Towards a Standardized Cybersecurity Certification Framework for the IoT

Sara N. Matheu-García, University of Murcia, Spain
José L. Hernández-Ramos, University of Murcia, Spain
Antonio F. Skarmeta, CTO Odin Solutions, University of Murcia, Spain
Gianmarco Baldini, JRC, Italy
Philippe Cousin and Franck Le.Gall, easy global market, France

Joint collaboration of H2020 ARMOUR project and the University of Murcia

ARMOUR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688237, but this document only reflects the consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

Dissemination Level

X	**PU**	Public
	CO	Confidential, restricted under conditions set out in Model Grant Agreement
	CI	Classified, information as referred to in Commission Decision 2001/844/EC

Abstract

The presence of IoT devices in the everyday life brings new cybersecurity threats affecting critical infrastructures as part of smart cities. To cope with this issue, the development of a cybersecurity certification framework represents an ambitious initiative, which has attracted an increasing interest from academia, industry and government institutions. However, beyond well-known issues related to expensiveness and flexibility of current solutions, the certification approach must address the dynamic and heterogeneous nature of IoT-enabled environments. In order to address such requirements, this work proposes an architectural framework that aims to provide a precise view of the involved concepts and processes based on security assessment and testing methodologies. While nowadays there is no silver bullet integrated solution, our approach is based on standards and specific technologies currently used in the scope of European initiatives, in order to promote a more standardized vision of a cybersecurity certification framework for the IoT.

Key words— Cybsersecurity Certification, Internet of Things, Security Risk Assessment, Security Testing, Labelling.

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688237, but this document only reflects the consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

Content

Acknowledgements

The authors acknoweldge the contribution or discussion of these topics with many relevant partners of the European Cyber Security Organisation (ECSO), Alliance for Internet of Things Innovation (AIOTI), European Telecommunications Standards Institute (ETSI) and the Horizon 2020 ARMOUR project. Acknowledgment does not imply full agreements on the recommendations provided by this report.

This work has been partially funded by the European Commission through the H2020-644852 ARMOUR EU Projects, the Spanish National Project CICYT EDISON (TIN2014-52099-R) granted by the Ministry of Economy and Competitiveness of Spain and CHIST-ERA PCIN-2016-010.

Acronyms and Abbreviations

AIOTI	Alliance for the Internet of Things Innovation
ARMOUR	Large-Scale experiments of IoT security Trust
BITAG	Broadband Internet Technical Advisory Group
CAP	Cybersecurity Assurance Program
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CPA	Commercial Product Assurance
CSPN	Certification de Sécurité de Premier Niveau
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
EAL	Evaluations Assurance Levels
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FIRE	Future Internet Research & Experimentation
FIT	Future Internet of the Things
ICSA	International Computer Security Association
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MBT	Model based testing
NFC	Near field communication
NIST	National Institute of Standards and Technology
OCL	Object Constraint Language
OWASP	Open Web Application Security Project
PP	Protection Profiles

QR	Quick Response
RBST	Risk Based Security Testing
SUT	System under test
TOE	Target of Evaluation
TTCN	Testing and Test Control Notation
UML	Unified Modelling Language

Glossary

Definition	Description	Source
Asset	Anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission	ISO 27000
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system	FIPS 200 (1)
Information Security Continuous Monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.	SP 800-137 (2)
Risk	Effect of uncertainty on objectives, a positive or negative deviation from what is expected.	ISO 31000
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.	CNSSI-4009 (4)
Security Label	Information that represents or designates the value of one or more security relevant-attributes (e.g., classification) of a system resource.	CNSSI-4009 (4)
Security Metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT security metrics must be based on IT security performance goals and objectives.	NIST Special Publication 800-55 (6)
Security Testing	Process to determine that an information system protects data and maintains functionality as intended	CNSSI-4009 (4)

Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational as-sets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	FIPS 200 (1)
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats	ISO 27000

Input documents

Security for IoT, and in particular certification and labelling, has received significant attention from the government, industry and research communities. This document has been written taken into account this and, therefore, a high number of reports and studies related with the topic has been used as input.

This section identifies some of the main reports published in the last years regarding IoT security from standardization and regulatory bodies. It should be noted that other documents related security testing, risk assessment, certification and labelling have been considered, since the proposed certification methodology is based on the ETSI proposal for risk-based Security Assessment and Testing .

These documents are also listed in the References section. Some of them are publics,

- European Telecommunications Standards Institute (ETSI): Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies (2015) (7)
- Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security and Privacy in the Hyper-Connected World (2016) (8)
- European Commission (EC) & Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security & Privacy in IoT (2017) (9)
- European Cyber Security Organisation (ECSO): State of the Art Syllabus v1 (2017) (10)
- European Union Agency for Network and Information Security (ENISA): Smart grid security certification in Europe Challenges and recommendations. December 2014. (11)
- European Commission (EC): Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems (2016) (12)
- Infineon – NXP – STMicroelectronics – ENISA: Common Position On Cybersecurity (2016) (13)
- DIGITALEUROPE: Views on Cybersecurity Certification and Labelling Schemes (2017) (14)
- ENISA: On the security, privacy and usability of online seals. An overview (2013) (15)
- ETSI: Methods for Testing and Specification (MTS). The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language (2015) (16)
- Broadband Internet Technical Advisory Group (BITAG): Internet of Things (IoT) Security and Privacy Recommendations (2016) (17)
- International Computer Security Association (ICSA): Internet of Things (IoT) Security Testing Framework (2016) (18)
- NIST: CAESARS Framework Extension. An Enterprise Continuous Monitoring Technical Reference Model (2012) (3)
- IoT Security Fundation: IoT Security Compliance Framework (2016) (19)

and others are restricted to ECSO WG 1:

- ECSO WG 1: European Cyber Security Certification: A Meta-Scheme Approach (2017)
- ECSO WG 1: Basic Framework for Cyber Security Assessments (2017)
- ECSO WG 1: draft document with scope and initial description of activities (2017)

1. INTRODUCTION

Nowadays, security aspects represent one of the most significant barriers for the adoption of large-scale Internet of Things (IoT) deployments (20). Almost every day we can see in the news something related with cyber security and attacks. One of the more named attacks was the Mirai IoT botnet, where several devices were used to perform a DDoS attack against big platforms such as Amazon or Spotify. The vast majority of these devices were IoT devices. In this sense, manufacturers of IoT devices are working together with standardization bodies, to build the next generation of more secure and standardized devices, but certification of security aspects remains as an open issue. Security threats are increasing due the ubiquitous nature of the next digital era, transforming these aspects into a major concern for companies, governments and regulatory bodies. In this respect, a suitable security certification scheme (21) would help to assess and compare different security technologies, in order to provide a more harmonized IoT security view to be leveraged by end consumers. The term certification is used as described in the NIST definition (3), "*a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system*". As a result of this process, it is expected a cybersecurity label (labelling process), which contains *information that represents or designates the value of one or more security relevant-attributes* (NIST definition).

Indeed, the European Cyber Security Organisation Working Group 1 (ECSO WG 1) (22) is working on standardisation, certification, labelling and supply chain management, developing a roadmap for the development of security standards and certification. The European Union Agency for Network and Information Security (ENISA) (15) also discusses the main challenges regarding security and privacy of online seals and proposes solutions, such as a label or icon showing the different dimensions of security and verified automatically.

However, a proper certification approach for security in IoT must overcome different obstacles that are inherent to this paradigm. On the one hand, the high degree of heterogeneity of devices is in conflicting with the need for objective comparisons regarding security aspects. On the other hand, due to the dynamism of typical IoT environments, the certification approach must take into account these changing conditions, in which the product will be operating. Therefore agile self-assessment schemes and test automation environments will need to be created and evolved to ensure products have minimum security level appropriate for a specific context (14), and that the security level is updated throughout the device's lifecycle (23). Indeed, this is also reported by ENISA in (11) and the Workshop on Security and Privacy on IoT (9): "a security assessment would have to cover all components of the architecture of a connected system, while taking the life cycle of the device into account."

Towards this end, a clear identification of threats and vulnerabilities is key to guarantee the success of the approach. In addition, the methodology must cope with the business requirements and needs from the IoT market. It means that security certification approaches should be efficient and cheap, so the product launch in the market is not delayed. Another challenge is how to communicate the result in a way that is understood by the user (15).

To cope with these challenges, this work presents a certification approach for IoT security based on two building blocks, risk assessment and testing. In this sense, the objective of the certification process is labelling the device's security within a specific configuration (protocols, key lenth, ciphersuite, etc.) and context. This work proposes an instantiation of the risk assessment and testing methodology proposed by the European Telecommunications Standards Institute (ETSI) in (7), focusing on the risk assessment. This proposal is part of the methodology being implemented and developed in the European ARMOUR project[1], whose objective is to automate the security evaluation, in particular the testing, and therefore, to make the certification process in IoT faster and easier.

2. Challenges for an IoT cybersecurity certification framework in the IoT lifecycle

Security issues are of major concern for IoT devices users. For this reason, vendors should ensure that security is guaranteed and monitored during the whole life cycle of their devices, since the device is created. The main purpose of this section is to motivate the need for cybersecurity certification framework through an overview of the main requirements that must be addressed during the different stages of the device's lifecycle.

2.1. The IoT lifecycle

Nowadays, the application of security mechanisms and protocols to manage the lifecycle of smart objects is one of the most critical challenges in the IoT paradigm. In the same way, a security certification framework should be present in all the phases of the device's lifecycle.

The proposed lifecycle shown in Figure 1 is based on the work presented in (24). Following its description, the device's lifecycle begins when it is manufactured to be later installed and commissioned within a network. During this phase, the device is provisioned with security credentials through the application of bootstrapping mechanisms. Then, the device is in the operational phase providing the functionality for which it was manufactured. In this stage, the application of security mechanisms is essential so that the object can interact with other devices in a secure way. Furthermore, a device can be in an updating (or management) stage, in which it can be updated or configured by the manufacturer or owner. Finally, it can be recommissioned, decommissioned or discarded, which requires appropriate mechanisms for the revocation of credentials that were obtained during the previous stages.

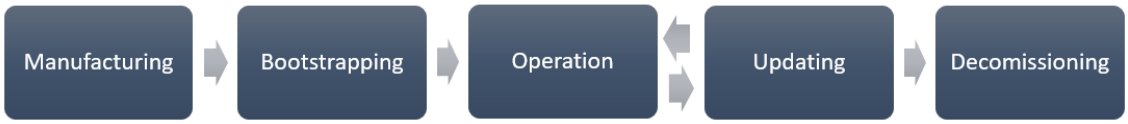

Figure 1 Phases of an IoT device lifecycle

In the next subsections, the challenges associated to the definition of a cybersecurity certification framework related with each phase of the IoT lifecycle are discussed furthermore.

[1] http://www.armour-project.eu

2.1.1. Manufacturing

The device's lifecycle begins when it is manufactured to be later installed and commissioned within a network. In this phase, the device is created, programmed and tested, so the initial level of security is established. In this stage, manufacturers are responsible for carrying out the initial security certification for the device.

During manufacturing, it is important to pay attention to the best security practices for programming and the adequate implementation of them, testing the device in order to check it. In this phase, as a result of a certification process, a cybersecurity label can already be assigned. The cybersecurity label can add extra recognition at the time of the product, improving its sales by offering not only a certified security level, but also the guarantee of having passed through the certification process. Consumers can then have a comparison mechanism facilitating their understanding through a simple and visual label. However, some challenges have to be addressed in this first phase. In (11), ENISA remarked the need for the harmonization of a security certification mechanism, which would make promoting and delivering new products more convenient for manufacturers. Regulatory bodies have an important role here, promoting the creation of security framework through the consensus, orchestrating its development and setting the basis for it.

2.1.2. Bootstrapping

The bootstrapping phase starts when the device is installed and configured in a certain context. This process usually consists of a set of procedures in which a device joins a network in a certain domain (health, house, industry…). During the bootstrapping, the cryptographic material statically configured during manufacturing in the device is used to derive dynamic credentials and keys to be used during its operation.

In this sense, this phase gives additional information related to the security provided by the device, and the security level that is required in the domain where the device is deployed. This information should be taken into account in the certification process. On the one hand, the security provided can be obtained from the device's datasheet in which the supported protocols and cryptographic algorithms could be reflected. On the other hand, the security level required can be obtained from the analysis of the different existing domains by consulting the corresponding experts and laws associated to the deployment domain. These two levels of security must be compared in order to come up with a realistic view of the device's security in a specific context.

2.1.3. Operation and Updating

During the operation stage, the device is providing the functionality for which it was manufactured. In this phase, the device should be monitored, since new security threats can be discovered or a new patch/update can be installed, and consequently, the device's security level can be modified. Indeed, this stage may involve procedures related to software updates or patches by the manufacturer, as well as configuration tasks by the owner, influencing also in the security level offered. Consequently, the management process should be supported by mechanisms that allow the ownership transfer to be done correctly to ensure that only

legitimate and authorized users are able to manage their devices. In this sense, the set of security considerations during the operation stage are also applicable for this phase.

Both the changes produced by an updating process, and the modifications produced by a unexpected event (e.g. the discovery of a new threat) led to a new security level, so the cybersecurity label has to be updated through a *recertification* process. The realization of such process through an easy and fast methodology represents one of the major challenges for the definition of a cybersecurity certification framework.

2.1.4. Decommissioning

Decommisioning or end-of-life refers to the process of removing an ICT component or system from active status. In this phase, IoT devices, which could store sensitive information should be decommissioned through processes ensuring that such information is not available when the device loses its active status. Indeed, the huge amount of data generated by IoT devices and the sensitivity level of the information, are crucial aspects. In particular, in scenarios such as e-health or smart buildings, disclosure of user data could reveal sensitive information such as health status or daily habits. Furthermore, the decommissioning of a device could derive on the need of the revocation of the cybersecurity label. In this sense, manufacturers and certification entities could be required, so this process can be done without the need to put additional efforts to end users.

2.2. Considerations for an IoT cybersecurity certification framework

This section aims to provide a set of some of the most significant challenges for the definition of a cybersecurity certification framework. This analysis is based on the current efforts from organization and regulatory bodies in Europe, such as ENISA, AIOTI, ECSO or DIGITALEUROPE.

- Heterogeneity of existing schemes: Nowadays, the very broad range of existing security certification schemes for products, systems, domains, solutions, services and organizations (10) derives on a heterogeneous environment of solutions, making difficult understanding what is needed to achieve a certain level of security in each context or technology. This heterogeneity also makes comparing certified devices more difficult, especially when these devices are certified with different certification approaches, countries and contexts. Currently, there is no a unified solution that copes with these problems, facilitating the process of comparing and assessing the security level of different IoT deployments.
- Burden of existing approaches: The existing approaches are usually expensive, slow and complex, requiring formal documentation and processes. It could potentially imply the manufacturer cannot afford the certification costs, or the delay for the release of the device in the market.
- Standardization: In spite of current approaches' limitations, the intended cybersecurity certification framework should be based (as much as possible) on the existing standards and approaches, taking advantage of their strong points.
- Dynamicity: One of the main problems is that security is itself a very dynamic concept. At the end of the certification process, a device could be secure, but this condition can change at any time. This makes a lightweight recertification process very important for a successful approach. A certification scheme should cope with this, taking into account

the update of the security label, after patching the device or upon the discovery of a new potential vulnerability.

