IoT solution information security certification conceptual framework

IoT solution information security

On improving the transparency and accountability of IoT Solutions through an Open World perspective

Luiz Otavio Duarte
Facti - Fundação de Apoio à Capacitação em Tecnologia da Informação
luiz.duarte@facti.com.br

José Augusto de Lima Prestes
Facti - Fundação de Apoio à Capacitação em Tecnologia da Informação
jose.prestes@facti.com.br

ABSTRACT

The rapid growth of Internet of Things (IoT) solutions development and the rise of agile development utilization, combined with the so-called “low touch economy” and the recent discussions on privacy and data protection brought several demands related to Information Security. Despite the existence of several efforts – either academic or not – focused on the definition and implementation strategies for certification of Information Security models designed for Information Technology and Communications (ICT) solutions, these aren’t widely adopted. In addition, there are significant differences between typical IoT solutions and ICT solutions as traditionally presented, which ends up demanding different certification strategies. Continuous and more dynamic certification models (using cutting edge technologies such as blockchain, self-regulation, analytics, and artificial intelligence) are demanded in this context. This work discusses more effective forms of certification, using innovative edge concepts and technologies, at first aiming to identify a set of inhibiting factors, offenders, challenges or issues that need to be addressed correctly when developing an effective large-scale security certification model.

CCS CONCEPTS

• **Security and privacy** → Systems security; • **Software and its engineering** → Software creation and management; • **Information systems** → Information systems applications.

KEYWORDS

Internet of Things, Edge Devices, Security Certification, Information Security, Security Compliance

ACM Reference Format:
Luiz Otavio Duarte and José Augusto de Lima Prestes. 2021. IoT solution information security certification conceptual framework: IoT solution information security On improving the transparency and accountability of IoT Solutions through an Open World perspective. In *XVII Brazilian Symposium on Information Systems (SBSI 2021), June 07–10, 2021, Uberlândia, Brazil.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3466933.3466983

1 INTRODUCTION

Human development has increasingly demanded technological processes and technology not only to be affected but also developed collaboratively. This context considers actors such as final consumers, developers, Academia, and any other stakeholder. Society became aware and are demanding space for more active participation in technological development, especially concerning information security [1]. The mobilization to stop using any given mobile application when privacy policies change is a current example of this kind of end-users’ awareness and latent interest about Information Security issues. This evolution should also achieve the certification processes of IoT solutions for information security since end-users’ data – whether individuals or companies - is at risk.

At a first glance, an Information Security certification process for any technology may look something of low level of complexity. These processes generally consider three basic components: (a) technology, device or solution to be certified; (b) certification metrics; and (c) laboratories capable of attesting the compliance to the requirements.

Nowadays, it is expected that the technology to be certified has already been developed and is finalized, in such a way that for each model or version of a device a new certification process is required. At this very moment, we are not considering the individual certification of each single produced device – a situation that may be required for measuring systems or those that require the correct calibration. In some cases, the certification process involves sampling, including specific processes on the devices being certified.

Certification metrics are characteristics that can be verified. This verification process occurs through standardized methods, many of them similar to the ISO 17015 requirements [2]. Thus, a certifiable metric requires valid, repeatable and reproducible methods. As such requirements, their methods of observation or measurement uncertainties are usually defined by certifying entities, which have the necessary enforcement for that.

The laboratory component is related to those physical infrastructures (with their resources), which can implement processes to verify a requirement on a technology sample. It is expected that a group of requirements can be certified by a single laboratory. For example, all aspects of noise emission can be tested by the same laboratory that certifies this specific characteristic.

SBSI 2021, June 07–10, 2021, Uberlândia, Brazil
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8491-9/21/06…$15.00
https://doi.org/10.1145/3466933.3466983

When conducting a more exhaustive survey of the adequacy of the available strategies to carry out certification processes for information security of IoT solution it is necessary to consider methodologies such as those proposed by Common Criteria [3, 4] and established by FIPS-140.2 [5]. Other strategies to certify the quality of the IoT solution from its pre-conceptual stages must be considered; for the purposes of this type of processes, along the lines of Security Build In (which would allow to identify the maturity of information security in the solution architecture [6–8] and strategies established for IoT). The adoption of models similar to the Framework for Compliance proposed by the IoT Security Foundation [9] are mandatory in order to achieve the best standards in any certification methodology. In addition, it is desirable to consider tools strategies for effective technological development, such as the adoption of agile methods.

The local context of public policies also plays a key role in enforcing certifications and must be considered. For example, in the Brazilian context, it is necessary to consider the national Internet of Things plan [10], the relevant topics for making Internet of Things [11] and the IoT action plan for Brazil [12].

When considering these various aspects together with an Open World perspective, we identify a set of inhibiting factors, offenders, challenges or issues that need to be correctly addressed and that do not necessarily occur in non-IoT solutions. In this sense, from a systemic view, it is possible to identify a set of dimensions to be addressed: (a) The Open World Challenges and the IoT certification process; (b) Challenges Brought by IoT era; and (c) Information Security, Privacy and Data Protection Challenges.

This research article is structured as follows. In the second section we discuss the challenges for an IoT solution information security certification. In third section we discuss a certification framework for IoT Solution Certification, as a digital ecosystem. In fourth section we present a research case study, applying the proposed certification validation smart contracts against the top 20 public available IoT solutions. The conclusions are given in the last Section.

