EasyChair Preprint

№ 10470

Smart, Reliable, and Secure Systems for Emergency Management and Crisis

Mohammad Beyrouti, Abdelmadjid Bouabdallah,
Abed Ellatif Samhat, Ahmed Lounis and Benjamin Lussier

June 28, 2023

Smart, Reliable, and Secure Systems For Emergency Management and Crisis

Mohammad BEYROUTI
Directeurs de thèse : Abdelmadjid BOUABDALLAH, Abed Elatif SAMHAT (LEBANESE UNIVERSITY)
Encadrants : Ahmed LOUNIS, Benjamin LUSSIER
Équipe : SCOP, HEUDIASYC - UMR CNRS 7253

***Abstract*—The idea behind the Internet of Things (IoT) is to connect not only people and computers but also smart things like sensors, actuators, and control systems, enabling them to share and process data over the internet. IoT systems are valuable for emergency management because they can collect data from various smart objects, facilitating centralized decision-making. However, challenges related to operational safety and security must be addressed to ensure the reliability of IoT in critical applications. The objective of this thesis is to tackle these challenges by proposing a mechanism called the 2S-bag (safety-security bag), extending the rules checking from the already known Safety-bag components to both safety and security. This proposed mechanism continuously monitors and verifies safety and security requirements, thereby enhancing the reliability of IoT systems.**

***Index Terms*—Vulnerability assessment; attack scenario identification; security; safety; IoT healthcare; defensive mechanisms; fault tolerance.**

I. INTRODUCTION

The swift growth of IoT devices across different domains has created significant dependability challenges. Some key challenges encompass guaranteeing safety, integrity, confidentiality, and availability. IoT systems are composed out of a variety of software and hardware components comprising plenty of interconnected objects such as sensors, actuators, dashboards, communication elements, and more. Our research focuses on addressing security and safety issues in IoT systems, considering particularly the components communicating through wireless protocols:

- **Security Threats:** Cyber-attacks can compromise the system's confidentiality (resulting in data theft), availability (resulting in a denial of service), and integrity (resulting in data alteration). These attacks target critical vulnerabilities caused by the resource constraints of IoT devices (such as energy, processing power, memory, and so on) or errors in security mechanisms.
- **Safety Threats:** Faults can occur in any of the components of the IoT system and can lead to severe consequences, affecting the whole system as well as human interactions during emergency management.

II. CONTRIBUTION

To address these challenges, we aim to propose an independent component that will continuously check the IoT system to detect security and safety problems, in a similar way to the safety bag presented in [3], which seeks to detect and tolerate risks through online verification of safety necessities in autonomous vehicles. In our work, we intend to apply security properties to online verification in order to detect and tolerate cyber-attacks. We will call this component a 2S-bag (safety-security bag).

In order to study the safety and security properties of the 2S-bag and evaluate its performance, it is essential to be able to generate realistic cyber-attacks on the targeted system. Although the literature proposes several methods for security risks analyses, the attack identification remains a manual process relying on expert knowledge and depending heavily on the system.

We propose in our work novel process for identifying vulnerabilities with highest risk and generate realistic associated attack patterns in a specific IoT system. This process relies on existing risk studies and vulnerabilities databases. In our case, we used amongst other OWASP [1] Top Ten weaknesses in IoT and the CWE [2], CVE [3] and CAPEC [4] databases. The process consists of three steps: the first step identifies significant weaknesses based on their severity (for example, using a mapping that we generated between CWE and the OWASP Top 10 weakness categories for IoT). The second step identifies relevant vulnerabilities based on the system's IoT components and identified targeted weaknesses. The third step identifies attack patterns related to the vulnerabilities, for example combining attacks from the CAPEC database. The CWE, CVE and CAPEC databases represent trusted sources in defining fundamental weaknesses, vulnerabilities, and attack patterns in computing security. This proposed process could be used in security risk analysis by cyber-security experts in organizations as most methods require finding vulnerabilities in the system and possible attack scenarios, or in research works like ours to confront new defensive security mechanisms in IoT networks with representative cyber-attacks. Figure 2 represents a detailed block diagram of our proposed security assessment process, which consists of three steps. This process has been detailed in published international conference article [1].