- Scalability: The large amount of IoT devices to certificate makes necessary the adoption of a fast and automated proposal.
- IoT specific threat database: One of the main problems that has to face an IoT security certification framework is the inexistence of an IoT specific threat database. This database could help to centralize and control all the current threats for IoT and to have a starting point for certifying the security of the devices. In general, in the software environments these type of database already exist. Examples of them are CWE or the CAPEC.
- Need for aggregated certification: Another key point is that an IoT device could be composed by several components with different levels of security. This means that the security level of the whole IoT device depends of them, so the aggregation of the different security levels could be required.
- Cybersecurity label specification: The resulting cybersecurity label should provide a clear visibility of the security achieved, as recommended in (8). Bosch (25) adds that customers need to be able to compare the security achieved by different products without feeling overwhelmed with technical details. In this sense, there is a real need for defining a tradeoff between the simplicity of the cybersecurity label for non-experts consumers and the information offered. It should be noted, as already mentioned by ECSO, that a visual static cybersecurity label is not enough, since it should also cope with the dynamicity of security to reflect changes on the current security level. For this reason, the usage of a QR-code or NFC tag can help to check the status of the cybersecurity label in a fast an easy way.
- Influence of the context: The context in which the device will operate must be considered, in order to make devices comparable among each other. A possible solution could be obtaining the cybersecurity label for all the possible contexts and made them available through the QR-enabled cybersecurity label, which can be updated after the device is deployed on a specific context.
- Use of consistent security metrics: The security level offered has to be quantitative measured through certain metrics to obtain a more accurate security view. However, some of such metrics, such as *likelihood* or *impact*, are difficult to be measured, due to its complexity, which is reported in (24). Some approaches advocate the elimination of these metrics (e.g. the likelihood), such as the Common Weakness Scoring System (CWSS) (26), which will be described in the next section. Moreover, some authors try to obtain an objective value for likelihood through the usage of attack graphs (27).
- Multi-layer certification: A security certification framework has to take into account the IoT protocol stack in order to have an overall cybersecurity label that covers the entire configuration and the different threats that could be derived from each layer. Currently, there are existing approaches to aggregate risk marks from several layers such as the solution provided in the scope of the RASEN project (28). However, the certification of physical aspects could be challenging, especially if automation aspects need to be considered.
- Consider the device lifecycle: A security certification framework should address the different stages of an IoT device's lifecycle. On the one hand, the security of the device should be monitored during the whole lifecycle, in order to identify new potential vulnerabilities. On the other hand, the cybersecurity label should be updated, when a

cybersecurity recertification process is required because of a security change or update/aptching.

Finally, Table 1 provides a summary of the described challenges.

Table 1 Current challenges for a development of an IoT security certification framework

Challenge	Description
Heterogeneity of existing schemes	The very broad range of existing security certification schemes makes the understanding of a certain security level requirements more difficult. This aspect has a direct impact on the adoption of solutions to make IoT devices comparable among each other.
Burden of existing schemes	The existing schemes are usually expensive, slow and complex, requiring formal documentation and processes.
Standardization	A new certification scheme should take advantage of the existing standards as much as possible.
Dynamicity	A fast and easy recertification process is needed in case of updating or patching to cope with the dynamicity of security.
Consider the device lifecycle	The certification process should be done during the whole life cycle of the IoT device, coping with changes in the security.
Scalability	The large amount of IoT devices to certificate makes necessary the adoption of a fast and automated proposal
IoT specific threat database	An IoT specific database could help to centralize and control the current threats for IoT
Heterogeneity of the system	In a system composed by several devices, the overall security depends on them and it is difficult to measure it.
Cybersecurity label specification	Tradeoff between simplicity and cybersecurity information being provided to end users.
Influence of the context	The context where the device will be deployed is crucial to assess the provided security level.
Use of consistent security metrics	Some metrics such as likelihood are difficult to measure in an objective way.
Multi-layer based certification	The different layers of the IoT protocol stack derive in different threats that should be considered by the certification framework.

3. Security testing and assessment as the baseline towards a cybersecurity certification framework

Nowadays, there is an increasing interest to establish a general basis for security certification and labelling. In this sense, DIGITALEUROPE[2], that represents the digital technology industry in Europe, has published some recommendations for Cybersecurity Certification and Labelling Scheme, such as a dynamic cybersecurity label, self-certification, global support, test automation and low cost process. ECSO (10) has also done a wide state of the art focusing on standards that can be (potentially) used as the basis for assessing the overall cybersecurity of a product or component, an ICT service, a service provider, organization or a critical infrastructure. In this sense, our proposal is based on an ETSI proposal derived from the RASEN project (7), where concrete technologies and tools are proposed.

The current main security *certification* standard is the Common Criteria (CC) (29), where the security functional and assurance requirements are specified through Protection Profiles (PPs) for a Target of Evaluation (TOE), which is a set of software, firmware and/or hardware. However, it does not include risk assessment on evaluation results and the result is binary (i.e. it fulfils the profile or not). It uses Evaluation Assurance Levels (EAL) to describe numerically the depth and rigor of an evaluation. CC describes the set of general actions the evaluator has to carry out, but it does not specify procedures to be followed for those actions. In addition, it does not include risk assessment on evaluation results so the final decision in the certification is more binary (i.e. it fulfils the profile or not). CC provides assurance that the process of specification, implementation and evaluation of a product has been conducted in a rigorous, standard, and repeatable manner.

Even if CC is the main standard and it is well developed, there has been identified a number of limitations (30) (31), that are being taken into account by the CC community, such as the time and effort requested to execute an evaluation especially for the high EAL or the management of changes in the certified product. If the product is still in the growing phase from the market point of view, this cost can become a serious obstacle for commercialization (especially in IoT). CC has also a problem of lack of comparability, due to the difficulty in understanding the CC technical documents for the certification of a product, which make more difficult an objective comparison. Despite some disadvantages, CC is the main security certification standard, widely recognized and developed, so for the homogeneity of the terms, our proposal reuses the concepts of EAL and TOE.

Other important schemes are the Commercial Product Assurance (CPA)[3] aiming to evaluate commercial off-the-shelf products and developers, the Cybersecurity Assurance Program (UL CAP), which uses the UL 2900 standards[4] and the Certification de Sécurité de Premier Niveau (CSPN), that uses limited-time black box testing.

Although there is a huge variety of certification proposals, none of them is specific for IoT, forgetting challenges associated to these type of devices, such as the big dynamism related with

[2] http://www.digitaleurope.org
[3] https://www.ncsc.gov.uk/scheme/commercial-productassurance- cpa
[4] http://ulstandards.ul.com

new threats and updates that they have. The cost, effort and price of these mechanisms makes the recertification process more difficult to be performed.

The proposed IoT specific cybersecurity certification scheme (in the scope of the ARMOUR European project) is intended to provide a more standardized view based on the ETSI methodology. Specifically, it is built on top of risk assessment and testing processes, by considering an automated solution that could face the IoT challenges related with dynamicity and scalability. While the definition of this cybersecurity certification framework needs to address significant challenges (as previously described), the proposed approach is intended to serve as the baseline to for a more standardized version of the certification process for IoT.

3.1. The ETSI Risk-based Security Assessment and Testing Methodologies

The ETSI proposal described in (7) combines an extended security assessment derived from ISO 31000 and typical security testing activities following the standard ISO 29119. This methodology was initially developed and evaluated in the RASEN research project.

We consider the definition of a cybersecurity certification framework could be built on top of two main streams of this proposal: *Security Testing*, which is intended to discover flaws, vulnerabilities or other technical issues, and *Security Risk Assessment*, which is meant to analyze potential threats addressing legal or business issues. In addition, an initial process *Establishing the Context* is included to set up both processes. The activities *Monitoring & Review*, and *Communicate & Consult* are intended to set up the management perspective, continuously reacting and controlling the information derived from assessment and testing processes.

The proposal distinguished two main perspectives, a test-based risk security assessment (Figure 2, left) and a risk based security testing one (Figure 2, right). In the test-based risk security assessment, testing is used to guide and improve the risk assessment, adjusting risk values and providing feedback, whereas in the risk based security testing, risk assessment results are used to guide the testing, prioritizing the areas to be tested according to their risk.

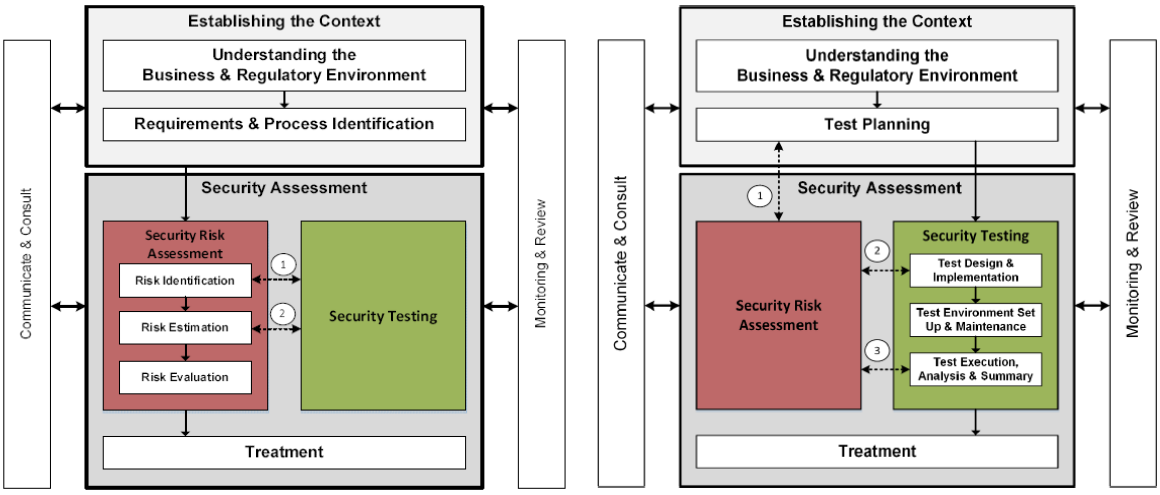

Figure 2 ETSI proposal for integrating risk assessment and testing

In this direction, this work proposes the use of specific technologies to help IoT stakeholders for security risk assessment and testing processes, as the main building blocks to build a security certification and labelling approach for IoT devices. As described below, it represents, in turn, an instantiation of the described methodology proposed by ETSI, as a way to avoid reinventing the wheel and to take advantage of it standardized basis.

In the next sections, different existing approaches and current efforts associated to theses processes are described.

3.1.1. Risk assessment

As part of this certification process, being able to measure the risk of different IoT security approaches is crucial to quantify their security level, since it allows comparing different configurations and scenarios. There are a high number of *risk assessment* methods managed by both commercial and non-commercial organizations. However, they are often subjective, specific for web applications or too large and complex. Examples of them are the DREAD Scheme (32), the OWASP Application Security Verification Standard Project[5], Microsoft's STRIDE (33) model or OCTAVE (34).

The Common Vulnerability Scoring System (CVSS) (26) consists of three metric groups that contains multiple metrics, like the Common Weakness Scoring System (CWSS) (35). Applying a formula to these metrics, a risk value between 0 and 100 is obtained. Conceptually, CVSS and CWSS are quite similar, but CWSS can be applied earlier in the process, before any vulnerability has been proven. In addition, CWSS has the advantage that explicitly supports *unknown* values when there is incomplete information. They are widely used standards, for example in CWE/SANS Top 25[6], in OWASP Top Ten[7] or in the National Vulnerability Database[8].

However, the risk assessment proposals for IoT are limited, and the majority of them are focused on a specific domain. In this sense, (36) describe a risk-based adaptive security framework for IoT in eHealth that will estimate and predict risk damages and future benefits using game theory and context-awareness techniques. The authors in (37) focus on Bluetooth technology, extending the calculation formula for Authentication of CVSSv2. In (38), the authors adapt the DREAD risk model to IoT and finally they recommend aggregating the DREAD score of the vulnerabilities using a weighted average function for which the weights have to be determined based on the system type. However, DREAD is not completely objective, and the results may change with different evaluators.

Authors in (39) propose a framework for modelling and assessing the security of the IoT in order to find potential attack scenarios, analyze the security and assess the effectiveness of different defense strategies. Moreover, a security analysis of IoT devices is proposed in (40), performed in a testbed environment using penetration testing methodologies such as port scanning, fingerprinting, process enumeration, and vulnerability scan. However, it does not give a general vision of all the dimensions of the security to advice the user, and it does not contemplate labelling as a way to describe the security result of the certification process.

[5] https://www. owasp.org
[6] http://cwe.mitre.org/top25
[7] https://www.owasp.org/index.php/Top_10_2017-Top_10
[8] https://nvd.nist.gov

3.1.2. Testing

Being able to test the security of the different IoT security approaches allows to prove the security level assigned to them. Some of the current security testing approaches are briefly described below and more detailed information can be found in (41).

In *penetration testing*, an application or system is tested from the outside, similar to an actual attack from a malicious third party, with limited information about the system under test and only able to interact with the system's public interfaces. This technique is generally manual and it is combined with the usage of black-box vulnerability scanners, which are used to identify security issues in applications.

Fuzzing is a technique consisting on passing into a target system valid and invalid message sequences to see if the system breaks, and if it does, what it is that makes it break. An important feature of fuzzing is that it requires no knowledge of implementation details of the target system. This type of technique is very useful to test injection attacks for example, and can be combined with other testing mechanisms.

Regression testing techniques are focused on the update of the device, ensuring that changes do not cause unintended effects on unchanged parts and changed parts of the software behave as intended.

Usage-based testing focuses the usage of a system. Instead of testing all parts of the system equally, the parts that are often used are tested intensively, while seldom or never used parts are ignored. There is also a combined version with fuzzing proposed in (42).

The *Risk Based Security Testing* (RBST) approach tries to improve security testing with the help of security risk analysis and the final results are test result reports. There are many different methods, some of them trying to identify test cases whereas others try to prioritize test cases.

Code based testing detects vulnerabilities by looking at the code. This can be performed manually or automatically using a specific tool.

However, compared to traditional testing methods, *Model-Based Testing* (MBT) is able to manage and accomplish testing tasks in a cheaper and more efficient way. Models represent the system under test (SUT), its environment, or the test itself, which directly supports test analysis, planning, control, implementation, execution and reporting activities. In addition, a large number of MBT tools have been developed to support the practice and utilization of MBT technologies in real cases (43).

It is worth noting that the testing methods can be combined creating new testing methods (e.g. MBT with fuzzing (44)) or complementing each other in different phases of the device life (42).

3.1.3. Monitoring and review

Monitoring is defined by NIST (3) as an "*ongoing observance with intent to provide warning. A continuous monitoring capability is the ongoing observance and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations*" In the same document, an example of monitoring architecture is proposed, based on different domains, such as vulnerability, patch, event, incident or malware Management.

In the ISO 31000, this activity refers to continuously monitor and review the appropriateness of the risk criteria, analysis, treatment, and the framework itself. The cycling process of Plan, Do, Check, Act applies to it, since the whole risk strategy needs to be considered as a constantly evolving element as the security objectives change over time. In the ISO 31000, when a risk changes, the risk treatment needs review, and this review should include all stakeholders, internal and external.