2 CHALLENGES FOR AN IOT SOLUTION INFORMATION SECURITY CERTIFICATION

Currently, work related to certification for information security of technological products usually addresses the issue by carrying out certification processes only on selected versions of finished products. [4, 5, 9] The general expectation is that these products change little – or even do not change after the completion of the certification process. This situation typically leads to one of three possibilities: (a) the product cannot evolve and incorporate new characteristics due to technical changes that would invalidate its certification; (b) new certification processes must occur more frequently; or (c) new versions of a pre-certificated product do not have subsequent certifications.

Related works, such as those developed by the Ministry of Science, Technology and Innovation - MCTIC [10] and the Brazilian Chamber of IoT [11], identify topics and relevant aspects applicable to the certification processes for information security. Such requirements point to the development of solutions adhering to the Open World strategies. These requirements are not present in widely used and used certification models.

Considering as an example the Brazilian market, conformity assessment of aspects such as gas emissions occurs through a network of accredited laboratories to carry out specific validations. For instance, the composition of laboratory tests on emission of greenhouse gases, energy efficiency, noise level, and graduation of biodegradable components compose the array of a certification on whether the component may be considered green (less harmful to the biosphere and more sustainable). This kind of conformity assessment are carried out by Brazilian National Institute of Metrology, Standardization and Industrial Quality - Inmetro [13]. Most of those standards and their requirements are discussed by technical chambers and are publicly available. However, the same process does not happen in the context of information security and it seems to be far from happening for IoT devices. Even with the efforts promoted internationally by organizations such as The National Institute of Standards and Technology - NIST [14], Institute of Electrical and Electronics Engineers - IEEE [15], and IoT Security Foundation [16], only certain specific certifications – such as PCI DSS from PCI Security Standards Council [17], required to operate with credit cards, or those with enforcement carried out by technologies like marketplaces – are obtaining relative small success. Studies like the one proposed by [18] show us that more than 80% of the sites that must be compliant with the PCI DSS have at least one violation of the PCI DSS that should have disqualified them.

In the context of IoT solutions, especially when new technologies are used, there is even a difficulty in finding compatible technical requirements for certification. [19]. Neisser et. al [20] presents a proposal for the management of certification processes using a decentralized system, based on block-chain and smart contracts. However, its focus is mainly based on the management of certifications carried out, not covering aspects of the laboratory process for verifying the certification requirements itself.

2.1 Certification and Open World Challenges

As pointed by Araujo [21] one of the biggest challenges for the Open World is in the information ecosystem development. The digital ecosystem paradigm makes it possible to change the sectoral metanarrative to a social metanarrative. This vision is based on collective intelligence, collaboration and engagement. An information security certification process based on open world paradigm, requires collaboration, transparency, information sharing, traceability, must consider the social fact and reduce bureaucracy.

Some challenges for implementing an Open World vision include: (a) the general costs that are evolved to pass through the certification process acts as a stop condition for several new technologies or organizations, as a typical entrance barrier that somehow places the effort to obtain a certification as a post-market effort; (b) the certification process does not consider all potential stakeholders. Actually, end-users have little to no participation of these processes; (c) the same lack of transparency also occurs in the requirements used and the technologies that have been positively validated; (d) ideally, there must be a just in time certification process that meets the evolution of any IoT solution technology.

Certifications such as Common Criteria and FIPS-140.2 are not very committed to such aspects. Besides that, another aspect that needs to be considered is the time to carry out by conventional certification processes. Even in solid and structured models, these processes are usually carried out in an impeding time. It makes sense that certifications related to complex environments or processes (such as those proposed by the ISO 27k series) demands several months, however, certifications aimed to evaluate solutions that are developed in an agile way to satisfy the increasing and urgent market demand of new technologies and products must be effective from a financial perspective – allowing companies to quickly certificate and send their products.

Finally, the certification process should encourage the development of communities to discuss technical requirements that establish post-validation processes (i.e. through digital contracts), encouraging the publication of the results achieved in an easily intelligible and traceable way.

2.2 Challenges Brought by IoT Era

IoT solutions are bringing a set of new challenges and adding another level of complexity to existing technological challenges. Among them, it is expected to consider [1]: (a) the distributed nature of IoT devices, which are developed to be used in different scenarios or operating environments – including their availability in public environments; (b) the exponential number of solutions made available by a large number of players, in different versions of software and hardware; (c) the limited capacity of resources, which is often part of IoT solutions, that impacts the possibility of using appropriate security mechanisms; (d) the need to ensure Information Security throughout the solution's life cycle until it is discontinued; and (e) the lack of an "one size fits all" approach for information security mechanisms.

To be considered an IoT solution it is expected, among other characteristics, the ability to exchange data via the Internet [22], even through gateways, brokers or similar. In a conventional architecture of an IoT solution, the following components are expected: an IoT hardware device, containing its firmware; pooling, data acquisition, data storage and data brokers systems - all with their hardware and software components, a service or IoT platform that runs on the Internet. [23].

