# Security certification and labelling in Internet of Things

Gianmarco Baldini, *Member, IEEE,* Antonio Skarmeta, Elizabeta Fourneret, Ricardo Neisse, Bruno Legeard, and Franck Le Gall

***Abstract*—In recent years, security and privacy aspects of IoT have received considerable attention from the industry and research communities. Because IoT will be more pervasive in the everyday life of the citizens, and it may be used in safety related applications (e.g., road transportation), its security threats may be more damaging than conventional Internet threats. Due to processing and memory constraints, the provision of security functions could be quite challenging in IoT. In addition, IoT devices must operate in a dynamic environment in terms of communication interfaces and fast upgrade cycle (e.g., patching), which imposes severe security requirements to designer and developers. Privacy aspects are also relevant because of the large amount of data collected by IoT sensors. In this context, the security certification of IoT devices is an important element to support the development and deployment of trusted IoT systems and applications. The objective of this paper is to investigate IoT security certification taking into consideration the current security certification frameworks, standards, and their related limitations identified by the industry and research communities. This paper proposes a new approach for security certification in IoT, which addresses the identified limitations and links formal models to testing and certification.**

***Index Terms*—security, certification, model based testing, Internet of Things.**

## I. Introduction

The Internet of Things (IoT) introduces a tighter connection between the cyberspace and the physical world as sensors and actuators are connected through various types of communication networks (e.g., WiFi, Cellular networks). The deployment of IoT devices in large scale applications and ICT infrastructures will grow considerably in time and it can radically change the way citizens interact with this technology. Many new applications in smart living or smart transportation are already transforming the way businesses operate. In this evolution, it is important to have guiding principles to foster the development of good IoT technology, which can be trusted and performs according to the user expectations. Cerf and Senges identify in [1] the following three maxims to guide good IoT designs: *a*) *re-imagine* ordinary objects with the power of the Internet,*b*) *foster* sets of objects and services, and *c*) *match* relevant objects and services for genuine user benefit. The authors also indicate the main challenges for the deployment of IoT, as the fragmentation of standards and the heterogeneity of technologies and applications can hamper the application of these maxims.

Gianmarco Baldini and Ricardo Neisse are with the European Commission - Joint Research Centre, Ispra, Italy

Antonio Skarmeta is with University of Murcia, Murcia, Spain

Bruno Legeard and Elizabeta Fourneret are with Smartesting Solutions & Services, Besancon, France

Franck Le Gall is with Easy Global Marker, Sophia Antipolis, France

Indeed, the intrinsic characteristics of inferring high dimensional data in IoT applications are sure to pose problems and challenges both in terms of spatial and temporal distribution. They will also impose additional requirements on safety, reliability, security, energy-efficiency, performance, robustness and cost-efficiency. This means that all mechanisms and features for the IoT need to be especially designed, duly tested and certified for large-scale deployments.

Security and Privacy aspects play an important role in the development of IoT for various reasons. IoT sensors will be able to collect data about users and their environments in almost real time and transmit it to other devices or the cloud. Regarding privacy, the ubiquity of IoT devices including smartphones, fixed/mobile cameras, smart cars or sensors in smart homes may provide continuous tracking and surveillance of users' activities, unless data collection and reporting is regulated in some way. Security will also play an important role in IoT as actuators will be used in many safety related applications like road transportation of remote healthcare.

Researchers and industry have investigated the application of existing security/privacy enforcement techniques and solutions to IoT but many open challenges still remain [2]. In our view, two challenges have a higher priority for a trusted deployment of IoT. The first is the *uncertainty and dynamic environment of IoT*. Uncertainty is intrinsic in IoT Systems due to novel interactions of embedded systems, networking equipment, smart sensors, cloud infrastructures, and humans. With respect to Security and Trust aspects, this uncertainty is a major potential cause of security breaches. While monitoring or misbehavior detection systems can be used to identify potential security breaches, a testing and certification phase with adequate coverage and linked to the main known security vulnerabilities can mitigate this uncertainty. The second challenge is the *scale and heterogeneity of future IoT systems* with different security standards [3], which may also change their configurations in time. This is pushing the technology limits for interoperability, security verification, and testing at a level that is not currently mastered by current techniques and tools. The matter in hand is the security assessment of such large, complex and heterogeneous IoT systems in their entirety.

