A combined cyber and physical attack resilience scheme for Health Services Critical Infrastructure

Andreas Papalambrou1, John Gialelis1,2,*, Dimitrios Serpanos1,2

1University of Patras, Electrical and Computer Engineering Department, University Campus, Rio Patras, Greece
2Industrial Systems Institute/ATHENA RC, Platani, Patras, Greece

Abstract. This work focuses on proposing the basic components of a resilience scheme that can be used for the protection of Health Services Critical Infrastructure (HSCI) and the protection of its key assets based on combined protection against cyber and physical attacks.

1. Introduction

Health Services Critical Infrastructure (HSCI) assets around the world are constantly being targeted by cyber-attacks as noted by the U.S. Federal Bureau of Investigation (FBI) in a Private Industry Notification (PIN) report issued in April 2014, stating that malicious attacks will increase against healthcare systems and medical devices due to lax cybersecurity standards, and a higher financial pay-out for medical records in the black market. Recent attacks, such as WannaCry ransomware in May 2017, which affected several health services worldwide, have proved to be an alerting confirmation of that forecast. In addition to cyber-threats, HSCIs are also prone to all-hazards, specifically natural hazards (earthquakes, wildfires, and flooding), technological or accidental malfunctions (hardware and software faults), adversarial/malicious attacks (physical and/or cyber caused by humans), as well as human errors.

According to a model proposed by the Institute for Critical Information Infrastructure Protection (ICIIP), the "security problem" is a potential compromise of safety / security and damage of the critical infrastructure. Those issues may be systemic (caused by the system or organizational design or culture), coming from internal personnel, or external by means coming from competitors, customers, terrorists and natural disasters. Due to the total reliance on ICT systems, the impact of a coordinated combined attack scenario including both kind of attacks, cyber and physical, could have disastrous consequences for the health of citizens worldwide. Cyber and system-theoretic approaches fail to provide appropriate security levels to HS, since they are often used in isolation and build on incomplete attack models, resulting in silos-like security management fragmented operational policies. Many attacks on Critical Infrastructures involving physical processes, exploit vulnerabilities on both physical and logical layers. In the Health Services domain, medical equipment and

* Corresponding author: gialelis@ece.upatras.gr

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
devices is a very valuable part of these CIIs that are physically protected and segregated. An attack on those systems usually requires the involvement of an insider or a physical intrusion on the infrastructure. Fraud, sabotage, accidents and theft increase the cost of provisioning HS since, the environments are becoming more complex. Until now, physical security is further down the list of priorities, so HSCIs are not designed with physical security in mind. Therefore, a credible defence system should invest in prevention, detection, response and mitigation. The basic objective of the defence system is to safeguard personnel, data, equipment, IT infrastructures, facilities and in general all assets of HSCIs. The defence strategy for protecting organizations’ assets should follow a layered approach meaning that when an intruder passes one layer, there will be additional layers to overcome to obtain an asset. In this study, a resilient integrated security solutions platform, able to seamlessly compose state of the art heterogeneous security components efficiently addressing cyber physical threats (CPTs) and information sharing (IS), is presented. Its main characteristics comprise, applicability to any HSCI; scenario and technology independence, consistency with standards.

The rest of the paper is organized as follows. Section 2 briefly presents the related state of the art, Section 3 depicts the HSCI threats the system addresses, Section 4 depicts the proposed layered architecture along with its subsystems, while in Section 5 the functionality of the integrated platform is discussed.