Dealing with IoT solutions implies in work with a very high level of abstraction. A specific version of a certain device model can also be very different from another version of other device in the same category. Comparatively, it is more or less like saying that the 2021 model of the Cessna Grand Caravan Ex aircraft and the 2021 model of the Jeep Gladiator are both vehicles.

A drone can be considered as an IoT device, at the same time as a so-called smart lamp or a life support device. Of course, the information security metrics in one group of devices must be quite different from those in other groups.

Classifying devices as sensors or actuators does little to help with the accreditation process. It is primarily necessary to establish a classification model that is more closely related to the application aspect of the device. Otherwise, it would be like establishing the same metrics for an IoT solution designed to operate in an ambulance as those established for an IoT solution marketed for a pet shop vehicle.

Therefore, certification processes demand the establishment of a classifying schema to aggregate the solutions into niches or categories of solution, defining appropriate metrics or requiring specific security controls for the adequate types of devices. Although complexity increases, granularity is a must in this case.

2.2.1 *Complex set of components on IoT Solutions.*

Generally, during the life cycle of an IoT solution one must consider the development of a set of hardware and software components, such as: (a) the hardware of the IoT device; (b) the firmware or software component of the IoT device; (c) The development of hardware and software components of gateways and broker systems; and (d) the service available through a data communication network, which commonly runs on Internet or applications on mobile devices, for example.

During the same life span, we can also have several revisions that are taken into operation. Thus, all revisions of the solution, until its discontinuation, are part of a solution life cycle. Of course, it is common to have different versions released concurrently with only a few modifications; corrections or hotfix versions may be developed in parallel with new releases versions.

Considering a certification point of view, we must ensure that any version of the solution was submitted to the certification procedures – or, at least, was in some way validated.

2.2.2 *The Agile Development.*

From the various concepts that integrate the agile development environment, two of them are of special interest for certification processes: (a) Continuous Integration and (b) Continuous Deploy. In these concepts, the solution – particularly on software components – is continuously integrated, tested and can also be placed for approval and production.

Considering the essential components of an IoT solution, it is expected that a given service component may be more susceptible to this approach, with new versions being generated on a daily basis. Firmware components can also use this strategy; however, it is expected that an IoT hardware device owns any kind of automatic update feature and that it can be recovered if this process does not occur as expected. It is not usually expected that a hardware component has several new hardware versions in a very short time basis: in these cases, greater care shall be taken in qualification models, approval, and other tests before its operation. After all, if the hardware was poorly designed, it will require a greater effort of technical maintenance, replacement, reimbursement etc.

In a comprehensive analysis, each new change made to any of the solution components results in a new version of the system as a whole. In other words, it requires a new deployment, with the integration of all components.

Development life cycles with fast deploys requires certification processes that are more efficient. If new features or corrections are generated on a daily basis, certifications should be part of the solution development flow.

2.3 Accountability, Information Security, Privacy and Data Protection Challenges

When dealing with information security certification, the mere presence of a security control or component does not mean that it was implemented or configured correctly. For instance, an event recording mechanism with high granularity that can be disabled during the operation should have a lower score than a simpler mechanism that cannot be disabled.

On the other hand, there are several forms to achieve the same goal. For example, a random number generator in hardware that consists of a transducer and an analog digital converter using radio frequency antennas can have a similar entropy that another hardware using another physical phenomenon – such as the use of the natural stochasticity of an memristor.

In some cases, the assessment of a characteristic is supported by statistical methods. The generation of random numbers, for instance, is as good as the absence of observed statistical patterns. Notwithstanding, for each data stream obtained from the random number generator we have a different dataset generated, which can somehow affect the reproducibility of the same test in different laboratories or scenarios. Therefore, it is mandatory to consider that we can have non-static methods that can be applicable to each and every solution when trying to validate the implementation of an information security mechanism.

When evaluating Information Security in any IoT solution, aspects such as confidentiality, integrity, and availability must be weighed differently given their classification or application. Thus, it is necessary to catalog the information security objectives in relation to the device classes.

Along with these difficulties, as pointed out by [1], information security concerns are multidisciplinary, including: (a) Protocol and network security; (b) Privacy and Data Protection; (c) Identity Management and Ownership; (d) Fault Tolerance; and (e) Cryptography and protocols. Additionally, it is necessary to consider particularities of local regulations, that may demand some level of adaptations in certification models.

For example, the auditability of a system may end up in conflict with some existing anonymity legal requirement. The existence of end-to-end encryption mechanisms can reinforce privacy, but it can also make it possible for criminals to exchange information that would be valuable for police investigators.

3 CERTIFICATION FRAMEWORK FOR IOT SOLUTIONS

3.1 Methodology

This research was carried out as part of a governmental funded Research Project in the scope of the Brazilian IoT Strategy. As presented in section 2, an empirical and qualitative methodological approach was used, through an exploratory survey on the strategies currently available for assessing Information Security compliance for technological solutions in general. From the survey carried out, requirements for a technological certification framework were identified and considered.

Some social requirements presented in [10] and [11], such as voluntary self-assessment and transparency processes, indicated that the use of an Open World perspective is pertinent. In this way, the development of three fundamental aspects of the proposed certification model were modeled in respect of both technical and Open World requirements: (a) certification requirements, (b) certification environment, and (c) certification process.

