

Cybersecurity Management Throughout the IoT Systems Lifecycle - the CERTIFY Approach

Stefano Sebastio^{1,3}[0000–0001–8905–9874], Sara Matheu^{2,3}[0000–0002–7997–5737], Antonio Skarmeta^{2,3}[0000–0002–5525–1259], Riccardo Orizio^{1,3}, Dimitris Karras³, Daria Schumm³, Burkhard Stiller³, Rosella Omana Mancilla³, Francesca Giampaolo³, Simon Tuck³, Thomas Bocek³, Vincenzo Cuomo³, Roland Atoui³, Sreedevi Beena³, Roberto Nardone³, Alessandro Cilardo³, Dinesh Sharma³, Rohit Bohara³, and Javier Parra-Domínguez³

¹ Collins Aerospace, Cork, Ireland
{stefano.sebastio, riccardo.orizio}@collins.com

² University of Murcia, Murcia, 30100, Spain
{saranieves.matheu, skarmeta}@um.es

³ The CERTIFY Consortium

Abstract. Cyber-attacks get more sophisticated every day, potentially affecting a large number of Internet of Things (IoT) -based infrastructures and raising security and privacy concerns in consumer and business products. The EU Cybersecurity Act (CSA) first and the Cyber Resilience Act (CRA) more recently have established the pivotal role covered by a cybersecurity management encompassing the full lifecycle of products and services, and a continuous certification process. CERTIFY defines a methodological, technological, and organizational approach towards IoT security lifecycle management. To ensure security compliance throughout the device lifetime, CERTIFY designs and implements a cybersecurity lifecycle management framework for IoT devices. The framework is intended to support the device security management by collecting and sharing relevant security information both internally (via monitoring and attestation services) and externally, e.g., by interacting with device manufacturers, threat databases, certification authorities, Information Sharing and Analysis Centers (ISACs), and more. The received information is meant to support a local decision making with respect to the security monitoring, updating, and configuration of the device. Moreover, this information sharing will enable a continuous risk assessment, gathering evidence that could agile future recertifications. CERTIFY provides IoT stakeholders with mechanisms achieving high-level of security to detect and respond to a wide spectrum of attack, in a collaborative and decentralized fashion. CERTIFY will validate the architecture through cutting-edge use cases and pave the way towards innovative security in a broad spectrum of IoT environments.

Keywords: Systems security · Security services · Hardware security implementation · Embedded systems security.

1 Introduction

Countless Internet of Things (IoT) devices get connected to the Internet every day, collecting, processing, and/or sharing massive amounts of information. The advent of 3GPP 5G [1] constituted a game-changer for massive IoT systems. However, enhanced connectivity in resource-constrained IoT devices coupled with the high amount of sensitive data they are managing, makes these systems a desired target for hackers. The Marriot⁴ and Colonial Pipeline [2] cyberattacks are just two most recent and known examples of successful hacks of IoT systems. As IoT systems manage more critical and sensitive data and infrastructures, attacks are expected to be ever more frequent and sophisticated. An estimated total cost of a data breach shows an increase of \$3.86 million in 2018 to more than \$4.45 million in 2023 (that is, an increase of approximately 15% in less than 5 years) [5]. This scenario caused a raising concern over security and privacy for both consumer and business products.

Recent EU initiatives such as the Cyber Security Act (CSA) [3] and the Cyber Resilience Act (CRA) [4] have stressed the importance of providing duty of care for the entire lifecycle of the products and the role of certification towards an effective cybersecurity management. Despite the marking of these pivotal milestones, their adoption to IoT-based systems is a non-trivial task. Heterogeneity, dynamic security landscape, and number of stakeholders part of the value chain complicate the scenario. Indeed, a single insecure device could hamper the security posture of the whole system. To that end, another key EU directive on cybersecurity, Network and Information Security (NIS) 2 [6] fosters a culture of cooperation in information and network security.

