The Danger of Missing Instructions: A Systematic Analysis of Security Requirements for MCPS

Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn*
The Center for Cybersecurity and Digital Forensics
Arizona State University
[jalamp,crubiome,zzhao30,gahn]@asu.edu

ABSTRACT

The proliferation of networked medical devices has resulted in the development of innovative Medical Cyber-Physical Systems (MCPS) that promise more coordinated and high quality of care for patients. Unsurprisingly, the cybersecurity of MCPS is of high concern, as they are life-critical systems that, if compromised, may result in dire consequences to the patient. A variety of security requirements have been developed over the past 10 years as a result of governmental acts such as HITECH in order to better secure and protect healthcare environments. However, it is unclear how applicable these requirements may be to MCPS infrastructures. As a result, this case study analyzes current healthcare security requirements and their applicability to MCPS using an approach that leverages ontological representations and automated requirement traversal techniques. Using such a methodology, we find that 70% of applicable requirements/risks for MCPS components are missing from the security documentation, including serious items such as Authentication, Data Encryption, DoS attacks, and Legacy Vulnerabilities. We also validate our results within real-world instances and find that almost half of the relevant requirements are not implemented within existing MCPS architectures.

CCS CONCEPTS

• **Security and privacy → Security requirements**; • **Computer systems organization → Embedded and cyber-physical systems**;

KEYWORDS

Medical Cyber-Physical Systems, Security Requirements Analysis

ACM Reference Format:
Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn. 2018. *The Danger of Missing Instructions:* A Systematic Analysis of Security Requirements for MCPS. In *ACM/IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE '18), September 26–28, 2018, Washington, DC, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3278576.3278602

*Dr. Gail-Joon Ahn is also affiliated with Samsung Research.

CHASE '18, September 26–28, 2018, Washington, DC, USA

ACM ISBN 978-1-4503-5958-0/18/09…$15.00
https://doi.org/10.1145/3278576.3278602

1 INTRODUCTION

Over the past 10+ years, there has been a proliferation of interconnected and networked medical devices, such as mobile ultrasounds, insulin meters, mobile heart sensors, smart patient monitors, and smart imaging systems. This has resulted in the development of innovative Medical Cyber-Physical Systems (MCPS), a promising new paradigm supporting the optimized and efficient provision of care services within healthcare organizations and networks [10]. MCPS consist of life-critical, distributed systems that are utilized to monitor, organize and control organizational, administrative and care-oriented services, with the ultimate goal of providing better care for patients. MCPS combine a variety of devices and systems, including Electronic Health Records (EHRs), Medical Systems (i.e. Radiology System), Wearable Devices, Patient Portals, Medical Devices and Controllers, and Patients and Medical Personnel. The entire MCPS is extremely interconnected, and relies on the continuous networked communication between devices, information systems, and people, in order to identify inefficiencies and continuously improve care practices. These systems are extremely promising, with the Department of Homeland Security even citing the great opportunities MCPS can have for the future US infrastructure and health sector [2].

Unsurprisingly, the cybersecurity of MCPS is of high concern, as these are life-critical systems that can result in dire consequences to the patient if compromised [10]. Securing MCPS is especially relevant considering the recent surge in attacks to healthcare organizations, medical systems and medical devices. For example, a report by the Cybersecurity company CryptoniteNXT found that there were 140 reported hacking incidents to healthcare organizations affecting more than 500 patients in 2017, and that 3,442,748 patient records were compromised due to hacking in 2017 [1]. In another example, in 2017, the FDA recalled 465,000 pacemakers and other medical devices from Abbott's (St. Jude Medical) due to security vulnerabilities [19]. Previously, former Vice President of the United States, Dick Cheney, even had his pacemaker partially disabled to prohibit network connections because he was worried about terrorists being able to target the device and kill him [12].