During the development of this research, principles of Design Science [24] were used. At the end of the process, general conceptual framework had been developed and validated through a set of experiments that focused on currently available IoT solutions, bringing theoretical requirements to the practical field.

3.2 Certification requirements

3.2.1 Open technical forums, transparency and traceability. Committees for defining security objectives, requirements for operational environments and requirements for verification processes must be open to the participation of all stakeholders, including end-users. All documents generated (including results of all the certifications carried out) must be publicly available.

3.2.2 The certification must be low cost. It is necessary to address the question about the entry costs. A security certification should be available for most IoT solutions, not just a small part of these solutions.

3.2.3 Voluntary with market enforcement, considering academic and technological aspects. It is expected that businesses and consumers in general rely on this type of model and recognize genuine value in the certification, composing a valuable element in any decision-making processes. Public Policies may strengthen these and other correlated perceptions.

3.2.4 Proposing the solution life cycle. In agile development, considering continuous integration and continuous deploy, numerous versions of an IoT solution in operation are expected. So, it makes more sense to check and approve a solution during the development life cycle than on selected isolated versions. The certification must be taken place when a stable version is committed. In other words, on every integration activity, a technical certification for security must occur.

3.2.5 The version of an IoT solution is the set of versions for each component of this solution. A complete IoT solution involves the use of numerous hardware and software components. Each of these components can have a different development process, with different versions and certifications. In a systemic view, an executable version of the IoT solution is made up of all versions of its components, including any changes made to them.

3.2.6 The certification of any version of the IoT solution relates to the sum of the certifications of the individual parts. Since each certification of the parties can have different objectives, each component shall have a different set of certifications. For example, the hardware component may have a certification for anti-tampering and other to electromagnetic emanations.

3.2.7 Different operating environments have different security profiles. Each operating environment shall have different requirements on how each component must be certified and which technical requirements must be met.

3.2.8 Different components have different security technical requirements. Each component shall be composed of smaller modules that have different security technical requirements. For example, in the hardware component, in a given random number generation module there is a requirement, which is the existing entropy measure. In the firmware component, on access control module, there is a security requirement which is authentication, access control and logging.

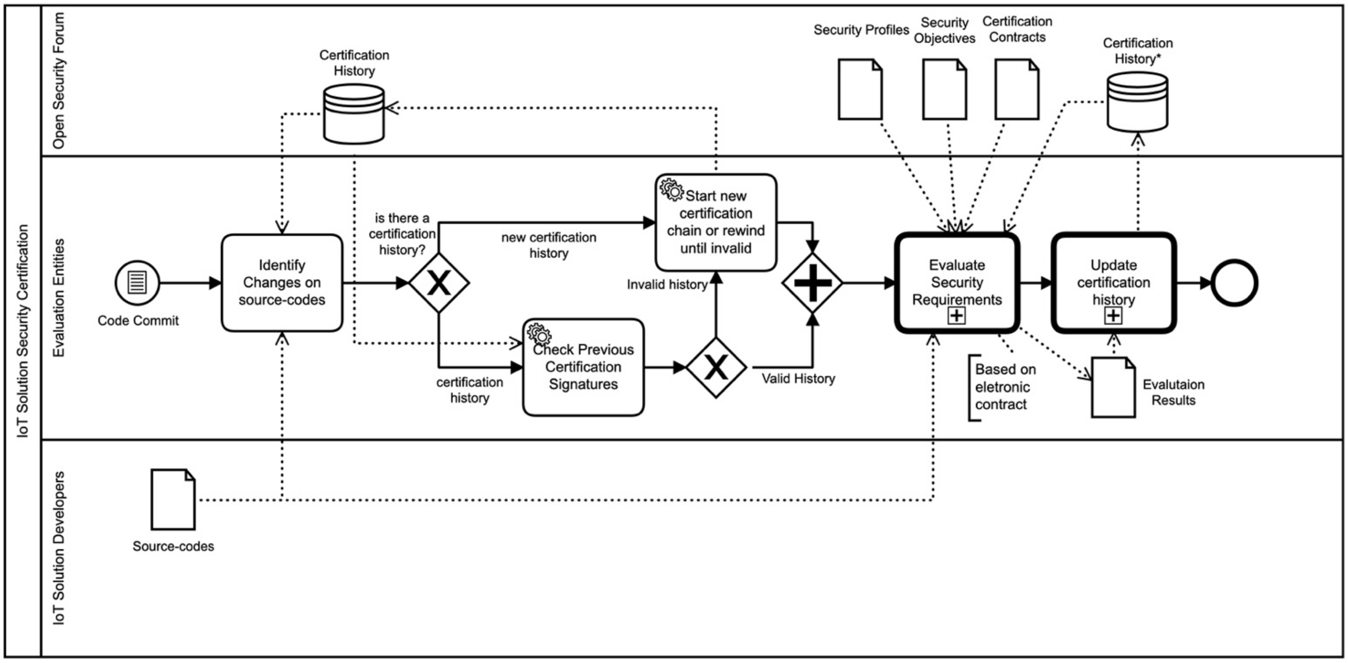

IoT Solution Security Certification
Open Security Forum
Evaluation Entities
IoT Solution Developers
Certification History
Security Profiles
Security Objectives
Certification Contracts
Certification History*
Code Commit
Identify Changes on source-codes
is there a certification history?
new certification history
Start new certification chain or rewind until invalid
Invalid history
Check Previous Certification Signatures
certification history
Valid History
Evaluate Security Requirements
Update certification history
Based on eletronic contract
Evalutaion Results
Source-codes

Figure 1: Main IoT Security Certification Framework.