In other words, it is important to address the security and privacy aspects of IoT from a testing and certification point of view. The question is '*can we apply security certification processes and frameworks to IoT?*' or new processes and standards must be put in place? As described in the subsequent sections of this paper, security certification has a long history which started in the defense domain, where the economic

context and operational requirements are radically different from the modern IoT applications. Nevertheless, there are examples where security certification has been successfully applied to small and constrained Information and Communication Technology (ICT) devices like smart cards [4].

This paper briefly describes the history of security certification in section II, the limitations identified by the industry and research community in section III, and how these limitations can impact an IoT security certification process. In section IV the key elements of a new security certification process especially suited for the features of IoT are described. These key elements are based on the evolution of existing security certification standards and include the use of formal modeling, automated test suites, deployment guidelines and the concept of labelling certified IoT products to support a transparent disclosure of the IoT product certification status. The concept of labelling is introduced and its use for the development and deployment of large-scale IoT applications is described. Finally, section V concludes this paper and discusses future developments.

## II. History of Security Certification

Security certification has been defined in various ways in literature. In this paper, we adopt the security certification definition from as NIST SP 800-37 [5] where it is defined as "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". Security certification is needed to ensure that a product satisfies its security requirements, which can be both proprietary (i.e., defined by a company for their specific products) and market requirements (i.e., defined in procurement specifications or market standards). In the latter case, these requirements are also defined to support security interoperability. For example, to ensure that two products are able to mutually authentication or to exchange secure messages.

As described in [6], the initial efforts to define a security testing and certification framework for products originated in the defense domain. An obvious reason was that the military systems are designed to operate in a hostile environment and must be protected against security threats, which are more likely to appear than in a commercial domain. In addition, there was the need to design a system able to support different access levels for classified and non-classified information, and support interoperability. Through various phases, described in detail in [7], which will not be repeated here, these initial needs produced the Orange book, which provided criteria for classifying system security into a series of levels of products evaluation (C1,C2,B1,B2,B3 and A1) depending on how carefully engineered were the mechanisms for assuring the confidentiality of classified information. The Orange book was published in August 1983 and it became a requirement for ICT systems processing classified information at more than one level. While this was a valuable and needed process to support trust in government systems dealing with secure and sensitive information, the certification process was lengthy and costly [6]. In fact, it could last 2-3 years, which was acceptable for the defense domain where a project or a product (e.g., a secure ICT system) could last for years and cost millions of dollars, but could be an issue for market distribution of a commercial product. The certification process also introduced a delay and certified products lagged behind the commercial state of art. In addition, the evaluation had to be performed by the National Computer Security Center, a division of the NSA, a government agency.

A similar system was set up in Europe called the Information Technology Security Evaluation Criteria (ITSEC), which eventually evolved to the Common Criteria also known as ISO 15408 [8]. In comparison to the Orange book, which was focused on protecting classified information, the Common Criteria is wider and permits systems and devices to be evaluated against a specific protection profile. In a similar way to the Orange book, Common Criteria also defines different levels of evaluation called Evaluation Assurance Levels (EAL) from 1 to 7. A significant difference from the Orange book is related to the certification laboratories. The Orange book process involved a government agency for certification, while in the Common Criteria process, products can be evaluated by competent and independent licensed laboratories to determine the fulfillment of particular security properties (e.g., protection profiles) or a certain assurance level. The Common Criteria is now a well adopted standard (ISO/IEC 15408) in the world for security certification and numerous protection profiles are already defined in many domains. An extensive description of Common Criteria would not fit in this paper and the reader can refer to [9]. Here we limit to identify the key concepts of Common Criteria, because these concepts will be used in the rest of this paper:

1) A Target of Evaluation (TOE) is defined as a set of software, firmware andor hardware possibly accompanied by guidance. The TOE may be an Information Technology (IT) product, a part or a set of IT products or a combination of these.
2) A Protection Profile (PP) expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures to fulfill those objectives.
3) A Security Target (ST) expresses security objectives of a specific ICT product and defines the functional requirements and assurance measures to fulfill those stated objectives. It also defines an implementation of the security requirements.
4) An Evaluation Assurance Levels (EAL) are formed from a taxonomy of assurance classes, families, and components. There are seven hierarchically ordered EALs increasing in assurance that serve to provide general-purpose assurance packages

Even if Common Criteria are currently the main security certification standard and it is well developed (now in version 3.1 revision 4), the research and industry community has identified a number of limitations, which will be described in the following section.

