Lego Methodology Approach for Common Criteria Certification of IoT Telemetry

George Suciu[1,2(✉)], Cristiana Istrate[1], Ioana Petre[1], and Andrei Scheianu[1]

[1] R&D Department, BEIA Consult International, Peroni 16, 041386 Bucharest, Romania
{george, cristiana.istrate, ioana.petre, andrei.scheianu}@beia.ro
[2] Telecommunications Department, University POLITEHNICA of Bucharest, Bd. Iuliu Maniu 1-3, 061071 Bucharest, Romania
george@radio.pub.ro

Abstract. In our days, almost every business relays on medium-to-high performance computer systems which presents the possibility of being the target of different threats that can exploit the vulnerable software, respectively hardware components. The concept of "security risk" can be described as a specific threat that using a specific type of attack presents the ability to exploit system vulnerabilities, action which will affect the entire integrity of the targeted systems. From this point of view, the main idea of this paper is to present a Lego methodology approach for Common Criteria certification that can be applied to IoT Telemetry systems. Furthermore, we present scenarios of implementation of our approach to increase robustness level applied for agro-telemetry system.

Keywords: Lego methodology · Common Criteria · IoT · Telemetry · Security

1 Introduction

Security certification for heterogenous Internet of Things (IoT) systems poses several challenges, as IoT devices become more ubiquitous. To discover the impact that security risks can have over a System Under Analysis (SUA), there must be specified very clearly the systems' description, considering two essential perspectives which present certain criteria, such as:

(a) **Information and functionality:**

- Evaluation of the security risks impact. An appropriate example can be the affected parts of systems' services, including data processing functions. This perspective is also known as **Aim of refinement**;
- **Criteria of partition:** Specific sections of the data or functions can require distinct security requirements which present unique criticality levels.

Á. Rocha et al. (Eds.): WorldCIST'19 2019, AISC 931, pp. 165–174, 2019.
https://doi.org/10.1007/978-3-030-16184-2_17

(b) **System architecture:**

- **Aim of refinement:** Every level of each component of a system can present a security risk potential. These levels must be detected in order to improve the security level of the entire system;
- **Criteria of partition:** Every component, such as software and hardware components or even an entire network, presents several security risks that can be traced. Because of this characteristic, the architecture of potentially vulnerable systems is divided into components, the specific risks of each component being identified.

In the computer security field, the threat concept is defined as an imminent danger situation that can exploit the vulnerabilities of a system in order to breach its security mechanisms. Threats can be divided into three main categories, as follows [1]:

- **Intentional threats** – represent premeditated invasive actions. The best example of intentional threats consists of computer crimes, including software attacks, theft, espionage, sabotage, etc.;
- **Unintentional threats** – represent accidental software modifications due to human mistakes or technical misunderstandings;
- **Natural threats** – represent several threats that can damage the physical equipment, such as: natural disasters, power failures, fires and floods.

The main idea of this article is the presentation of a Lego methodology approach for Common Criteria that can be applied to IoT Telemetry systems [2]. This methodology allows to select security functions according to a specific use case, integrate various evaluated and non-evaluated components, plug-and-play (exchange, add, remove and update) new components, perform additional tests to demonstrate a higher robustness level of some security functions. As it was previously specified, the natural and unintentional threats will be excluded from this work activity. The attention will be focused on the intentional threats. These threats can also be classified into 3 categories, as follows [1]:

- **Depletion:** the targeted sectors of these threats are data and resource availability. As an effect, a resource will be consumed faster than it can be replenished. After a period of time, a resource which is being attacked becomes depleted, fact that affects the target functionality;
- **Alteration:** in this case, threats occur when an unauthorized entity tries to modify private code or data, affecting in this manner the integrity of the target;
- **Disclosure:** when talking about disclosure, threats will affect only the information confidentiality, especially specific system information, such as backup and temporary files, patch levels, version numbers software distribution, etc.

The article will be structured in 5 Sections. The current Section represents the introduction, having the main purpose of providing sufficient information for a general idea of the security risks impact. In Sect. 2 will be analyzed the present work activities in this field, being mentioned only the most notable research efforts. The methodology approach for Common Criteria can be seen in Sect. 3, while several scenarios of implementation will be presented in Sect. 4. The last section of this paper draws the conclusions and envisions future work.

2 Related Work

The innovative developments in the Information and Communication Technology (ICT) field produce various embedded things/devices which contain sensors and have the property to transfer data among other objects [3].