3.2.9 *Security objectives and security profiles evolve with technology.* New types of attacks and threats emerge daily with the development or maturation of technology. The safety profiles of each component in each operating environment shall evolve during all the solution's life cycle.

3.2.10 *Different security profiles require different evaluation granularity.* The level of scrutiny required by the security profile must require a different effort according to the desired application. For example, the scrutiny of a security objective related to the process of securely updating an IoT solution employed for sensing home environmental temperature would be less critical than the scrutiny required for this same security objective for a commercial solution - as temperature sensing of environments that maintain vaccines.

3.2.11 *Open accreditation and smart contract driven.* Accreditation of certification laboratories must take place in an open manner, where security objectives are verified using smart contracts. Similar to Blockchain solutions, several laboratories - as miners, in this appropriate analogy - may receive the demand for validation of the same requirement, increasing the level of certainty and reducing bias possibilities.

3.3 Certification environment

The objective of the framework is, by meeting the requirements presented, to allow the establishment of a digital, collaborative and multi-disciplinary ecosystem. To achieve these objectives, it is composed of numerous actors, components and activities.

3.3.1 *Actors.* The framework may have at least the following set of actors:

End-users of the solution, who have the power to choose which IoT solution to purchase based on the information received in the certification process. An end-user can also be a developer, part of open technical forum groups, or even an evaluator entity.

Developers of IoT solutions are the ones that develop or integrate software or hardware components in order to build an IoT solution. A developer may also include institutions that integrate main activity is to present the IoT solutions developed for the certification process.

Open technical forums are public or private institutions with qualified technical staff to carry out discussions regarding this matter. Its activities are related to the collaborative development of digital smart contracts for verification and validation of a certain information security objective, in addition to the establishment of guidelines as to the number of operational environments, their requirements and the way of presenting their validations.

Evaluator entity: It is an institution that has sufficient technical capability to check the adequacy of an IoT solution pursuant to the conditions of a previously established digital contract.

3.3.2 *Framework components.* The main components of the framework are the following:

Certification history database: is a historical database that keeps track of the results of certification processes over the time. Its structure can be centralized or distributed. Each one of the entries in this database is digitally signed by evaluators and are responses to a certification request made by the developer of the IoT solution.

Security Profiles: are the set of all security profiles defined by open technical forums. Each security profile defines which technical requirements must be present and at what restriction level they

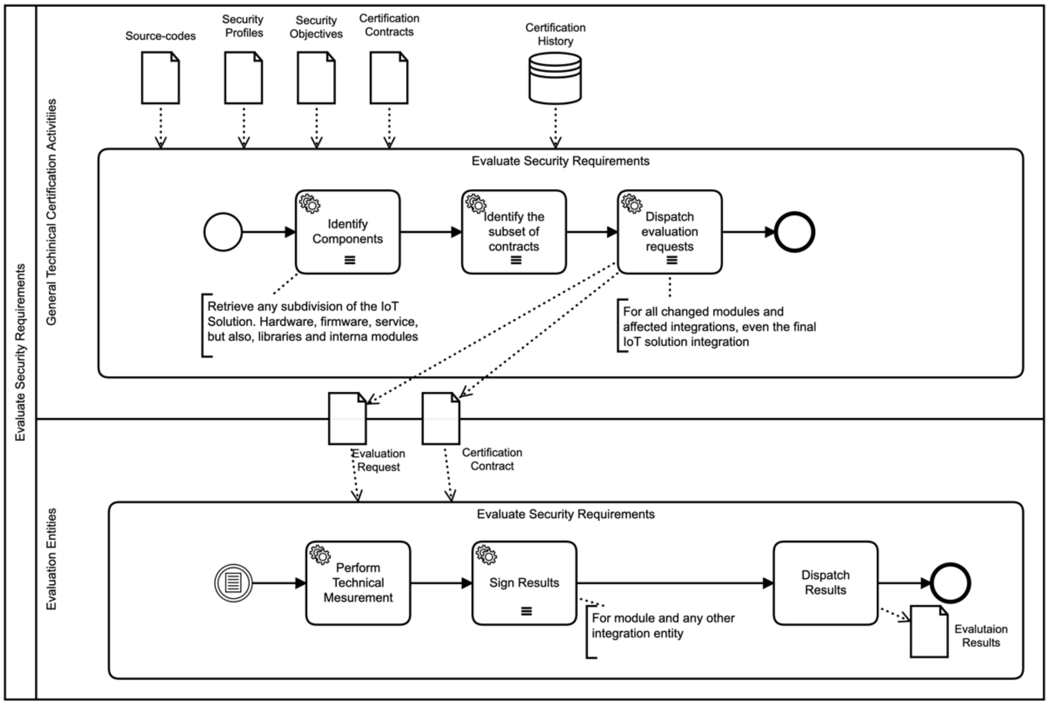

Evaluate Security Requirements
General Techinical Certification Activities
Source-codes
Security Profiles
Security Objectives
Certification Contracts
Certification History
Evaluate Security Requirements
Identify Components
Identify the subset of contracts
Dispatch evaluation requests
Retrieve any subdivision of the IoT Solution. Hardware, firmware, service, but also, libraries and interna modules
For all changed modules and affected integrations, even the final IoT solution integration
Evaluation Request
Certification Contract
Evaluation Entities
Evaluate Security Requirements
Perform Technical Mesurement
Sign Results
Dispatch Results
For module and any other integration entity
Evalutaion Results