2 Objectives

CERTIFY aims at providing IoT stakeholders with tools and mechanisms necessary to achieve a guaranteed level of security, by empowering them to detect, evaluate, and respond to virtually any possible attack in a collaborative and decentralized fashion throughout the entire lifecycle of IoT-enabled systems. The CERTIFY methodology is based on international standards and frameworks (e.g., MUD file [7] and Zero Trust [8]) and poses the sharing of information and security evidence among stakeholders (e.g., auditors, manufacturers, users, Information Sharing and Analysis Centers - ISACs) at its core. Moreover, this information sharing will enable a continuous risk assessment, gathering evidence that could agile future recertifications.

The CERTIFY project works toward designing and implementing a novel framework for managing the cybersecurity of network-connected IoT devices throughout their whole lifecycle. Indeed, we advocate that only a holistic way of managing device security can strengthen cybersecurity resilience while providing an opportunity for cost reduction. The CERTIFY cybersecurity lifecycle management framework is based on: i) security by design; ii), continuous security

⁴ <https://techcrunch.com/2022/07/06/marriott-breach-again/>

assessment and monitoring; iii) timely detection, mitigation, and reconfiguration; iv) secure device update; and v) security information sharing. The CERTIFY objectives can be summarized as follows:

- Cybersecurity situational awareness for IoT-enabled environments through a multi-stakeholder sharing of threats and mitigations.
- Secure reconfiguration and maintenance of customizable embedded devices by means of open hardware primitives and services.
- Perform security operational management based on bootstrapping, enrolment, attestation and monitoring of attacks and malicious behaviors.
- Foster knowledge delivery via wide dissemination, capacity building and supporting standardization activities.
- Validation of the CERTIFY framework in diverse IoT-enabled ecosystems.

3 Cybersecurity Lifecycle Methodology for IoT Systems

The CERTIFY lifecycle (pictorially represented in Figure 1) starts with the *design* of the device. At that time requirements are considered, the risk assessment is performed considering the target application domain and a certification may be requested. Moreover, keys, certificates and behavioral profiles used during the enrollment are built and securely stored by the manufacturer (some information are stored on the device while others remotely). Once deployed, the device *bootstrapping* takes care of the secure boot, enrollment, and configuration in the domain. During *operations*, device attestation and monitoring are performed to identify the presence of any suspicious event. New threats, vulnerability and patches may be identified by exploiting internal and external information. These may summon *update*, upgrade and reconfiguration. Changes performed on the device and an evolved threat landscape are also considered while collecting the evidence needed for a continuous risk assessment and the potential need to trigger a device recertification. A complete lifecycle includes also the case of device *repurposing* (i.e., when it no longer fulfills a given purpose) and *decommissioning* (requiring the proper application of data cleaning policies and default reconfiguration).

3.1 Dealing with Cybersecurity Changes

In today's rapidly evolving digital landscape, it is essential to address cybersecurity dynamically. This requires proactively assessing the impact of each change and adapting accordingly at the appropriate level. Changes happen regularly as a consequence of new or revised code, as well as of evolution of the threat landscape. Assessing and classifying (e.g., in minor, major, or non-interfering) the impact of these changes is crucial. Indeed, in case of major impacts, a deeper evaluation needs to be conducted to determine the security changes required to preserve a secure state.

The CERTIFY process ensures continuous cybersecurity compliance and risk management by dynamically analyzing the impact of changes on devices and continuously monitoring the security certification status. It considers:

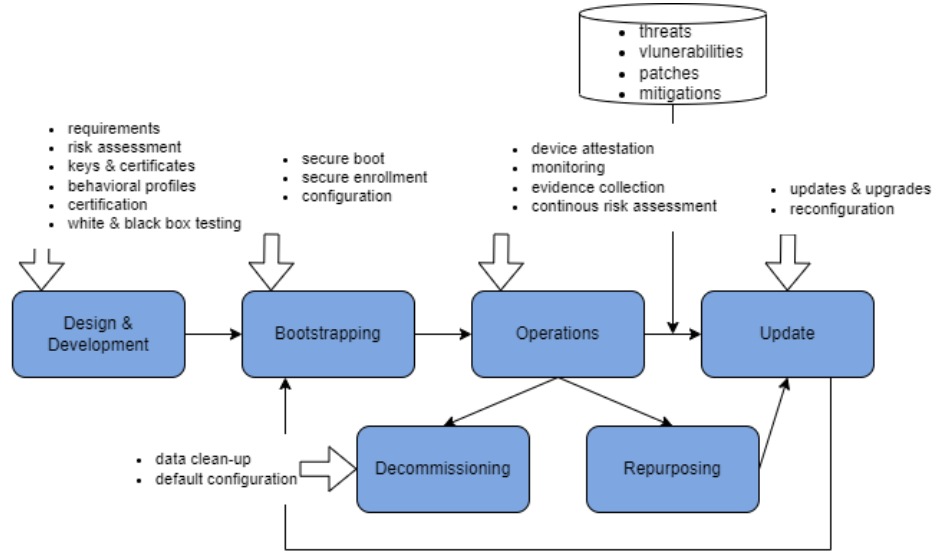


Fig. 1. The enhanced cybersecurity lifecycle in CERTIFY.

- continuous impact assessment: any changes made to IoT devices, or their environment will be continuously and dynamically monitored in real-time.
- automated evaluation: evaluate changes (exploiting also past events for prediction) and decide if a re-evaluation or re-assessment is necessary.
- real-time monitoring and reporting: a dashboard continuously updating the certification status, reflecting any changes made to the device or its environment, and alerting relevant stakeholders when appropriate.
- continuous re-evaluation and re-assessment: processes performed continuously ensuring that the device is always evaluated against the most recent threat landscape.
- recertification service: the overall device, including any new software from the manufacturer, can be (re-)certified according to the latest secure configuration and updated knowledge on related threats collected during operations.

The information sharing mechanism posed at the heart of the CERTIFY methodology incorporates external and internal knowledge. Indeed, by knowing the actual configuration of the devices performed by the domain owner, and the threats identified during operations either in the domain (through runtime monitoring and intrusion detection) or externally by the manufacturer or ISACs (Information Sharing and Analysis Centers), it is possible to build a more accurate and updated picture of the risks. Moreover, CERTIFY eases a continuous certification, by (i) allowing device manufacturers to update the product details, (ii) providing access to all the relevant information to the certification bodies for review and evaluation, and (iii) displaying the current certification status.

3.2 Cybersecurity in each Phases of the Lifecycle

IoT-enabled services require a comprehensive and adaptive management of the cybersecurity throughout their lifecycle. Indeed, as emphasized by the EU CSA and CRA, a more trustworthy digital ecosystem is achieved only through certification and a management of the entire product lifecycle. Security by design practices, continuous certification and compliance, and collaboration among stakeholders in charge of monitoring the device status are key components. The CERTIFY cybersecurity lifecycle management framework is intended to monitor, update, assess and configure the device according to the security information received both internally (self-assessment, attestation and monitoring) and externally (e.g., manufacturer, threat databases, certification authority). At the same time, the framework will share the relevant security information with the external sources, in a symbiotic way.

Manufacturing: Design and Development. In this phase, the device is designed, created, programmed, and tested, so the initial level of security is established. In this stage, all the actors in the supply chain (i.e., component designer, integrator, software and library developer) are part of the process, while the manufacturer is responsible for carrying out the initial security evaluation of the device. Adoption of best security practices for design, production and testing can ensure an adequate implementation. As new vulnerability and threats are continuously discovered, defining a comprehensive and common standard methodology for cybersecurity testing, evaluation and certification is a complex task. On the one hand, the wide variety of schemes and requirements hardens the goal of an objective comparison on the achieved security and between certified products. On the other hand, the context (regulation, domain, etc.) determines the security level required for a particular product and thus needs to be considered. This problem is exacerbated by out-of-date certificates that offer a false sense of security.