## III. Limitation and challenges of current security certification schemes in IoT

In this section, we identify the main limitations pointed out in literature for Common Criteria. Note that we do not endorse them but we refer them to describe (in the subsequent sections of this paper) how our proposed framework can mitigate these limitations or address them.

One of the main critics to Common Criteria is the length and effort requested to execute a Common Criteria evaluation especially for the high EAL. One of the first papers to highlight this issue was [10], who remarked that the costs for protection profile and security target formulation are significant. While this cost is absorbed by the government for military related projects, in the commercial world, this cost must be absorbed by the vendors. 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). The authors in [11] also discussed the complexity of the process and the high cost of Common Criteria (CC) security certification. Vendors have to spend a large effort on preparation for the evaluation, which adds to the cost and time of the evaluation itself. High assurance level (as EAL4) certification can take even 2 years, which can slow down considerably the placement of the product on the market [11]). In the IoT world, this would be even less acceptable because the fast placement in the market is an important element of business success for IoT manufacturers and service providers.

In addition [10] pointed out that there may be conflicting views between the protection profile specifications and stakeholders view on how the product is placed in the system. In other words, there may be a risk of misinterpretation because the protection profile definitions are difficult to link to the user requirements. This risk was also highlighted by [6] where it pointed out that CC are not well matched to the needs of the control systems world because a security certification scheme must be able to cope with dynamic systems, dynamic threats and real users working in real organisations. The integration with existing systems is an important aspect because it must complement, rather than conflict with, existing safety certification mechanisms or security frameworks already implemented or deployed in the system. But above all, its function is to provide assurance to asset owners that the systems and components they buy from the vendor community are fit for purpose. This aspect was also pointed out in [12] , where commonly used protection profiles often do not correspond to the functionality requirements of users.

The integration of security certified products in existing system is not only a matter of perception of the users or integration in existing systems, but it also points out to the so called composition problem [10]. The issue is if the level of security assurance certified with common criteria can be composed for different products to be integrated in a larger systems. In [10], it is pointed out that requirements traceability from systems security requirements to PP and to TOE of the single products may not be one-to-one or straightforward especially for systems, which can consist of multiple products that might or might not be evaluated. The risk of the lack of traceability between the users needs and the results of the CC certification was also discussed in [6]. The link between CC product certification and system security was also analyzed in [13], which poses the question on how users can be sure that an CC evaluated product improved his or her IT system security? The problem is that few, if any, metrics exist to support this question, and without them, it is impossible to assess the cost-benefit ratio for performing an evaluation. There is a need for a system-level approach to security, and the metrics to support such an approach, otherwise the authors in [13] conclude that these views lack a solid foundation.

Another issue raised by the industry and research community is the management of changes in the CC certified product. As described in [11], CC certificates a particular version of the product in certain configurations. Any changes to the configuration or any updates to the product that affect the TOE, which is the part of the product that is evaluated, may invalidate the certification. This is not a desirable situation, given that products evolve and may be updated at a very high pace and the certification must not be frozen to a specific version of the product. The need to address dynamic changes is especially true for IoT products where patching or changes in configuration are often needed to mitigate security threats. The authors in [14] pointed out that this risk is exacerbated in CC security certification because CC assurance requirements tend to be inspired by the traditional waterfall software development methodology, while most of the modern software is produced using modern agile paradigms. The risk that CC may fail to deal satisfactorily with systems that are patched frequently was also raised by [6].

The comparability of CC security certifications has been another issue raised by the research and industry community, even if it is has been mitigated by recent initiatives as described in subsequent paragraphs. As described in [11], though the CC scheme is a widely recognized international standard, there are several concerns regarding the consistency of the assessments by the evaluating laboratories located in different countries. Organizations and initiatives like CC Recognition Arrangement (CCRA) and SOG-IS are indeed one of the most appropriate solutions to mitigate this risk but they do not prescribe monitoring and auditing capability (at the publication time of [11]). The risk of competing security national certification schemes was also highlighted by [15] and [13]. The challenge to draft comparable CC evaluations goes beyond national or local differences, but it is also an issue for creating harmonized security certifications across a wide range of technologies [15]. Lack of comparability is also due to the difficulty in understanding the CC technical documents for the certification of a product, which make more difficult an objective comparison. One of the main objectives of CC is to allow consumers to compare certified products on the market in an objective way from a security point of view. However, certification documents are filled with legalese and technical jargon. Hence, comparison is not straightforward nor easy [11].