One of the key ways to go about protecting important infrastructures is through the development of specific security requirements [11]. Recently, there has been a significant governmental push to improve the cybersecurity of healthcare environments, realized through the passing of federal acts including the HITECH Act in 2009 [18] and the Cybersecurity Act of 2015 [17]. These acts have resulted in the development of cybersecurity requirements for healthcare including the HITRUST Common Security Framework (CSF) [6], HealthIT.gov security pamphlets [15] and the Report on Improving Cybersecurity in the Health Care Industry [5],

that elucidate risks to healthcare organizations as well as sets of security measures that should be implemented in order to better protect healthcare organizations, information systems, devices, medical personnel, and patients.

Now, these governmental requirements are great for the general healthcare case; however they are not specifically tailored to MCPS, and as such it is unclear how applicable they may be for such systems. For example, they may fail to take into consideration systematic changes and new security requirements that may be necessary to adequately secure MCPS. Therefore, there is a need to understand and analyze current healthcare security requirements for MCPS in terms of their requirements coverage and relevance for use in these systems. With this in mind, this paper presents a systematic analysis of current healthcare security requirements and their applicability to MCPS using a methodology that leverages ontological representations and automated requirement traversal techniques. We will present our findings in terms of covered and crucial missing requirements (such as Authentication and Data Encryption) as well as covered and missing risks to MCPS (such as DoS Attacks and Malware). We will also validate such results in real world contexts, and identify cases where the missing requirements from the documents are also missing from the infrastructures, as well as where the requirements are implemented within the infrastructures, despite not being within the documentation.

In this paper, we provide the following contributions: first, we provide a systematic methodology to analyze requirements using ontologies and requirement traversal techniques, second, we present novel findings of covered and missing security requirements within healthcare cybersecurity documentation for MCPS, and third, we validate our findings within 4 real MCPS infrastructures. This paper is organized as follows: first we will go over some important background topics in Section 2 and describe our methodology to conduct our case study in Section 3. Next, we will elucidate our findings using our approach and will validate them using real-life MCPS infrastructures in Section 4. Finally, we will describe some pertinent related work in Section 5, and conclude the paper in Section 6.

2 BACKGROUND

Ontology Projections. Ontologies provide a convenient means to model complex real-life domains in a structured and intelligent manner, understandable by both computers and humans [11]. Ontologies work by leveraging entities and their properties, where entities represent the objects of a domain and properties define the relationships amongst such entities. Ontologies are ideal due to their ability to cohesively combine information from diverse sources, i.e., complex documentation from various unique organizations.

Ontology projections, or traversals, allow for the intelligent retrieval of specific entities or properties based on user queries [11]. Projections work by pulling together different aspects of entities, such as their relationships, properties, contextual information or environmental constructs. By helping the user understand related entities, determine entity specifications, and discern environmental or contextual information surrounding a concept, security requirements and their relationships between other concepts (such as components) may be identified and evaluated. In this way, comprehensive analysis of security requirements may be completed.

As a part of previous work [9], we developed 4 different types of ontology projections, namely, *Scenario*, *Domain*, *Goal* and *Risk* projections. *Scenario* projections provide facts describing a system that include agent behavior and environmental context. They provide a broad picture of the ontology elements and their relationships, allowing for a generalized introductory understanding of specific concepts. For instance, a Scenario projection for a Medical Device may include a variety of relationships to other entities, such as being *targetedBy* the DoS Attack, *implementing* the security feature Device Monitoring, *including* Measures to Protect Patient Safety, *accessing* the component Network and *following* the requirement of Access Control. *Domain* projections describe a domain taxonomy relative to a specific topic and categorize concepts, allowing for further expansion and understanding of the types and specification of entities. For example, a Domain projection for a Pacemaker may show that it is a subclass of Implantable Devices, which is a subclass of Medical Devices, which is a subclass of Devices, which is a subclass of MCPS Components. *Goal* projections allow for the user to understand the context for the achievement of specific goals within MCPS systems. These projections contain objectives the system must achieve to enter into a state of security, and include factors such as protecting system components, implementing security features, counteracting risks, identifying properties of components, or protecting security principles. A Goal traversal for the Network component may return a variety of Network Rules Requirements including Connection Management, Network Segregation and Segmentation, Monitoring and Intrusion Detection. Finally, *Risk* projections are a type of super-projection that summarize the set of risks and relations relevant to a specific MCPS component. They use multiple other projections (mainly Goal and Domain) within them, and match relationships between risks, principles, components, and requirements. For instance, a Risk projection for a Pacemaker is shown in Fig. 4, depicting the set of related Requirements, Security, Threats and Attacks for the device.