2. Background and Related Work

Currently, there are several international organizations and companies involved in cyber and/or physical security of health services. Antivirus companies, such as Karperksy Lab [1], are offering customized solutions for health services, aiming at protecting the computer infrastructure against cybersecurity attacks (virus, ransomware), as well as data encryption services. Various companies exist offering specialized cyber security services aiming at healthcare providers, such as Axway [2] (real-time operational intelligence), Agari [3] (secure against phishing attacks), Skycur [4] (protect against mobile malware, device vulnerabilities and physical attacks), Arxan [5] (attack prevention for IoT and embedded apps in medical devices), NCC Group (IoT consultancy for cybersecurity and risk mitigation), Hashed Health [6] (blockchain use for IoT security) and MedCrypt [7] (data encryption between medical devices and real-time anomaly detection). The US National Health Information Sharing and Analysis Center (NH-ISAC) [8] is a non-profit organization for sharing intelligence on cyber or physical threats, incidents and vulnerabilities, advice and best practices, mitigation strategies and other information relevant to health services. The NH-ISAC database can be linked to cloud software platforms, such as Perch [9], which provides an interface to access information related to the operator, as well as to share intelligence back to the community. HSCIs are more or less prepared when addressing cyber risks in the Information Technology (IT) domain (i.e., everything related to patient records) since they are using standard equipment, software and solutions but they are not in the same situation when addressing risks in the Operational
Technology (OT) domain. Particularly HS facilities, are managing thousands of devices and many different networks, with high real-time low-latency constraints, with controls at different levels, with strong privacy requirements on the collected and processed data. Most of these devices are completely black boxes and some of them are built on top of standard Operating Systems (OS). HSCI security operators have limited information about the equipment, about the installed software and about how to protect both. In most cases, it is not even possible to patch them without losing the guarantee of the manufacturer.

3. HSCI threats, Model and System Targets

A systematic approach for defending against any physical or cyber-attack or a combination on HSCI is still missing. The European Council in 2004 defined a programme for Critical Infrastructure Protection (EPCIP) to the doctrine and programmes created to identify and protect critical infrastructure that, in case of fault, incident or attack, could seriously impact both the country where it is hosted and at least one other European Member State. Towards this direction, European Union Agency for Network and Information Security (ENISA) has proposed a Threat Taxonomy that classifies threats based on type (cyber and physical attacks) and their characteristics [10]. The purpose of this taxonomy is to establish a point of reference for threats encountered, while providing a possibility to shuffle, arrange, amend and detail threat definitions.

These characteristics of cyber and physical attacks must be united under the same model in order to protect the HSCI. Therefore, the best candidate model is an expansion of the ICIIP model. The diagram of the modified ICIIP model with the extensions and alterations dedicated to our concept is depicted in Figure 1. The proposed model identifies the elements of people, domain policies, technology and finally the processes involved. We are assured that Systemic Security Management (SSM) will be a management approach to security which serves the HSCI, which combines both cyber-attacks, and the people and processes of physical attacks. SSM is built around a set of core principles whose intention is to ensure an optimal balance of protection, while maintaining the ability to provide health services among the patients. It is an approach designed to make it possible to provide their services, yet ensuring that the CI is protected. The nodes are connected with six dynamic interconnections, which are referred as “tensions”. The basic tensions that connect the nodes are governance, culture, architecture, enabling & support, emergence, and human factors. Below the nodes are described with respect to HSCI point of view:

Process, means the explicit, formal means by which things get done in an organization. This node requires from the HS providers to decide to those policies that the administrators should enact to keep their organizations secure. These policies and processes should involve all levels within the organization (e.g. clinics, IT, logistics, etc.).
Technology, is specifically assigned to develop and implement technological approaches for the protection of the CI. This will require more effort in order to resist against cyber and physical attacks, but also improving the tensions of the “architecture” of the organization, dealing with human factors like collaboration between users, and attention to the technology role in enabling and support, to achieve optimal security.

Figure 1 Critical Information Infrastructure Protection model

People represent the human resources element who need to act not only in fundamental security but also in security in more complex systems, by receiving training for CI’s security. The human factor is vital in the security management, but this model adds concerns for culture and emergence as added tensions that must figure prominently in any enhancement of security.

Domain policies, focus on the need to design structures and strategies that enable the health services provider to create competitive advantages, understand the risks and adopt policies that elevate security to a first priority.