Figure 2: The Evaluate Security Requirements Sub-process.

must be satisfied for a given operating environment. For example, if the device is classified as a smart vacuum cleaner (which performs its activities in a residential operating environment), the set of requirements to be met shall include the non-dissemination of environmental images that may be captured by any type of embedded sensors. On the other hand, this requirement can be quite the opposite in the case of a smart environmental monitoring system - that is deployed in the same residential environment to avoid physical violations.

Security Technical Requirements: are the set of all requirements that can be imposed on a specific type of IoT solution, regardless of its operational environment. Each requirement corresponds to an information security component, characteristic or posture that affects defined information security objectives - for instance, availability, integrity, authenticity, confidentiality, non-repudiation, and non-tractability. These requirements are stablished by open technical forums.

Certification Contracts: A certification contract establishes how an assessment entity should carry out the process of checking and validating a specific requirement. The guarantee of reproducibility and repeatability is given through the use of smart contracts, programmatically established and digital signed by the open technical forums.

Source-codes and target components: represent the set of all physical and logical components developed or used in the integration of an IoT solution. They involve documentation and source codes, as well as binary codes and hardware devices.

3.3.3 Certification activities. The activities of the certification process correspond to tasks that are performed by one or more actors using specific components. More complex tasks are called subprocesses, as is the case with the Evaluate Security Requirements sub-process. All activities established in the proposed framework are:

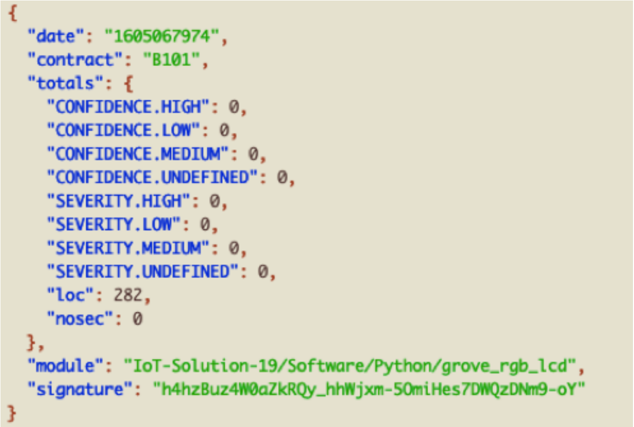
Identify Changes on source-codes
Start new certification chain or rewind until invalid
Check Previous Certification Signatures
Evaluate Security Requirements
Identify Components
Identify the subset of contracts
Dispatch evaluation requests
Perform Technical Measurement
Dispatch Results
Sign Results
Update certification history
Store Results

3.4 Certification process

The certification process that can be seen in Figures 1 and 2 above was modeled considering all the actors, activities and sub-processes. A certification begins within the process of continuous integration or the commit of codes. Therefore, a request for certification is issued to evaluation entities. These entities should then check the current status of the certification, identify the security profiles, security objectives and the applicable certification contracts. With

Table 1: Top 20 IoT solutions selected for the research case study

IoT Solution	Iot Solution
home-assistant/core	saltstack/salt
jopohl/urh	platformio/platformio-core.git
ubuntu/microk8s	Open-Source/tuya-convert
DT42/BerryNet	loklak/loklak_IBM_Home_Automation
phodal/iot	snapcore/snapcraft
MentatInnovations/datastream.io	home-assistant-libs/pytradfri
thingsboard/thingsboard-gateway	Nekmo/amazon-dash
smartHomeHub/SmartIR	aws/aws-iot-device-sdk-python
Telefonica/HomePWN	HackerShackOfficial/Smart-Security-Camera
DexterInd/GrovePi	jczic/MicroWebSrv



```
{
  "date": "1605067974",
  "contract": "B101",
  "totals": {
    "CONFIDENCE.HIGH": 0,
    "CONFIDENCE.LOW": 0,
    "CONFIDENCE.MEDIUM": 0,
    "CONFIDENCE.UNDEFINED": 0,
    "SEVERITY.HIGH": 0,
    "SEVERITY.LOW": 0,
    "SEVERITY.MEDIUM": 0,
    "SEVERITY.UNDEFINED": 0,
    "loc": 282,
    "nosec": 0
  },
  "module": "IoT-Solution-19/Software/Python/grove_rgb_lcd",
  "signature": "h4hzBuz4W0aZkRQy_hhWjxm-5OmiHes7DWQzDNm9-oY"
}
```

Figure 3: Digital signed result of a certification contract execution.