To tackle this inherent dynamism in cybersecurity, CERTIFY will consider a security evaluation and certification approach based on modeling, allowing to test the design of the device from the very beginning and automating the security assessment by combining security testing and risk evaluation toward an objective and automated process. CERTIFY will explore approaches to also benefit from information collected during deployment and operations. The results of continuous evaluation can be embedded in a *behavioral profile* associated with different levels of security with some recommendations (policies) to consider during operations. This profile reduces the attack surface, and it could be used to monitor suspicious behaviors during operations. The behavioral profile is based on an extension of the MUD standard [7] and contains both security recommendations from the manufacturer and from the certification to perform a secure deployment. In particular, the use of the MUD, will be extended to create augmented security profiles to govern the intended behavior of IoT devices throughout their lifecycle.

Deployment and Bootstrapping. The deployment includes the domain and network configuration of the device according to specific processes and procedures. During the bootstrapping the configuration *pre-provisioned* by the manufacturer is used. It includes cryptographic material (i.e., certificates, keys and related parameters), statically configured during the device manufacturing. This is used during the device bootstrapping and domain enrollment to derive the cryptographic material used in operations. The need to reduce the attack surface since the device joins the target domain has been manifested by recent botnets attack [9]. Thus, beside access control techniques and secure boot, ensuring that the device behaves as expected starting from its initial actions in the network is also needed.

To address such challenge (even more complex in massive IoT systems), the IETF Manufacturer Usage Description (MUD) standard aims to define the intended behavior of the device through Access Control Lists (ACLs). These restrict the communication to/from a certain device. With the MUD file, policy requirements for a device joining the network can be translated to network access specific policies. However, the MUD specification is focused on the definition of network access control policies, which is insufficient to establish enough countermeasures. Moreover, the standard does not give any indication on how to translate and enforce the MUD policies. In CERTIFY, the extended behavioral profile generated during the manufacturing phase will guide the deployment of such recommendations before the device is able to access the network. Therefore, the device will not be allowed to interact with other components or access network resources until it is not properly identified, configured, and authenticated, ensuring that the network will not be compromised once the device has access to it.

Operations. In this phase, the device should be monitored, since new security vulnerabilities and threats can be discovered or a new patch/update can be installed. Consequently, the device security level goes through a continual change. Therefore, a continuous reassessment should be done and a recertification process should be started if needed. Attestation and monitoring are two key approaches to cybersecurity. Runtime attestation leverages the Root of Trust (RoT) to provide signed evidence about the integrity of the device to verify that it has not been tampered with. Monitoring includes a wide set of solutions from network protection (e.g., Intrusion Detection Systems - IDS) to malware detection. Detection techniques are often categorized into signature and behavior-based techniques. Signature-based intrusion detection approaches seek for runtime traces matching a specific pattern of malicious behavior while behavior-based approaches look for anomalous runtime features. To overcome potential limitations in the achieved accuracy, the Security Information and Event Management (SIEM) technologies provide insightful correlation of security information monitored from different sensors, enhancing the detection of security threats.

The CERTIFY cybersecurity lifecycle management framework integrates monitoring and attestation techniques with secure configuration deployment, assessment and information sharing. By linking the runtime detection with the mitigation suggested by manufacturers, threat databases, or certification authority (e.g., update or new configuration), it is possible to timely protect device and system once a vulnerability is identified. In CERTIFY such an information exchange is enabled by an extension of the threat MUD [10]. Moreover, CERTIFY will combine the security evaluation methodology developed during the manufacturing phase with runtime metrics used for a continuous security evaluation (including e.g., information about key lengths, protocols, ports). In the deployment stage of the device, the computed security risk can be used to deny network access to the device if a critical risk for the other network components is supposed to take place. Throughout the device lifecycle the runtime evaluation determines if the configuration of the device must be changed to maintain an adequate level of security. CERTIFY envisions a continuous communication among stakeholders by integrating security information received from external sources with the one collected in the domain. Despite the proliferation of Cyber-Threat Intelligence (CTI) solutions, issues concerning security, trustworthiness, privacy and provenance still exist. CERTIFY contributes to such a challenge with a privacy preserving CTI solution. Thanks to the extended threat MUD file information about new vulnerabilities, updates, patches, reconfigurations, potential zero-days attacks is exchanged. This knowledge is also useful when assessing how a modified threat landscape affects devices' operations and their software, and if there is a need for recertification.

