Modelling Cyber-Physical Security in Healthcare Systems

Fatma-Zohra Hannou, Faten Atigui, Nadira Lammari, and Samira Si-said Cherfi(✉)

CEDRIC, Conservatoire National des Arts et Métiers (CNAM), Paris, France
{fatma-zohra.hannou,faten.atigui,nadira.lammari,samira.cherfi}@lecnam.net

Abstract. Health organizations are critical cyber-physical infrastructures. By relying on last technological advances, healthcare organizations are now able to provide more personalized services through open and controlled platforms. Unfortunately, these new technologies that rely on common communication interfaces and standards, enhance security breaches and exposes hospitals to several threats.

The paper presents an ontology that allows (1) modelling cyber-physical security concepts in healthcare systems and (2) helps designing incidents propagation mechanisms by focusing on cyber-physical interactions among critical assets.

Keywords: Critical health services · Cyber-physical assets · Ontology-based model · Cyber-physical incidents · Security attacks scenario

1 Introduction

Healthcare organizations are complex socio-technical systems with the involvement of humans, business processes and sophisticated cyber-physical systems (CPS). They integrate cyber and physical infrastructure where patients, their health and their security are in the center. In CPS, frontiers between cyber and physical worlds are becoming more and more blurred. Indeed, with the recent advances in cloud computing, the Internet of Things (IoT) and other information technologies, the face of healthcare systems is changing. By adopting the usage of Electronic Patient Records, wearable sensors or in-home remote patients monitoring, healthcare organizations are now able to provide more personalized services. This progress induces sharing information about health services, resources availability (beds and medical personnel) or patients' data through open and controlled platform. It also offers new opportunities for new applications such as disease treatment, medical research, care services, etc. Unfortunately, these developments rely on common communication interfaces and standards and thus enhance security breaches exposing hospitals to several threats.

Besides, as healthcare organizations deal with human being health and lives, damages are mostly more severe. According to the Ponemon IBM data breach

© Springer Nature Switzerland AG 2021
S. Nurcan and A. Korthaus (Eds.): CAiSE Forum 2021, LNBIP 424, pp. 100–108, 2021.
https://doi.org/10.1007/978-3-030-79108-7_12

report [13], healthcare organizations had the highest costs associated with data breaches with $6.45 million. To increase the efficiency of solutions, it is necessary to examine all the problem facets.

2 Problem Statement

To a better understanding, we present an example of a cyber-physical attack scenario. Alike any critical infrastructure, the hospital has a building management system, including a network of connected cyber-physical objects dedicated to building management automation. Connected objects are implemented to control accesses (camera) or measure some indicators (temperature sensors, fire detectors, etc.). In a very simplified way, we assume that the temperature management includes three parts: sensors, PLC (Programmable Logic Controller) receiving measures and processing data, and actuators such as air cooling or heating to act on the hospital's air.

An attacker targets the temperature management system and executes the following sequence:

1. The attacker identifies the maintenance company operating in the hospital and gets the technical maintainer email;
2. He/she sends a spearfishing email;
3. He/she acquires control of the maintainer computer;
4. He/she goes to the hospital and steals the access codes to the technical room;
5. He/she enters the technical room which hosts the building management interfaces;
6. He/she connects to the building management system and identifies the PLC;
7. He/she simulates a fake temperature sensor indicating low temperature in different areas;
8. **Result:** the cooling ventilation system does not start, the temperature rises excessively in the concerned sectors.

The direct serious consequences on the hospital's processes are: the unavailability of surgery rooms, patients suffering from injuries can be super-infected or contaminated by viruses, data-center crashes, leading to the unavailability of the hosted servers services and of course, hospitals reputation and loss of trust. The behavior described in the previous example exploits several information on assets, their vulnerabilities, the protection mechanisms in place, their interconnections as well as the nature of the attack and its ability to propagate.

The purpose of the work presented in this paper is to propose a solution able to:

- identify the critical assets and their properties;
- evaluate the risk to which they are exposed tacking into account the nature of assets, their relationships, and the protections in place;
- provide information to help prevent the propagation of incidents in case of attacks;

The remaining of the paper is organised as follows: Sect. 3 reports on related works. Section 4 presents our solution including both knowledge acquisition and knowledge conceptualisation before concluding.

3 Related Work

Ensuring system's security and facing cyber or physical attacks raised major concerns for both practitioners and academics. As commonly known knowledge bases, we mention the Common Vulnerabilities and Exposures (CVE)[1], the Common Weakness Enumeration (CWE) (See footnote 1), and the Common Vulnerability Scoring System (CVSS)[2]. In [14], the authors present the Unified Cyber security Ontology (UCO) that unifies most commonly used cyber security standards. The NIST institute promotes a more general vulnerabilities ontology [4].

