	
11	**Protection of data in transit**	**4.5**	**4.8**	**7**
12	**Data input validity**	**4.13**		

note all related security objectives of each document. We divided this mapping into three levels based on – what we consider – realistic evaluation time (either performed by vendors or by CABs). The first level is intended to be completed within five business days. The second and third levels are respectively designed for nine and fifteen days. Depending on a risk analysis or marketing requirements, the device may be evaluated according to one of the three levels. The mapping for every level is provided in Tables II, III and IV.

We chose categories in Table II as they are the most simple and consensual. OWASP, designed to be as simple as possible, has almost all of his security objectives covered within the first level. Topics 1, 2 and 3 are essentially straightforward. Topic 4 refers to any software accessible from outside of the device (either from internet or from the LAN). This includes open ports, API, running servers, etc. This also includes hardware debug ports. Topic 5 refers to the guided installation of the device by the end user. The idea is to verify that default configuration and/or installation wizards put the device in a secure state. Topic 6 deals with how clear are the guides provided with the device in order to inform the end user and/or the administrator on security, privacy, and configuration. Topic 7 aims at verifying how third party components (software, libraries, stacks, etc) are manages (at least if they are clearly identified). Topics 8 and 9 (in brackets) are not directly mentioned by any of ETSI, CTIA and OWASP. Authors added these based on their experience of security. Topic 8 requires that the device can be clearly identified with a version number or equivalent while topic 9 follows topic 7 and implies that the certified version on the device is not affected by any known vulnerability (CVE). Topic 9 also applies for hardware vulnerabilities such as Meltdown [6], Zombieload [7] and more recently LVI attack [8]. No security is required for data in transit at this level which may be controversial. The idea behind is that this level should be limited to devices either that do not communicate, or do not communicate any sensitive data. Any device transferring sensitive data should be *de facto* put in level two or three.

The second basic level presented in Table III updates topic 2 to second level in CTIA and adds a few new topics (changes regarding Table II are shown in bold). Topic 10 ensures especially that no unauthenticated changes can be made and that administrator accounts must differ from user accounts. Topic 11 deals with protection of transferred data. It mainly states that messages shall be encrypted and signed and that keys must be managed securely. Finally, topic 12 requires that user inputs are checked to avoid code execution and under/overflows.

The third basic level presented in Table IV updates topic 2 to third level in CTIA and adds a few new topics (changes regarding Table III are shown in bold). Topic 13 deals with personal data and can roughly be summarized by compliance with EU's GDPR. Topic 14 requires the device to have a secure boot chain while topic 15 is related to the protection of data stored on the device. This topic differs from topic 3 "Securely storing sensitive data" in the sense that here, all the memory is protected, either by physical means such as scrambling or by file system encryption.

B. Discussions

As one can see in Tables II, III and IV regarding CTIA, our mapping can either follow CTIA levels (e.g., for topic 2. Keep software up to date); or have a fixed CTIA level in all tables (e.g., for topic 1. Password management). Depending on the topics, CTIA level following ours means we consider they are adapted to a certification at the basic level. On the other hand, a fixed CTIA level means that either lower CTIA levels are not challenging enough; or that higher CTIA levels are too demanding. Also, as the evaluation duration is currently not fixed within the Cybersecurity Act, proposing three levels has multiple benefits. First, it will help EU working groups to decide about how much requirements a device shall respect, without exceeding what will be considered as the maximal certification duration. Second, depending on specific classes of product, the Cybersecurity Act may officially require tougher evaluations. Finally, it will allow CAB to design private schemes around Cybersecurity Act, for demanding companies.

a) Coverage:: In the mapping presented above, we tried to maximize coverage, while choosing topics relatively close from one framework to others. Moreover, we tried to only select security objectives that can reasonably be asked to a device at the Cybersecurity Act basic level. Doing so, we obtain a coverage of existing framework as presented in Table V. As OWASP is simple and straightforward, it gets high coverage. ETSI is a quite balanced framework and gets a comfortable coverage at level 3. Finally, regarding CTIA, our first level already includes requirements from CTIA's level 2 and 3. Thus, we computed the coverage of all our levels against CTIA's

TABLE IV. MAPPING FOR THIRD BASIC LEVEL

ID	Topic	ETSI	CTIA	OWASP
1	Password management	4.1	3.2	1
2	Keeping software up to date	4.3	**5.5, 5.6**	4, 5
3	Securely storing sensitive data	4.4		7
4	Minimizing exposed attack surface	4.6	5.17	2, 3, 10
5	Ensuring the initial state is secure			5, 9
6	Analyzing admin. and user guides	4.2, 4.12	4.1	8
7	Third-party components management			5
(8)	Unique reference of the device			
(9)	Resistance to known vulnerabilities			10
10	Authentication and access-control		4.3, 4.4	
11	Protection of data in transit	4.5	4.8	7
12	Data input validity	4.13		
13	**Personal data management**	**4.8, 4.11**		**6**
14	**Secure boot**	**4.7**	**5.11**	
15	**Protection of data at rest**	**4.4**	**5.15**	**6**

level 3. It appears that this level is actually quite challenging for devices targeting a Cybersecurity Act basic level. For instance, topics such as "5.12 – Threat monitoring" or "5.16 – Tamper evidence" seem more destined to a Cybersecurity Act substantial or even high level of certification. This explains that we purposely exclude such topics and got a low coverage of CTIA.