Governmental Security Acts and Requirements. Over the past 10 years there have been a variety of governmental acts released in order to better secure healthcare environments. Explicitly, two main acts have had significant impact on improving healthcare cybersecurity. First, the American Recovery and Reinvestment Act (ARRA) of 2009 was released specifying the Health Information Technology for Economic and Clinical Health (HITECH) Act that elucidates specific security requirements healthcare environments need to contend with in order to provide secure care [18]. The HITECH act was instrumental in the creation of HealthIT.gov [15], an informative government-run website that provides, along with other general health technology information, specific pamphlets and resources for protecting healthcare organizations in terms of security and privacy. Next, responding to the continued cyberattacks occurring to healthcare organizations throughout the United States, the Cybersecurity Act of 2015 put together the Health Care Industry Task Force to address security risks and challenges specific to healthcare [17]. This task force developed the Report on Improving Cybersecurity in the Health Care Industry [5], released in June 2017, which specifies applicable risks to healthcare as well as the group's future recommendations for addressing such risks.

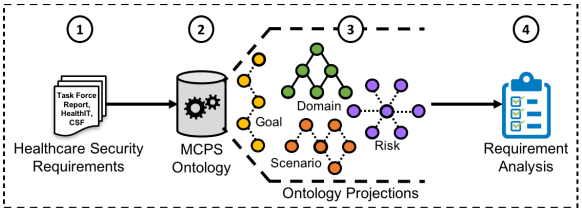

Figure 1: Our Requirements Analysis Approach. (1) Healthcare security requirements are modeled in an ontology (2), and retrieved and analyzed using projections (3), thereby allowing for in-depth requirement analysis (4).

Additionally, in conjunction with, and as a result of the governmental healthcare security push, the HITRUST Alliance was formed in 2009 to develop a comprehensive cybersecurity framework for healthcare based on previous security requirements and frameworks [6]. This resulted in the HITRUST Common Security Framework (CSF), a comprehensive framework detailing the necessary set of security requirements for all healthcare organizations to ensure their cybersecurity.

3 METHODS

As mentioned in Section 1, although a variety of governmental healthcare security requirements have been released to address security concerns and challenges within general healthcare organizations, it is unclear how applicable such requirements may be to MCPS. For this case study, current healthcare security requirements were analyzed in order to determine their coverage, applicability and relevance for MCPS, and thereby identify any covered, inadequate or missing requirements. In order to conduct our analysis, the following steps were completed, as illustrated in Fig. 1: First, the set of healthcare documents containing the security requirements that would be analyzed were identified (1). Next, these requirements were modeled into an ontological representation (2). Finally, ontology projections developed intelligently retrieve specific requirements from the ontology (3), allowing for in-depth requirement analysis (4). We will describe our analysis steps in-depth in the following paragraphs.

Document Identification. As shown in Fig. 1 (1), the first step in our approach was identifying the documents containing healthcare security requirements that would be modeled and analyzed. As explained in Section 2, we chose documents originating from key healthcare cybersecurity-focused acts, including the HITECH act of 2009 and the Cybersecurity Act of 2015. Explicitly, the documents modeled included the HITRUST Common Security Framework (CSF), the Health Care Industry Cybersecurity Task Force's Report on Improving Cybersecurity in the Health Care Industry and HealthIT.gov security pamphlets. These documents were chosen because they are the most highly referenced for implementing security within healthcare environments, as they are believed to have the most comprehensive, high-quality and clear descriptions of requirements and their implementations. For instance, the HITRUST CSF is cited as the "most widely-adopted security framework in the U.S. healthcare industry" [6].

