PRELIMINARY COMMUNICATION

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Cyber-physical Threat Detection Platform Designed for Healthcare Systems

George Suciu, BEIA Consult International
Mari-Anais Sachian, BEIA Consult International
Ioana Petre, BEIA Consult International
Daniel Petrache, BEIA Consult International
Gabriel Petrescu, BEIA Consult International
Vasiliki Mantzana, KEMEA
Ilias Gkotsis, KEMEA
Fabrizio Bertone, LINKS
Luca Viarengo, CSI Piemonte
Silvia Andronello, CSI Piemonte

Address for correspondence: George Suciu, BEIA CONSULT INTERNATIONAL, Romania, e-mail: george@beia.ro

Abstract

Hospitals are responsible for delivering healthcare services to patients in need. These services are large and complex and get affected by multiple interacting actors, such as doctors, nurses, patients, citizens, medical suppliers, health insurance providers. Lately, hospitals around the world are one of the main targets when it comes to terrorist attacks, the cyber realm being the principal source. The healthcare sector is particularly vulnerable due to heavy involvement in patient personal and health information, time constraints, and complex day-to-day operations. In addition to cyber-threats, physical threats are increasingly growing and even healthcare facilities are not immune to them. Malicious intended people created cyber threatening attacks with the purpose to systematically collect evidence against the healthcare system, to advocate for the end of such attacks, and to endanger people's lives or to use the stolen personal data for bad intended actions. Henceforth it is necessary to build a platform that will get alerts and incidents at a fast pace in real-time to prevent any casualties at low cost. SAFECARE project aims to offer protection to hospitals and increase the compliance for the European regulations and security regarding ethics and privacy for health services. This paper presents a solution that will enhance security in hospitals. The primary platform will be built based on a BTMS (Building Threat Monitoring System) where events, incidents, and alerts will be transmitted by sensors from hospital rooms in real-time. Several scenarios were thought to simulate different types of attacks against hospitals and according to the scenarios, various prototypes will be built for assuring the security of the personal and patients from various hospitals.

Keywords

Security, Cyber-attack, Hospital, BTMS, Physical attack

1. Introduction

The exponential growth of technology and communication that the world has experienced in the past couple of decades has caused progress in numerous fields, including healthcare. With innovation (such internet-linked implantable medical devices, deep brain neurostimulators, and insulin pumps) also comes the potential danger to the infrastructure itself, such as cyberattacks (Martignani et al., 2017).

Cyberattacks have been increasing in the past years, with a 300% increase between 2014 and 2017 (Martin et al., 2017). While they do happen in many areas of daily life, such as airports and other critical infrastrcutures which rely on cloud computing (Suciu et al., 2018), one of the most targeted sectors is the healthcare sector, with over 110 million patients had their data stolen in the United States alone in 2015 (Martin et al., 2017) and ransomware rendering data useless (Poenaru et al., 2012). What distinguishes cyberattacks on healthcare organizations from others is that such attacks not only result in data and monetary loss but can also damage medical devices and infrastructure, thus putting patients' lives at risk (Jalali and Kaise, 2018). Healthcare systems face even more difficulties when attempting to provide security against attacks when compared to other organizations because they are usually more complicated due to the diversity of hospital sections and patient needs (Smet, 2002). Some of the issues specific to hospital environments are:

- Managing a diverse array of devices: A first issue is that the equipment used in a hospital, besides the fact that it varies widely depending on the hospital's section, it can also range from old to new, a fact that makes integrating every equipment into a security network a lot harder.
- Data protection regulations: as with any organization, they must abide by regulations regarding client data protection. However, in countries like the United States, or countries in the European Union, healthcare data is considered particularly sensitive, and thus it's protected under more strict laws (Larrucea et al, 2020).
- Complicated internal management and politics: all organizations feature internal politics, but the degree of specializations that is specific to hospital environments furthermore complicates their efficient management. Each department has different equipment needs, different workflows, and must tend to different patient needs.
- Underinvestment: The healthcare sector generally suffers from this problem; national health organizations usually receive around 2% of the annual budget, whereas other areas receive three or four times that amount (Jalali and Kaise, 2018).