As it can be observed, monitoring is not only related with detecting new threats or attacks. Monitoring is also in charge of monitor the state of the device, to detect changes in its security derived from new threats discovered, a patch, an update, a change on the scalability or the domain, etc. In addition, monitoring has the important mission of be updated in relation with the security needs in each domain, in order the certification mechanism could offer an updated and realistic vision of the security offered by a device.

Therefore, monitoring is not only an active activity during the first certification process, but also an important process during the operation phase of the device and it is key for the recertification process.

3.1.4. Communicate and consult

According to ISO 31000, this activity includes how to communicate key information to relevant stakeholders and how to manage the information. It is a two-way process that involves both sharing and receiving information about the management of risk. In our approach, as described in the next section, we have considered the *labelling* process to be part of this stage. this communication is done through the labelling, where the security level is communicated through a cybersecurity label that takes into account the security offered by the different available configurations and the security needed in a particular domain. This will be detailed in next section.

In this sense, the labelling schemes should provide a tradeoff between simplicity and the complexity of the information being provided. ENISA (15) recommends a multidimensional cybersecurity label that takes into account all the security dimensions. In (45), AIOTI states that the cybersecurity label should be considered more than a sticker, providing details about the state of the certificate and its validity. In addition, they state that the cybersecurity label should be dynamic enough to indicate the current security level and for this end, NFC or BLE connectivity could be used. As described in the next section, these considerations have been taken into account to define the proposed multidimensional cybersecurity label.

4. Proposed approach for a Cybersecurity Certification Framework

According to the proposals reviewed in the previous section, current “certification” approaches for IoT are focused on a specific context, in which labelling aspects are not considered. Indeed, we have seen how this lack has attracted an increasing attention from several important organizations, such as ENISA, ECSO or DIGITALEUROPE, which are actively working to build a more harmonized and widely accepted security certification ecosystem. In this direction, this work proposes the use of specific technologies to help IoT stakeholders for security risk assessment and testing processes, as the main building blocks to build a security certification

and labelling approach for IoT devices. The proposed approach represents, in turn, an instantiation of the standardized methodology proposed by ETSI (7) for assessment and testing, so it aims to design a certification methodology to foster interoperability and acceptance of different stakeholders. The certification process has been defined in the context of the ARMOUR project, whose objective is to provide duly tested, benchmarked and certified security and trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/Cloud testbeds properly equipped for security and trust experimentations.

Figure 3 shows the overall process of certification and risk assessment, derived from ETSI proposal based on ISO 31000 and ISO 29119 (7), and extended to include all the processes of the certification. This approach combines a test-based security risk assessment with a risk-based security testing workstream. The labeling activity has been integrated inside the communicate and consult process, since it is not considered in the ETSI proposal. In addition, although the original methodology includes a *Treatment* process (i.e. security controls and other countermeasures), this is not addressed in our instantiation. However, this treatment can be designed from the results of the *security testing and risk assessment* processes.

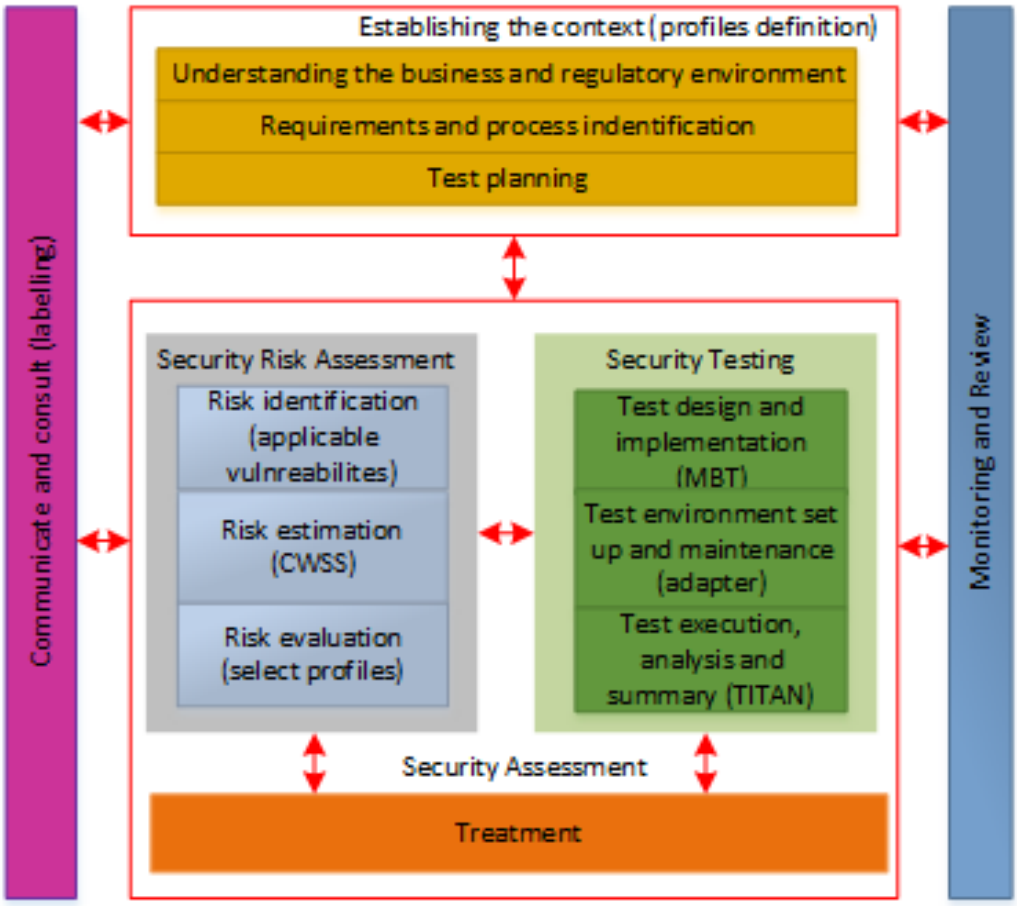

Figure 3 General overview of the certification process

ISO 27000 defines a vulnerability as “a weakness of an asset or group of assets that can be exploited by one or more threats”, where an asset is “anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission”. On the other hand, a threat is defined by NIST as “any circumstance or event with the potential to adversely impact organizational operations”. In this way, a vulnerability can lead to several threats.

As the cybersecurity framework uses as input an IoT threat database and currently, not known IoT threat database exist, we relied on the analysis done in the context of oneM2M standardization activities, which covers the whole IoT/oneM2M domain. From the threats considered in oneM2M, a mapping between them and eight general vulnerabilities is performed, as described in Table 2. We have extracted these vulnerabilities from some of the most referenced security aspects that can be found in current IoT literature (46) (47). The assignment has been done following the Table 3, where the relation between them is specified in the second column. The threat 12 (context awareness) is intended to be in the profiles defined in the next section. The purpose of this aggregation is to have a more compacted security dimensions and simplify the cybersecurity label, since it will show the security marks for each of them. In this way, this simplification from 21 threats to only 8 vulnerabilities will help the user to have a more understandable and easy view of the global security.

As explained in section 3, the establishment of a dedicated threat database for IoT is a current challenge, which will lead to a more adapted certification scheme specific for IoT. In case this database is created in the future, the methodology described in this paper will remain applicable. In that case, a mapping between the threats of the database and the eight vulnerabilities of the scheme will be required.

Table 2 Relation between OneM2M threats and the vulnerabilities considered

Vulnerability	Relation	OneM2M Threats
Lack of Authentication	Protection against a device with a non-valid ID	10,14
	Protection against a device with a valid ID but a non-valid authentication key or certificate	3, 13
	Cryptographic suite	1, 4, 19
	Protection against a server with a non-valid ID	10, 6, 14
	Protection against a server with a valid ID but a non-valid authentication key or certificate	4, 13
Lack of Confidentiality	Percentage ciphered (general)	7, 13
	Cryptographic suite	19
	Percentage ciphered (related with keys)	6
Lack of Authorization	Different profiles per device	8, 10
	Protection against a replacement with a more privileges key	13
DoS attack	Protection against attacks performed by a legitimate device	2, 14
	Protection against attacks performed by the server	5
	Protection against attacks changing the key of the device	3
Lack of Integrity	Percentage of integrity protection	8, 13
	Cryptographic suite	19
Replay attack	General protection	9
	Protection of the authorization mechanisms	17
Insecure cryptography	Dictionary attacks and related	19
	Cryptographic suite and key length	19
Lack of fault tolerance	Low cascade impact	11
	Exception control against buffer overflow	15
	Protection against injection attacks	16
	Control the input data	20
	Control scripts	21

The first process, which is called *Establishing the context is* related with understanding the business, regulatory environment, the laws and analyze which security level is required in each of them. For example, in a health context, confidentiality and availability could be considered two very important security properties that could not be as important in home automation. As a result of this process, several security profiles (e.g. A, B, C, D) related to the context will be

defined. The last activity of the first process, *the test planning*, is the activity of developing the test plan (objective, scope, order, testing technique etc.). In this activity, the techniques of testing are chosen regarding each vulnerability, as well as the order of the tests and their scope.

The second process, *Security assessment* includes the *security risk assessment* and the *security testing*. Inside *security risk assessment*, three activities are considered:

- *Risk identification*. This activity uses as input the general vulnerabilities provided by the external database. Taking into account TOE, this activity is in charge of selecting which vulnerabilities will be tested.
- *Risk estimation*. This activity assign a risk mark to each vulnerability. For this purpose, default values and test results (test report following the ETSI notation) from the *security testing* process are provided.
- *Risk evaluation*. This activity compares the result of the risk estimation with the profiles considered in the *Establishing the context* process. In this way, the TOE obtains a profile, the highest it fulfils in this specific context.

The *security testing* process is related to the creation of tests for testing security. However, in the ETSI proposal, the automation of this process is not contemplated. In this sense, the proposed instantiation is intended to use specific technologies to help for automating this process, easing the update of the cybersecurity label to cope with changing conditions in which the device operates. The integration of such approaches is being done in the scope of the ARMOUR project. It also comprises three activities:

- *Test design and implementation*. This activity aims to design a test suite to obtain metrics and use it in the risk estimation, testing therefore, the risk's grade of each vulnerability.
- *Test environment set up and maintenance*. The execution of the tests suites is ensured through test adaptors, which are needed to adapt the generated test code to each IoT device.
- *Test execution, analysis and summary*. The tests designed in the previous activity are executed. From the execution, it is gathered information related with the result of the tests and related with some metrics, for example time.

Finally, the figure 3 shows additional support activities like *Communication and Consult* and *Monitoring and Review.* The first one is meant to continuously control and react to the changes on the device security. The second one is meant to gather information from inside (risk, context, etc.) and outside (experts, databases, laws, etc.) the process, and to communicate it in an appropriated way. The communication and consult activity also includes the labelling. With the data collected from the test execution, taking into account the profile obtained, the context and the certification execution (explained in the following section), the certification process generates a cybersecurity label, helping the user to know the security level of the TOE.

As shown in Table 3, the challenges discussed in section 2 can be associated the different activities and process of the ETSI proposal. In this way, for example the need for a specific IoT threat database is linked with the general process of certification.

Table 3 Certification process related challenges

Challenge	Certification process
Heterogeneity of existing schemes	Establishing the context
Burden of existing schemes	General
Dynamicity	Monitoring & Review/Testing/Communicate and consult
IoT specific threat database	General
Scalability	Monitoring & Review/ Communicate and consult
Cybersecurity label specification	Communicate and consult
Heterogeneity of devices	General
Take the device lifecycle into account	General
Heterogeneity of the system	General
Influence of the context	Establishing the context
Metrics	Risk assessment
Multi-layer based certification	Risk assessment/Testing/Communicate and consult

One of the main challenges is the security management during the device's lifecycle. In the proposed approach, the certification process is intended to manage the security of the IoT device's lifecycle, as shown in Figure 4.

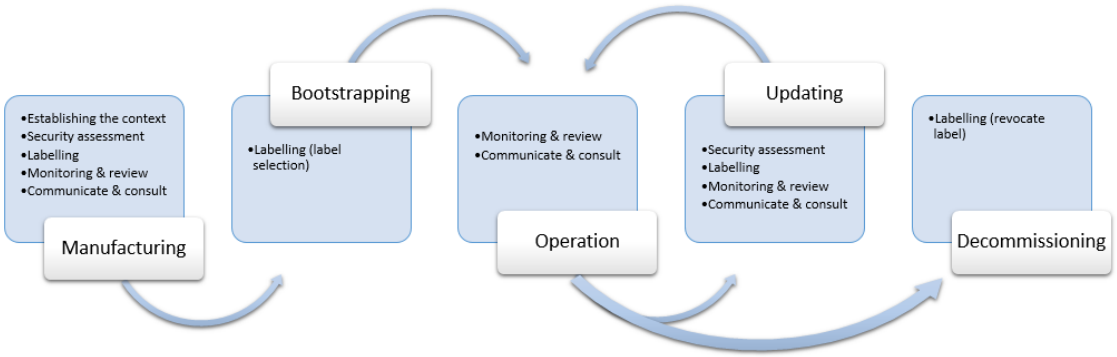

Figure 4 Relationship between the Certification activities and the device lifecycle

There are some preliminary steps after initializing the certification process, which are the establishment of the threat database, the analysis of the different existing contexts and their regulatory environment, creating from this information the set of profiles available for certification (yellow boxes in Figure 5). Because of this, several profiles are created (*establishment of context*).

