IoT Security Assessment through the Interfaces P-SCAN Test Bench Platform

Thomas MAURIN
Univ. Grenoble Alpes
F-38000, Grenoble, France
CEA, LETI, MINATEC Campus,
F-38054, Grenoble, France
thomas.maurin@cea.fr

Laurent-Frédéric DUCREUX
Univ. Grenoble Alpes
F-38000, Grenoble, France
CEA, LETI, MINATEC Campus,
F-38054, Grenoble, France
laurent-frederic.ducreux@cea.fr

George CARAIMAN
LCIE Bureau Veritas
Fontenay-aux-Roses, France
george.caraiman@lcie.fr

Philippe SISSOKO
LCIE Bureau Veritas
Fontenay-aux-Roses, France
philippe.sissoko@lcie.fr

***Abstract* — The recent, massive and always-growing usage of communicating objects exchanging data over interconnected networks makes these objects vulnerable to cyber-attacks. Ranging from mainstream industrial devices to IoT products, the P-SCAN test platform is designed as a convenient solution to democratize connected objects security assessment. Associated to guidelines easing the definition of a device security target, the platform provides a library of test suites which enables automating the process of testing security features on the device's communication interfaces. As technologies evolve, the platform is designed to be scalable and customisable (new interfaces, new standard test suites, specific test cases with respect to new Common Vulnerabilities and Exposures) to detect potential vulnerabilities.**

This paper explains the identified business needs and market segment, the related value proposition and gives an overview of the provided technical solution.

Keywords — Internet Of Things, IoT security assessment, automated security testing, interface testing, vulnerability detection

I. Introduction

Due to the significant added value provided by connected devices, the Internet of Things (IoT) has been a hot topic for the past several years and their adoption has been rapid. Moreover, enhancing a typical legacy industrial device with connectivity features drastically widens the frontiers of its manufacturer's historical business field.

But, as providers first focused on functional features, power consumption or communication capabilities, security aspects of the developed and deployed solutions were at the bottom of the list of priorities. However, as IoT spreads in virtually any kind of installations, it is now perceived as a new entry door for malicious people or organizations. Stuxnet worm, Mirai botnet or Saint Jude Medical Pacemakers massive recall, cyber-attacks examples mentioned in mass-media definitely raise public awareness on the threats of unsecured IoT.

Mainstream security is now mandatory to ensure sustainability of all IoT businesses, making the security assessment of this wide, heterogeneous market a real challenge.

To tackle this issue, Bureau Veritas (BV) and CEA Leti joined forces to develop an innovative approach to IoT cybersecurity testing, tailored to the market needs [1].

II. Cybersurity of Iot Devices

A. Iot Devices and Market Penetration

The IoT is built upon the concept of remotely monitoring and controlling something via a connected solution. This is made possible by embedding connectivity features to new devices or enhancing legacy ones with added sensors, actuators and communication capabilities. That is the case for Operational Technology (OT) devices – traditionally associated with manufacturing and industrial environments with strong safety concerns, and their modernization through convergence with Information Technology (IT). Hence, any IoT device exposes communication interfaces through which it is configured, operated, monitored, upgraded and maintained. We define here an interface as the combination of a hardware media (wired connector, wireless chip) and a communication protocol stack upon which the device is accessed.

The attack surface is the whole set of vulnerabilities that can be potentially exploited by an attacker of a device or a communication network. As each IoT device integrates at least one or several communication interfaces, the huge and increasing number of connected *Things* (20 billion in 2020 [2]) expands the overall attack surface of the global IoT world into unprecedented proportions.

Besides, IoT devices are the low-hanging fruits for potential attackers: they are fairly easy to compromise and may be connected to high-value networks. The detection of ongoing attacks is highly unlikely without a constantly modernized toolkit and deep state-of-the-art knowledge of cyber-attacks.

As long as consumers or industrial users of IoT devices may not all be aware of such requirements, security complexity must be abstracted to them. They should accept to rely on renowned trusted third-parties who provide trustworthy security assessments, labels and certifications.

Moreover, in order to establish or extend their business, IoT solution providers can not just gage the cyber risk. They must

definitely mitigate it "by design". At least, they have to ensure that security concerns are properly taken into account during the development process and that the shipped products meet the expected (even implied and not standardized) and adequate security levels, as claimed by ENISA and major European device manufacturers [3]. Providing solutions with security warranties, assessed by external independent trusted third-parties constitute a market differentiator, which is becoming an increasingly important criterion.