Thus, healthcare systems suffer from an increased vulnerability caused by a combination of factors, including limited resources, fragmented governance, and complicated management. This paper presents a solution that will offer a reliable platform for security in a healthcare system that centralizes events, incidents, and alerts and assures the safety for both the personnel and the patients.

The rest of this paper is divided as follows: Section 2 analyses the already present literature, Section 3 presents the architecture of the cyber-physical security solution offered by SAFECARE, Section 4 shows the data exchange layer of SAFECARE platform, including an impact analysis of the platform on the healthcare system with its advantages and disadvantages, while Section 5 indicates the conclusions of the paper.

2. Related Work

Healthcare organizations have several assets that are essential for their operation and should be protected. Within the assets that can be attacked are the buildings and facilities, data, interconnected clinical Information Systems, mobile client devices, networking equipment, identification systems, networked medical devices, and remote care systems. It has been reported that the two most critical hospital's assets are the patients' health and their records (ENISA, 2016). The first one can be affected in many ways, such as by turning off a critical medical device that can cause a serious injury to a patient. Patient records contain valuable information, such as Personal Identifiable Information (PII) and health-related information that can be profitable information for attackers.

Healthcare organizations and their assets suffer from vulnerabilities that attackers can exploit to damage the environment and cause disruptions; and can be either cyber (application & OS, control gaps and design flaws, lack of smart sensors etc.) or physical (lack of access management, video monitoring, security agents, policy, collaboration with police and firefighters etc.). Attackers have different goals, as they might wish to cause damage, obtain a ransom, causing the interruption of service, or collect data to prepare future impacting attacks.

Health structures should enhance the cyber and physical measures that will support them in managing crises. The management of a crisis does not start when a crisis occurs. The planning and coordination for the response to any type of incident must be performed well in advance of an actual event. Crisis management has been defined as “the developed capability of an organization to prepare for, anticipate, respond to and recover from crises” (British Standard Institute - BSI, 2014). The full cycle of crisis management can be described in four phases:Preparedness, Response, Recovery, and Mitigation. The concept of the cycle implies an ongoing process that tries to eliminate disruptions, to provide immediate assistance to affected ontologies, to reduce disaster losses and to improve the conditions of the affected communities. Usually, the crisis management cycle is triggered by an event and begins with a response to that event. As the main aim is to respond to the specific threat, crisis management programs often prioritize the preparedness and response phases, leaving limited resources to address recovery and mitigation. A systems approach to crisis management suggests a different understanding of the crisis cycle that balances resources among the four phases.

Healthcare organizations can take practical steps to protect themselves and reduce the effects of an attack, such as to strengthen resilience, as resilient organizations are less likely to be attacked and suffer less harm when attacks occur. The primary activities established by the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST) are from one hand the identification of the critical assets (hardware and software), and data flows within the organization, and from the other the implementation of countermeasures in a prioritized manner in order to protect their systems, data and infrastructure (National Academies of Sciences, Engineering, and Medicine, 2015). Moreover, hospitals and healthcare organizations should not only invest on cyber security measures but must also adopt technologies that support limiting damages in case of an attack (e.g. network segregation, data encryption etc.) (INFOSEC, 2019).

In addition to cyber protection measures, hospitals should also focus on physical protection and they should introduce new technologies and upgrade existing ones in order to ensure the security of their most valuable assets such as people, infrastructure, and property. Typical systems include among others the following: (a) Fences/Walls, (b) Guards, (c) Building control, (d) Intrusion detection and access control, (e) Video surveillance, (f) Audio surveillance, (g) CBRN sensors and (h) Physical Security Information Management (PSIM) systems.

It is also crucial that healthcare staff (including researchers, administrators, front desk workers, medics, transcriptionists, handlers of medical claims to IT, and technical staff) should be properly trained on physical and cybersecurity issues (Martin G., 2017). Last but not least, healthcare organizations need to develop and adopt common healthcare security standards and adopt a clear security policy and response plan.

3. Architecture of SAFECARE

SAFECARE aims to bring together the most advanced technologies from the physical and cybersecurity spheres to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects (SAFECARE project, 2018). The underdevelopment solution will focus on health service infrastructures and will work towards the creation of a global protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment.