Developing Infrastructure. Once the documents were identified, the next step was modeling the documents in our ontology

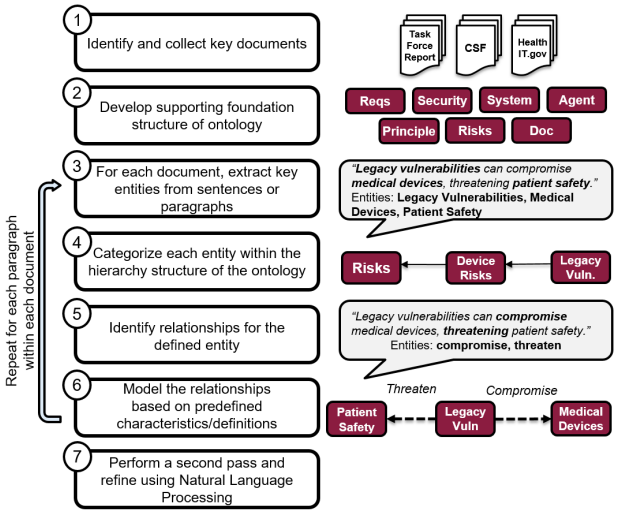

Figure 2: Document Modeling. (1) the foundation of the ontology is developed, (2) documents are identified, (3,4) key entities are extracted and categorized, and (5,6) relationships between entities are identified and modeled. This process is repeated for each paragraph for each document. Finally, (7) a second pass is performed using Natural Language Processing to refine the ontology.

so they could be analyzed. For this purpose, we developed a document modeling algorithm, described in detail in Figure 2. The MCPS Ontology we built comprises more than 720 pages of source documents and contains about 150 entities and 50 different relationships. An example view of the ontology is shown in Figure. 3. Then, we developed and implemented our 4 ontology projections (as described in Section 2).

Overview of MCPS Components. Once our infrastructure was developed, we began our requirements analysis by performing a series of projections surrounding MCPS components, security requirements and risks. First, we obtained a broad overview of the types of relationships and contextual information surrounding components and requirements. The point of this step was to better understand the way data was defined within the ontology (and thereby the documentation), such that structured in-depth analysis could be conducted later. In order to complete this step, a series of Scenario projections were performed for all MCPS components in order to understand general relationships and properties of the entities, and gain an overall understanding of their contexts.

Classification of Requirements and Risks. Next, we analyzed the classes and categorization of requirements and risks (i.e. attack and threat vectors). This was done to better understand the types of requirements and risks contained within the ontology, such that analysis relating the requirements/risks to MCPS components could be conducted and understood later. To complete this step, Domain traversals were used to effectively understand the classification of requirements/risks.

Identification of Relationships. Then, we identified all of the relationships between MCPS components and Requirements, and MCPS Components and Risks. A relationship between a component and a requirement or risk indicates that the requirement/risk

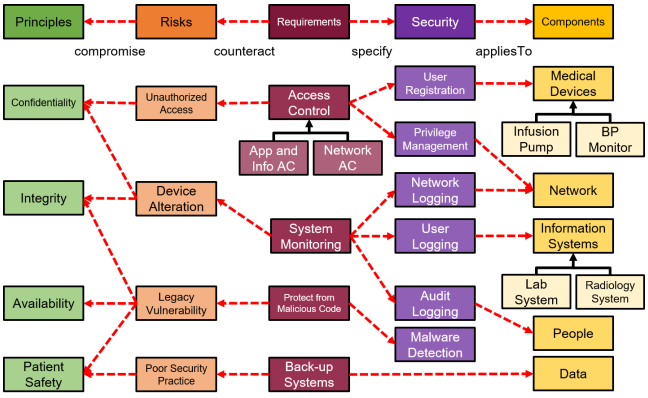

Figure 3: Example Ontology View. There are a variety of Requirements such as Access Control that *counteract* Risks like Unauthorized Access and *specify* Security elements like User Registration. In addition, Risks such as Unauthorized Access may *compromise* Principles like Confidentiality, and Security such as User Registration *applies to* MCPS Components such as Medical Devices.