Update. This phase involves procedures related to software updates or patches proposed by the manufacturer, as well as configuration tasks requested by the domain manager, which can also influence the security level achieved. Constraints posed by device and network resources increase the complexity of the update delivery calling for efficient approaches to deal with the requirements of manufacturers, software providers, end users and devices. In particular, the realization of a secure update/patching process requires suitable protection of software images, so that only legitimate and authorized software providers are enabled to update a certain device through a secured software. Furthermore, the communication of such software/firmware should be based on lightweight representations, as well as efficient cryptographic algorithms and security mechanisms to be used even in resource-constrained devices and networks. Several standardization activities, such as the IETF Software Updates for Internet of Things (SUIT) working group in 2017, have been established to develop a secure solution for the software/firmware update process in IoT environments. In particular, the SUIT solution defines a communication architecture and the information model of manifest files to describe firmware images based on recent security standards, such as the CBOR (Concise Binary Object Representation) Object Signing and Encryption (COSE) protocol. However, these efforts are mainly focused on communication security aspects, and they must be combined with additional techniques to man-

age the complexity of IoT systems and deployments such as dependencies among software components and their different versions. Moreover, scalability (and efficiency) issues must be examined in scenarios where a large number of devices needs to be updated.

More recently, distributed ledger technologies - DLT (e.g., blockchain) have attracted interest as a building block for managing updates. The EU Blockchain Observatory and Forum, and lately the International Association for Trusted Blockchain Applications (INATBA), promote a common approach for the interoperable deployment of blockchain solutions. The DLT could be leveraged for software updates by providing a transparent ledger to manage the different versions of software elements composing an IoT device or system. E.g., each manufacturer could be represented by a blockchain node sharing software components' information, including software versions, associated vulnerabilities, or other data. Manufacturer, business sector or country of operations could also pose security and privacy restrictions. In such a case limits persists as multiple implementations could hamper interoperability. CERTIFY explores the interledger approach to interconnect different DLT implementations through an interoperable and efficient framework.

Decommissioning and Repurposing. As the threat landscape evolves, the device may need to be reconfigured, updated, or upgraded. At some point, the changes required to maintain the assurance level of a given domain (dispatched through the extended MUD file) could not match anymore resources and capabilities available on the device. For example, a patch may require more storage space than what is available considering how the device is used in the domain, or a mitigation is so severe to require a re-design of the chip and the device might not possess all the hardware features required for the mitigation to be successful. In such a scenario two main options are left: repurposing and decommissioning. In the first instance, a subsystem with different cybersecurity requirements is identified, and the device can be repurposed to fulfill its new role. The device is reconfigured before reuse, offering an opportunity for cost saving. In the latter case, if the device cannot respect anymore the assurance level required by the domain, or if the discovered vulnerability raises new security risks and the suggested mitigation process cannot take place, the device is decommissioned. The decommissioning process ensures that no information previously stored is leaked. This process executes proper clean-up policies on confidential data used for the device deployment (e.g., digital certificates, secure keys) and collected during operations (e.g., data stored in memory and involving intellectual properties). All in all, the device is restored to the manufacturer's default configuration ensuring that all information related to the domain operations is properly erased.