In the paper [4], a study has been conducted regarding the methods through which the equipment from a use case on a smart service in the industrial maintenance domain are securely transmitting their data. The paper examines two solutions focused on isolation and execution environment security, namely a Security Controller and the ARM TrustZone. For their comparison, a system that takes a device's snapshot authentication has been designed. The results demonstrate increased flexibility when using the TrustZone technology and a much secure physical environment for the Security Controller. Finally, it is conducted that the best approach is only based on the desired use case. The article also proposes a hybrid solution that increases the security of industrial applications, which could bring a contribution to the future Industrial Internet of Things (IIoT).

Furthermore, there is a recent survey about technical approaches, functional requirements, and on overall, the security status based on the OpenFog's [5] architecture. The OpenFog Consortium designed the Fog Nodes functional security requirements by adopting the Common Criteria standard. The Fog Nodes bolster a trusted computing environment as well as a secure service provisioning and also the hardware virtualization. Therefore, by using these entities, the multi-tier omnipresent communication-computing infrastructure which encompasses a multitude of devices and covers sophisticated hierarchies of application areas and administration, will have a more trusted environment due to increased security levels.

The IoT paradigm emerged into the car tracking technology, is being described in [6]. The paper describes the IoT's role in designing a car tracking system as well as the needed standards, principles in order to have an increased quality factor. Reliability engineering is the concept behind these standards. Common criteria plays an important role by assuring consistency and error management, these being the basic fundamental features a system must have to guarantee it matches the function for which it was designed.

3 Methodology Approach for Common Criteria - Lego Methodology Concept

The Common Criteria (CC) represents an international standard regarding computer security information (ISO/IEC 15408) [7]. Furthermore, Common Criteria is a framework in which SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) can be foreseen in an ST (Security Target) [8].

The CC assessment methods are performed on systems and computer security items. The product or the system which represents the subject of the evaluation is called Target of Evaluation (TOE). The evaluation has to examine if the security requirements are accomplished; this is performed through Protection Profile (PP), Security Target

(ST) and Security Functional Requirements (SFRs) [9]. The PP is a document created most often by the user or by the community and its major role is to detect security requirements for a class of security devices significant for a specific target. Retailers have the possibility to implement items that submit with one or more PPs, but they also can have their products evaluated against those PPs. In this particular case, a PP can be considered a template for the ST products. ST represents the document that identifies the security features of the main goal of the evaluation. The TOE is evaluated against the SFRs settled in its ST; this allows the retailers to suit the evaluation in order to match with the abilities of their item. SFRs stipulate the functions that can be provided by an item. Common Criteria has a specific list consisting of these functions, and the list can be different depending on the type of the evaluation even if the targets of the evaluation are the same type [10].

The evaluation procedure makes an attempt in the process of determining the degree of reliability of the product's security characteristics by quality assurance procedures, represented by SARs and Evaluation Assurance Level (EAL). SARs represent depictions of the actions carried out through the product`s evolution and evaluation to provide the supposed security functionality. The requirements from the CC catalog are documented in PP and ST. EAL is the numerical evaluation which describes the depth and the harshness of an evaluation. Each EAL is correlated with a package of SARs which includes the full development of an item. Common Criteria stipulates 7 levels of EAL, EAL1 being the most fundamental with low costs, while EAL7 is the most rigorous and the most expensive. Higher EAL does not suppose a more precise security, it only intends to assure that the TOE has been verified with higher accuracy [11].

3.1 Lego Methodology Concept

The 'Lego methodology' was developed to resolve the limitations introduced by the current composition approaches and concentrates on the evaluation of a list set in advance of Security Functions (SF) necessary in a use-case already existent [12]. This solution allows a global and unique Evaluation level (EAL LEGO) of the composite Platform with different robustness levels (Vulnerability ANalysis (VAN)-HIGH, VAN-Moderate, VAN-LOW) among security functions within the Platform (see Fig. 1).