is specifically applicable to that MCPS component. In order to complete this step, we used Goal and Risk projections. Goal projections start with a concept and retrieve specific entities related to that concept based on a goal. In our case, we performed goal projections for MCPS components, looking for related requirements or risks. Additionally, Risk projections work for a single concept, and pull out all related requirements, security measures, threats and attack vectors. We used Risk Projections to pull out these relationships for MCPS components, and determine the relations between components and requirements/risks. For example, in the Risk Projection shown in Fig. 4 there is a relationship of *implements* between the Requirement *Asset Management* and the MCPS Component *Pacemaker*. This indicates *Asset Management* is applicable to the *Pacemaker* component because this relationship is within the ontology (and therefore listed within the healthcare security documents).

Mapping of Requirements and Components. Finally, we kept a mapping of all of the relationships between MCPS components and requirements/risks. These relationships were mapped using graphical depictions, such as the ones shown in Figs. 5 and 6, until a cohesive picture of all of the relationships between requirements/risks and MCPS components were obtained. From there, we were able to identify missing requirements/risks, or ones that were not applicable to specific MCPS components but should have been. For instance, in the Risk projection for the Pacemaker in Fig. 4, we can see various requirements relevant to the device. However, *Access Control* and *Data Encryption* are not shown within the Risk projection, indicating they do not have relationships with the device and therefore are not described as requirements for a Pacemaker within the documentation. However, both requirements *are* applicable to a Pacemaker, as evidenced by the numerous hacking cases that have disrupted the functioning of Pacemakers as a result of lacking access control or data protections such as encryption [1]. This indicates we have identified the missing requirements of

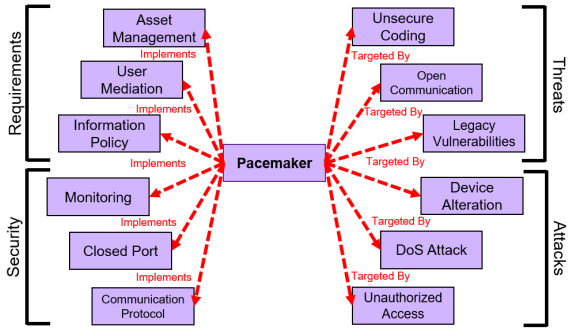

Figure 4: Risk Projection for a Pacemaker.

Access Control and *Data Encryption* for the MCPS component *Pacemaker*.

4 RESULTS

As stated in Section 3, we aimed to analyze requirements in terms of their coverage, applicability and relevance for MCPS, in order to identify covered and missing requirements. Following the methodology outlined previously, we performed a series of projections and identified a variety of missing requirements for MCPS components, which were then validated using 4 real-life MCPS infrastructures.

Requirement Findings. Overall, we analyzed 60 requirements, 56 MCPS components, and 20 risks. Of the 56 components, 24 had applicable requirements. Interestingly, we found that there were missing requirements for a variety of MCPS components, with 32 components having *no* requirements attained to them whatsoever, including *Decision Support*, *Medical Devices*, *Wearable Devices*, *EHR*, and *Sensors*, as shown in Fig. 5 in the dark boxes on the right, highlighted in gray. We are defining missing requirements as the identification that there were no security requirements specifically tailored for, or applicable to, that MCPS component as detailed in the documents we analyzed. It is important to note that although some requirements may, in practice, be relevant to the component (such as *Access Control* for *Medical Devices*), we were only analyzing their coverage within the documentation, and therefore only linked requirements with the components the documents said they were applicable to. In this case, these missing requirements indicate that there are no specific security measures contained within the documents applicable to the afore-mentioned MCPS components. Additionally, of the 56 components, 39 had applicable risks, and 17 components were missing requirements between MCPS components and specific risks. For instance, there were no risks defined for *Decision Support*, *Mobile Devices*, *Wearable Devices*, and *Sensors*, as shown in the dark gray boxes on the right in Fig. 6.