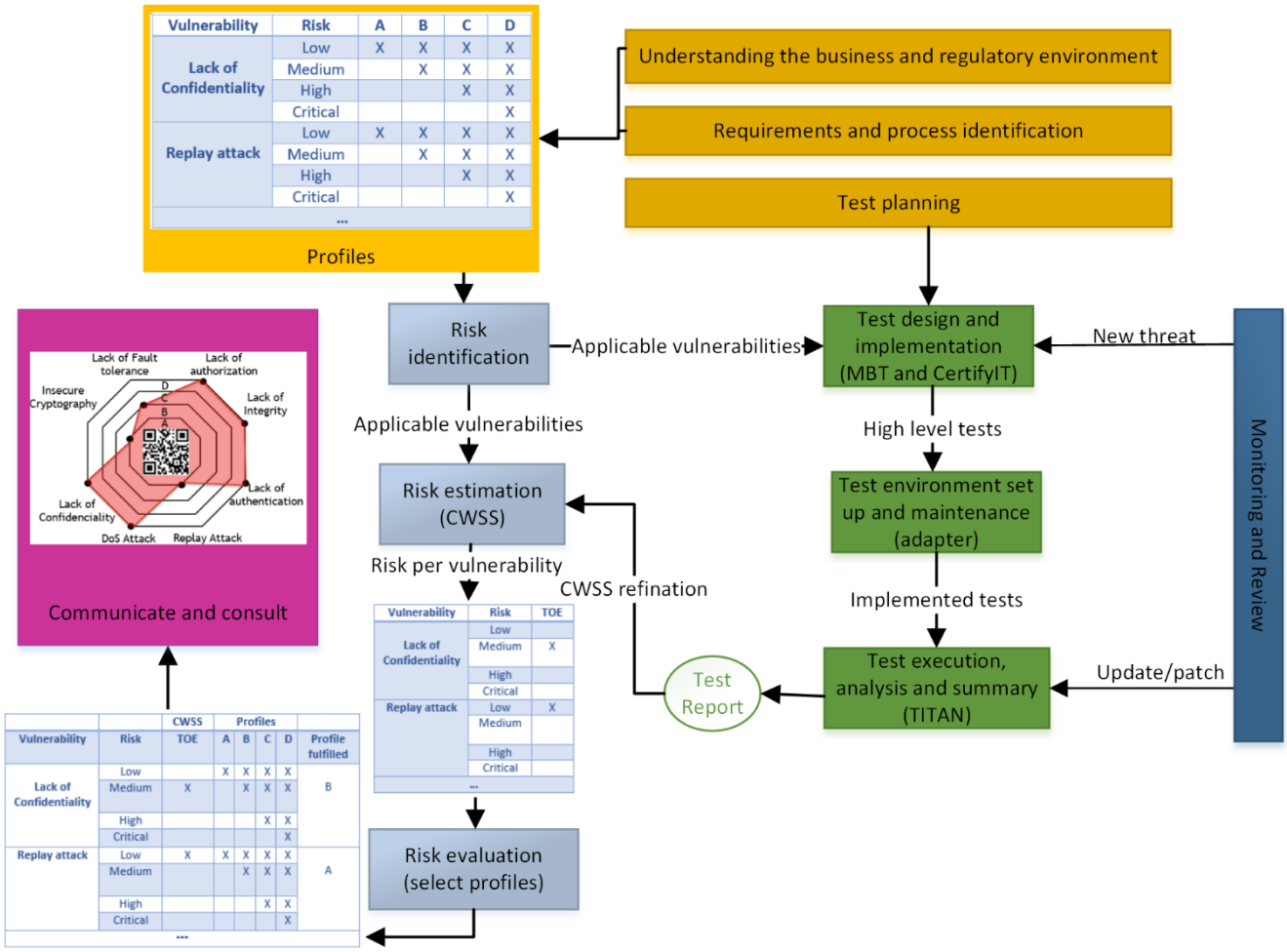

Figure 5 Relationship among the certification activities

In the manufacturing phase, all the certification process must be done until the cybersecurity label is obtained. We identify the applicable vulnerabilities, design (following the technique established in the *test planning*), implement and execute the tests and use the test report to refine the risk estimation (*risk assessment and testing*). As the context is yet unknown, the result of the process derives on multiple cybersecurity labels for the configuration supported and the available contexts (*communicate and consult*). in this sense, the seven contexts defined in (19) can be considered. The QR is charge of giving access to all the different labels. The label also includes the certification execution in order to indicate how the certification process has been performed (self-certification, third party, etc.).

During the operation phase of the device the *monitoring and review* activity should be active in order to check if any changes have been produced and act consequently.). This can include a patch, an update or a new threat discovered. On the one hand, if a new threat is discovered, the this process triggers the *test design* activity, in order to model it. As in the certification process, the test is generated in CertifyIT and executed by means of TITAN (*test execution, analysis and summary*). It may be not necessary to change the adapter if we already have the basic functionality implemented (*test environment set up and maintenance*). From the test report, the risk mark is updated in the security *risk assessment* process, and finally, the label is updated with the new profile fulfilled (*communicate and consult*, *labelling*). On the other hand, if an update or patch is detected, the *monitoring and review* triggers directly the *test execution, analysis and*

summary activity and follows the process previously described so the label can be updated accordingly.

Another event can be a caused by a reownership. In this case, the new owner has to select the appropriate label according to the new context where the device is installed.

Finally, when the device is no longer used, the label must be revoked. In this sense, the user or administrator (or even the manufacturer) of the device could communicate it in the QR link in order to revocate the label in an easy way. In addition, the way the information is removed from the device should be part of the vulnerabilites considered in the certification approach.

Following sections are intended to describe the instantiation of the ETSI architecture by using concrete approaches and technologies. We detail each process and how they are intended to be executed.

4.1. Establishing the context through general vulnerabilities and profiles definition

This first process is composed by three activities that aim to set up the certification process, as shown in Figure 6.

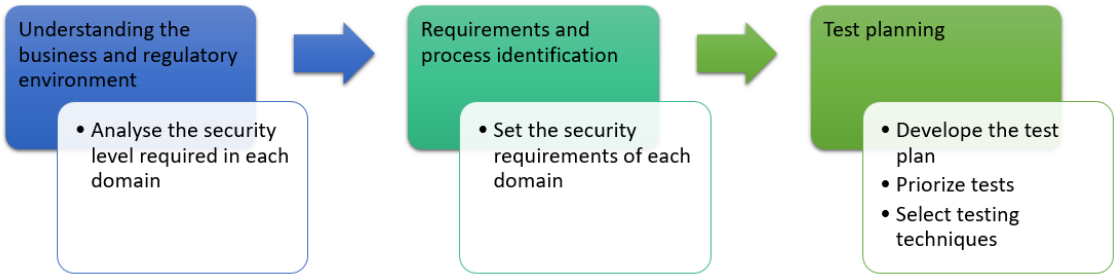

Figure 6 Establishing the context process

In the first activity, *understanding the business and regulatory environment*, a risk analysis is performed in order to determinate which level of security is needed in a specific domain. Experts in each context could be required to perform this analysis. It includes understanding the laws and the regulation environment. In this way, we add the context variable to the cybersecurity label, which will be reflected in the profiles associated to each of them, coping with one of the challenges previously described.

From this analysis, the next activity, *requirements and process identification*, defines several profiles (A, B, C, D…), (e.g. in a similar way to the European energy label). The number of profiles can be modified to make the security level more accurate. The profiles indicate which level of security must be achieved by the TOE in each vulnerability considered and for a specific context to obtain each profile, following the notation of Table 4. In this example, a TOE obtains the A profile if it has a low risk level in confidentiality. It is worth noting that if a TOE fulfils one specific profile, it also fulfils the lower ones, so if A profile is obtained, it also fulfils B, C and D profiles.

Once the requirements of each domain are set up, the next step is *planning* and defining the tests. This phase includes analyzing the security of the device and design what tests should be implemented. Although it is not considered in this activity, planning could be used to prioritizing

the tests in order to perform a fast regression testing in case of a recertification process. This process is explained furthermore in the next sections.

This process interacts with the two transversal activities. On the one hand with *Communication and Consult* since it needs communication with the security experts in each context. One the other hand with *Monitoring and Review* to monitor the environment, keeping updated the profiles and the discovered threats.

Table 2 Example of profile definition

Vulnerability	Risk	A	B	C	D
Lack of Confidentiality	Low	X	X	X	X
	Medium		X	X	X
	High			X	X
	Critical				X
Replay attack	Low	X	X	X	X
	Medium		X	X	X
	High			X	X
	Critical				X
...					

4.2. Security testing: the ARMOUR approach

From the vulnerabilities considered, the security tests that are used during the security risk assessment process are produced, allowing us to refine the risk associated to each vulnerability. This tests can be used to find out if a threat is present or not (e.g. establish a communication with a non-valid key) or to obtain metrics (e.g. number of messages protected against replay attack).

The three low level activities corresponding to security testing are shown in Figure 7, and they will be explained below.

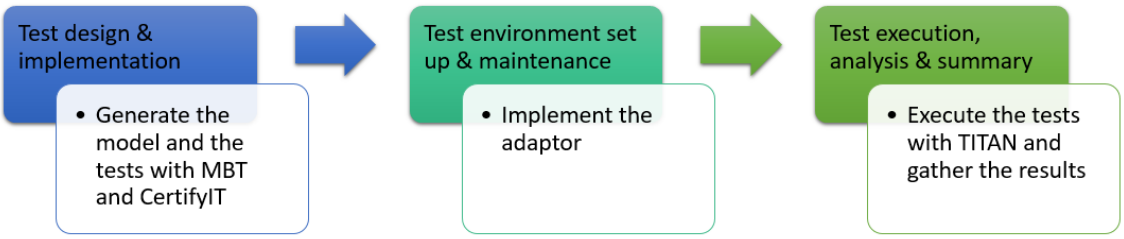

Figure 7 Security testing activities

In the ETSI proposal, security testing is not intended to be automated, which is crucial to cope with the dynamicity of security and with the recertification process. However, in ARMOUR project, and therefore our proposal, this process is intended to be automatized (48) by means

of automatic test generation and execution tools to derive on a more agile and easy certification process, as shown in Figure 8.

Figure 8 Automation of the testing process

In the first activity, *Test design and implementation*, a test suite is designed to test the risk's grade of each vulnerability. To automatize this process, a Model-based testing (MBT) approach is used to specify the tests and their behavior (49). MBT has shown its benefits and usefulness for systematic compliance testing of systems (50). In this approach, the structure of the system is modelled by Unified Modelling Language (UML) class diagrams, while the system behavior is expressed in Object Constraint Language (OCL)[9], using the CertifyIt tool (49). Functional tests are obtained by applying a structural coverage of the OCL code describing the operations of the IoT system under test. We export the tests defined in MBT in Testing and Test Control Notation (TTCN) v.3 language using the tool CertifyIT. The main goal of the use of TTCN-3 in the proposed approach is the systematic and automatic testing of security properties in IoT devices for improving efficiency and scalability.

Secondly, in the *Test environment set up and maintenance* activity, we use adapters, a middle interface between the TTCN3 and the device code, to cope with the particularities of each IoT device.

Finally, in the *Test execution, analysis and summary* activity, we execute the tests on a local or external large-scale testbed such as FIT IoT Lab, where we test the implemented scenario by means of TITAN. TITAN is a TTCN-3 compilation and execution environment for different platforms that in combination with CertifyIt create executable tests, whereas FIT IoT-LAB offers the large-scale testbed on which the test cases are executed.

With the automation of this process, if a new threat is discovered, the recertification process can be done in a cheap, fast and easy way, which is key to address the dynamic nature of cybersecurity in IoT.

The results of the tests will help to establish the security level (cybersecurity label) in a more refined way, since they are used during the security risk assessment process, allowing us to measure the risk associated to each vulnerability.

It is worth noting that the proposed mechanisms for the automation are independent of the methodology used to automate the process. ARMOUR project has helped to validate this specific combination, but other one is also possible

4.2.1. Relationship with the other processes

In the Figures 9 and 10, the possible interactions with the security testing are shown.

In first place, the monitoring process can detect a new vulnerability, an update or another event that may cause a security change. In this case, the monitoring can triggers a test execution activity in order to verify if there has been a change in the test report, leading to a new security

[9] http://www.omg.org/spec/OCL/2.4

level. If the monitoring detects a new threat, it should be modeled in order to create the correspondent security test (Figure 9).

Although it is not considered in our proposal the ETSI methodology offers la possibility of performing a vulnerability priorization through the risk assessment to execute the tests from the more risking vulnerability to the less risking (Figure 10). This could be interesting in case of a regression testing, where an update has been performed and we want to know in a fast way if there is a security change, coping with the problems of wasted time and money that the recertification may cause.

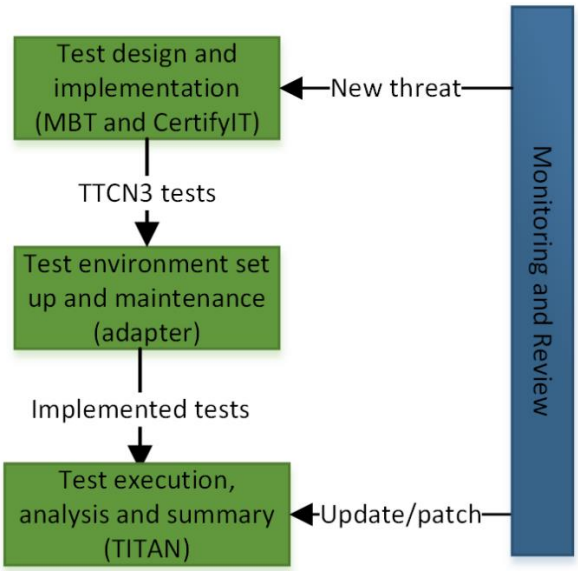

Figure 9 Interaction of the certification processes with the testing (a)

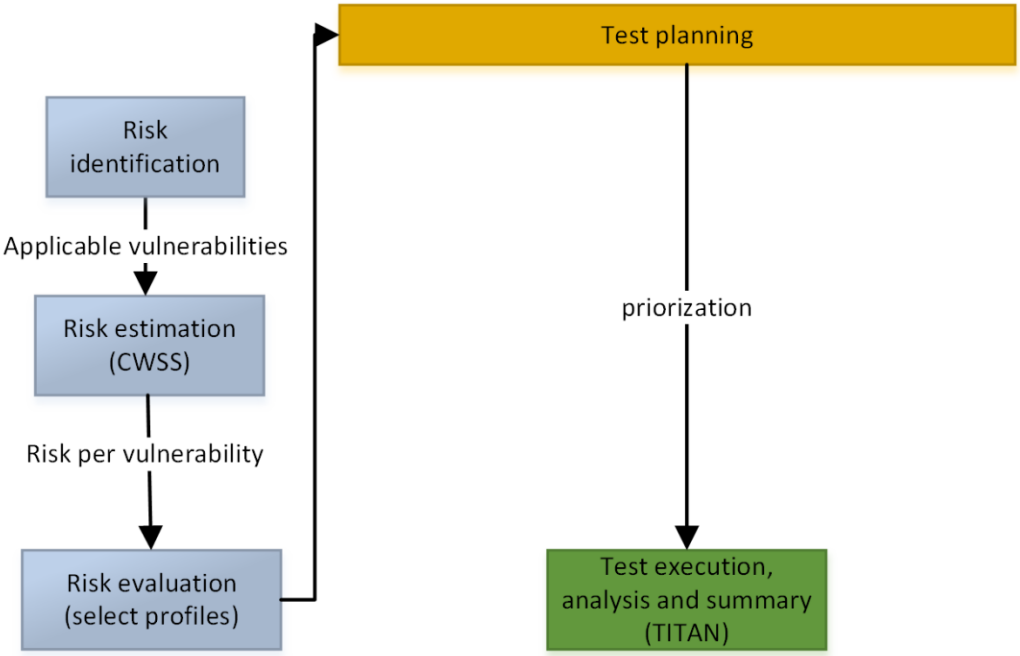

Figure 10 Interaction of the certification processes with the testing (b)

4.3. Security risk assessment based on CWSS

Risk assessment process is intended to provide different results from testing to serve as the baseline for the certification scheme, providing a risk mark associated to the vulnerabilities considered in order to be able to compare different scenarios and to be used by the certification to obtain the final cybersecurity label. This mark will be used to select the profile fulfilled by the TOE, established in the previous process. Towards this end this methodology is based on the identification of different metrics per functional block (e.g. lack of authentication), that is, the factor taken into account in the risk mark. The test report including the tests results, helps to increase the trust level on the risk associated to each vulnerability in IoT products and solutions.

Security risk assessment is composed by three main activities, as shown in Figure 11.

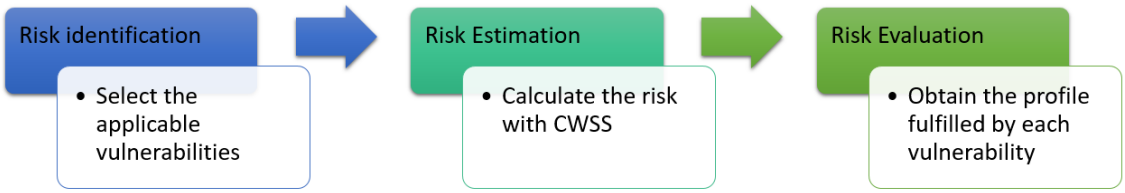

Figure 11 Risk assessment activities

In the *risk identification*, from the vulnerabilities considered in the *establishment of context* process the potential ones that can be applicable to the scenario and context are identified. The rest of the general vulnerabilities will be labelled by default with a low risk if the vulnerability cannot be exploited or with critical risk if the TOE does not have protection against it.

