A SECURITY RISK PERCEPTION MODEL FOR THE ADOPTION OF MOBILE DEVICES IN THE HEALTHCARE INDUSTRY

by
Alex Alexandrou

Submitted in partial fulfillment
of the requirements for the degree of
Doctor of Professional Studies
in Computing

at

Seidenberg School of Computer Science
and Information Systems

Pace University

July 2015

Approval Page

We hereby certify that this dissertation, submitted by Alex Alexandrou, satisfies the dissertation requirements for the degree of Doctor of Professional Studies in Computing and has been approved.

7/15/15

Dr. Li-Chiou Chen
Chairperson of Dissertation Committee

Date

7/15/15

Dr. Lixin Tao
Dissertation Committee Member

Date

7/15/15

Dr. Jane Bear-Lehman
Dissertation Committee Member

Date

Seidenberg School of Computer Science and Information Systems
Pace University 2015

Abstract

A Security Risk Perception Model for the Adoption of Mobile Devices in the Healthcare Industry

by
Alex Alexandrou

Submitted in partial fulfillment
of the requirements for the degree of
Doctor of Professional Studies
in Computing

July 2015

The widespread adoption and use of mobile devices in medical institutions, while beneficial, can also create security concerns for healthcare practitioners: physicians, nurses, information technology (IT) administrators, and healthcare management. To understand how healthcare practitioners perceive the security risks associated with mobile devices, the author developed a research model. This model suggests that a healthcare practitioner's security perception is related to multiple subjective beliefs which could indirectly impact their behavior intentions when using the devices and adopting security controls in the workplace. Furthermore, the research studied the differences in perception among healthcare practitioners when mobile devices are provided either by healthcare institutions, Hospital-Provided-Devices, (HPD) or by themselves, Bring-Your-Own-Devices (BYOD). The study incorporates mixed research by layering two different methods. First, using quantitative research, the author conducted an empirical study of a proposed model, recruiting 264 healthcare practitioners from three hospitals and its affiliated clinics to participate in a written survey. Second, using a post-survey qualitative interview, the study constructed open-ended questions to investigate the safeguard cost of using mobile devices to access medical information. Through the empirical study, the researcher discovered that the factors that impact the healthcare practitioner's behavior depend on how the mobile devices are provided. The results provide an insight into how mobile devices are used in the healthcare industry.

Acknowledgments

I would like to offer my appreciation and deepest gratitude for the assistance and guidance provided by my advisor Dr. Li-Chiou Chen, who had faith in me. This research would not have been possible without her guidance, and many hours of supervision and countless revisions.

I also want to thank Dr. Fred Grossman, who pushed me and questioned every single aspect of this research. After five years of hard work, I will finally get my weekends back.

I want to acknowledge Dr. Lixin Tao, Dr. Charles Tappert, Ms. Chris Longo, and other Pace professors and administrators for their support and guidance.

I am also indebted to the members of my dissertation committee Dr. Li-Chiou Chen, Dr. Lixin Tao, and Dr. Jane Bear-Lehman.

I am deeply grateful to Mr. Monir Doss, the CFO of Medisys, Christine Thompson, Maurice Rupnaraine for his technical expertise and encouragement, and Sylvia Russakoff for her relentless help in writing.

Finally, my thanks to all the administrators, nurses, physicians, technicians and students in the three hospitals and clinics I studied for their participation in this research. I greatly appreciate the time they invested in answering all my questions. This research would not have been possible without their participation.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The adoption of smartphones and tablets has transformed our everyday lives. Information that took time to find is now available in a single click by using Google or an application for the Internet or smart device known as an "app". As healthcare technology has advanced with the adoption of the Electronic Medical Record (EMR) and the Electronic Health Record (EHR), mobile devices have quickly became one of the technological choices among healthcare practitioners. They have gained popularity among physicians, nurses and medical students, even though some medical institutions do not support them due to security considerations. Because of this development, information technology (IT) departments in healthcare organizations must have a strategy to support these devices while protecting confidential data. The high cost of information structure, and support, along with security issues and required compliance that accompanies it are of vital importance to small community hospitals and medical practices, regardless of whether or not they decide to support the use of mobile devices.

1.1 Problem Statement

One of the most important and challenging issues that healthcare practitioners must deal with is how to secure the personal information of patients and address their privacy concerns when mobile devices are used. The vulnerability of mobile devices in the healthcare environment makes them an attractive target for hackers attempting to collect personal information on a massive scale [86]. Federal regulations, such as the Health

Insurance Portability and Accountability Act[1] (HIPAA) and the Health Information Technology for Economic and Clinical Health Act[2] (HITECH), require protection of medical records but specific mechanisms for doing this are not included. As a result, this research is aimed at first understanding the risks of using mobile devices whether they are Hospital-Provided-Devices (HPD) or Bring-Your-Own-Devices (BYOD). The second goal of this research is to understand how healthcare practitioners perceive the security risks of using mobile devices in the healthcare environment, and how this risk perception affects their intent to use the devices as well as their inclination to adopt the security controls that are required.