These are important findings, as these missing requirements can result in vulnerabilities and cyber-attacks to MCPS systems, as indicated by the red devils in Figs. 5 and 6. One of the first ways to better protect systems is to determine, through requirements, what security measures need to be implemented to deter threats and attacks. If these requirements do not exist or are not specific to particular system components, these security measures may not be implemented *correctly* or may not be implemented *at all*, and the component will therefore not be protected against a variety of attack vectors and threats.

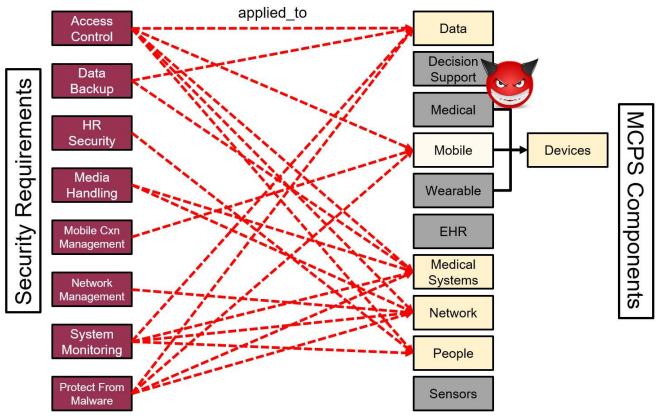

Figure 5: Missing Requirements for MCPS Components. The dark gray boxes on the right indicate no requirements are applicable to these specific components, and thus, that they have missing requirements.

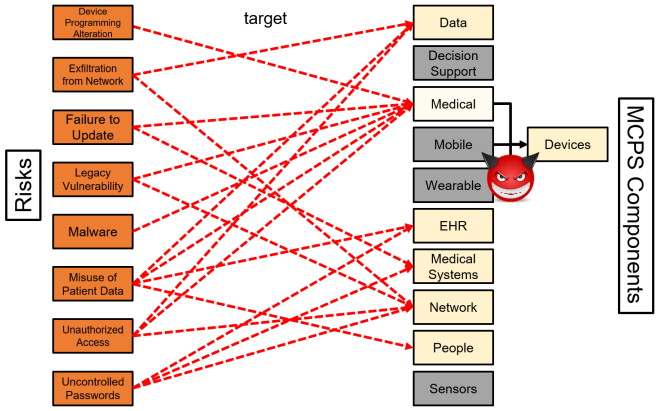

Figure 6: Missing Risks for MCPS Components. The dark gray boxes on the right indicate no risks are applicable to these specific components, and thus, that they have missing risks.

Validation of Findings. In order to validate our findings, we determined if the missing requirements were also contained in real-life MCPS infrastructures. We studied two open-source EHRs (OpenMRS and Open EMR) and two open-source MCPS simulations used in real healthcare environments. OpenMRS is an open-source healthcare software platform that enables the provision and management of healthcare services in developing countries, is used by 1,845 sites around the world, and has over 6.3 million active patients [7]. OpenEMR is an ONC Certified HIT 2014 Edition Complete EHR, one of the few Meaningful Use compliant open-source EHRs, and is installed internationally in more than 15,000 healthcare facilities, and used by more than 45,000 practitioners, serving more than 90 million patients [14]. OpenICE is an open-source integrated clinical environment that connects medical devices and clinical applications and supports the integration and development of the Medical Internet of Things [16]. It is currently implemented in the Interoperability Lab in Cambridge, MA and being used in Massachusetts General Hospital. Finally, Sofia2 SmartHealth is an

Figure 7: Validation Findings of implemented and missing requirements within the documentation and MCPS infrastructures.

open-source Smart Health platform that includes a cloud-based user dashboard to track an individual's health and lifestyle data, as well as the integration and tracking of medical and wearable devices [8]. It is used widely throughout Spain and Latin America. For our validation infrastructures we only used open-source projects due to ease of access. However, each was used widespread through a variety of real-world healthcare environments, thus still enabling us to verify our findings.