Targets of a defence system must make use of state-of-the-art Information and Communication Technology (ICT) addressing the protection of the HSCI with respect to Physical and Cyber Security, covering the security cycle in four dimensions as follows:

- Prevention: maximum utilization of state-of-the-art ICT tools for new means of training, awareness, preparedness & anticipation;
- Detection: state-of-the-art ICT- based methodologies and tools for detecting HSCI physical and cyber threats in an early stage;
• Response: state-of-the-art ICT intelligent tools for advance alerting and response capabilities instead of opening new vulnerabilities as well as protection of privacy of humans;

• Mitigation: state-of-the-art ICT tools and techniques for mitigation and post-incident investigation;

Critical Infrastructure Protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.

4. Layered Defence System Architecture

In order to implement the defence based on a layered, we propose the following basic components that can build a complete scheme for tackling these risks:

• A Virtual Training Environment (VTE) for simulation of a HSCI that can be used for identification of infrastructure vulnerabilities, for deploying cyber and/or physical preventive, responsive and mitigation measures as well as increasing personnel situational awareness.

• A Threat Analysis and Risk Assessment System responsible for fusing multiple modalities that describe the security profile of the HSCI and based on that, to assess the risk that the HSCI undergoes for various possible threats and determine the potential cascading effects of a detected threat in the two different domains (physical and cyber).

• A Decision Support System (DSS) responsible for evaluating the current risk and threat status and supporting the operators formulating the prevention, response and mitigation actions that should be applied.

• A Security Actions Enforcement System that will emerge and enforce the proper cyber and/or physical security modules and components in order to realize the desired end-to-end security behaviour in all four dimensions (prevention, detection, response, mitigation – PDRM) as well to share timely and relevant information to diverse target groups;

• A federated Knowledge Base comprising all knowledge accrued.

5. System Functionality

To facilitate methods and approaches towards prevention, detection, response and mitigation of the combination of physical and cyber threats to the HSCI, there exists the challenge of building a robust but efficient system. A single technological approach that can meet the requirements for each combination of physical and cyber threat can be accomplished by incorporating large sets of related technologies in a coordinated and interoperable manner as a System of Systems (SoS) concept as shown in Figure 2. The term system of systems can mean different things in various domains. SoS technology is believed to more effectively implement large, complex, independent and heterogeneous
systems working cooperatively towards obtaining higher capabilities and performance than it would be possible under the traditional system view. This statement fits perfectly within the broad threat management context that we address. The systems proposed are the building blocks of the proposed platform and are supported on three main pillars. The pillars constitute the base upon which every component should lean, and they manifest the conceptual foundations of the proposed platform along with the technical requirements and their interdependencies. The three pillars consist of:

i) the Threat based Risk Assessment

ii) the Simulator Environment and

iii) the Security Enforcement Pillar.

Figure 2 System of Systems

The Threat based Risk Assessment pillar is responsible for fusing multiple modalities that describe the security profile of the HSCI and based on that, to assess the risk that the HSCI undergoes for various possible threats. The cornerstone of this pillar is the threat analysis and risk assessment engine that implements the aforementioned functionality. The engine’s operation is supported by the following three components:

* Security metrics provide the means to measure and evaluate the quality of the security that protects the HSCI.
• Detection mechanisms utilize the cyber and physical security tools to deliver accurate and in time possible intrusion events detection.

• The attack models formulate the possible attacks for which the platform is building its detection, prevention, response and mitigation tools and mechanisms for.

The Security Enforcement pillar utilizing state of the art artificial Intelligence techniques and methods comprises the security enforcement execution engine as its main component. The Simulator Environment operates as the driving force of the platform. The two main components of this pillar consist of the simulation platform and the workflow generator for the prevention response and mitigation actions

6. Conclusions

The proposed components in the layered architecture can together deliver a Cyber-Physical security solution to holistically encounter cyber and physical threats within HSCIs. This holistic solution addresses end-to-end security in any HSCI regardless the underlying components (devices, equipment, systems, buildings, humans) and interconnections, which are indeed unknown at design and development phase. There are no limits to the complexity of the addressed CI. The proposed methodology is able to put together any kind of security module being it HW, SW, or human to realize an end-to-end security behaviour. Specifically, humans, equipment, systems, IoT devices, etc., are among the possible “building blocks” for maximum security.

References

[8] https://nhisac.org