In doing this, SAFECARE solution will be designed, tested, validated and demonstrated, which will optimize the protection of healthcare organizations against cyber and physical threats. The SAFECARE holistic approach is composed of 3 main technological, namely: (a) physical security solutions; (b) cyber security solutions and (c) integrated cyber-physical security solutions. The physical security solutions and the cybersecurity solutions consist of smart modules and efficient integrated technologies to respectively improve physical security and cybersecurity. More specifically, physical security solutions embed integrated intelligent video monitoring and interconnect building monitoring systems as well as management systems. While cybersecurity solutions correspond to cyber monitoring systems as well as threat detection systems related to IT, BMS (Building Management Systems) and e-health systems. Both physical security solutions and cyber security solutions are interconnected thanks to the integrated cyber-physical security solutions. The integrated cyber-physical security solutions consist of intelligent modules to integrate different data sources and better take into account the combination of physical and cyber security threats.

Operators for both the Building Threat Monitoring System and the Cyber Threat Monitoring System receive notifications about identified threats in real-time and can confirm or reject the alert. When the human operators from Security Operation Centers (SOC) confirm incidents, they are passed to the Impact Propagation and Decision Support Module that considering all available information computes impacts on the involved assets, as presented in Figure 1.

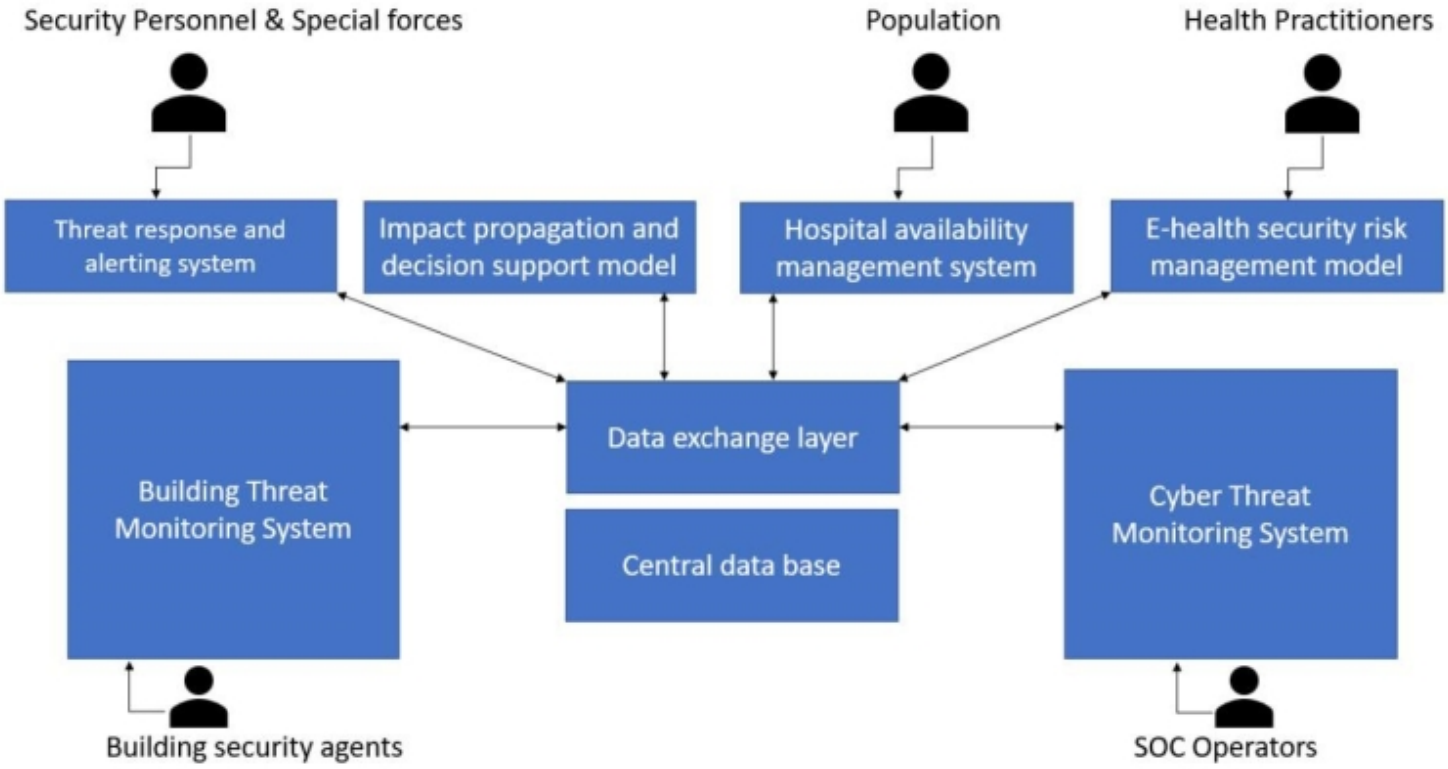

Figure 1. SAFECARE architecture and interconnections

When assets get marked as unavailable, either from the impact computed by the module or explicitly by an operator for any reason, the information is published through the Hospital Availability Management System and is then available to internal or external actors. This particularly facilitates the routing and spread of patients between multiple facilities during emergency situations. The information is made available in OASIS standard EDXL-HAVE format (OASIS, 2019) so that it can be automatically processed by other compatible management systems.

During the project lifecycle, close collaboration and continuous engagement with leading hospitals, national public health agencies and security forces across Europe, will ensure that SAFECAREs global solution is flexible, scalable and adaptable to the operational needs of various internal and external stakeholders (involved in Healthcare Infrastructure security incidents) across Europe, and meet the requirements that derive from the newly-emerging technologies and standards.