In order to be able to obtain the profile that is used for the labelling, in the *risk estimation* it is obtained a risk mark associated to each vulnerability considered. Taking into account that CWSS is simple, well defined, its metrics comprises the majority of the metrics of the other risk assessment methods described in section 3 and that it is recommended by the ITU-T in X.1525[10], it has been chosen to perform the risk assessment with its particular metrics shown on Table 5 (35).

Table 3 CWSS metrics

Group	Metric	Summary
Base Finding	Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited
	Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness
	Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.
	Internal Control Effectiveness (IC)	The ability of the control to render the weakness unable to be exploited by an attacker.
	Finding Confidence (FC)	The confidence that the reported issue is a weakness that can be utilized by an attacker.

[10] https://www.itu.int/rec/T-REC-X.1525/en

Attack Surface	Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.
	Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.
	Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.
	Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.
	Level of Interaction (IN)	The actions that are required by the human victim(s) to enable a successful attack to take place.
	Deployment Scope (SC)	Whether the weakness is present in all deployable instantiations of the software, or if it is limited to a subset of platforms and/or configurations.
Environmental	Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.
	Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness.
	Likelihood of Exploit (EX)	The likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.
	External Control Effectiveness (EC)	The capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.
	Prevalence (P)	How frequently this type of weakness appears in software.

Some metrics of CWSS have been modified, since CWSS is intended to be used in software environments and our purpose is a risk assessment for IoT. These considerations are:

- Internal Control Effectiveness is set to Non-Applicable, since it is considered that it is a software property not applicable to general IoT environments.
- Business Impact is set to Non-Applicable, since the context is considered after, in the profiles.
- Finding confidence is set to Non-Applicable, since the scenario is being evaluated before the device is attacked.
- Some of the CWSS metric values are obtained from the tests execution. The reason of doing it, is to perform a better adaptation of CWSS to the IoT environment, gathering the value of the metrics directly from the practice, from a security test.
- Some of the CWSS metric values are set by default taking into account the vulnerability.

Finally, the subscores and the general score for each vulnerability are calculated by means of the CWSS formula:

$$S_v = BF_s \cdot AS_s \cdot E_s$$

where BF_s, AS_s and E_s are the subscore metrics of CWSS (Base finding, Attack surface and Environment) that are calculated (using the CWSS notation of Table 5) as:

$$BF_s = [(10 \cdot TI + 5 \cdot (AP + AL) + 5 \cdot f(TI)] \cdot 4$$

$$AS_s = [20 \cdot (RP + RL + AV) + 20 \cdot SC + 15 \cdot IN + 5 \cdot AS]/100$$

$$E_s = [(10 + 3 \cdot DI + 4 \cdot EX + 3 \cdot P) \cdot EC]/20$$

where

$f(TI) = 0$ if TI =0; otherwise $f(TI) = 1$.

Finally, in the *risk evaluation* activity, to obtain the profile fulfilled, the CWSS score intervals are associated with 4 risk levels (low, medium, high and critical). We determine the profile comparing the results obtained in the risk assessment with the profiles available for the specific context, choosing always the highest profile fulfilled for each vulnerability. For example, in Table 6 a TOE has obtained a Medium risk level in Lack of Confidentiality, which allows it to obtain B, C and D profiles. However, it will obtain the highest one, in this case the B profile. This process is repeated for all the vulnerabilities.

Table 4 Evaluation of a TOE

		CWSS	Profiles				
Vulnerability	**Risk**	**TOE**	**A**	**B**	**C**	**D**	**Profile fulfilled**
Lack of Confidentiality	Low		X	X	X	X	B
	Medium	X		X	X	X	
	High				X	X	
	Critical					X	
Replay attack	Low	X	X	X	X	X	A
	Medium			X	X	X	
	High				X	X	
	Critical					X	
Lack of authentication	Low	X	X	X	X	X	A
	Medium			X	X	X	
	High				X	X	
	Critical					X	
...							

As the profile is an important part of the cybersecurity label, this process has a close communication with the labelling activity, providing the results from the assessment.

4.3.1. Relationship with the other processes

As commented before, the metrics of CWSS are used to estimate the risk associated to a vulnerability. In the ETSI proposal, the testing report is used to estimate the likelihood and the consequence, metrics that are difficult to calculate due to the imprecision and inefficiency. In our proposal, the testing report is used to refine the metrics of CWSS (e.g. sniffer report with

the key length used), obtaining more objective results, following the process described in Figure 12.

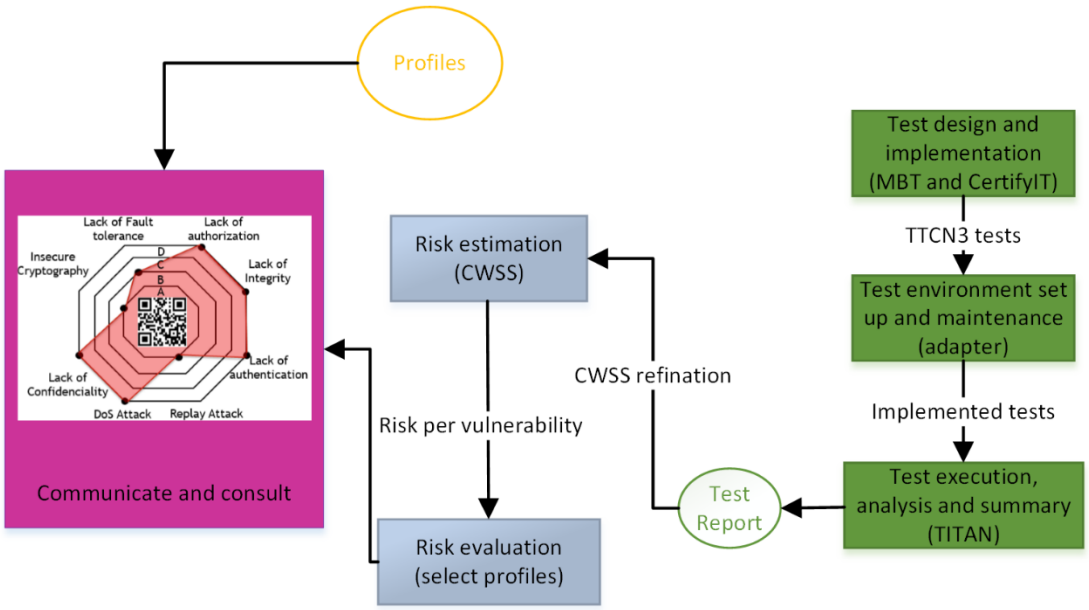

Figure 12 Interaction of the certification processes with the risk assessment (a)

As a result of an updating or patching event, the monitoring can initiate in a re-execution of the tests in order to detect a change in the vulnerabilities. It could occur that a vulnerability that was not applicable in the past (e.g. authorization) is applicable now, being considered in the risk identification activity (Figure 13) and performing later the risk estimation in order to have a more accurate risk level.

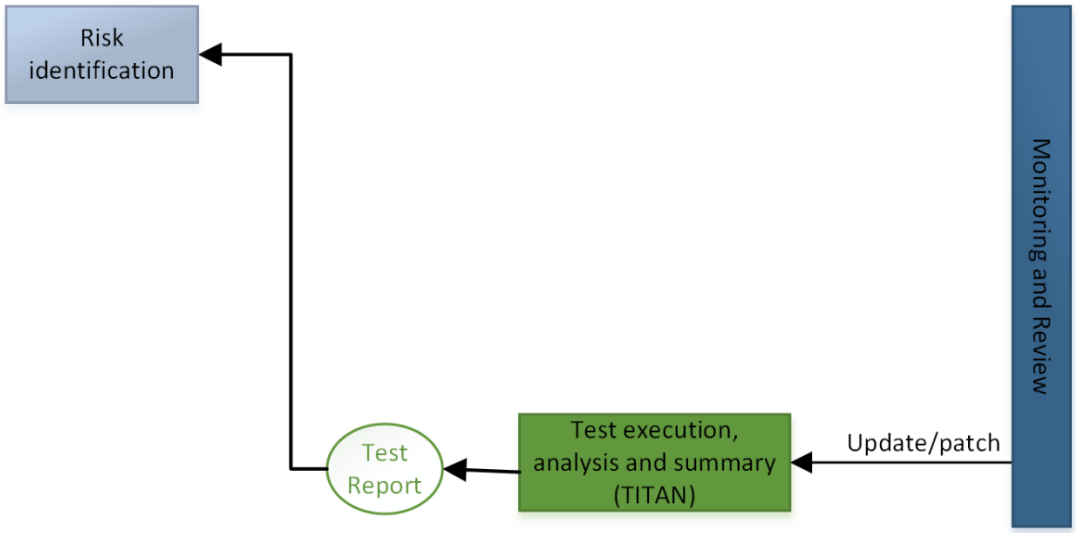

Figure 13 Interaction of the certification processes with the testing (b)

4.4. The need for Monitoring tools and mechanisms

The main concept of a certification monitoring system for cybersecurity is to design, develop and deploy a system, which is able to collect and correlate events and data from the devices and systems to detect security changes, due to new security threats, intrusion attacks, the exploitation of security vulnerabilities, an updating, a patch a change on the context of the device, etc.

Although the instantiation of this activity is not addressed in our proposal, it is used to detect both expected security changes (updates and patches) and unexpected security changes (new discovered threats). In this sense, there should be a monitoring activity of the database containing the IoT threats to detect a new one and to assess if the threat is applicable to the device being monitored. In addition, there should be also a monitoring activity of the patches and updates performed by the manufacturer and a monitoring of the changes produced by the user, that is, reownering (change of owner), changes on the scalability, etc.

If the *monitoring* detects a new threat, the *test design* activity is in charge of model it, incorporating this new event in the *security risk assessment* and producing a new label. If the detected event is already contemplated, the *monitoring* starts the *test execution* activity in order to verify if there has been a change in the test report, leading or not to a new security level. Another scenario could be that the event cause a new applicable threat not considered before, in this situation, the tests report is used to discover it and be used as input for the *risk identification* activity.

Although it is not considered, monitoring can also have a threat discovering function by means of the usage of scanning tools. In this case, when the scanning process inside the monitoring detected a new threat, the recertification process is performed in order to update the resulting label. In case a new threat is discovered, the general database could be updated, and the resulting value from risk assessment could be used to give an approximated risk value for the threat.

4.5. Labelling: a multidimensional perspective

As an output of the general certification process, a cybersecurity label associated to the risk of the scenario tested is obtained. For this approach, it should be noted that labelling has to take into account the context of the scenario that is being tested and the certification execution. For this reason, and based on CC approach for trying to homogenize the terms, three mains aspects are considered to be included in the cybersecurity label:

- TOE (Target of Evaluation): In CC, a TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance. In this case, the TOE also includes the protocol tested and the context where it has been tested.
- Profiles (level of protection): A, B, C and D. The level of protection is related to the risk associated to the tested scenario.
- Certification execution: The proposed certification execution follows the same levels of EALs than CC.

It is faced a tradeoff between the simplicity necessary for the understanding by a non-expert consumer, and the information presented in the cybersecurity label. Following the

recommendations of ENISA (15), as security requirements are in fact multi-dimensional, the result of the evaluation need to be communicated appropriately to the user. For this reason, the cybersecurity label includes the profile of each general vulnerability considered, in addition to the certification execution and the TOE. In this way, the user is provided with more information and a false sense of security is not shown, since for example, a bad mark in confidentiality could be compensated with a good mark in authentication if the marks are combined by means of an arithmetic function. For making this visual, the usage of an octagon like the triangle in (45) is proposed, where the vertices are the eight general vulnerabilities and the internal lines, the profiles. At the same time, the visual concept of more area more risk helps a non-expert consumer to understand the cybersecurity label.

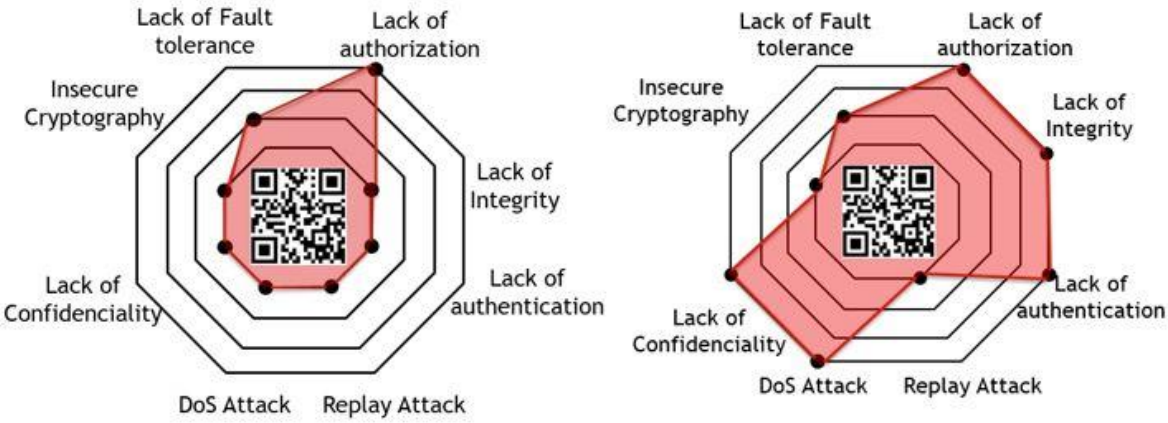

Figure 14 Examples of multidimensional cybersecurity labels obtained by two different TOEs

In addition, as security is a dynamic concept, the usage of a QR as cybersecurity label is proposed to be updated in case of a new vulnerability is discovered in the product. In this way, if the product security has to be updated, and therefore recertified, the procedure will be automatic, since the tests are already designed. Therefore, the communication to the user could be instantaneous. This process of recertification is contemplated through the parallel process of monitoring, in this case the state of the device and the recertification process through the security assessment. The proposed design for the cybersecurity label is shown in Figure 14.

5. Evaluation of the proposal and future directions

The proposed methodology is not intended to cope with all the challenges related with the design of a cybersecurty framework, but it is intended to provide a basis to build it, solving some of the main challenges described in section 2.

In this sense, the proposal takes into account the whole lifecycle of an IoT device. The certification process is not exclusive of the manufacturing phase, but it includes monitoring the devices during it lifecycle and recertificate it in case there is a change on the security level offered or needed. The inclusion of the domain in the cybersecurity label and therefore the applicability of the proposal to all of them, copes with the heterogeneity of existing schemes, providing a unique and integrated scheme for security certification. The definition of a specific domain can be based on the recent proposal in (19), which defines Consumer (domestic), Enterprise, Industrial, Medical, Automotive, Public agency and Critical National Infrastructure domains.

The automation of the testing process by means of technologies such as MBT, CertifyIT and TITAN to design, generate and execute the security tests, derives on an easy, fast and cheap recertification process, coping with one of the major challenges of a cybersecurity certification framework: the dynamicity of security. One of the reasons to perform a recertification is an update, patch or new threat discovery affecting the device. In this case, the monitoring process should detect this change and assess if a recertification process is required. However, a change on the security level can be also triggered due to a reownership that changes the configuration or the domain. The scalability is also addressed in the sense that the certification scheme is intended to be performed in a fast and cheap manner, in order to cope with the high amount of devices that has to need certified.