4 Use Cases

CERTIFY will validate the architecture through cutting-edge use-cases later extended with the definition of a stakeholders demonstration. The three use cases part of the project are:

- Secure device management in a connected aircraft cabin system: the deployment of a multitude of IoT connected devices will usher in the era of intelligent aircraft cabin where availability, integrity and confidentiality for software and data running over them must be preserved.
- Smart micro-factories: smart production environments are merging Operational (OT) and Information Technology (IT) building a pervasive computing system that includes also legacy components.
- Tracking and monitoring of artworks: ensuring that artworks are properly handled during their transport and exhibition is a main concern for all the involved stakeholders (owner, courier, insurer, museum, etc.). Such a challenge can be addressed by adopting lightweight embedded devices attached to the artworks and acting as black box by logging events during transport.

5 Conclusions and Future Work

CERTIFY inherits from recent EU initiatives such as CSA, CRA and NIS-2 the core role covered by certification, lifecycle management and information sharing. Indeed, in its framework CERTIFY considers: i) current certification status and reports, as baseline for describing the security profile of a device including security controls, policies, recommended configuration (by means of the extended MUD) and assurance level according to domain of deployment; ii) behavioral profile, as a way of describing the expected functioning of the device; iii) threat modeling and risk assessment, that from a baseline built at design time is continuously updated thanks to the information sharing and the usage of the threat MUD; iv) change impact analysis, to dynamically understand, from internal and external information, how changes in the threat landscape, and applied security controls and policies may impact the security posture of the system; v) recertification from testing results, by leveraging a complete assessment of the reached security level and exploiting the artifacts collected throughout the device lifecycle to request and support an agile recertification process in case the device should not meet anymore the requested Security Assurance Level (SAL).

In a nutshell, CERTIFY is like a watchdog that makes sure that certified IoT devices are maintaining their level of assurance during the whole lifecycle. Since the onboarding phase, CERTIFY provides domain owners with the information to securely configure the device and use it in the intended operational environment. During operations, in case a change occurs, it does so by collecting threats and dispatching mitigations through the extended (threat) MUD file. In case such a change impacts the certification status, authorities and the manufacturer can exploit the information sharing enabled by CERTIFY.

As next step, CERTIFY will complete the development of its architecture and validate its approach through its three use cases. Its ultimate aim is to pave the way toward innovative security in a broad spectrum of IoT environments thanks to the definition of stakeholders demonstrations that can foster engagement with relevant actors and ensure sustainability of the results.

Acknowledgments. Research partially supported by the EU through the Horizon research and innovation program CERTIFY (grant agreement no. 101069471) and the Swiss SERI (grant agreements no. 22.00165 and 22.00191). The European Commission’s and Swiss SERI’s support for the production of this publication does not constitute an endorsement of the contents, which reflects the views of the authors only, and neither the Commission nor the Swiss Confederation can be held responsible for any use which may be made of the information contained therein.

References

1. 5G System Overview, <https://www.3gpp.org/technologies/5g-system-overview>. Last accessed 14 Mar 2024
2. Colonial Pipeline hack explained: Everything you need to know, <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>.
3. European Union (EU): Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
4. European Union (EU): REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454>
5. IBM Security: Cost of a Data Breach Report 2023. IBM (2024)
6. European Union (EU): DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). <https://eur-lex.europa.eu/eli/dir/2022/2555>
7. Lear, E., Droms, R. and Romascanu, D.: RFC 8520 Manufacturer Usage Description Specification. In: RFC (2019), <https://doi.org/10.17487/RFC8520>
8. Rose, S., Borchert, O., Mitchell, S. and Connelly, S.: Zero Trust Architecture. In: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD (2020), <https://doi.org/10.6028/NIST.SP.800-207>
9. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas: DDoS in the IoT: Mirai and Other Botnets. In: Computer, vol. 50, no. 7, pp. 80-84, IEEE (2017), <https://doi.org/10.1109/MC.2017.201>
10. NIST: Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD). In: NIST SPECIAL PUBLICATION 1800-15B (2021), <https://doi.org/10.6028/NIST.SP.1800-15>