## IV. Proposed certification process

### A. Key Elements

The proposed certification process has been defined by the authors of this paper in the context of the Horizon 2020 ARMOUR project, which started in February 2016. The ARMOUR project aims to provide duly tested, bench-marked and certified security and trust technological solutions for IoT and especially for large scale IoT deployments. Suitable duly tested solutions are needed to cope with security, privacy and safety in the large scale IoT deployments, because uncertainty is intrinsic in IoT Systems due to novel interactions of embedded systems, networking equipment, smart sensors, cloud infrastructures, and humans. While, various security solutions have been proposed by the research and industry community, testing is an important element to support the secure and trusted deployment of IoT systems.

The overall flow of the security testing and certification process proposed by ARMOUR is depicted in Fig. 1.

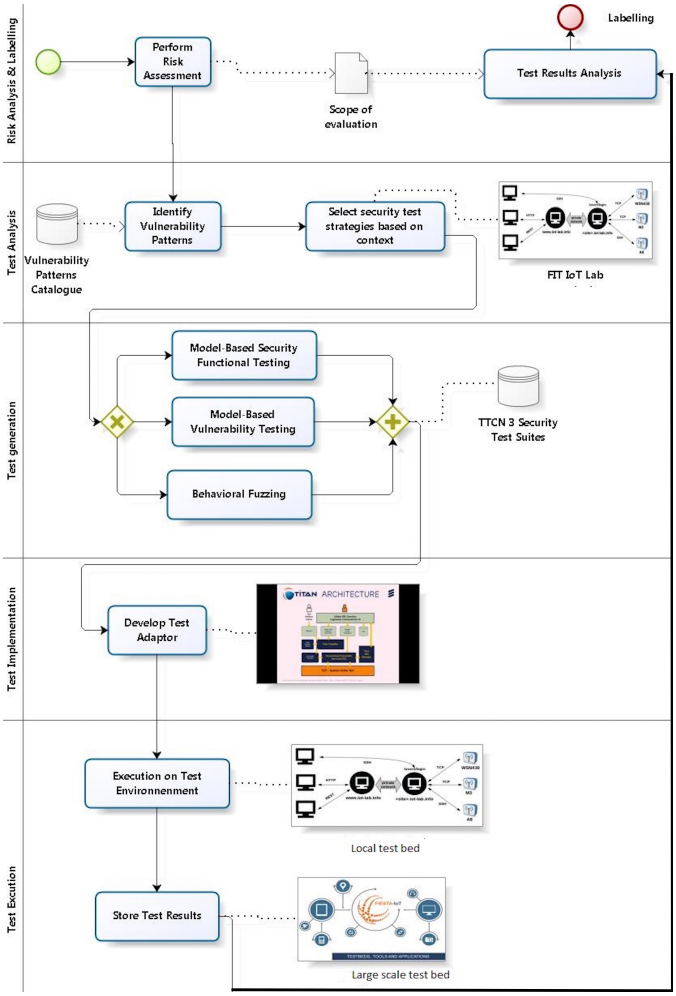


Fig. 1. Overall ARMOUR security certification process

The process is composed by the following main phases:

1) A risk analysis is performed for a specific domain or set of applications where the IoT device must operate with a specific level of assurance. This is a similar way to the Evaluation Assurance Levels of Common Criteria) and it can be thus consequently associated to a label.
2) The knowledge of the identified potential threats and vulnerabilities is gathered in a form of *vulnerability patterns*, which must be addressed and evaluated in the subsequent testing phases. Note that the threats and vulnerabilities are specific for a context (i.e., single domain or set of applications) and they are used as input to an appropriate model-based security test strategy.
3) The security test strategies generate test suites based on models. The models formalize the system's behavior, its structure and the *security test patterns* that define the test procedure of the vulnerability patterns.The aim of this phase is to create a complete set of test suites in TTCN3 using models, specific for the IoT system and the domain.
4) The execution of the test suites defined in the previous phase in a specific operating environment is ensured through test adaptors. This phase is needed because each IoT device or system will have its own specific interfaces and behavior and test suites require wrappers to support the execution of the tests.
5) The tests are executed on a local or external large-scale testbed. The ARMOUR project will use both a local test bed and a large-scale test bed at FIT IoT Lab, having more than 2000 nodes. The results of the test execution are gathered into FIESTA semantic testbed and are used as a proof to validate the security certification label, which was defined in phase one.