For our validation, a subset of 10 security requirements and 10 risks were identified, and each of the infrastructures were studied to determine whether or not they met and implemented these requirements. This subset of requirements (shown on the left in Fig. 7), was hand-picked based on the most general, wide-reaching and relevant requirements to be studied, and includes smaller, more specific sub-requirements. For instance, the requirement *Access Control* includes the sub-requirements of *Network Access Control*, *Device Access Control*, *Personnel Access Management*, etc. We used the criteria specified within the documents about what steps needed to be achieved in order to meet the requirement to determine whether the requirement was implemented or not. For example, in order to meet the *Access Control* requirement, the system must implement an access control model and use a policy that is established, documented, and reviewed, as explained in the HITRUST CSF [6]. From here forward, "requirements" are inclusive of both requirements and risks (with a total of 20 requirements).

Our results are summarized in the depiction shown in Fig. 7. We identified four key findings listed in order from best to worst scenarios: we found that 1) requirements were both in the documents and implemented in the infrastructures (16.25% of cases), 2) requirements were NOT in the documents but implemented in the infrastructures (35% of cases), 3) requirements were in the documents but NOT implemented in the infrastructures (13.75% of cases) and 4) requirements were NOT in the documents and NOT

implemented in the infrastructures (35% of cases). These are shown in the key below in Fig. 7. By infrastructure, OpenMRS implemented 40% of the requirements, OpenEMR implemented 100% of the requirements, OpenICE implemented 15% of the requirements, and Sofia2 implemented 50% of the requirements. Comprehensively, 70% of the requirements were NOT contained within the documentation. Additionally, 48.75% of the requirements were NOT implemented within the infrastructures.

Overall, we validated that security requirements missing from the documentation were also missing from some MCPS infrastructures, especially the OpenMRS and OpenICE architectures. For instance, OpenICE did not implement the requirements *Authentication*, *Data Encryption* and *Malware Protection*, and did not protect against the risks of *DoS*, *Malware*, and *Open Ports*. Positively, we also identified instances in which, even though not listed in the documentation, infrastructures successfully implemented security requirements. For instance, OpenEMR implemented and protected against all of the requirements/risks we analyzed, from *Access Control* to *Unauthorized Access*.

5 RELATED WORK

A variety of approaches have studied health organizations' security requirements in EHRs, medical information systems and mobile devices. For instance, Farhadi et al. [3] and McKnight and Franko [13] studied EHRs and mobile devices respectively, in terms of their compliance with HIPAA and Meaningful Use requirements. In another example, Uwizeyemungu and Poba-Nzaou [20] studied health information systems in Europe for their compliance with basic security measures, defined in terms of Confidentiality, Integrity and Availability. Each of these approaches reported lack of compliance with security requirements for some percentage of the organizations studied. However, none of these studies performed an in-depth analysis of comprehensive requirements; rather, their analyses were high-level, in which they only looked at broad categories of security mechanisms as defined within standards such as HIPAA. In addition, various approaches have studied medical devices and mobile health applications within body sensor networks (BSNs). For example, Gope and Hwang [4] studied a network and developed their own set of broad security requirements to protect BSNs. However, none of them performed an extensive review of current security requirements, nor evaluated their potential applicability to BSNs. Moreover, although BSNs may be included within a MCPS, they themselves are not MCPS, and thus requirements developed for BSNs may not be comprehensive enough for all MCPS.

6 CONCLUSIONS AND FUTURE WORK

In this case study, we have analyzed current healthcare security requirements for MCPS using an approach that leveraged ontological representations and automated requirement traversal techniques. We have identified requirements that are applicable and missing for MCPS, and have validated our findings within current MCPS implementations.

