Security and Privacy Challenges for Healthcare: Minitrack Overview

Miloslava Plachkinova
University of Tampa, USA
mplachkinova@ut.edu

George Grispos
University of Nebraska at Omaha, USA
ggrispos@unomaha.edu

Abstract

The synthesis of information technology into the healthcare industry is creating an environment that is conducive to security and privacy challenges for both industry and academia. As a result, this minitrack is dedicated to reporting the state-of-the-art and recent advancements in this problem domain. Hence, research in this minitrack will examine various responses to these challenges including 'MedDevRisk: Risk Analysis Methodology for Networked Medical Devices' and 'Understanding users' health information privacy concerns for health wearables'. These research contributions highlight the growing need to investigate and address security and privacy concerns in the context of the healthcare industry, especially in light of recent events such as the WannaCry ransomware attack.

1. Introduction

The synthesis of information technology into the healthcare industry is creating opportunities and challenges for both practitioners and academicians. Medical and healthcare systems have transitioned from stand-alone systems into networked data-centric devices [1]. This changing landscape has raised concerns regarding the security and privacy of both healthcare systems and patient information.

This minitrack is dedicated to reporting the state-of-the-art and recent advancements in the field of security and privacy related to healthcare environments. This is only the second year that this minitrack has been promoted at the Hawaii International Conference on System Sciences (HICSS) and submissions were once again received from both research and industry professionals worldwide.

This year we received five submissions, of which only two were accepted for publication. The low number of submissions is, perhaps, an indication of the emerging nature of this research domain. Each submission went through a rigorous peer-review process involving several reviewers, in addition to multiple follow-up rounds with the authors. The submissions which were accepted for publication are 'MedDevRisk: Risk Analysis Methodology for Networked Medical Devices' and 'Understanding Users' Health Information Privacy Concerns for Health Wearables'. A summary of each paper is provided below.

2. MedDevRisk: Risk Analysis Methodology for Networked Medical Devices

Katherine Seale, Jeffrey McDonald, William Glisson, Harold Pardue, and Michael Jacobs from the University of South Alabama, argue the need for risk assessment models to be utilized to help identify security vulnerabilities in medical settings. In order to address the need for actionable risk assessment criteria for healthcare organizations, Seale, et al. introduce a novel framework called *MedDevRisk*.

The MedDevRisk framework integrates several approaches, which are commonly used in both government and industry. These include the STRIDE threat model, Common Vulnerabilities and Exposures (CVE), and the Common Vulnerability Scoring System (CVSS). This framework also proposes the relational integration of network device information with their attendant security threats and potential remediation steps. Seale, et al. go on to argue that the consolidation of this data can provide underlying relationships which can answer risk assessment questions pertinent to both lower-level administrators and higher level managers that make decisions on money and resources.

The results from the technical aspects of this research indicate that it is possible to successfully integrate relational data models with threat vulnerability asset associations. The implementation of the MedDevRisk model with data from an operational medical simulation training unit

URI: http://hdl.handle.net/10125/50300
ISBN: 978-0-9981331-1-9

demonstrates that the model can be used to generate actionable threat assessment criteria for healthcare organizations. Seale, et al. go on to state that future work will extend this research to include larger data samples and more diverse medical devices. In addition, Seale, et al. also propose the idea of automating data collection from static documents, web-based reports, or schemas that acquire data in real-time from multiple sources.

3. Understanding Users' Health Information Privacy Concerns for Health Wearables

Mortiz Becker from Ludwig Maximilian University of Munich focuses on privacy concerns for healthcare wearables. More specifically, Becker attempts to answer the question: What factors influence the health information privacy concerns of health wearable users? Hence, Becker uses the health information privacy concerns model [2] to address privacy concerns with health information technologies and developed an interview guide on the six dimensions of the model (Collection, Unauthorized Secondary Use, Improper Access, Errors, Control and Awareness).

Becker then undertook seven semi-structured focus groups with six users of health wearables and applied a rigorous iterative thematic analysis to empirically understand users' mindsets regarding their health information privacy concerns. By reviewing the conducted codes in the literature, Becker enhances the theoretical understanding of health information privacy concerns by proposing three central factors (Dilemma of Forced Acceptance, State-Trait Data Sensitivity and Transparency). This thematic map can be used by other researchers to further examine the understanding of privacy perception of health wearables users and help practitioners to develop privacy-friendly devices.

While Becker's study focused on actual users of health wearables, future work will focus on *potential* users of these devices in order to better understand their motivation to use such devices. In particular, this study will examine if potential users are influenced by stricter privacy laws, for example the European Union's new General Data Protection Regulation (GDPR).

4. Potential Research Roadmap

Data breaches continue to impact organizations around the world [3]. As a result, potentially personal and sensitive information related to patients and their medical history could be a risk. Hence, a future research agenda for the healthcare community should involve addressing these risks through proactive measures. The two papers presented in this minitrack already outline two proactive approaches, with regard to identifying risks associated with medical devices and the privacy concerns of individuals who wear health wearables. However, there is much to be done. Research efforts need to focus on healthcare security and privacy challenges that are relatively new and understudied. For example, challenges related to Health Information Exchange (HIE) at national levels, cloud solutions and their impact on security and privacy, multimedia health data privacy, big data impact on healthcare environments, and the impact of regulations such as GDPR.

5. Contributions and Conclusions

The Security and Privacy Challenges for Healthcare minitrack at HICSS-51 focuses on research that attempts to address concerns related to security and privacy in the healthcare domain. Recent technological advancements in this domain demonstrate the need to better understand challenges associated with collecting, storing, and handling patient information generated by next-generation healthcare devices and systems. The papers presented in this minitrack offer a unique and novel perspective on some of these challenges. Given the relatively new face of this research area, it is important to continue involving both practitioners and researchers with interdisciplinary backgrounds so that potential solutions can continue to be deployed in healthcare environments. The research undertaken by researchers and practitioners at various institutions should motivate the community to continue to work in the field. We hope to continue providing both scholars and healthcare professionals with an outlet at HICSS to share their work with the community.

6. References

[1] Grispos, G., Glisson, W.B., and Choo, K-K.R., "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach", Connected Health: Applications, Systems and Engineering Technologies, IEEE/ACM International Conference on. IEEE, 2017.

[2] Kenny, G., and Connolly, R., "Drivers of Health Information Privacy Concern: A Comparison Study ", Proceedings of the 22nd Americas Conference on Information Systems (AMCIS), 2016, pp. 1 – 10.

[3] Breach Level Index Website - http://breachlevelindex.com – accessed on October 14, 2017