Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

Security and Privacy Challenges for Healthcare: Minitrack Overview

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

Au Vo
San Francisco State University, CA, USA
auvo@sfsu.edu

Abstract

The growing use of information technology in healthcare provides many opportunities for improving quality of care, better patient support, and health outcomes. However, it also opens the door to many individuals with malicious intentions who are looking for ways to compromise healthcare systems, data, and various medical devices.

This minitrack provides a venue for researchers and practitioners to share their state-of-the-art and recent advancements in the field of healthcare security and privacy. These findings come as a result of the increasing need to protect patients' data through initiatives such as the General Data Privacy Regulation (GDPR) in the European Union or the integration of smart devices for healthcare monitoring and clinical decision-making. The following studies present a much needed analysis of the current issues in the field of security and privacy for healthcare and provide directions for future research contributions.

1. Introduction

The growing use of information technology in healthcare provides many opportunities for improving quality of care, better patient support, and health outcomes. However, it also opens the door to many individuals with malicious intentions who are looking for ways to compromise healthcare systems, data, and various medical devices.

This minitrack provides a venue for researchers and practitioners to share their state-of-the-art and recent advancements in the field of healthcare security and privacy. These findings come as a result of the increasing need to protect patients' data through initiatives such as the General Data Privacy Regulation (GDPR) in the European Union or the integration of smart devices for healthcare monitoring and clinical decision-making. The following studies present a much needed analysis of the current issues in the field of security and privacy for healthcare and provide directions for future research contributions. This is the third 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 ten submissions, of which only four were accepted for publication. This is double the number of submissions we got in the previous year and indicates the growing research interest in solving complex issues in the field of security and privacy. 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 "A Bleeding Digital Heart: Identifying Residual Data Generation from Smartphone Applications Interacting with Medical Devices", "No Risk, More Fun! Automating Breach of Confidentiality Risk Assessment for Android Mobile Health Applications", "A Novel Privacy Preserving Search Technique for Stego Data in Untrusted Cloud", and "The Impact of Persuasive Messages on the Disclosure of Personal Health Information". Following are the abstracts of each paper.

2. A Bleeding Digital Heart: Identifying Residual Data Generation from Smartphone Applications Interacting with Medical Devices

George Grispos of University of Nebraska, Omaha, William Bradley Glisson and Peter A. Cooper of the Sam Houston State University demonstrate how smartphone applications integrated with medical devices can be compromised and residual data can be used to compromise users' protected health information.

The integration of medical devices in everyday life prompts the idea that these devices will increasingly have evidential value in civil and criminal proceedings. However, the investigation of these devices presents new challenges for the digital forensics community. Previous research has shown that mobile devices provide investigators with a wealth of information. Hence, mobile devices that are used within medical environments potentially provide an avenue for investigating and analyzing digital evidence from such devices.

The research contribution of this paper is twofold. First, it provides an empirical analysis of the viability of using information from smartphone applications developed to complement a medical device, as digital evidence. Second, it includes documentation on the artifacts that are potentially useful in a digital forensics investigation of smartphone applications that interact with medical devices.

3. No Risk, More Fun! Automating Breach of Confidentiality Risk Assessment for Android Mobile Health Applications

Thomas Brüggemann of blueworld GmbH, Cologne, Germany, together with his colleagues Tobias Dehling and Ali Sunyaev from Karlsruhe Institute of Technology, in Karlsruhe, Germany discuss confidentiality risks associated with mobile health application.

With the rapidly rising number of mobile health (mHealth) applications (apps), it is unfeasible to manually review mHealth apps for information privacy risks. One salient information privacy risk of mHealth apps are confidentiality breaches. We explore whether and how static code analysis is a feasible technology for app review automation. Evaluation of our research prototype shows that, on average, our prototype detected one breach of confidentiality risk more than human reviewers. Contributions are the demonstration that static code analysis is a feasible technology for detection of confidentiality breaches in mHealth apps, the derivation of eight generic design patterns for confidentiality breach risk assessments, and the identification of architectural challenges that need to be resolved for wide-spread dissemination of breach of confidentiality risk assessment tools. In terms of effectiveness, humans still outperform computers. However, we build a foundation for leveraging computation power to scale up breach of confidentiality risk assessments.

4. A Novel Privacy Preserving Search Technique for Stego Data in Untrusted Cloud

Mohammad Saidur Rahman, Ibrahim Khalil, Xun Yi, and Tao Gu from RMIT University, Melbourne, Australia investigated a novel approach to perform searching for stego health data data in untrusted clouds.

We propose the first privacy preserving search technique for stego health data in untrusted cloud in this paper. The Cloud computing is a popular technology to the healthcare providers for outsourcing health data due to flexibility and cost effectiveness. However, outsourcing health data to the cloud introduces serious privacy issues to the patient. For example, dishonest personnel of the cloud provider may disclose patient sensitive information to business organizations for some financial benefits. Using steganography, patient sensitive information is hidden within health data for privacy preservation. As a result, stego health data is generated. To the best of our knowledge, no method exists for searching a particular stego data without disclosing any information to the cloud. We propose a framework for privacy preserving search over stego health data. We systematically describe each component of the proposed framework. We conduct several experiments to evaluate the performance of the framework.

5. The Impact of Persuasive Messages on the Disclosure of Personal Health Information

Moritz Becker of LMU Munich, Germany and Christian Matt of University of Bern, Switzerland present an investigation on the impact of persuasive messages related to the disclosure of personal health information.

Individuals’ disclosure of personal health information (PHI) holds substantial benefits for providers, but users are often reluctant to disclose. While providers can employ persuasive messages, little is known about their effects in the sensitive context of PHI disclosure. To address this research gap, we conduct a web-based experiment with 529 non-users of health wearables (HWs) to examine the influences of persuasive messages (attribute framing and argument strength) on individuals’ PHI disclosure. We reveal that individuals tend to disclose more PHI when they experience persuasive messages with more positively framed HW attributes or messages with higher argument strength concerning data collection. We enable researchers to uncover the impact of persuasive messages in highly sensitive data environments and provide practitioners with workable suggestions to have individuals disclose more PHI.

6. Contributions and Conclusions

The Security and Privacy Challenges for Healthcare minitrack at HICSS-52 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 studies undertaken by researchers and practitioners at various institutions should motivate the community to continue to work in the field. We hope to continue providing the community with an outlet at HICSS to share their work and propose novel solutions to complex issues in the field.