Based on the modeled security breach, we can classify the existing work into two main categories: risk & threat, and attacks & incident modeling approaches. For each category, a particular attention is given to ontology-based and healthcare dedicated contributions.

Risk & Threat Modeling Framework. The European Commission reported a generic classification of threats in which natural hazards are distinguished from non-malicious man-made hazards and malicious man-made hazards [15]. In [5], the author present an ontology-based approach that provides classification, relationships, and reasoning about vulnerabilities and threats.

For physical risk assessments, in [16], the authors present an ontology of hazards and threats that could affect a critical infrastructure. In the healthcare field, the work presented in [7], provide an overview of the cyber threats that jeopardize smart hospitals. In [2], the authors present taxonomies of threats for healthcare infrastructures.

Attack and Incident Modeling Framework. The MITRE provides the CAPEC[3] knowledge base that reports attack patterns in cyber security. In [11], the authors propose a taxonomy for classifying security incident that focuses on the cross domain and impact oriented analysis. The work presented in [10], provide a detection model for events occurring in CPS. In [1], the authors propose a model-driven framework based on EBIOS [6] and on attack trees method, in order to identify the critical parts of the systems.

The study of the state of the art shows that the provided standards, knowledge bases, and research contributions differ according to their main objectives: storing the common vulnerabilities, modeling or assessing risks and threats, or modeling incidents and their cascading impacts. Despite the escalating integration of networked cyber and physical components, physical security and cyber security remain handled separately. A security mechanism should be designed for the entire system rather than addressing only a part of it [3]. It is important

[1] https://cve.mitre.org/.
[2] https://www.first.org/cvss/.
[3] https://capec.mitre.org/index.html.

to provide an approach that considers the different aspects of both cyber and physical security and provides a semantic description of the assets, their vulnerabilities, and the kinds of threats that could affect them, as well as the incidents and their cascading effects.

4 An Ontology for Cyber-Physical Security Management

Existing ontology construction approaches [8] present common 3 main phases that we follow to build our ontology, i.e. **knowledge acquisition** (Sect. 4.1), **conceptualization** (Sects. 4.2; 4.3), and **implementation** (Sect. 4.4).

4.1 Knowledge Acquisition

This activity involved security experts, either belonging to the hospital staff (end-users) or other stakeholders by the means of questionnaires and preformatted files, onsite attack scenarios simulations and discussion workshops for validation. Afterward, this knowledge is refined based on literature taxonomies and security standards for better genericity and adequacy with the field practices. During this process we had to manage 2 main issues: (i) **heterogeneity of terminologies**: the interviewed experts came from hospitals belonging to 3 different countries (France, Italy, and Netherlands), so they use different terminologies, and (ii) **difficulties to get engagement**: collecting business experts' knowledge is a heavy and time consuming task.

To successfully conduct this process, we collaborate with our partners to develop 12 security attack scenarios classified into three groups: physical, cyber, or hybrid, based on the attacks and impacts types. These scenarios are confidential, but the example shown in the introduction, is inspired by one of these scenarios. For each scenario, we carried out the following actions:

1. Phase 1: identify the list of involved assets, the related risks, and the protections in place;
2. Phase 2: identify the inter dependencies between assets and the information about the surrounding infrastructures;
3. Phase 3: collect knowledge about the propagation process and how it is related to both the nature of incidents and the type of assets.

4.2 SafecareOnto: Assets Identification

An overview of the obtained ontology is shown in Fig. 1 with a central module said `Core ontology` and two related and additional modules dedicated to `protection` and `impact propagation`.

The Core Ontology captures the static knowledge about critical assets and their structural relationships detailed in Table 1. `An asset` is an entity that someone places value upon. Within healthcare services context, assets could be business assets such as "personal data" or support assets such as "IT devices".

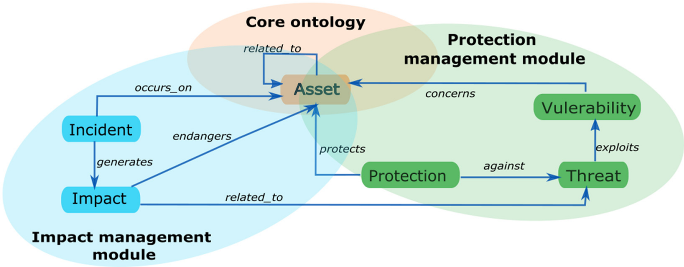


Fig. 1. The conceptual view of SafecareOnto

The Protection Management Module describes protection of assets against attacks. Each asset could have one or several weaknesses said `vulnerabilities` that could be exploited by a `threat` that is a potential of impairment of an asset. A `protection` could be an asset or a policy that protects an asset from `threats`. For example, a camera is protection against a threat that is unauthorized access.