We are currently implementing this process on a health care IoT application presented in figure 1. The proposed system

1. https://owasp.org/
2. https://cwe.mitre.org/
3. https://nvd.nist.gov/
4. https://capec.mitre.org/

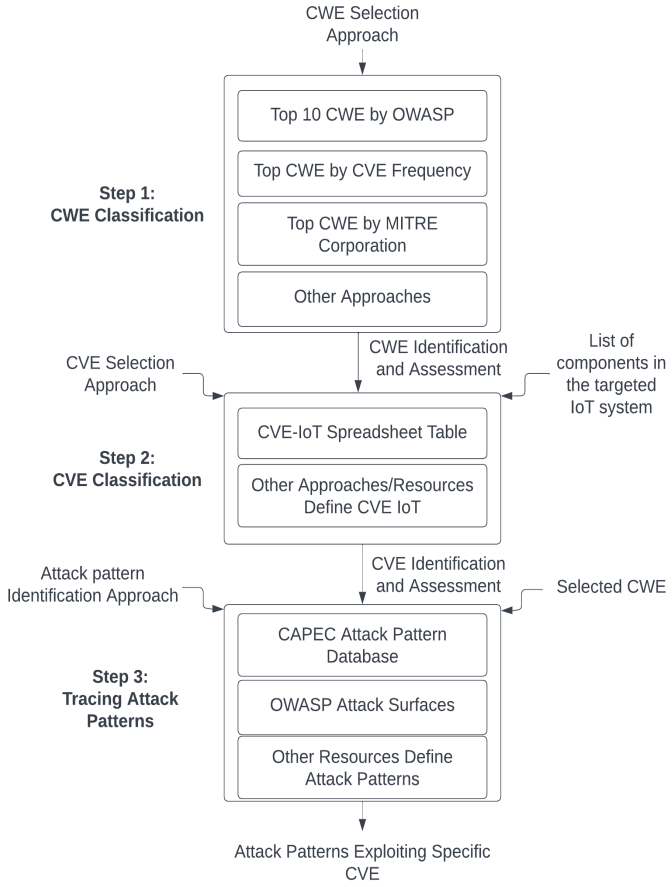

Fig. 1. BPMN Diagram of the Security Assessment Process

conforms to the ISO IoT architecture [2], and aims through IoT sensors and actuators to monitor a patient's health signs and administer treatments when needed. We intend to publish this work in a journal article during fall 2023.

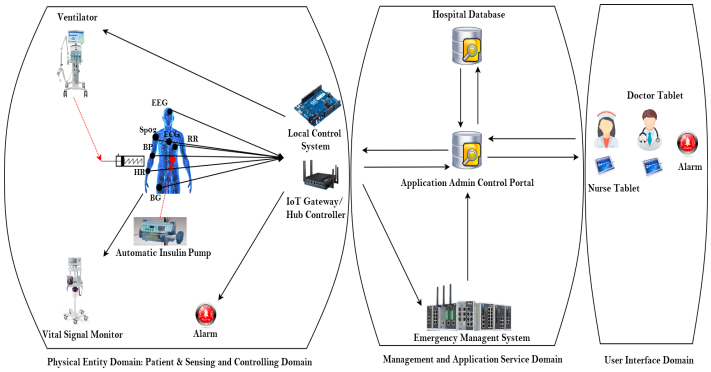

Fig. 2. Typical IoT network in healthcare applications based ISO IoT architecture

III. Conclusion and Future Perspectives

During the first and second years of this thesis, we extensively examined various related works on IoT architectures and standards for IoT systems, drawing insights from the existing literature. As part of our research, we proposed a vulnerability and attack identification process to find and evaluate realistic cyber-attack scenario in IoT systems. Our contribution was published in an international conference.

We are currently implementing this process on a medical application. From this, we aim to determine the security requirements and derive rules that the 2S-bag could implement to tolerate these attacks.

Additionally, we aim to identify faults that pose threats to the safety of the target IoT system application. Finally, our aim is to develop a 2S-bag capable of detecting and tolerating all or some of the identified safety and security threats. We plan to validate the effectiveness of the 2S-bag through simulations involving injected faults and simulated attacks.

Acknowledgment

The thesis is funded by the research direction of UTC, in the context of the IRP Adonis project and Region Hauts-de-France. My thesis work has started on November 22, 2022 under the co-supervision of the University of Technology of Compiègne and Lebanese University followed by ADONIS internship at Heudiasyc (Heuristics and Diagnosis of Complex Systems, UMRCNRS 7253) laboratory.

References

[1] Mohammad Beyrouti, Ahmed Lounis, Benjamin Lussier, et al. « Vulnerability and Threat Assessment Framework for Internet of Things Systems ». In: *2023 6th Conference on Cloud and Internet of Things (CIoT)*. 2023, pp. 62–69.

[2] Lefayet Sultan Lipol and Jahirul Haq. « Risk analysis method: FMEA/FMECA in the organizations ». In: *International Journal of Basic & Applied Sciences* 11.5 (2011), pp. 74–82.

[3] Crubille Paul, Lussier Benjamin, Schön Walter, et al. « Validation of Safety Necessities for a Safety-Bag Component in Experimental Autonomous Vehicles ». In: *2018 14th European Dependable Computing Conference (EDCC)*. 2018, pp. 33–40.