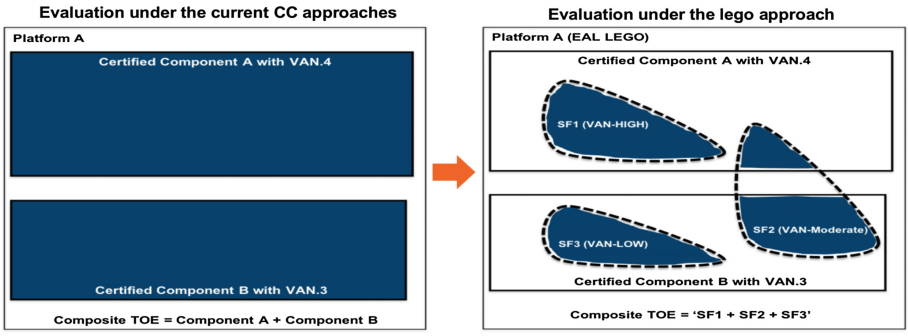

Fig. 1. Evaluation under current CC approaches vs. evaluation under Lego methodology approach

This methodology permits the selection of certain security functions related to a use case, the integration of different evaluated and non-evaluated parts, the installation and utilization of new components, and the execution of additional tests to demonstrate an increased robustness level of the security functions. This methodology leads to the following benefits:

- Evaluation with decreased effort, time and at low cost by reducing the perimeter of the evaluation, making the evaluation of the platform fast and easy;
- Dynamic plug-and-play integration by updating, adding, removing or replacing a Component with less effort;
- Possibility of obtain different robustness levels and increasing the level of robustness of required security functions within the system;

The following roles are considered in the Lego methodology:

- Component Developer: Entity developing the Component; it might also be the sponsor of the Component evaluation;
- Component Evaluator: Entity performing the Component evaluation;
- Component Certification Body: Entity performing the Component certification;
- Composite Platform Integrator: Entity integrating the Components in the Platform; it might also be the sponsor of the Composite Platform evaluation;
- Composite Platform Evaluator: Entity performing the composite Platform evaluation;
- Composite Platform Certification Body: Entity performing the composite Platform certification;
- Composite Product Evaluation Sponsor: Entity in charge of contracting the composite product evaluation.

In the concept of Lego Methodology, several suppositions are taken into consideration, such as: each Component is certified and completely specified, the objectives required by the working environment of each Component are well-defined, the Integrator should know the components functionality, the Platform has a fixed number of components in order to be certified, etc.

The described Lego methodology can be employed for demonstrating the compositional evaluation within a platform designed for security through isolation, called ODSI (On Demand Secure Isolation) [13]. The ODSI Platform combines the following independent certified components with different security levels (see Fig. 2):

(a) Configuration Manager: Certified Component was providing the Isolation security function (SF-ISO) between memory partitions. It is the base component on which the security of SFs DISP, AUTH, COMM and KEYM is built;
(b) Administration Manager: Certified Component providing the Dispatch security function (SF-DISP) of commands between partitions;
(c) Network Manager: Certified Component providing the Authentication (SF-AUTH) and the Communication (SF-COMM) security functions;
(d) Keyring Manager: Certified Component providing the key storage security function (SF-KEYM).

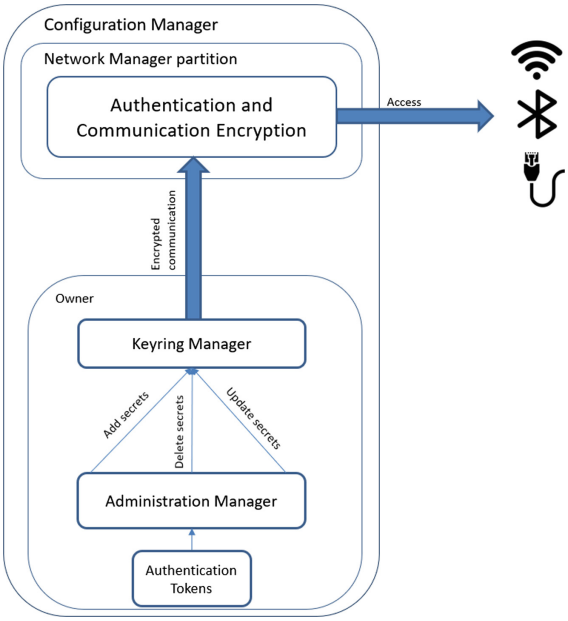

Fig. 2. The architecture behind the Network Manager, Keyring Manager and Administration Manager interaction

4 Scenarios of Implementation

In this section, there will be presented two scenarios of implementation, one being more of a general overview of the Lego methodology approach on increasing the robustness level of a SF within the CC Component and the other presenting the Agro-Telemetry use case that utilizes the CC compliant ODSI platform.

4.1 Scenario 1 - Increase the Robustness Level of a Given SF Within the Component

In this scenario, the re-evaluation effort will focus on testing that the SF1 can resist at a security level higher than VAN.3 and that no other part of the Component A1 can affect or decrease this security level.