*Phase 3* is the core component of the security certification process and it is based on a Model-Based Testing (MBT) approach, which has shown its benefits and usefulness for systematic compliance testing of systems that undergo specific standards that define the functional and security requirements of the system [16].

The proposed approach for labelling and certification is based on two main modules:

1) the MBT CertifyIt technology generating tests based on the Test Purpose formalism (hereafter denoted as TP) and fuzzing algorithms;
2) the TTCN3 test cases, generated from the MBT model, that are executed using TITAN;

The dedicated language called Test Purpose Language used to guide the test case generation [17]. It is used to express functional security requirements and security test patterns. The TP language is based on regular expressions and allows the test engineer to conceive its scenarios in terms of states to be reached and operations to be called. The language relies on combining keywords, to produce expressions that are both powerful and easy to read by a test engineer. The syntax of the language makes it possible to design test purposes as a sequence of quantifiers or blocks, each block being composed of a set of operations (possibly iterated at least once, or many times) and aiming at reaching a given target (a specific state, the activation of a given operation, etc.). On the other hand the Testing and Test Control Notation (TTCN) v.3 language has been widely used for many years (in the previous versions) to

test large communication systems [18]. In our context TTCN-3 test cases are generated from the MBT model. They contain modules that make possible the execution, as they contain the type, port and component declarations and definitions, templates, functions, test cases and control part for executing the test cases. The control part can be seen as the main function in other programming languages as C or Java. [19].

The advantages of combining MBT and TTCN are the following:

1) The automation of the test supports a faster and more uniform testing.
2) The adoption of MBT supports a formal definition of the tests and the security requirements, which drives the certification. In addition, they can be used to support harmonization of the tests for security certification.

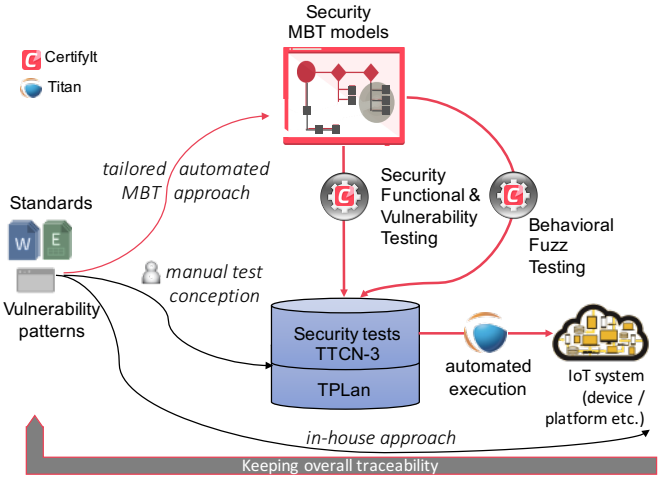


Fig. 2. Model Based Security Testing

The detail of the application of MBT to IoT testing is provided in Fig. 2. The structure of the system is modeled by Unified Modelling Language (UML) class diagrams, while the system's behavior is expressed in Object Constraint Language (OCL), using the CertifyIt tool [20]. Functional tests are obtained by applying a structural coverage of the OCL code describing the operations of the IoT system under test. This approach in the context of security testing is complemented by dynamic test selection criteria called Test Purposes (TP) that make it possible to generate additional tests that would not be produced by a structural test selection criterion, for instance misuse of the system (Model-Based Security Functional Testing) and vulnerability tests, trying to bypass existing security mechanisms (Model-Based Vulnerability Testing).