Furthermore, as the proposal is based on a standardized methodology of ETSI, it has been taken advantage of their strong points, not reinventing the wheel and favoring its acceptation, in the sense that the process is approved by a regulated body.

Finally, the design of the cybersecurity label includes the recommendations proposed by organizations such as ENISA or AIOTI, coping with the tradeoff between simplicity (with the subjectivity associated) and technical information being provided. In addition, the cybersecurity label is to be updated with the current certification process and security level, thanks to the usage of a QR code.

Finally, a brief summary of the challenges addressed is shown in Table 7.

Table 5 Challenges addressed by our proposal

Challenge addressed	Solution
Heterogeneity of existing schemes	The usage of profiles derives on a valid certification process for all domains and devices.
Consider the device lifecycle	The certification process is active during the whole lifecycle.
No applicability of existing schemes	Simple and fast once the automation process is established. It is based on well-known standards.
Standardization	Based on well-known standards
Dynamicity	Fast recertification process due to testing process automation.
Scalability	Fast recertification process due to testing process automation.
Cybersecurity label specification	Usage of a QR-code in the cybersecurity label to keep it updated, visual (more area, more risk) and useful (spider chart with the general vulnerabilities).
Influence of the context	Labelling for all the contexts in the manufacturing phase

It should be noted, that some of the challenges have not been addressed in the proposed approach, and they are intended to be part of our future work .

Moreover, the cybersecurity label of one device could be affected by another one with which it is connected, something that should be carefully reviewed. In addition, although the dynamicity of the security is addressed through the automation of the certification process, in case of very mobile devices that alters their domain or configuration, it should be investigated if the

recertification process, even being fast, compensates the up to date cybersecurity label, and if it is possible to do.

Another key point is the certification of multiple layers of the protocols stack. By now, in the context of the ARMOUR project, some of the experiments being considered are focused on application and transport layers (see Figure 15), but it could be extended and combined with certification at internet and link layer, considering specifics threats for it. The physical layer should be studied, since it is difficult to anticipate the physical security conditions that the device will have, before it is deployed. Currently, there are existing approaches to aggregate risk marks from several layers such as the one presented in RASEN project (28) by means of the usage of vignettes in CWSS. However, it should be analyzed if this proposal could be extended to IoT.

Although it has not been considered, lack of privacy is a challenging aspect that should be taken into account as a main vulnerability, and that should be part of the cybersecurity label, offering the consumer a clear level of the privacy provided and the associated risks. In this sense, the inclusion of Privacy Impact Assessment (PIA) process could help to define such aspects to be part of the certification framework.

Finally, the creation of an IoT threat database is out of the scope of the cybersecurity certification framework. In this sense, examples such as the National Vulnerability Databased (NVD) in the U.S can be considered for the definition of such database in the context of IoT for Europe.

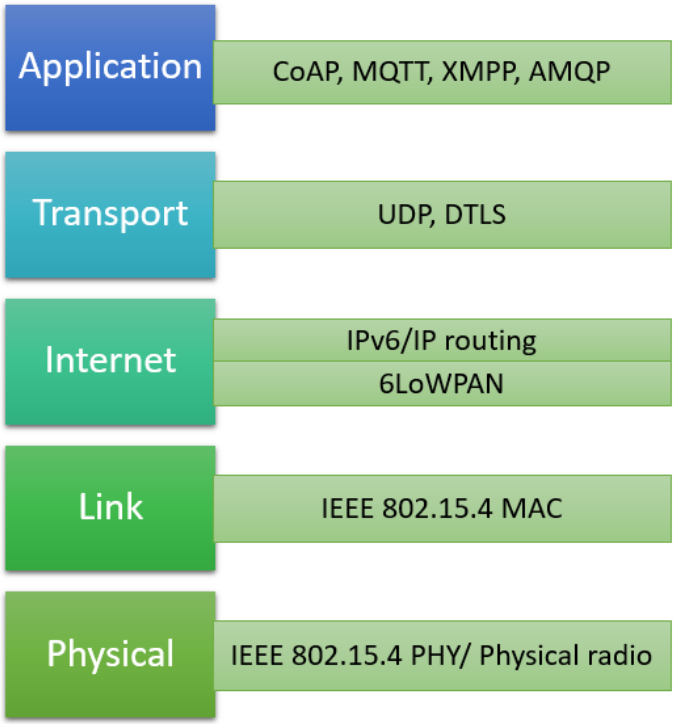

Figure 15 IoT stack

6. Conclusion

Nowadays, the IoT ecosystem demands for large-scale deployments, where devices can provide a high level of security, in order to cover typical vulnerabilities and contributing to the acceptance of these type of devices. In this sense, a cybersecurity certification framework for IoT can help to support the development and deployment of trusted IoT systems, empowering testers and consumers with the ability to assess security solutions for large-scale IoT deployments. The development of this framework has to cope with several challenges, such as the heterogeneity of the devices and existing schemes, the design of the cybersecurity label and the inexistence of a dedicated IoT threat database. However, the most important challenge is the dynamic nature of security, making necessary that the proposal includes a recertification process in an easy, cheap and fast manner. Towards this end, there is a real need to consider a systematic and automated methodology that enables scalable testing approaches for security aspects in IoT.

This document aimed to provide an initial description of the proposed cybersecurity framework based on the ETSI proposal and two ISO standards, but coping with some of the challenges discussed and considering the labelling as a resulting process of security testing and assessment. The proposal also takes into account all the device lifecycle phases and deal with one of the major challenges associated to security testing, the dynamicity. This dynamicity can be due to a patch, an update, a change of the scale or domain or a new threat discovered. In this sense, when a change in the security conditions is detected in the monitoring activity, a recertification process is performed, involving security assessment and labelling processes. As the proposal also includes the automation of the whole process by means of technologies such as MBT, CertifyIT and TITAN to design, generate and execute the security tests, the recertification process is made in an easy way, only being needed to model the test (if necessary) and re-execute all the previous security tests to obtain the new risk value.

While the definition of a cybersecurity certification framework still needs coordinated efforts from stakeholder and regulatory bodies, the proposed approach is intended to serve as a cornerstone to define a more consistent and standardized approach.

References

1. **NIST.** *FIPS 200.* 2006.

2. —. *Special Publication 800-137.* 2011.

3. —. *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model.* s.l. : NIST Interagency Report 7756, 2012.

4. **Committee on National Security Systems.** *Glossary.* 2015.

5. **NIST.** *Glossary of Key Information Security Terms.*

6. —. *Performance Measurement Guide.* 2008.

7. **ETSI.** *Methods for testing & specification; risk-based security assessment and testing methodologies.* 2015.

8. **AIOTI.** *Report on Workshop on Security and Privacy in the Hyper-Connected World.* 2016.

9. —. *Report on Workshop on Security & Privacy in IoT.* 2017.

10. **ECSO.** *State of the Art Syllabus.* 2017.

11. **ENISA.** *Smart grid security certification in Europe. Challenges and recommendations.* 2014.

12. **European Commission.** *Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems.* 2016.

13. **Infineon, NXP, STMicroelectronics and ENISA.** *Common Position On Cybersecurity.* 2016.

14. **DIGITALEUROPE.** *Digitaleurope's views on cybersecurity certification and labelling schemes.* 2017.

15. **ENISA.** *On the security, privacy and usability of online seals. An overview.* 2013.

16. **ETSI.** *Methods for Testing and Specification (MTS). The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language.* 2015.

17. **BITAG.** *Internet of Things (IoT) Security and Privacy Recommendations.* 2016.

18. **ICSA.** *Internet of Things (IoT) Security Testing Framework.* 2016.

19. **IoT Security Fundation.** IoT Security Compliance Framework. 2016.

20. *Security of the internet of things: perspectives and challenges.* **Q. Jing, A.V. Vasilakos, J. Wan, J. Lu and D. Qiu.** 8, 2014, Wireless Networks, Vol. 20, pp. 2481–2501.

21. **European Commission.** *Proposal for a regulation of the council on ENISA. Cybersecurity Act.* 2017.

22. **ECSO WG 1.** Standardization certification labeling and supply chain management.

23. *Security Risk Assessment in Internet of Things Systems.* **Jason R.C. Nurse, Sadie Creese and David De Roure.** s.l. : IEEE C omputer Society, IT Pro, 2017.

24. *Security Challenges in the IP-based Internet of Things.* **T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keohy, S. S. Kumary, and K. Wehrle.** 2014, Springer Journal on Wireless Personal Communications.

25. **BOSCH .** *Political Viewpoint. Security in IoT.* 2017.

26. **FIRST.** Common vulnerabilities scoring system (CVSS). 2014.

27. *An Attack Graph-Based Probabilistic Security Metric.* **L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia.** London, UK : s.n., 2008. 22nd Annual Working Conference on Data and Applications Security.

28. **RASEN project.** *D3.2.3, Techniques for Compositional Test-Based Security Risk Assessment v.3.* 2015.

29. **CCRA.** Common criteria.

30. *A quantitative analysis of common criteria certification practice.* **S. P. Kaluvuri, M. Bezzi and Y. Roudier.** 2014. International Conference on Trust, Privacy and Security in Digital Business.

31. *Applying the common criteria in systems engineering.* **Sullivan, F. Keblawi and D.** 2006, IEEE Security Privacy.

32. **Microsoft.** DREAD scheme.

33. **MICROSOFT.** The STRIDE threat model.

34. **R. A. Caralli, J. F. Stevens, L. R. Young and W. R. Wilson.** *Introducing OCTAVE allegro: Improving the information security risk assessment process.* s.l. : CERT, 2007.

35. **MITRE.** Common weakness scoring system (CWSS). 2014.

36. *Risk-based adaptive security for smart iot in ehealth.* **Balasingham, H. Abie and I.** 2012. 7th International Conference on Body Area Networks.

37. *Assessing vulnerabilities in bluetooth low energy (BLE) wireless network based iot systems.* **Chan, Y. Qu and P.** 2016. IEEE International Conference on Intelligent Data and Security.

38. *Optimal security design in the internet of things.* **Sebestyén-Pál, H. Sándor and G.** 2017. Digital Forensic and Security (ISDFS), 5th International Symposium.

39. *A framework for automating security analysis of the internet of things.* **M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim.** 2017, Journal of Network and Computer Applications.

40. *Let the cat out of the bag: A holistic approach towards security analysis of the internet of things.* **V. Sachidananda, S. Siboni, A. Shabtai and Y. Elovici.** 2017. 3rd ACM International Workshop.

41. **M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu and A. Pretschne.** Security Testing: A Survey. s.l. : Elselvier, 2016, pp. 1-51.

42. *Improving Security Testing with Usage-Based Fuzz Testing.* **M. A. Schneider, S. Herbold, M. Wendland and J. Grabowski.** 2015, Risk Assessment and Risk-Driven Testing.

43. *A Survey on Model-Based Testing Tools for Test Case Generation.* **W. Li, F. Le Gall and N. Spaseski.** 2017. The 4th International Conference on Tools and Methods of Program Analysis.

44. *Online Model-Based Behavioral Fuzzing.* **M. Schneider, J. Grossmann, I. Schieferdecker and A. Pietschker.** 2013. IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops.

45. **Smart-Grid Task Force Stakeholder Forum.** *Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the smart metering systems.* 2016.

46. **K. Moore, R. Barnes, and H. Tschofenig.** Best current practices for securing internet of things (IoT) devices. 2016.

47. *Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks.* **Køien, M. Abomhara and G. M.** 2015, Journal of Cyber Security, Vol. 4, pp. 65–88.

48. *Security certification and labelling in internet of things.* **G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard and F. Le Gall.** 2016. IEEE 3rd World Forum on Internet of Things (WF-IoT).

49. *A subset of precise UML for model-based testing.* **F. Bouquet, C. Grandpierre, B. Legeard, F. Peureux, N. Vacelet, and M. Utting.** 2007. 3rd int. Workshop on Advances in Model Based Testing. pp. 95–104.

50. *MBT for global platform compliance testing: Experience report and lessons learned.* **G. Bernabeu, E. Jaffuel, B. Legeard, and F. Peureux.** 2014. 25th IEEE International Symposium on Software Reliability Engineering Workshops.

51. **Commercial product assurance (CPA).**

List of figures

List of tables

7. APPENDIX: Example of the proposal application

In this appendix, it is shown how to apply the certification methodology to one of the ARMOUR experiments (EXP1) and to one specific vulnerability: Lack of Confidentiality. We assume the *establishment of context* process, since it is not particular of a specific TOE.

The EXP1 is mainly motivated by the need to consider suitable mechanisms for security credential management and distribution, so IoT devices can interoperate securely during their operation. These aspects about key and credential management need to be built on top a secure approach for bootstrapping, since this represent the root of trust of an IoT device's lifecycle. Specifically, EXP1 is based on the use of CoAP and DTLS protocols, so IoT devices can request security credentials (group keys in this case), which are used later for a secure operation. Figure 16 provides an overview of the required interaction among the Device and the Attribute Authority (AA), which is responsible for generating and distributing such credentials.

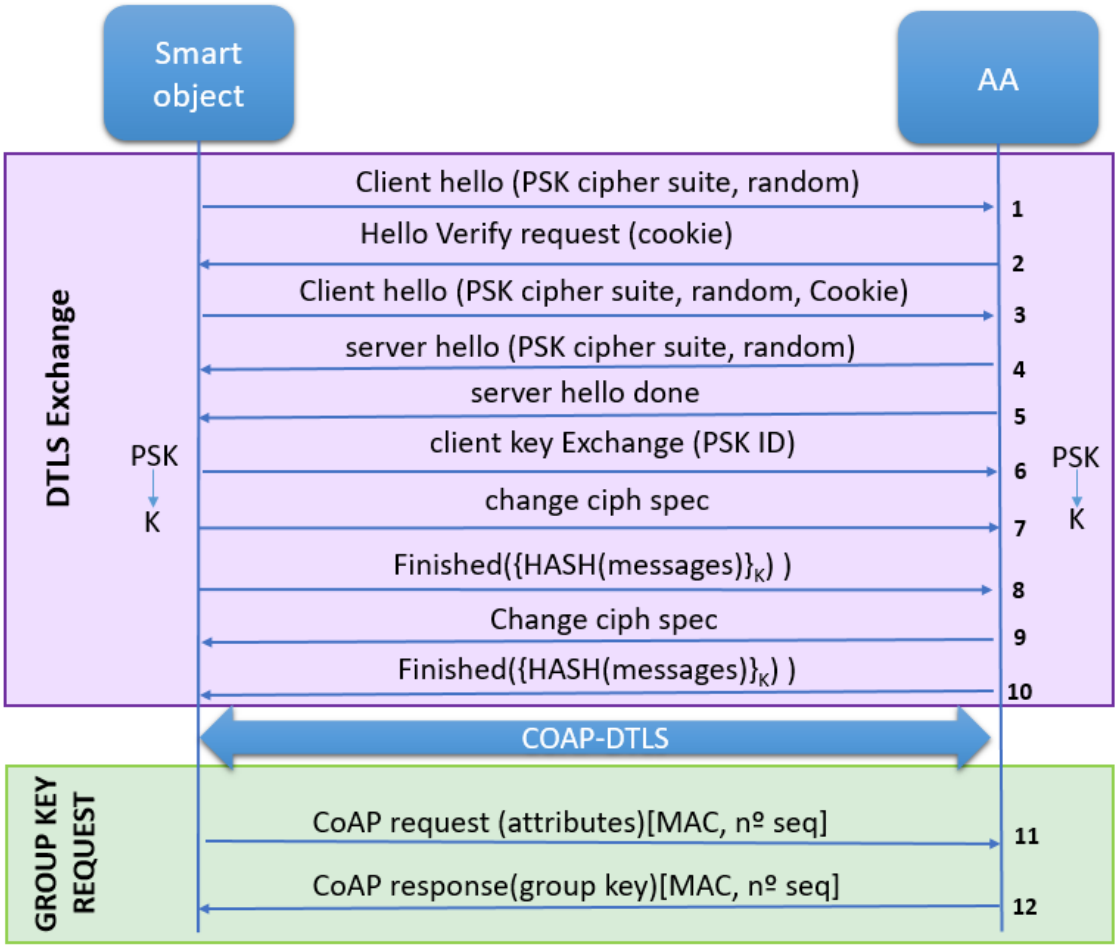

Figure 16 Experiment 1

7.2 Risk Identification

In this activity, we select which vulnerabilities we are going to tests. In this case, we have selected lack of confidentiality. It is applicable since the experiment uses ciphering and has exchanges sensitive data.