Healthcare has typically taken a backtracking approach when it comes to security, in which the necessary security patches are applied to technology solutions *after* cyberattacks or major life-threatening vulnerabilities are found. As indicated by our findings, security is also not being fully addressed within current guidelines for MCPS, which are themselves new systems. As a result, there is a great opportunity to address and implement these missing requirements as future work, such that future iterations of MCPS may be designed with security in mind from the very beginning, following current and adequate security documentation.

ACKNOWLEDGMENTS AND DISCLAIMER

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780 and by a grant from the Center for Cybersecurity and Digital Forensics at Arizona State University. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of United States Government or any agency thereof.

REFERENCES

[1] CryptoniteNXT Research Team. 2017. *Health Care Cyber Research Report for 2017.* White paper. CryptoniteNXT.
[2] Department of Homeland Security. 2017. Cyber-Physical Systems Security. https://www.dhs.gov/publication/cyber-physical-systems-security
[3] Maryam Farhadi, Hisham Haddad, and Hossain Shahriar. 2018. Compliance of Electronic Health Record Applications With HIPAA Security and Privacy Requirements. In *Security and Privacy Management, Techniques, and Protocols*. IGI Global, 199–213.
[4] Prosanta Gope and Tzonelih Hwang. 2016. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal* 16, 5 (2016), 1368–1376.
[5] Health Care Industry Cybersecurity Task Force. 2017. *Report on Improving Cybersecurity in the Health Care Industry.* White paper. U.S. Department of Health Services.
[6] HITRUST Alliance. 2017. HITRUST Common Security Framework (CSF). https://hitrustalliance.net/hitrust-csf/.
[7] OpenMRS Inc. 2016. OpenMRS. https://openmrs.org/
[8] Indra. 2018. Sofia2 Smart Health. https://sofia2.com/demostradores.html
[9] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn. 2017. OntoEDS: Protecting Energy Delivery Systems by Collaboratively Analyzing Security Requirements. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. 1–10.
[10] Insup Lee, Oleg Sokolsky, Sanjian Chen, John Hatcliff, Eunkyoung Jee, BaekGyu Kim, Andrew King, Margaret Mullen-Fortino, Soojin Park, Alexander Roederer, et al. 2012. Challenges and research directions in medical cyber–physical systems. *Proc. IEEE* 100, 1 (2012), 75–90.
[11] Seok-Won Lee, Robin A Gandhi, and Gail-Joon Ahn. 2007. Certification process artifacts defined as measurable units for software assurance. *Software Process: Improvement and Practice* 12, 2 (2007), 165–189.
[12] Bonnie Malkin. 2013. Dick Cheney had heart device partially disabled to thwart terrorists. www.telegraph.co.uk/news/worldnews/northamerica/usa/10390468/Dick-Cheney-had-heart-device-partially-disabled-to-thwart-terrorists.html.
[13] Randall McKnight and Orrin Franko. 2016. HIPAA compliance with mobile devices among ACGME programs. *Journal of medical systems* 40, 5 (2016), 129.
[14] OEMR. 2018. OpenEMR. www.open-emr.org/
[15] ONC. 2017. HealthIT.gov: Privacy & Security Resources & Tools. http://healthitd8.ahrqstg.org/topic/privacy-security/privacy-security-resources-tools.
[16] MD PnP Research Team. 2018. OpenICE. www.openice.info/
[17] US Congress. 2015. S.754. www.congress.gov/bill/114th-congress/senate-bill/754
[18] US Department of Health and Human Services and others. 2009. HITECH Act enforcement interim final rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf.
[19] US Food and Drug Administration. 2017. Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St Jude Medical's) implantable cardiac pacemakers. https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm
[20] Sylvestre Uwizeyemungu and Placide Poba-Nzaou. 2016. Security and Privacy Practices in Healthcare Information Systems: A Cluster Analysis of European Hospitals.. In *ICISSP*. 37–45.