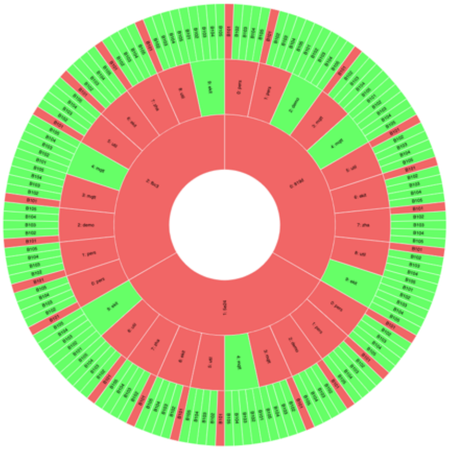


Figure 4: Graphical representation of a continuous certification.

these information, technical validations (which can occur in different validation entities) are carried out. The results obtained are signed and made available in a centralized or distributed manner.

4 DEFINITION AND APPLICATION OF RESEARCH CASE STUDY

To assure the validity and usability of a continuous certification process for IoT solutions for security, using certification contracts, a research activity was carried out in order to develop fundamental aspects of the proposed framework. Considering that several components of the framework depend on the interaction with numerous external actors - including open groups that still need to be institutionalized -, this case study was carried out by running the Evaluate Security Requirements sub-process. In addition [20] it demonstrates the viability of functionalities for managing certification processes based on a collaborative strategy.

In order to reproduce and repeat the findings, it is important to define the context in terms of selecting IoT solutions, their modules, integration versions and certification contracts.

4.1 Case study context

In December 2020, a search was conducted on the GitHub[1] platform, which handles a large number of open source projects. Among the available repositories we identified those that had IoT in their description. From these projects, we selected those that had source code written in Python (since the certification contracts that were used presuppose to be written in this language). To identify projects with great engagement we selected those with the most stars (a metric that allows to identify if a project is active and of interest to the community). From the responses obtained, we selected the top 20 repositories. The selected repositories can be seen on following Table 1.

4.2 Execution framework activities on case study context

For each one of the IoT solutions, the *Identify Components* activity was performed; thus, its modules were programmatically established. The objective was to define certifiable subparts for each of the IoT solutions. Basically, for each solution, the directories that

[1] More information about GitHub platform can be found at https://github.com.

contained files with *py* extension were identified, ordering them by those with the largest number of files in custody. Finally, of them all, a limit of ten modules per IoT solution was taken.

Once the 20 IoT solutions were established, each with up to 10 modules, the versions that passed through the certification process were established. Three versions were defined for each of the solutions. These versions were also programmatically defined based on commits made on the GitHub platform. Imagining a solution with 100 commits, the upper half (of more recent commits) was considered. The commit numbers 50, 75 and 100 had their full codes scrutinized.

To perform the activity *Identify the subset of contracts*, we made the selection and execution of a set of five certification contracts from technical validations made available by a static source code analysis tool: the bandit[2] tool, version 1.6.2 (which allows identifying points of attention for Information Security in source codes written in Python) was used for this purpose, with the following checks being selected: *B101 - assert_used*, *B102 - exec_used*, *B103 - set_bad_file_permissions*, *B104 - hardcoded_bind_all_interfaces*, and *B105 - hardcoded_password_string*.

4.3 Findings

The total number of technical evaluations carried out for the case study and use was 3000 validations using certification contracts, generating 20 graphic representations of the information security postures, one for each scrutinized IoT technology. In addition, all 3000 were digitally signed for later custody. An example of the signed result of applying the B101 contract against the DexterInd / GrovePi solution can be seen in the Figure 3.

The Figure 4 shows the execution of the set of five certification contracts against a solution. In the innermost arch, first level, the three selected and verified versions are shown. The version values are the tags of the commits made in the source code. The second level presents the verified modules (in this example, actions were carried out on the modules *pers-0*, *pers-1*, *demo*, *mqtt-0*, *mqtt-1*, *util*, *ekit-0*, *zha*, *util*, and *ekit-1*. The third level represents the result obtained from the execution of a specific contract from B101 to B105: whenever an issue is found, the graph is red; otherwise, green.

Aiming greater credibility in the results of the assessments, it is possible to require that all of these are carried out by more than one certification laboratory, each performing the same procedures.

5 CONCLUSIONS

The revolution that IoT solutions are constantly bringing us is undeniable, allowing the connection between devices, objects and people. In this context, a set of complex challenges arises for Information Security and Data Protection research by and large, including the certification processes for IoT devices on an Open World perspective. In particular, the lack of collaborative, transparent, continuous certification processes.

We tried to bring in this work these set of challenges and inhibiting factors, which are in fact motivators for the progress of the knowledge area on certification processes of IoT devices in a large-scale fashion for Information Security. In addition, a proposal for a collaborative framework was presented considering the expansion of roles and actors involved in the device certification process. A case study of the application of some of the framework's activities was carried out against a set of solutions currently available on the market. The goal is to aid the development of processes with a higher degree of maturity, which in fact influence and respond to the needs of end users and can take advantage of cutting-edge academic and technological developments.

For future work, it is planned to develop a pilot project for the full application of the proposed framework for a specific group of IoT devices used in a specific operating environment. Considering specific characteristics of Brazilian Economy, it is expected to develop some kind of application in the context of Agriculture 4.0. This objective seems adherent to the purposes of this work because this market contains a complex supply chain and its businesses are constantly improving their products aiming to reduce costs; so, it seems initially correct to assume that, as mentioned before, many devices in e.g., precision agriculture will be updated and have newer versions in considerably short cycles, demanding agile certification processes like the presented framework.