7.3 Test design and implementation

According to the proposed methodology, once the vulnerabilities are selected, in this case the *lack of confidentiality*, MBT is used to generate the model for the TOE and OCL to specify the TOE behaviour and to define the test purposes. This modelling approach includes the generation of a UML diagram class for the experiments. This way, Figure 17 shows the UML diagram generated from EXP1, Figure 18 shows the behaviour of the receiveResponse() in OCL from the smart object and Figure 19 the test purpose definition. Taking into account the set of entities defined in the diagram, the process can be described as follows:

1. The Sensor establish a secure communication channel through DTLS with the AA.
2. The Sensor makes a Request to the AA in order to obtain a Group_Key after being established a secure communication channel through DTLS.
3. The AA extracts the set of attributes of the Sensor that is included in the Request.
4. The AA generates a Group_Key associated to these attributes and sends it to the Sensor in a Response.
5. The Sniffer intercepts the messages exchanged between the Sensor and the AA in order to gather information about the Group_Key.

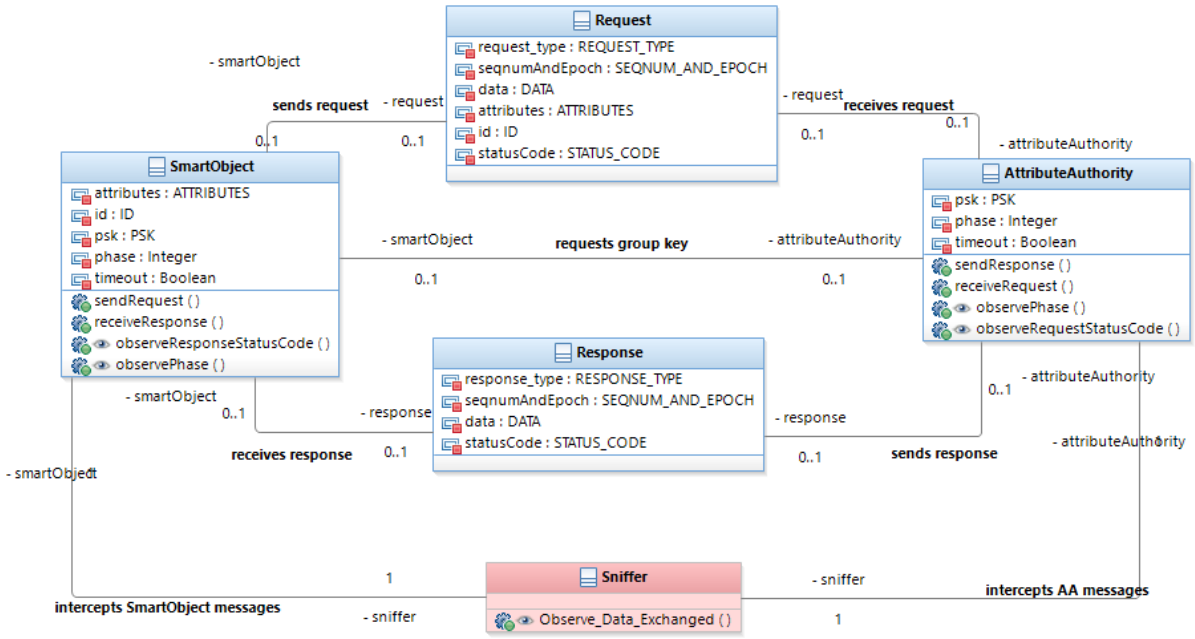

Figure 17 UML diagram for EXP1

```
---@REQ: SMART_OBJECT
if (self.response.seqnumAndEpoch=SEQNUM_AND_EPOCH::VALID_SEQNUM_AND_EPOCH) then
    if (phase=1 and self.response.response_type=RESPONSE_TYPE::HELLO_VERIFY_REQUEST and p_Response_type=RESPONSE_TYPE::HELLO_VERIFY_REQUEST) then
        phase=2
        ---@AIM: RECEIVED_HELLO_VERIFY
        ---@AIM: RECEIVE_TO_ANSWER
    else
        if (phase=3 and p_Response_type=RESPONSE_TYPE::SERVER_HELLO) then
            phase=4
            ---@AIM: RECEIVED_SERVER_HELLO
        else
            if (phase=4 and p_Response_type=RESPONSE_TYPE::SERVER_HELLO_DONE) then
                phase=5
                ---@AIM: RECEIVED_SERVER_HELLO_DONE
                ---@AIM: RECEIVE_TO_ANSWER
            else
                if (phase=6 and self.response.response_type=RESPONSE_TYPE::AP_UNKNOWN_PSK_ID and p_Response_type=RESPONSE_TYPE::AP_UNKNOWN_PSK_ID) then
                    self.observeResponseStatusCode(self.response.statusCode)
                    ---@AIM: RECEIVED_ERROR_ID
                    ---@AIM: END_HANDSHAKE
                else
                    if (phase=8 and self.response.response_type=RESPONSE_TYPE::DECRYPT_ERROR and p_Response_type=RESPONSE_TYPE::DECRYPT_ERROR) then
                        self.observeResponseStatusCode(self.response.statusCode)
                        ---@AIM: RECEIVED_DECRYPT_ERROR
                        ---@AIM: END_HANDSHAKE
                    else
```

Figure 18 Modeling the TOE behavior using OCL

```
Test Purpose definition
Tags  @AIM: SMART_OBJECT/RECEIVED_COAP_RESPONSE
use any_operation any_number_of_times to_activate behavior_with_tags {AIM: SMART_OBJECT/RECEIVED_COAP_RESPONSE}
```

Figure 19 Test purpose definition for lack of confidentiality

As the sniffer will be integrated in the execution platform, the test purpose consists only in performing the whole exchange in a normal way, until the smart object receives the last CoAP Response with the group key.

The test purpose will be exported to CerifyIT in order to generate all the intermediate steps, validating it (Figure 20). Finally, it will be published it in TTCN3 language (Figure 21).

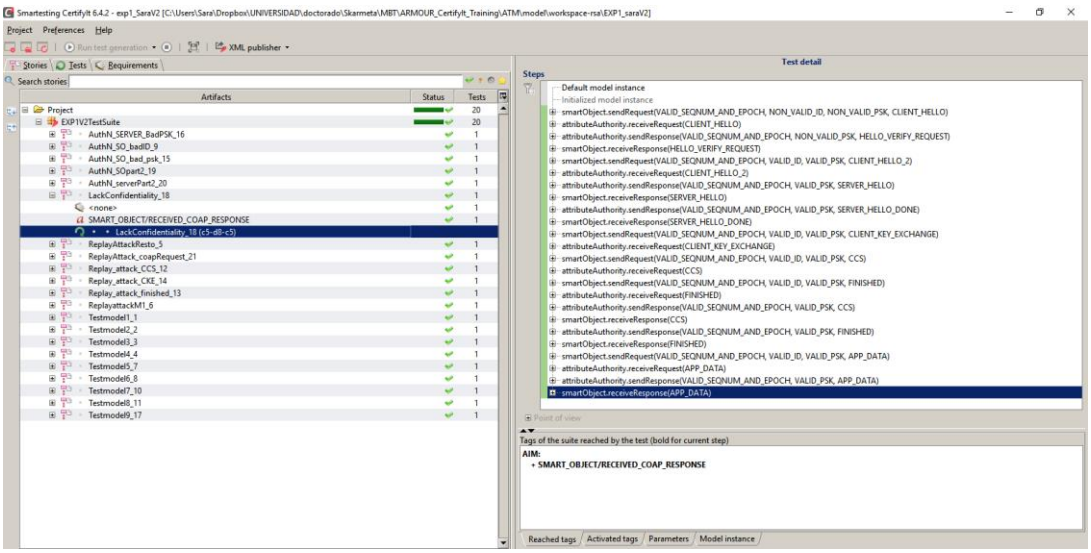

Figure 20 Test generation in CertifyIT for lack of confidentiality

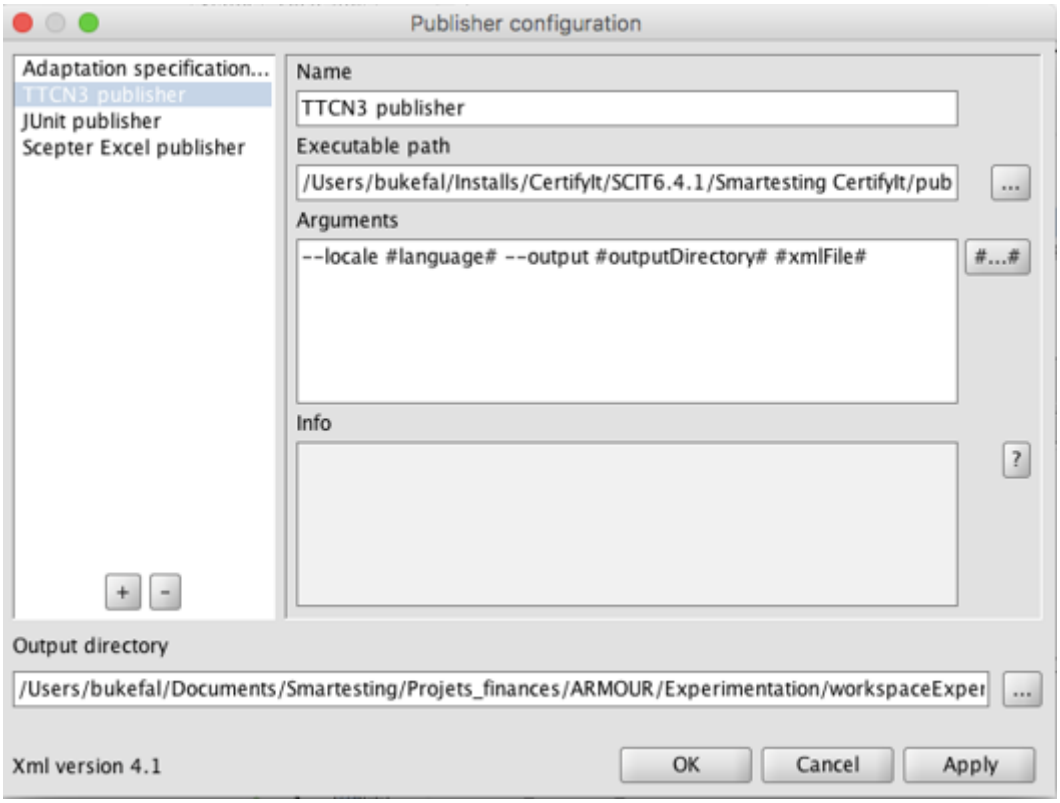

Figure 21 Test exportation in CertifyIT to TTCNv3 language

7.3 Test environment set up and maintenance

In this phase, the main work is to link the generated test case in TTCNv3 with the real implementation of the TOE. CertifyIT generates an interface (adapter) that must be implemented by the TOE in order to make possible this link (Experiment controller, EC, in the Figure 22). The EC is in charge to send certain commands through serial communication to the TOE leveraging on the lack of confidentiality test execution.

As we are testing Confidentiality, we also need a sniffer that is integrated inside the execution platform, that in this case is FIT IoT Lab.

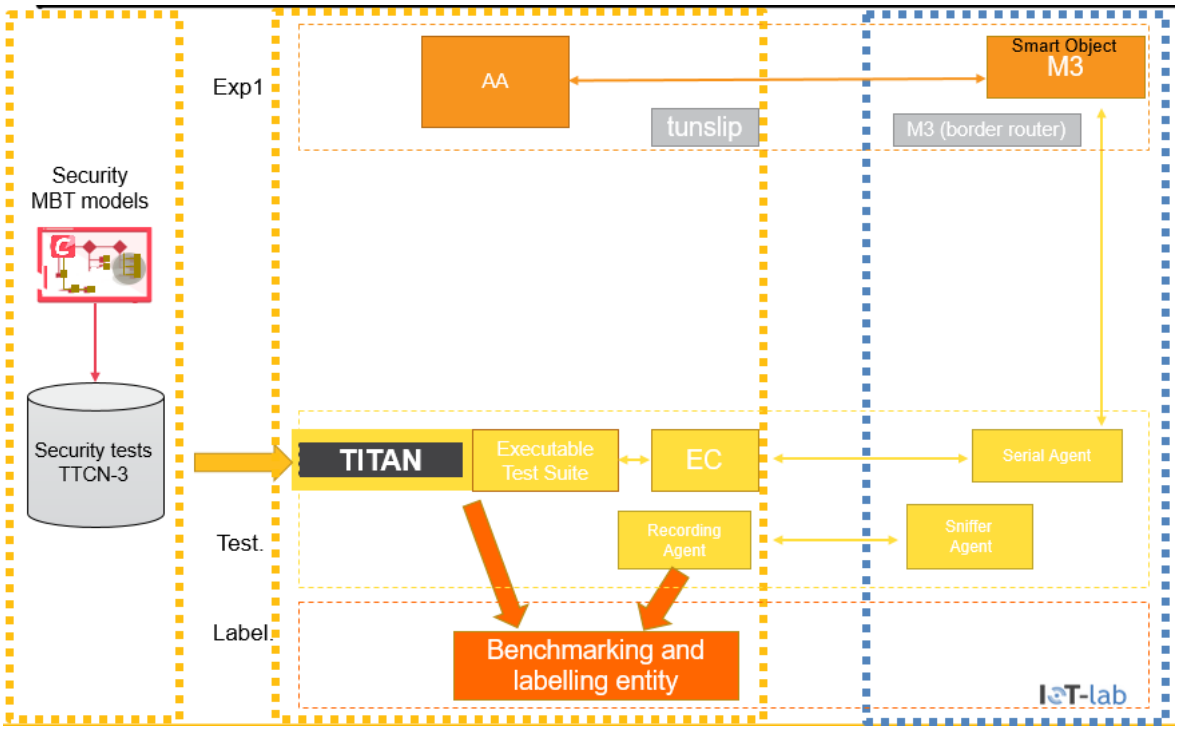

Figure 22 Overall process of security testing in ARMOUR

7.4 Test execution, analysis and summary

The experiment is executed in FiT IoT Lab. This platform allows us to execute the experiment at large scale, an interesting property useful to test denial of service attacks. For the lack of confidentiality, we only need one smart object and the AA. In addition, we use a border router, to connect the smart object that is inside FiT IoT Lab and the AA, which is in a remote server.