The Impact Management Module defines the concepts that are essential to the computation of impact propagation and provide indicators to help decide about the suitable countermeasures to face attacks. It relies on `Incident` and `Impact` concepts.

An incident is adverse actions performed by a threat agent on an asset. When an `incident` occurs, there is a risk that it propagates to related assets. An `impact` is the result of such propagation. This propagation needs to be precisely qualified and/or quantified to efficiently help decide about the mitigation plans.

4.3 SafecareOnto Conceptualization

During the conceptualisation phase, the concepts and their relationships are refined. For space consideration, only the asset concept is detailed.

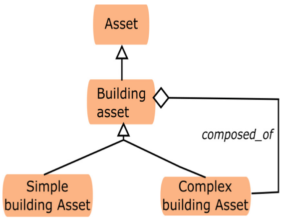
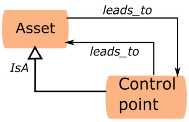
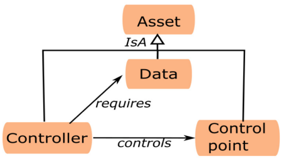
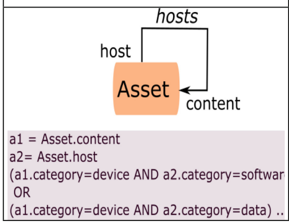
. **Asset** concept is a subclass of owl: Thing ($Asset \sqsubseteq \top$) and is further specialised into a set of subclasses that constitute a partition of the concept "Asset" since they have no common instances and that their union completely covers the concept "Asset" as defined for the domain [9].
  - **Support Asset** concept ($SupportAsset \sqsubseteq Asset$) gathers all the assets that help the achievement of the hospitals missions. The specialisation into more precise concepts considers propagation channels.
    * $ITAsset \sqsubseteq SupportAsset$
    * $NetworkedMedicalDevice \sqsubseteq MedicalDevice \sqsubseteq SupportAsset$
    * etc.
  - **Business Asset** ($BusinessAsset \sqsubseteq Asset$) is an asset that is directly related to the hospital mission such as care processes, personnel, etc.
    * $StaffAsset \sqsubseteq BusinessAsset$

  * $BusinessProcess \sqsubseteq BusinessAsset$
  * etc.

Relations Identification. The relationships depict how assets interact in the healthcare context and what are their properties. We have identified two families of relations:

– The first one corresponds to concepts Attributes (data properties in OWL): a staff `hasRole`, a building `hasLevel`, a software `hasVersion`, etc.

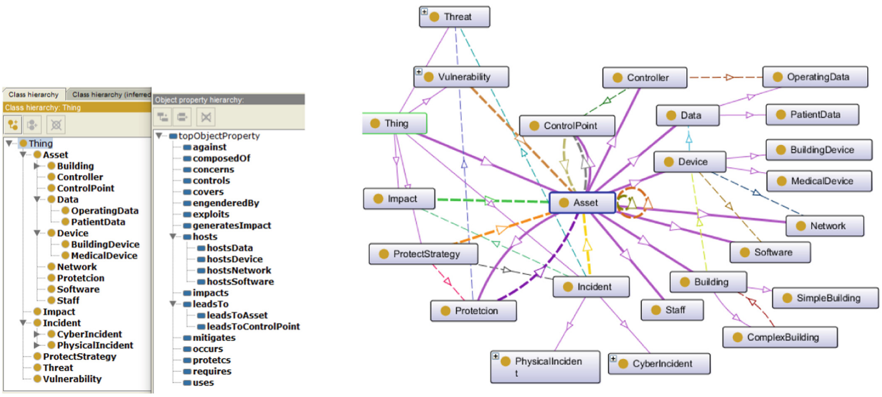
Table 1. Structural patterns

Pattern	Description
	The whole-part pattern assumes that if an incident happens on a whole, then it could impact its parts. Inversely, if parts are attacked, the whole could also suffer from the consequences of the attack. This pattern applies to several assets and essentially to assets representing locations. In SafecareOnto, they are referred to as `Building assets`. the propagation through theses structures are essentially "physical incidents" such as "unauthorized access". For example, an intrusion on one floor of a hospital could potentially affect all the rooms on that floor.
	Leads to pattern captures the access and communication possibilities between assets. This access applies for both physical or cyber flows and is materialized through a specific asset referred to as `Access point`. As an example we could mention a door that allows access from a room to another or a port that is a communication end point in a network. An access point could be one way or bidirectional to represent the possible flow directions explicitly.
	Controls pattern allows specifying the conditions and mechanisms for granting or revoking access to assets. The pattern is composed of three elements: the `Controller` applies the access policy, the `Control point` representing the access point and the `Data` representing the policy applied by the controller. For example, a smart card based system is composed of: the access rights stored locally or remotely, door readers to check whether data on the card is consistent with the policy and the door.
	The hosts-content pattern assumes that if an incident happens on an asset named `host asset` then the content, referred to as `content asset` could be affected by this incident. The structure of the pattern is enriched by rules to enhance the validity of the relationships description. For example, if the host is a device, IT or medical, a content could be software.