4. Data exchange layer integration and analysis

In order to implement an integrated security system that considers both physical and cyber threats, vulnerabilities, incidents and impacts, a unique central point of information analysis, together with a common communication layer.

In SAFECARE solution, this has been implemented with a module called Data Exchange Layer. All other monitoring and processing modules and tools keep a continuous and real-time connection with the Data Exchange Layer to communicate with each other.

The communication channel uses the MQTT (MQ Telemetry Transport) protocol, where a central broker acts as an aggregation point and each module implements a client and communicates through dedicated topics.

MQTT has the advantage of being a public and free protocol, with a rich ecosystem of open-source applications and development libraries available for most programming languages. This enables each submodule to be freely implemented using the preferred development environment.

The Data eXchange Layer allows all the other modules to communicate with each other in near real time and provide relevant interfaces to extract data stored in the database. Five types of dynamic-data messages are defined:

- Incident: message generated by the monitoring tools;it reports information related to the incident, it is validated by human operators and it triggers decision-making modules.
- Impact: reports the potential impacts after an incident occurs allowing prevention of potential cascading effects.
- Threat response: provides a predefined reaction plan to mitigate the effects of incidents and improve time to response.
- Notification: exchange the communication between Threat response and alerting system and Mobile alerting system.
- Availability: reports the updated availability of assets involved in the incident.

The actual information that is required to be kept is stored inside a Central Database that is directly linked with the Data Exchange Layer, as presented in Figure 2. Two main classes of data are stored in the database. The first contains a set of *static* information that is typically constant for a long period of time, like the medical department of the hospital, its facilities, the devices available to each department and so on.

The second class of data stored is *dynamic* data and includes live information on the environment like detected incidents, their impacts, the availability of resources like services and assets and so on.