To raise the global security level of connected devices, recent IoT standardized communication protocols integrate security features or define guidances, to be implemented by manufacturers to protect the device, its data and its users. Tools or methodologies to assert standard implementation correctness are not always available. And as the protocols embed even more features (even security ones), they get more prone to implementation flaws [4].

B. Existing Cybersecurity Evaluation Possibilities

Most existing mainstream cybersecurity offers come from the IT field (computer, storage, networking devices…), inherently managing communications and data/system security concerns. They are not adapted to the IoT paradigm where devices embed usually lower computation resources, various (often proprietary) protocols over a large panel of media: ZigBee, BlueTooth, WIFI, NFC, USB, CAN, JTAG but also Cellular, LoRa or ETHERNET…

Common Criteria for Information Technology Security Evaluation (CC) and associated Common Methodology (CEM) provide a framework to deliver evaluation within an international agreement scheme. Evaluations driven by ITSEF-licensed laboratories check the consistency of the product's security target (the crossover of the common protection profile and the specific product features). CC is mainly dedicated to IT products with strong security concerns such as banking, access control or governmental applications. CC evaluation's complexity, delay and costs are too restrictive in regards of most IoT commercial and technical requirements.

Some standards are emerging to complement legacy OT standards like the future IEC62443-4-2 "Technical Safety Requirements for IACS components" or attempting to structure a minimum baseline assessment upon private scheme [5]. Evaluation and certification tools start to integrate cybersecurity testing on the basis of legacy OT safety conformance or IT pen testing approaches.

In this global context, we envision a growing market niche where security evaluations are tailored to meet the concerns of the IoT providers.

III. P-SCAN APPROACH

The P-SCAN offer is based on a highly automated cyber-security service where *(i)* assessment of security features is performed though the communication interfaces *(ii)* with respect to the device's complexity and relevant low-to-medium security level *(iii)* in accordance to IoT business constraints (quick-to-market, incremental, low-cost) and *(iv)* managed by a trusted third-party.

P-SCAN is a highly configurable and scalable automated test-bench. Its architecture is inspired from research work conducted in the Security dept. of CEA Leti [6]. It is composed of a main tester station driving several access-heads (AH). AHs hold the specific components required to challenge security functions implemented in the evaluated device, through all its interfaces. Collections of security test cases are available in an incremental library, grouped by test suites (a collection of test cases dedicated to testing a given security feature).

An evaluation methodology is also specified. It will be shared with BV's clients in order to define with them specific security targets, to ensure that technical and documentary requirements are met to enable relevant evaluations to be carried out under the suitable conditions to produce the expected results. Then, the operator from BV responsible for the evaluation will define the appropriate test plan by selecting and parametrizing the relevant test cases made available in the test library. This library is regularly updated by CEA-Leti's security engineers with new test cases targeting new protocol layers, new CVEs and state-of-the-art possible vulnerabilities. Once parametrized accordingly, the test plan is automatically run and P-SCAN produces an evaluation report and clear Boolean verdicts for all executed test cases.

IV. CONCLUSION

In this paper, we describe some aspects related to the cybersecurity for IoT. We identify a niche in a promisingly growing market and tailor an offer to respond to the associated segments' needs. This offer is built upon following assets: *(i)* a rigorous methodology defined by seasoned security experts, *(ii)* a strong, relevant and coherent partnership between BV and CEA-Leti, which combines scientific and technical excellence, worldwide recognition and trusted renown parties in security and evaluation areas, and *(iii)* a dedicated powerful tool which will meet demanding technical and business requirements such as high automation and incremental scalability capabilities associated with optimized operational costs.

We believe that with such an approach, we will help providers in their device development. The issuance of a future BV "cybersecurity for IoT" label would also bridge the gap towards the current security assessment certifications.

REFERENCES

[1] R. Hooper, A. Dell "Bureau Veritas to Unveil Disruptive Approach to Cyber Security Testing and Innovative Smart Wear Testing Solution at Mobile World Congress", February 2017

[2] Gartner "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", Feb. 2017

[3] ENISA "Infineon – NXP – STMicroelectronics – ENISA Common Position On Cybersecurity", December 2016

[4] B. Seri, G. Vishnepolsky, "BlueBorne Technical White Paper", 2017

[5] UL "UL2900-1 Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements", Sept. 2016

[6] J.C. Fonbonne, "Automated and Remote Security Fuzz Testing Tool for IoT Devices", C&ESAR 2016, Nov. 2016