ACKNOWLEDGMENTS

We are grateful to the anonymous reviewers for their helpful comments, which have helped us to significantly improve the manuscript quality. This research was granted by Brazilian Federal Government agency Finep - Financiadora de Estudos e Projetos (http://www.finep.gov.br/) under the Project Open Technology Platform for Internet of Things and their Applications ("Projeto Plataforma Aberta de Tecnologias para Internet das Coisas e suas Aplicações"), Agreement #01.16.0053.00). The views and conclusions contained in this document are solely those of the authors and should not be interpreted otherwise.

REFERENCES

[1] R. Roman, P. Najera and J. Lopez. 2011. Securing the Internet of Things. In *Computer*, vol. 44, no. 09, pp. 51-58,. doi: 10.1109/MC.2011.291

[2] General requirements for the competence of testing and calibration laboratories. 2006. ISO/IEC 17025, International Organization for Standardization/International Electrotechnical Committee, Geneva.

[3] Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, ISO/IEC 15408-1:2009, International Organization for Standardization/International Electrotechnical Committee, Geneva, 2009.

[4] C. Preschern. 2012. Catalog of security tactics linked to common criteria requirements. In Proceedings of the 19th Conference on Pattern Languages of Programs, page 7. The Hillside Group,

[5] FIPS PUB 140-2: Security Requirements for Cryptographic Modules. NIST. July 26, 2007.

[6] Wyk, K.R. & McGraw, G.. 2005. Bridging the Gap between Software Development and Information Security. In *Security & Privacy*, *IEEE.* 3. 75- 79. 10.1109/MSP.2005.118.

[7] Joanna Cecilia da Silva Santos, Katy Tarrit, and Mehdi Mirakhorli. 2017. A Catalog of Security Architecture Weaknesses. 220-223. 10.1109/ICSAW.2017.25.

[8] IoT Security Foundation. 2019. IoT Security Reference Architecture for the Healthcare, Retrieved May 07, 2021 from: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/05/IoT-Security-Reference-Architecture-For-The-Healthcare-Industry.pdf

[9] IoT Security Foundation. 2018. IoT Security Compliance Framework, Retrieved May 07, 2021 from: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf

[10] MCTIC. 2018. Documento de referência do plano nacional de internet das coisas IoT.BR. Retrieved May 07, 2021 from: http://otd.cpqd.com.br/otd/wp-content/uploads/2018/12/Cartilha-PLANO-NACIONALDE-INTERNET-DAS-COISAS_192x245_WEB.pdf

[11] Câmara IoT. 2016. Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil.. Retrieved May 07, 2021 from: http://www.abinee.

[2] More information about bandit tool can be found at: https://github.com/PyCQA/bandit

org.br/informac/arquivos/aiot.pdf

[12] BNDES e MCTIC, Internet das Coisas: um plano de ação para o Brasil, Relatório Final do Estudo - Produto 9a, 2018. Retrieved May 07, 2021 from http://www.mctic.gov.br/mctic/export/sites/institucional/inovacao/paginas/politicasDigitais/arquivos/estudo_iot/fase_3/produto-9A-relatorio-final-estudo-de-iot.pdf

[13] Inmetro. Brazilian National Institute of Metrology, Standardization and Industrial Quality. Retrieved May 07, 2021 from https://www.gov.br/inmetro/

[14] NIST. National Institute of Standards and Technology. Retrieved May 07, 2021 from https://www.nist.gov.

[15] IEEE. Institute of Electrical and Electronics Engineers. Retrieved May 07, 2021 from https://www.ieee.org.

[16] IoTSF, IoT Security Foundation. Retrieved May 07, 2021 from https://www.iotsecurityfoundation.org.

[17] PCI Security Standards Council. Retrieved May 07, 2021 from https://pt.pcisecuritystandards.org.

[18] Sazzadur Rahaman, Gang Wang, and Danfeng (Daphne) Yao. 2019. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 481–498. DOI: https://doi.org/10.1145/3319535.3363195

[19] Kang, S.; Kim, S. 2017. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. *In Symmetry 2017*, 9, 233. https://doi.org/10.3390/sym9100233.

[20] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini and A. Skarmeta. 2019. Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices, In *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2019, pp. 1-6, doi: 10.1109/CSCN.2019.8931384.

[21] Renata Araujo. 2017. Information Systems and the Open World. In: I GranDSI-BR - GrandResearch Challenges in Information Systems in Brazil 2016-2026. Special Committee on Information Systems (CE-SI): BrazilianComputer Society (SBC), pp. 42–51

[22] Recommendation ITU-T Y.2060, Overview of the Internet of things, Retrieved May 07, 2021 from http://www.itu.int/rec/T-REC-Y.2060

[23] JEON, Jonghong; IN, Minkyo; LEE, Seungyun. Considerations on Standardization of WoT. W3C's Web of Things Workshop.

[24] Bax, Marcello. (2014). Design science: filosofia da pesquisa em ciência da informação e tecnologia. In. XV Encontro *Nacional de Pesquisa em Ciência da Informação* – ENANCIB 2014. 42. 3883-3903.