Security and Privacy Challenges for Healthcare: Minitrack Overview

Miloslava Plachkinova
Information and Technology Management Department
University of Tampa, FL, USA
mplachkinova@ut.edu

George Grispos
Lero – The Irish Software Research Centre
University of Limerick, Limerick, Ireland
george.gispos@lero.ie

Abstract

The Security and Privacy Challenges for Healthcare minitrack at HICSS-50 provides a unique perspective on the emerging field of information security and privacy advancements in healthcare. Three high quality papers were selected for the minitrack, which represent a wide range of research interests. These include evaluating the tension between sharing and protecting health information, assessing risk to ambulatory medical devices using attack-graph threat modeling, and privacy-aware research and development in wearable health technology. While distinct, these papers touch upon a very common growing concern in our society, namely addressing security and privacy concerns during the collection, storage and handling of Protected Health Information (PHI) and electronic health records.

1. Introduction

As technology is incorporated into more aspects of healthcare environments, the number of security incident and data breaches affecting healthcare providers and organizations is increasing [1]. This introduces a variety of challenges for both medical professionals and researchers. One of these challenges involves protecting the security and privacy of patient Protected Health Information (PHI) and electronic health records from unintentional disclosure.

The Security and Privacy Challenges for Healthcare minitrack was proposed for the first time at the 50th Hawaii International Conference on System Sciences (HICSS). Submissions to the minitrack have come from both researchers and industry professionals from around the world. The high-quality submissions to the minitrack resulted in an acceptance rate of 33%. The minitrack this year focuses on identifying and validating technical solutions and strategies that aim to improve the protection of healthcare information. The main research topics covered this year include evaluating the tension between sharing and protecting health information, assessing risk to ambulatory medical devices using attack-graph threat modeling, and privacy-aware research and development in wearable health. These three topics, while distinct, further emphasize the need for more security and privacy research in the field of IT healthcare.

2. A Framework for Evaluating the Tension between Sharing and Protecting Health Information

The research conducted by Chad Anderson from Northern Kentucky University, Richard Baskerville from Georgia State University and Curtin University, and Mala Kaul at University of Nevada, Reno focuses on evaluating the tension between sharing and protecting health information. Their idea was to propose a new theory related to information security control and provide explanations for this phenomenon. This paper was nominated for the Best Paper Award.

These researchers argue that Health Information Exchange (HIE) is expected to improve the quality and cost of healthcare. However, the sustained use of HIE by healthcare providers has been difficult to achieve. This is because of a number of factors that influence this process, including concerns for the security and privacy of the exchanged information. Moreover, Anderson, et al. argue that the tensions between the benefits of HIE resulting from collaboration and information sharing and the security risks inherent in the exchange process are not well understood by the community.

Hence, Anderson, et al. propose an information security control theory to explain this tension. This theory is then evaluated through a qualitative case study involving a HIE organization in the Western United States. The case study was utilized to evaluate the HIE's information security policy development process. Anderson, et al. conclude that their theory

URI: http://hdl.handle.net/10125/41597
ISBN: 978-0-9981331-0-2

provides a framework through which the community can better understand security policy development processes.

3. Assessing Risk to Ambulatory Medical Devices Using Attack-Graph Threat Modeling

Patrick Luckett, Jeffrey McDonald, and William Bradley Glisson from the University of South Alabama argue that assimilating new technologies (such as medical devices to monitor a patient's vital signs) into the healthcare domain creates an environment that is conducive to malicious activities. To this extent, Luckett, et al. present attack graph modeling as a viable solution for identifying vulnerabilities, assessing risk, and forming mitigation strategies to protect ambulatory medical devices.

This is a topic of growing concern for both medical professionals and patients, who are beginning to integrate more medical devices in the healthcare field. The research highlights the need to model medical ambulatory devices separately from traditional medical devices. Luckett, et al. argue that this is because certain attack vectors pose greater risk to these devices, including physical attacks and social engineering.

Luckett, et al. begin by conducting a review of the literature examining relevant work concerning attack graph models and examine the security and privacy risks associated with medical devices. The researchers then propose a model of a theoretical ambulatory device that consists of three sensors that are used to monitor a patient's vital signs. The sensors communicate through a wireless signal to a cellular smart phone, which runs an application that processes, analyzes, and stores the data. The researchers then use this theoretical device to present an attack graph modeling example, which is used to highlight vulnerabilities and mitigation strategies that need to be considered when designing ambulatory medical devices with similar components.

4. Towards Privacy-Aware Research and Development in Wearable Health

Michelle De Mooy at the Center for Democracy & Technology, Washington, District of Columbia and Shelten Yuen at Fitbit, Inc. have worked together to present an interesting perspective on privacy-aware research related to the increased use of wearable devices. Such collaborations between research and business professionals demonstrates the practical applications of the research concepts discussed at HICSS and showcases the broader impact our discipline is making on society.

De Mooy and Yeun argue that wearable sensor technology has the potential to transform healthcare and that the investigation and testing of sensors in the commercial sector can offer several insights. These include identifying ways to leverage biometric data, improving individual health through better products and advancing the public good through research

However, De Mooy and Yeun go on to state that any research into wearable technology and sensor data must be done in a manner that takes into consideration ethical dilemmas and respects user privacy. The contribution of the paper is a report on the findings of a yearlong investigation with Fitbit, into how to build recommendations on ethics and user privacy in wearable device research.

5. Contributions and Conclusions

The Security and Privacy Challenges for Healthcare minitrack at HICSS-50 focuses research that attempts to address concerns related to security and privacy in the healthcare domain. Recent technological advancements in the healthcare domain demonstrate the need to better understand the challenges associated with collecting, storing, and handling protected health information and electronic health records. 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 work done by researchers and practitioners at various institutions should motivate the community to continue to work in the field. We hope through the HICSS minitrack to provide an outlet for both scholars and healthcare professionals to share their work with the community.

6. References

[1] Kelly Jackson Higgins (2016). Healthcare Suffers Estimated $6.2 Billion in Data Breaches. Available Online: http://www.darkreading.com/threat-intelligence/healthcare-suffers-estimated-$62-billion-in-data-breaches/d/d-id/1325482