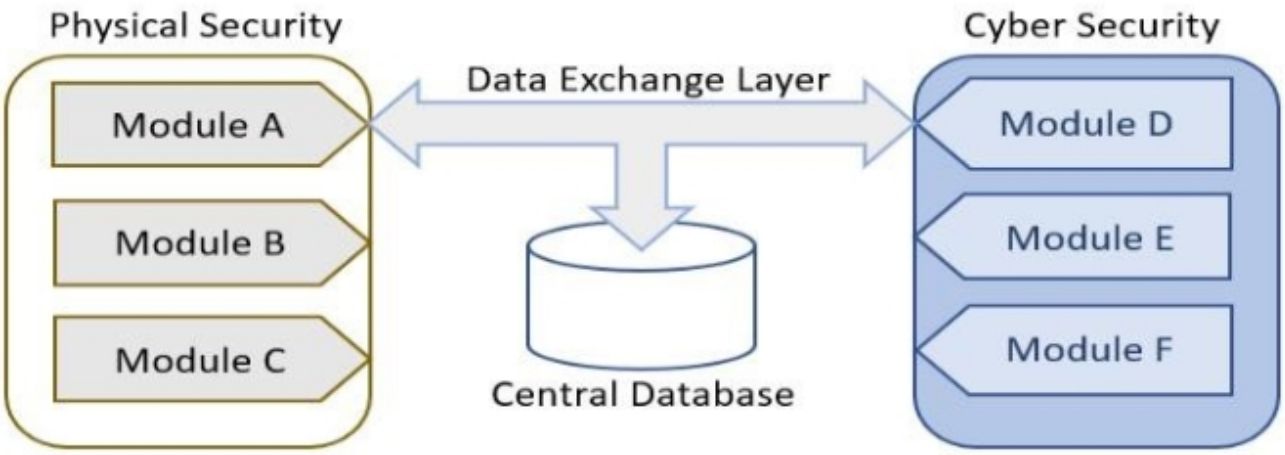

Figure 2. Data Exchange Layer Integration

All static and dynamic data is considered and analyzed to assess threats and potential impacts of incidents. This way the system is able so to keep a real-time overview of the status of all the ecosystem of the considered healthcare infrastructure and alert relevant operators in case of necessity.

As seen in Figure 3, the SWOT analysis of the SAFECARE platform was made in order to see how the solution provided by the project can affect the personnel and patients of hospitals if it would be put on the market, ongoing forth that the healthcare infrastructure being in a significant need of such platforms.

Figure 3. SWOT Analysis of SAFECARE platform

In SAFECARE solution, some modules are dedicated to the notification of human operators via multiple means, like SMS messages, phone calls etc. Furthermore, by using MQTT the interoperability is ensured with other data exchange layers and formats such as HL7.

5. Discussion and Conclusions

This paper analyzed cyber-physical threats for healthcare systems and presented the way the SAFECARE project will provide a safe environment to healthcare services by assuring the security of doctors, patients and other personnel in hospitals primarily. As such, the architecture and data exchange layer using MQTT were detailed. As future work we envision to implement and test the platform in three hospitals which belong to the consortium.

Acknowledgment

This work has been supported in part by European Union’s Horizon 2020 research No. 787002 (SAFECARE project).

References

British Standard Institute (BSI). (2014). *BS11200: Crisis Management – guidance and goodpractice* . BSI.

ENISA. (2016). *Securing Hospitals: A research study and blueprint. Independent SecurityEvaluators.* Ανάκτηση 2019, από https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf

INFOSEC. (2019). *INFOSEC institute.* Ανάκτηση 10 2019, από Hospital Security: https://resources.infosecinstitute.com/category/healthcare-information-security/security-awareness-for-healthcare-

professionals/hospital-security/

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, 20(5), e10059.

Larrucea, X., Moffie, M., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. Computer Standards & Interfaces, 69, 103408.

Martignani, C. (2019). Cybersecurity in cardiac implantable electronic devices. Expert review of medical devices, 16(6), 437-444.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358, j3179.

National Academies of Sciences, Engineering, and Medicine (2015). *Guidebook on BestPractices for Airport Cybersecurity.* Best Practices for Airport Cybersecurity. Washington, DC: The National.

OASIS. (2019). Emergency Data Exchange Language (EDXL) Hospital AVailability Exchange (HAVE) Version 2.0

Poenaru, Vlad Andrei, George Suciu, Cristian George Cernat, Gyorgy Todoran, and Traian Lucian Militaru. "Attacking the cloud." ICEST 2012

SAFECARE project. (2018). *Grant Agreement Number 787005, European CommissionH2020.* Ανάκτηση 11 2019, από https://www.safecare-project.eu/

Suciu, G., Scheianu, A., Vulpe, A., Petre, I., & Suciu, V. (2018). Cyber-attacks–the impact over airports security and prevention modalities. In World Conference on Information Systems and Technologies (pp. 154-162). Springer, Cham.