We obtain two main files from the test execution. The first one is the TITAN log, which helps us to know if the execution of the test has been performed correctly or not. The second one is the sniffer trace. This trace will be parsed in order to obtain valuable information to fill the CWSS metrics in a more refined and objective way.

In Figure 23, we have the Wireshark trace obtained from the execution of EXP1. We can see the general flow of DTLS exchange and some packets labelled with “Application data” that contain the finished DTLS message ciphered and the delivery of the group key, also encrypted. All the payloads of these packets of data are completely encrypted, as we can see in Figure 24. However, we can see the version of DTLS, which can be a source of information for a hacker if it is a weak version, a version with some bugs that can be exploited. We also can see epoch and sequence number, which can be exploited for a replay attack.

1	0.000000	aaaa::a682	aaaa::1	DTLSv1.	131	Client Hello
2	0.003441	aaaa::1	aaaa::a682	DTLSv1.	124	Hello Verify Request
3	0.252077	aaaa::a682	aaaa::1	DTLSv1.	163	Client Hello
4	0.260107	aaaa::1	aaaa::a682	DTLSv1.	184	Server Hello, Server Hello Done
5	0.667887	aaaa::a682	aaaa::1	DTLSv1.	104	Client Key Exchange
6	0.667906	aaaa::a682	aaaa::1	DTLSv1.	78	Change Cipher Spec
7	0.667913	aaaa::a682	aaaa::1	DTLSv1.	117	Hello Request
8	0.676223	aaaa::1	aaaa::a682	DTLSv1.	131	Change Cipher Spec, Hello Request
9	2.995869	aaaa::a682	aaaa::1	DTLSv1.	141	Application Data
10	2.999868	aaaa::1	aaaa::a682	DTLSv1.	100	Application Data
11	3.207658	aaaa::a682	aaaa::1	DTLSv1.	125	Application Data
12	3.212344	aaaa::1	aaaa::a682	DTLSv1.	119	Application Data
13	3.531732	aaaa::a682	aaaa::1	DTLSv1.	126	Application Data
14	3.536090	aaaa::1	aaaa::a682	DTLSv1.	119	Application Data
15	3.843856	aaaa::a682	aaaa::1	DTLSv1.	126	Application Data
16	3.849807	aaaa::1	aaaa::a682	DTLSv1.	119	Application Data
17	4.251749	aaaa::a682	aaaa::1	DTLSv1.	126	Application Data
18	4.256315	aaaa::1	aaaa::a682	DTLSv1.	119	Application Data
19	4.571839	aaaa::a682	aaaa::1	DTLSv1.	126	Application Data
20	4.575652	aaaa::1	aaaa::a682	DTLSv1.	119	Application Data

Figure 23 Wireshark capture of exp1. Device 1.

```
⊟ Datagram Transport Layer Security
  ⊟ DTLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 1
      Sequence Number: 1
      Length: 64
      Encrypted Application Data: 00010000000000016c6b5c6e1b5a9f07fc37b8934765f5ce...
```

Figure 24 Content of an application data message.

The rest of the packets of the DTLS communication are in clear. In Figure 25 we can see the session ID, the cookie and the random number, that could also be exploited in an elaborated replay attack. It is worth noting that we can also see what cipher suite and key length is going to be used. This is a good source of information for hackers, which can use it to decide if the key length is weak or if the cipher suite used has security bugs.

```
⊟ Datagram Transport Layer Security
  ⊟ DTLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 0
      Sequence Number: 1
      Length: 86
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 74
        Message Sequence: 1
        Fragment Offset: 0
        Fragment Length: 74
        Version: DTLS 1.2 (0xfefd)
        Random.gmt_unix_time: Jan  1, 1970 01:00:17.000000000 Hora estándar romance
        Random.bytes
        Session ID Length: 0
        Cookie Length: 32
        Cookie (32 bytes)
        Cipher Suites Length: 2
      ⊟ Cipher Suites (1 suite)
          Cipher Suite: TLS_PSK_WITH_AES_128_CCM_8 (0xc0a8)
```

Figure 25 Client Hello message content.

By means of a script, we parse the trace to obtain the following values, that will be used in the *risk assessment* process:

- percentage of non ciphered data = 90%
- key length = 128 bytes
- cryptographic suite used = AES
- TITAN test status = PASS

7.5 Risk Estimation

The test report is going to be included in the CWSS following the Figure 26. The CWSS metrics we are going to set up with the testing are two. One the one hand, the *Technical Impact*, related with the percentage of non ciphered data, since this value represents the potential result that can be produced by the weakness. On the other hand, *the External control*, related with the cryptographic suite and the key length used to cipher as well as the NIST recommendations (Figure 27). As the key length and cipher suite are recommended by the NIST, the CWSS value for this metric is *Best available*, that in numeric terms corresponds to 0.3 (35).

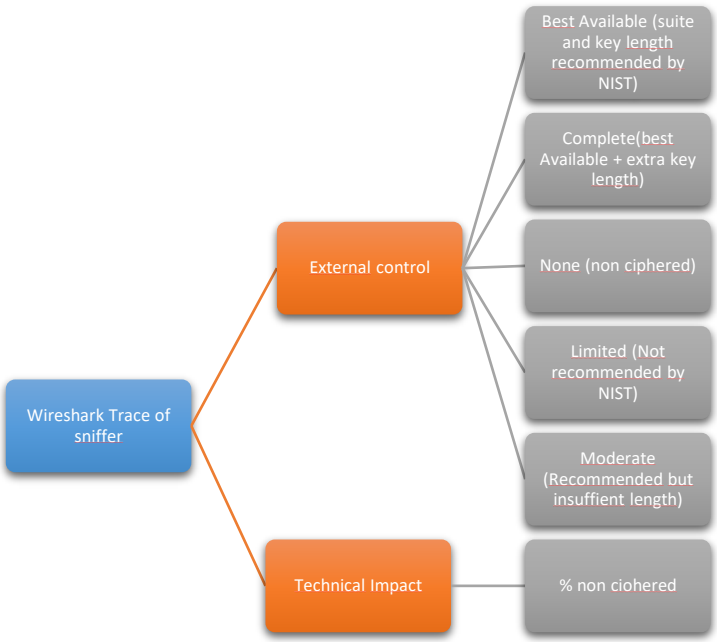

Figure 26 Integration of security testing in risk assessment for Lack of Confidentiality.

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

Figure 27 NIST key length recommendations

A resume of the CWSS metrics used for the risk estimation activity are shown in Tables 6, 7 and 8. Remember that some of the metrics are set up by default such as the Internal control effectiveness, the finding confidence or the Business impact.

Table 6 Risk estimation for Lack of Confidentiality. Base Metric.

Base Metric	Value
Technical Impact (TI)	Test return value
Acquired Privilege (AP)	None:0
Acquired Privilege Layer (AL)	Quantified:0
Internal Control Effectiveness (IC)	NA: 1
Finding Confidence (FC)	NA: 1

Table 7 Risk estimation for Lack of Confidentiality. Environmental Metric.

Environmental Metric	Value
Business Impact (BI)	NA : 1
Likelihood of Discovery (DI)	High:1
Likelihood of Exploit (EX)	High:1
External Control Effectiveness (EC)	Test return value
Prevalence (P)	Widespread:1

Table 8 Risk estimation for Lack of Confidentiality. Attack Surface Metric.

Attack Surface Metric	Value
Required Privilege (RP)	None:1
Required Privilege Layer (RL)	Network:0.7
Access Vector (AV)	Internet: 1
Authentication Strength (AS)	None: 1
Level of Interaction (IN)	Automated:1
Deployment Scope (SC)	All: 1

By sniffing the data, the attacker cannot acquire any privilege, so the values related to this (*acquired privilege* and *acquired privilege layer)* are none and quantified set to zero. For the attack surface metrics, we set the *required privilege* to none, since the attacker does not need any privileges to sniff, only access to the Internet, so the *required privilege layer* is network and the *access vector*, Internet. The attacker does not require authentication and user interaction, so *authentication strength* is set to none and *level of interaction* is set to automated. This vulnerability is present in all the devices of the experiment, so the *deployment scope* is all.

Finally, in environmental metrics, the *likelihood of discovery and exploit* is high, since it is easy to use this vulnerability without knowledge, and the *prevalence* is high, taking into account that this type of attack is frequently performed to discover sensitive data or ways to exploit another vulnerability.

We obtain the mark for this vulnerability applying the CWSS formula:

$$BF_s = [(10 \cdot 0.94 + 5 \cdot (0 + 0) + 5 \cdot 1] \cdot 4 = 56$$

$$AS_s = \frac{[20 \cdot (1 + 0.7 + 1) + 20 \cdot 1 + 15 \cdot 1 + 5 \cdot 1]}{100} = 0.94$$

$$E_s = \frac{[(10 + 3 \cdot 1 + 4 \cdot 1 + 3 \cdot 1) \cdot 0.3]}{20} = 0.3$$

$$S_v = BF_s \cdot AS_s \cdot E_s = 15.792$$

7.6 Risk Evaluation

The next activity, *Risk Evaluation*, performs the mapping between the CWSS risk and the intervals. We calculate the maximum and minimum value, dividing the possible medium values in four equal ranges of risk. The maximum value is calculated with Technical impact equal to one and External control equal to one, whereas the minimum is the same but with zero values. Taking into account this, the intervals are shown in Table 9 and the obtained risk in lack of confidentiality is Medium.

Table 9 Risk intervals for Lack of Confidentiality

Interval	CWSS Risk
Low	[0-14.1)
Medium	[14.1-28.2)
High	[28.2-42.3)
Critical	[42.3-56.4]

Finally, we compare the results with the profiles available in the domain. Table 10 shows this comparison. The CWSS risk obtained by Experiment 1 is Medium, so it fulfils profiles B, C and D. As we always choose the highest one, the profile obtained in *Lack of Confidentiality* is B.

Table 10 Risk evaluation for Lack of Confidentiality

		CWSS	Profiles				
Vulnerability	**Risk**	**EXP1**	**A**	**B**	**C**	**D**	**Profile fulfilled**
Lack of Confidentiality	Low		X	X	X	X	B
	Medium	X		X	X	X	
	High				X	X	
	Critical					X	

7.7 Labelling

Following the recommendations for the label, Figure 28 shows the resulting label for the whole experiment 1. As we can see, the B profile obtained in Lack of Confidentiality is reflected as a point of the spider chart, colored in yellow. The QR is intended to be linked with extra information related with the different profiles, the test report, the validity of the label and so on.

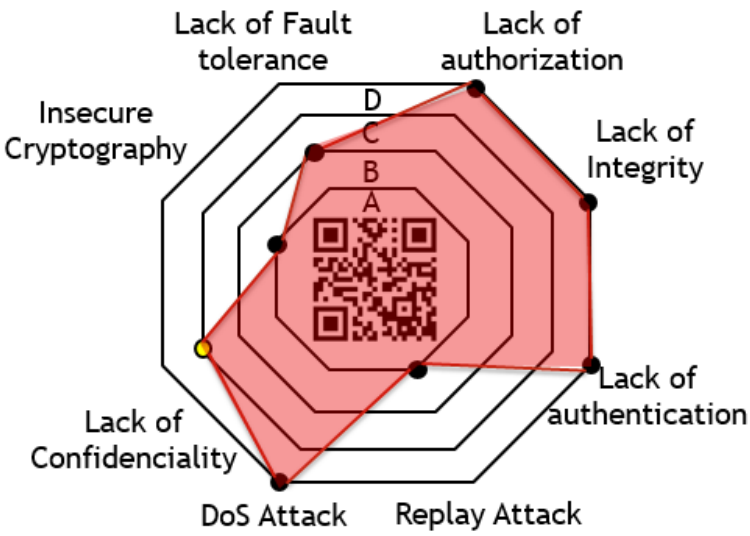

Figure 28 Labelling for Experiment 1.

Finally, in Figure 29, there is a demo showing at the right side the TITAN log with the test status (PASS), at the left side the Wireshark trace of the sniffer and in the middle, the labelling demo with the gathered values from the testing and the CWSS risk estimation.

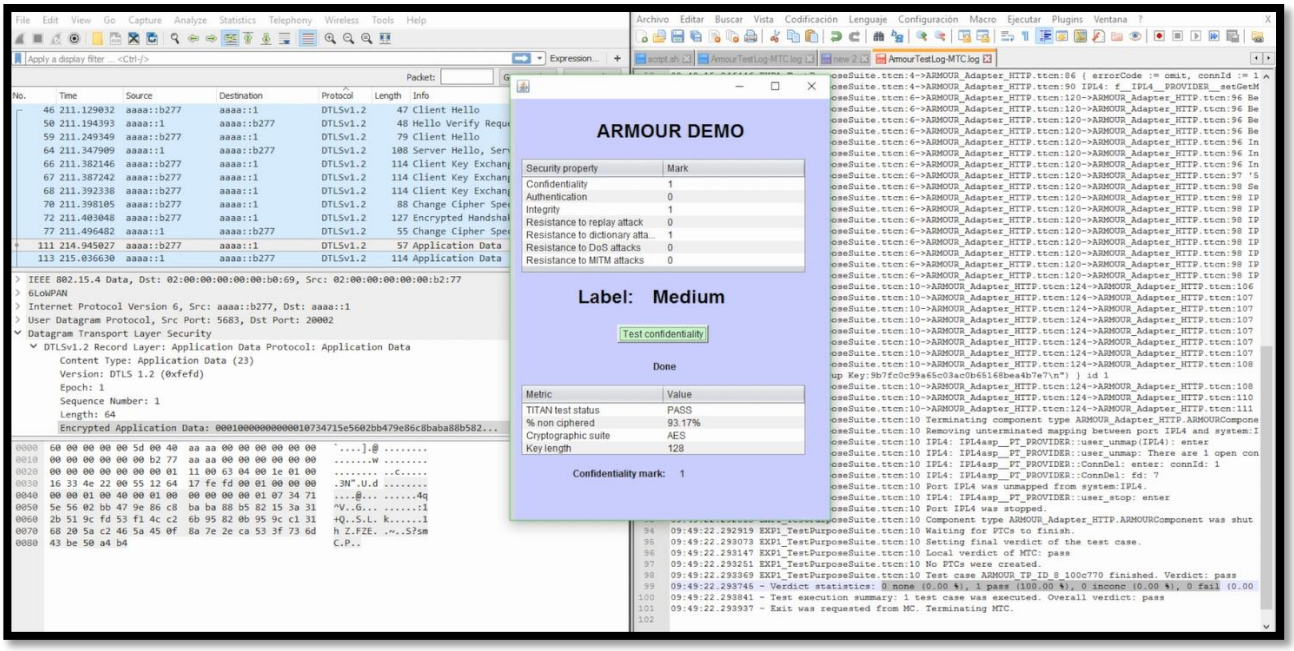

Figure 29 Demo Labelling for Experiment 1.