To address the uncertainties described in the introduction the application of fuzzing methods are proposed (Behavioral Fuzz Testing). The testing tool relies on the principle to rapidly generate as higher as possible number of fuzzed tests with high number of steps in a given period of time using a weighted random algorithm. The generated tests are valid with respect to the constraints in the MBT model. Thus, contrary to most fuzzers, the produced test cases on the one hand are syntactically correct with respect to the system's inputs. On the other hand, as it uses a weighted random algorithm and measures the coverage of the behaviors, it avoids duplication of the generated tests, which makes the test evaluation and assessment easier[21].

### B. Labeling

A labelling scheme can be created to give a straightforward indication on the level of certified security of a product. The label can be associated to the following dimensions (see a pictorial description in Fig. 3:

1) Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that the successful certification to a specific EAL level does not measure the security of the system itself, it simply states at what level the system was tested.
2) Protection profile for a specific domain (energy, road transportation and so on). Each protection profile can be associated to a specific level of assurance (dimension 1). Each domain has its own specific features and configuration environment, which must take in consideration for the security certification and deployment. For example, the security certification of a crypto-module for the road transportation may not be valid for the energy sector. This is why, the label must have a separate dimension to identify the domain.
3) A label to define how the certification was achieved: self-certification, third-party compliance assessment and so on.

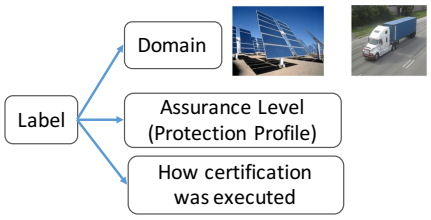


Fig. 3. Dimensions of the certification label

### C. Benchmarking

In order to provide a label it is important to be able to correlate the security testing over the different system elements and aggregated properties associated to the levels. One of the main objectives of the ARMOUR project is to define an approach for Benchmarking Security and Trust technologies for large-scale IoT in order to provide the connection between testing and labelling processing. ARMOUR will establish a security benchmark for end-to-end security by building up on the testing framework defined previously. In order to do this an identification of metrics per functional block should be provided (authentication, data security etc) to perform various micro- and macro-benchmarking scenarios on the target deployments. Micro-benchmarks provide statistics for a specific function of an application and help to understand the performance of subsystems associated with a smart object, and are useful to identify possible performance bottlenecks at architecture level, allowing embedded hardware and software engineers to compare and asses the various design trade-offs with respect to the component level design.

The following dimensions and metrics will be considered:

- security attacks detection,

- defence against attacks and misbehaviour,
- ability to use trusted sources and channels,
- levels of security & trust conformity, etc.

Benchmark results will be collected from the TTCN-3 test suite execution and datasets will be made available via the FIESTA testbed. Once the metrics from the evaluation are collected, they will be used to categorized them (taxonomy) in different functional aspects and based on this provide a label approach to the security assessment of the IoT on certification. Additional benchmarks of reference secure and trusted IoT solutions will be performed in order to establish a baseline ground-proof for ARMOUR experiments but also to start to create at proper benchmarking database of secure and trusted solutions proper for the large-scale Internet-of-Things. The final objective it is to provide to the security benchmarking an assurance that should include a measure of our level of confidence on IoT security properties.

| Challenge | Mitigation approach by the proposed framework |
|---|---|
| Lack of comparability of security certification | the proposed framework defines models, which have the same format across the different security certifications. In addition, the models describe in a unambigous way the security threats and associated test cases. |
| Incremental changes | the framework can easily generate (in MBT and TTCN) test suites which address the incremental changes, so that the test and security certification is only targeted for those changes. |
| Missing links between user requirements and protection profile | The MBT models can create an association between the user requirements and the test suite to execute on the IoT product. |
| Long security certification process | The proposed testing framework support the automation of the test using the TTCN language, does making the security certification process much faster than with conventional means. |
| Potential lack of testing coverage | The test framework produces an high number of fuzzed tests with high number of steps using a weighted random algorithm to widen the test coverage |
| System-level approach to security | A procedure is defined to go from risk analysis, vulnerability patterns, test generation and evaluation and KPI collection |
| Metric for security and privacy | The proposed framework will define several metrics either for Micro-benchmarks and Macro-benchmarks |

TABLE I
CHALLENGES OF SECURITY CERTIFICATION ADDRESSED AND HOW THEY ARE ADDRESSED BY THE PROPOSED FRAMEWORK

## V. Conclusion and Future Developments

It is a major necessity to provide tools for IoT stakeholders to evaluate the level of preparedness of their system to IoT security threats. In this paper we propose a methodology to proceed to a certification process in order to define the security analysis and the testing setup needed for doing the evaluation. Also, we propose a labeling schema that could be applied based on the metrics and systematic evaluation that could be put in place using the ARMOUR approach.