A. Actors

The following Actors are considered in this scenario:

- Same Evaluator of the Component A1 and the SF1;
- Component Developer;
- Product Evaluation Sponsor:
  - This actor may be the Component Developer.

B. Assumptions

The following assumptions are considered for the evaluation under this scenario:

- Component A1 is CC-certified;
- The re-evaluation of SF1 and the evaluation of A1 will both be conducted by the same evaluation facility. The benefits of this assumption are the following:
  - a full evaluation of the Component A1 conducted by the new evaluation facility is not required;
  - delivery of all evaluation evidences (documents, source code, samples) to the new evaluation facility is not required;
  - the base evaluation results can be reused.
- The source code of the Component A1 is identical between the base certification and the reevaluation of SF1.

C. Inputs and Required Evidences

The following inputs are required prior to the evaluation under this scenario:

- ST, TDS (Target-of-Evaluation Design), FSP (Functional SPecification), ATE (Assurance TEsts) of the Component;
- SFRs that fulfill the SF1 are clearly identified and the rationale is provided in the Security Target;
- The SF1-Interfaces and Modules that implement the SF1 are described in the TDS and FSP Documents;
- Interactions between SF1-Interfaces and the other interfaces of the Components A1 are described in the TDS (TOE Design) document;
- SF1-Interfaces and Interactions are tested, and the conducted tests are described in the ATE Document.

D. Additional Requirements during Re-evaluation

The goal of the Lego certification within this scenario may be achieved by the following means:

- Requirements to be fulfilled by the Component Developer or the Product Evaluation Sponsor:
  - Additional information of each SF1-Interfaces may be required. This information will provide the evaluator with a better understanding of how this security function is performed. These additional details of SF1-Interfaces can be included in the TDS and the FSP documentation if the SF1-Interface is an external one (TSFI);
  - Additional information of the interactions between SF1-Interfaces and the other interfaces of the Component A1 may be required. This information will provide the evaluator a better understanding of how the SF1 interacts with the other parts of the component. These additional details about interactions can be included in the TDS;
  - The evaluator may require a characterization of the SF1-Interfaces at the implementation level (e.g. description of parameters passed from a SF1-Interface to another, variables, data identified for this SF1-Interface that are going to be used by other interfaces, return values from those interfaces, etc.). Such complete characterizations of SF1-Interfaces are meant to allow their exercise during reviewing and testing. These additional details can be included in the TDS and the FSP documentation if the SF1-Interface is an external one (TSFI);

  - Since they play no role in testing, it is not mandatory to describe at an implementation level the SF1-Interfaces that have no interaction with the other interfaces of the component;
  - Additional functional depth tests by the developer may be required to determine if all SF1-Interfaces and Interactions are completely tested. These additional tests can be provided in ATE.
- Requirements to be addressed by the Evaluator:
  - Compliance analysis of the updated evidences;
  - Additional penetration and/or independent tests by the evaluator may be conducted to determine if the SF1 is resistant at a level higher than VAN.3.

4.2 Scenario 2 – Agro-Telemetry System

In this scenario, it is presented the implemented Agro-Telemetry System. This system is used for precision agriculture and has two functions: data acquirement and data transmission along with processing. The first function allows sensors to collect data on temperature, humidity sunlight and actuators to execute commands in order to activate mechanic systems, such as irrigating. The data transmission and processing function illustrate the technique of sensor data transportation from the gateway to server; information is processed by the server and is presented to users through Web interface. This use-case handles two types of data: business and security data. Business data consists of raw information collected from sensors, representing the processed data produced by the server, while security data is residing on user credentials, log data, system configuration (see Fig. 3).

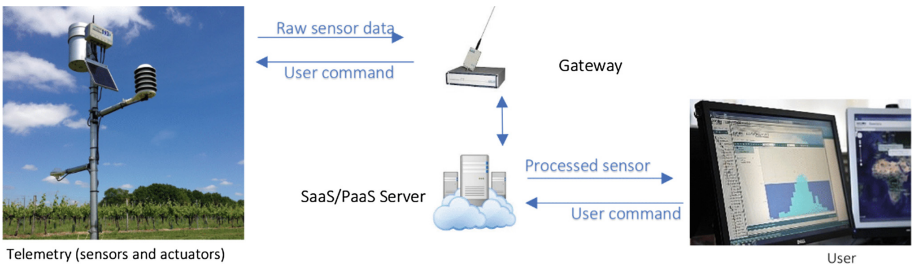

Fig. 3. Agro-Telemetry system

Table 1 concretizes the impacts of feared events.