TABLE V. COVERAGE OF EXISTING FRAMEWORKS

Level	ETSI	CTIA	OWASP
1	46%	29%	90%
2	62%	47%	90%
3	85%	59%	100%

IV. Related Works

There are some works on consumer IoT security certification. In may 2018, Cihon et al. [9] wrote a report on how to increase adoption of the proposed European cybersecurity certification framework. This document was written prior to the adoption of the Cybersecurity Act but studies the political, societal and economic aspects resulting from a common policy. In June 2018, Brass et al. [10] published a survey on cybersecurity standards for IoT. This work is really complete and provides a very precise overview of all IoT certification schemes existing at the time. Their survey is not directly related to the Cybersecurity Act and thus does not focus on the main candidates (including US regulations). Moreover, it lists existing standards rather than comparing them. Yet it sheds a light on most crucial aspects and challenges of certification of IoT devices and show the trade offs between maximizing the security of product and have legislations actually applicable. It is worth noting that given the rapid pace of the domain, frameworks such as Eurosmart and CTIA were not published at that time and thus are not included in the comparison.

In July 2019, the US NIST institute released the first version of NISTIR 8259 [11]. This internal report aims at giving manufacturers voluntary recommendations regarding cybersecurity of their devices. No mention seem to be made about regulation in this document. However in September 2019, the US Chamber of Commerce released a public letter [12] to the authors of NISTIR 8259. They state that they support the NIST report and mention that they believe policymakers in the U.S. and internationally need to align their IoT security with NISTIR 8259. Still in September 2019, the ENISA Advisory Group proposed an opinion paper [13] related to the security of consumer IoT. As an important note, this group is made of stakeholders including industry and academia and does not necessarily convey the view of ENISA. They recall the key elements of cybersecurity for such market and what ENISA can bring as a cybersecurity agency. While this article does not explicitly compares existing evaluation frameworks, it lays the foundations of which requirements could actually be selected for the basic level. In particular, authors emphasize the importance of certification schemes at European level but in contrast state that it should not impede the pace of innovation. In November 2019, Softic [14] proposed an analysis of the impact European certification of IoT on devices, consumers and business. Sadly, this thesis seem now inaccessible following the demand of the author.

V. Conclusion

In this paper, we discussed about the upcoming common cybersecurity certification framework for Europe in the context of the Cybersecurity Act. We proposed a survey of existing evaluation and certification schemes for consumer IoT and compared them based on various criteria. This allowed to (i) place them in the context of a global certification process, (ii) see how they are designed to and, (iii) what are the technical content they tackle and at which level of precision. We then proposed a unified evaluation scheme for the basic level of the Cybersecurity Act, based on existing schemes. This unified scheme lead by Bureau Veritas has two main objectives: (i) be a candidate for official certification scheme for the basic level; and (ii) maintain compliance with existing schemes to allow certification companies to maintain their services independently of the chosen scheme. Future works include speaking in depth with both ENISA, association and groups authoring existing framework in order to have their opinion on the unified mapping and to allow interested stakeholders to discuss with Bureau Veritas. Some use cases on various products with different purpose and security level could help

 ISBN: 978-1-61208-821-1

seeing if the mapping brings enough security to components and does not miss critical properties.

REFERENCES

[1] ETSI, "Etsi en-303-645," Tech. Rep., May 2018.

[2] CTIA, "Cybersecurity certification test plan for iot devices," Tech. Rep., Aug. 2018.

[3] OWASP IoT Security Team, "Internet of things: Top 10," OWASP, Tech. Rep., 2018.

[4] Eurosmart, "Iot device certification scheme," Tech. Rep., Apr. 2019.

[5] R. Atoui, J. Bennett, S. Cook, P. Galwas, P. Gupta, J. Haine, H. Trevor, C. Hills, R. Marshall, M. John et al., "Iot security compliance framework," IoT Security Foundation, 2016.

[6] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, "Meltdown: Reading kernel memory from user space," in 27th USENIX Security Symposium (USENIX Security 18), 2018.

[7] M. Schwarz, M. Lipp, D. Moghimi, J. Van Bulck, J. Stecklina, T. Prescher, and D. Gruss, "ZombieLoad: Cross-privilege-boundary data sampling," in CCS, 2019.

[8] J. Van Bulck, D. Moghimi, M. Schwarz, M. Lipp, M. Minkin, D. Genkin, Y. Yuval, B. Sunar, D. Gruss, and F. Piessens, "LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection," in 41th IEEE Symposium on Security and Privacy (S&P'20), 2020.

[9] P. Cihon, G. M. Guitierrez, S. Kee, M. Kleinaltenkamp, and T. Voigt, "Why certify? increasing adoption of the proposed eu cybersecurity certification framework," Master's thesis, Cambridge Judge Business School, May 2018.

[10] I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, "Standardising a moving target: The development and evolution of iot security standards," June 2018.

[11] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "Core cybersecurity feature baseline for securable iot devices: A starting point for iot device manufacturers," National Institute of Standards and Technology, Tech. Rep., July 2019.

[12] K. Megas and M. Fagan, "Subject: Draft NISTIR 8259, core cybersecurity feature baseline for securable iot devices: A starting point for iot device manufacturers," Sept. 2019.

[13] E. A. Group, "Opinion: Consumers and iot security," Tech. Rep., Sept. 2019.

[14] D. Softic, "Cybersecurity and certification: The impact of the european cybersecurity certification framework on the security and safety of iot devices, consumers and businesses," Master's thesis, University of Oslo, Nov. 2019.

 ISBN: 978-1-61208-821-1