– The second family of relations results from our analysis of propagation channels. This analysis revealed that there exist some structural patterns that help reasoning on propagation of incidents according to their nature (cyber or physical). We detail some of these patterns in Table 1.

4.4 SafecareOnto Implementation

To implement the ontology, We have used Protégé [12], which is an ontology and knowledge base editor that enables the construction of domain ontologies,and comes with visualization packages. Figure 2 depicts an extract of the Safecare ontology designed in Protégé. Here, we present concepts that belong mostly, to the core ontology like `Asset` that could be `Staff`, `Device`, `Data`, or `Building`, etc. with their links, as for instance, a `Device hots Data`. Also, we show the concept `Threat`, `Vulnerability`, and `Protection` that belong to the protection management module as well as, `Impact` and `Incident` that belong to the impact management module.



(a) Class hierarchy and Object properties

(b) Ontology Graph

Fig. 2. SafecareOnto implementation in Protégé

5 Conclusion and Future Work

Healthcare systems lack a formal knowledge repository to assist security managers for effective security solutions design. In this paper, we propose an ontology-based model for both cyber and physical security in healthcare systems able to support incident propagation and mitigation reasoning. Our modular ontology is built around a core ontology focusing on assets, and comprises protection and impact propagation modules.

The knowledge acquisition process conducted with experts provided a business domain expert knowledge that we still analyse to construct a decision support system for risks mitigation. The modular structure of the solution proved to be very useful as the acquisition of domain knowledge could not be done on one shot given the variety and geographical spread of stakeholders. The next step is to develop the protection and the impact management modules.

Acknowledgment. This work is part of the SAFECARE project. This project has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens", challenge of the Horizon 2020 Research and Innovation program of the European Union, under grant agreement 787002.

References

1. Abdallah, R., Motii, A., Yakymets, N., Lanusse, A.: Using model driven engineering to support multi-paradigms security analysis. In: International Conference on Model-Driven Engineering and Software Development, pp. 278–292 (2015)
2. Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S., Upton, D.: A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. **4**(1), tyy006 (2018)
3. Ashibani, Y., Mahmoud, Q.H.: Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. **68**, 81–97 (2017)
4. Booth, H., Turner, C.: Vulnerability description ontology (vdo): a framework for characterizing vulnerabilities. Technical report, National Institute of Standards and Technology (2016)
5. Choraś, M., Flizikowski, A., Kozik, R., Hołubowicz, W.: Decision aid tool and ontology-based reasoning for critical infrastructure vulnerabilities and threats analysis. In: International Workshop on Critical Information Infrastructures Security, pp. 98–110 (2009)
6. EBIOS: Ebios risk manager - the method. https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf (2019)
7. ENISA: Cyber security and resilience for Smart Hospitals. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (2016)
8. Fernández-López, M., Gómez-Pérez, A., Juristo, N.: Methontology: from ontological art towards ontological engineering (1997)
9. Horridge, M., Knublauch, H., Rector, A., Stevens, R., Wroe, C.: A practical guide to building owl ontologies using the protégé-owl plugin and co-ode tools edition 1.0. University of Manchester (2004)
10. Ma, M., Liu, L., Lin, Y., Pan, D., Wang, P.: Event description and detection in cyber-physical systems: an ontology-based language and approach. In: 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp. 1–8. IEEE (2017)
11. Miller, W.B.: Classifying and cataloging cyber-security incidents within cyber-physical systems (2014)
12. Musen, M.A.: The protégé project: a look back and a look forward. AI Matters **1**(4), 4–12 (2015)
13. Ponemon, I.: Cost of a data breach 2019 report (2019)
14. Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A.: UCO: a unified cybersecurity ontology. In: Workshops at the 30th Conference on Artificial Intelligence (2016)

15. Theocharidou, M., Giannopoulos, G.: Risk assessment methodologies for ci protection. part ii: A new approach. Technical report EUR27332 EN (2015)
16. Trucco, P., Petrenj, B., Bouchon, S., Mauro, C.D.: Ontology-based approach to disruption scenario generation for critical infrastructure systems. Int. J. Crit. Infrastruct. **12**(3), 248–272 (2016)