Table 1. Impacts of all feared events

Severity	Example of feared event	Possible impact
Critical	Alteration of Business data	User commands are modified, causing over-irrigating
Critical	Disclosure of Security data	Hacker obtains user credentials to intrude Agro-Telemetry system by masquerading as Admin
Important	Unavailability of Data Processing function	Agro-Telemetry system cannot process sensor data, causing abnormal situation in the farm undetected

Regarding the threats analysis, there will be described some examples of contra measures to each threat that relates to a feared event. When alteration of Business data is involved, a man-in-the-middle attack may interfere on the network. As a contra measure, a deployment of an ODSI token verification service for user authentication will be performed. This action is provided by the Network Manager whose Certified Component supplies the Authentication (SF-AUTH) and the Communication (SF-COMM) security functions. Disclosure of Security data implies threats on the gateway such as the side-channel attack which can be prevented by deploying a technique called ODSI end-to-end encryption that embodies the Certified Component of the Administration Manager which provides the Dispatch security function (SF-DISP) of commands between partitions. Considering the unavailability of the Data Processing function, a possible threat accomplished on the server is the Denial of Service (DOS) attack which can be countered when an ODSI isolation BIP technique is deployed on the server through the Configuration Manager's Certified Component which provides the Isolation security function (SF-ISO) between memory partitions.

5 Conclusions

As shown in this paper, Lego Methodology offers an encouraging and feasible way in order to extend the current CC approach to support and facilitate composition and allow the evaluation of IoT platforms. The Lego Methodology applied on ODSI platform allows a secure communication with a remote entity, end-to-end encryption, key management and secure storage without the limitations brought in by the present composition approaches. As future work we envision developing an application in a real-world context and perform the compositional evaluation.

Acknowledgements. This work has been supported in part by UEFISCDI Romania through projects ODSI, ToR-SIM and PARFAIT, funded in part by European Union's Horizon 2020 research and innovation program under grant agreement No. 777996 (SealedGRID project) and No. 787002 (SAFECARE project).

References

1. Jouini, M., Rabai, L.B.A., Aissa, A.B.: Classification of security threats in information systems. Procedia Comput. Sci. **32**, 489–496 (2014)
2. da Cruz, M.A., Rodrigues, J.J., Paradello, E.S., Lorenz, P., Solic, P., Albuquerque, V.H.C.: A proposal for bridging the message queuing telemetry transport protocol to HTTP on IoT solutions. In: 3rd International Conference on Smart and Sustainable Technologies (SpliTech), pp. 1–5. IEEE (2018)
3. ETSI France, Orange France: Internet of Things Global Standardisation-State of Play (2018)
4. Lesjak, C., Hein, D., Winter, J.: Hardware-security technologies for industrial IoT: TrustZone and security controller. In: IECON 2015-41st Annual Conference of the IEEE Industrial Electronics Society, pp. 002589–002595. IEEE (2015)

5. Martin, B.A., Michaud, F., Banks, D., Mosenia, A., Zolfonoon, R., Irwan, S., Zao, J.K.: OpenFog security requirements and approaches. In: IEEE Fog World Congress (FWC), pp. 1–6. IEEE (2017)
6. Thomas, M.O., Rad, B.B.: Reliability evaluation metrics for internet of things, car tracking system: a review. Int. J. Inf. Technol. Comput. Sci. (IJITCS) **9**(2), 1–10 (2017)
7. Bialas, A.: Common criteria IT security evaluation methodology–an ontological approach. In: International Conference on Dependability and Complex Systems, pp. 23–34. Springer, Cham (2018)
8. Communications Security Establishment. https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/main. Accessed 01 Oct 2018
9. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 4 (2012)
10. Common Criteria for IT security evaluation. https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2017_50en.pdf.pdf. Accessed 01 Oct 2018
11. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5 (2017)
12. Chae, H., Lee, D.H., Park, J., In, H.P.: The partitioning methodology in hardware/software co-design using extreme programming: evaluation through the lego robot project, pp. 187. IEEE (2006)
13. Suciu, G., Istrate, C., Petrache, A., Schlachet, D., Buteau, T.: On demand secure isolation using security models for different system management platforms. In: Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies IX, vol. 10977, p. 109770R (2019)