The security certification of IoT proposed in this paper takes into consideration the existing security certification frameworks, standards, and their respective limitations identified by the industry and research communities. This certification process will provide a system-level approach to security and the metrics to support it. The lack of this certification process is actually a gap in the security and privacy area of IoT that has the potential to clearly increase the confidence on the ongoing IoT deployments in the real world.

Finally in Table I we summarize how the challenges identified and described in section III are addressed by the proposed framework

## Acknowledgement

This work was done in the context of the ARMOUR project Grant id 688237 of the Horizon 2020 Call ICT-12-2015 Integrating experiments and facilities in FIRE+.

## References

[1] V. Cerf and M. Senges, "Taking the internet to the next physical level," *Computer*, vol. 49, no. 2, pp. 80–86, Feb 2016.

[2] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.

[3] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: A standardization perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265–275, June 2014.

[4] G. Bernabeu, E. Jaffuel, B. Legeard, and F. Peureux, "Mbt for global platform compliance testing: Experience report and lessons learned," in *Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 66–70.

[5] S. NIST, "800-37," *Guide for the Security Certification and Accreditation of Federal Information Systems*, 2004.

[6] R. Anderson and S. Fuloria, "Certification and evaluation: A security economics perspective," in *2009 IEEE Conference on Emerging Technologies Factory Automation*, Sept 2009, pp. 1–7.

[7] S. B. Lipner, "The birth and death of the orange book," *IEEE Annals of the History of Computing*, vol. 37, no. 2, pp. 19–31, Apr 2015.

[8] G. Troy, "Introduction to the common criteria for it security (iso 15408)," 1999.

[9] CCRA, "Common criteria," http://www.commoncriteriaportal.org.

[10] F. Keblawi and D. Sullivan, "Applying the common criteria in systems engineering," *IEEE Security Privacy*, vol. 4, no. 2, pp. 50–55, March 2006.

[11] S. P. Kaluvuri, M. Bezzi, and Y. Roudier, "A quantitative analysis of common criteria certification practice," in *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 2014, pp. 132–143.

[12] ECORYS, "Security regulation, conformity assessment and certification final report volume 1: Main report," http://www.projectara.com/, October 2011.

[13] J. Hearn, "Does the common criteria paradigm have a future? [security and privacy]," *IEEE Security Privacy*, vol. 2, no. 1, pp. 64–65, Jan 2004.

[14] K. Beznosov and P. Kruchten, "Towards agile security assurance," in *Proceedings of the 2004 workshop on New security paradigms*. ACM, 2004, pp. 47–54.

[15] NCSA, "Common criteria reforms: Better security products through increased cooperation with industry," October 2011.

[16] G. Bernabeu, E. Jaffuel, B. Legeard, and F. Peureux, "MBT for global platform compliance testing: Experience report and lessons learned," in *25th IEEE International Symposium on Software Reliability Engineering Workshops, ISSRE Workshops, Naples, Italy, November 3-6, 2014*, 2014, pp. 66–70.

[17] J. Botella, F. Bouquet, J. Capuron, F. Lebeau, B. Legeard, and F. Schadle, "Model-based testing of cryptographic components - lessons learned from experience," in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation, Luxembourg, Luxembourg, March 18-22, 2013*, 2013, pp. 192–201.

[18] C. W. et al., "An introduction to ttcn-3," 2011.

[19] J. Grabowski, D. Hogrefe, G. Réthy, I. Schieferdecker, A. Wiles, and C. Willcock, "An introduction to the testing and test control notation (ttcn-3)," *Computer Networks*, vol. 42, no. 3, pp. 375–403, 2003.

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

[21] J. Lorrain, F. Dadeau, E. Fourneret, and B. Legeard, "Mbeetle - un outil pour la generation de tests a-la-volee a l'aide de modeles," in *15th edition of Approches Formelles dans l'Assistance au Developpement Logiciels (AFADL)*. GDR-GPL, 2016.