This research will provide healthcare administrators with insight on how to manage mobile devices in the healthcare environment. The research focuses on two scenarios: first, the BYOD scenario where healthcare practitioners are allowed to use their personal mobile devices in the workplace to access EMR and EHR; and second, the HPD scenario where mobile devices are provided and maintained by the healthcare institutions themselves.

The use of BYOD poses additional security challenges for healthcare administrators. A previous survey[3] showed some difference in opinion between what IT managers and IT employees think are the most important requirements for BYOD devices. To facilitate further understanding of this issue, this research examines a set of hypotheses related to security risk perception for both the BYOD and HPD scenarios. Finally, the research

[1] http://www.hhs.gov/ocr/privacy/hipaa/understanding/
[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
[3] http://www.samsung.com/us/pdf/byod/2013_BYOD_Index_20130103c.pdf

examines factors that contribute to these perceptions of risk (or lack thereof) and how best to communicate these security risks to healthcare practitioners.

This study includes a quantitative component (a web survey) and a qualitative component (post-survey interviews). Furthermore, the interviews will elicit information on how familiar healthcare practitioners are with safeguards to counteract security risks (authentication, password, malware, loss of devices, Wi-Fi security, Bluetooth attacks), and whether they perceive the costs that these safeguards may impose on their work. The qualitative results will both strengthen and validate the quantitative results.

1.2 Main Research Questions

The primary focus of this study is to understand how the risks to information security posed by the use of mobile devices to access patients' medical and personal information are perceived by healthcare practitioners. We defined "perceived security risk" as the subjective judgment of the healthcare practitioner regarding information security when using a mobile device.

The increased use of mobile devices by healthcare practitioners can easily result in a security breach of health and medical information, as well as result in hefty federal fines. Taking into consideration the literature and industry experts (chapters 2 & 3), this researcher wanted to examine the risk perception of healthcare practitioners regarding the security of mobile devices accessing EMR.

Specifically, the following are the main research questions that this research study will answer:

- What are the security risks perceived by healthcare practitioners regarding the use of HPD in the workplace? What factors impact the risk perception for HPD? What factors impact their willingness to adopt security controls required for the use of mobile devices?
- What are the security risks perceived by healthcare practitioners regarding the use of BYOD in the workplace? What factors impact the risk perception for BYOD? What factors impact their willingness to adopt security controls required for the use of mobile devices?
- Are the perceived security risks different between BYOD and HPD and among different groups of healthcare practitioners?
- How can healthcare practitioners be made aware of both security risks and security controls when using mobile devices in the workplace?

Chapter 2

Security and Privacy Issues Using

Mobile Devices to Access Electronic Medical Record Systems

When EMR and EHR first became standard in medical offices and healthcare institutions, laptop and desktop computers were the main devices for accessing them. At the present time, (2015) healthcare institutions use either thin-client or laptop computers placed in carts, or desktop computer stations, which are typically placed on nursing units or embedded in hallways. The thin-client is designed to serve as the client-server architecture and is intended to be a small device. The majority of the data processing occurs on the hospital servers. With the adoption of EMR and EHR in healthcare institutions, all information related to patient care, including basic demographic information, treatments, medications, and billing, must be entered in the EMR/EHR database. As a result, there are not enough computers for every healthcare practitioner to enter information at the same time. This need for more hardware promotes the use of mobile devices by healthcare practitioners. Furthermore, since mobile devices are lighter than laptops or desktops, they are easier to use at the bedside.

Healthcare institutions as well as government agencies are looking at these devices to replace laptops and desktops, mainly for cost reduction. The new mobile devices are considered handheld computers rather than phones or entertainment devices (tablets).

Mobile devices have thus become one of the primary technological tools for healthcare practitioners. Due to their powerful computing capacity, relatively large screen size, high-resolution display, and relatively low cost, these devices are transforming

healthcare. In a recent study by EPOCRATES[4] 49 percent of 1,063 healthcare practitioners already use smartphones and tablets during the day. The use of mobile devices is surpassing that of computers among healthcare practitioners for accessing patient information such as medication dosages, medical records, and medical references, as well as for communication with other practitioners. The report continues to find that tablet use increased from 19 percent within one year. With new innovations, such as Google Glass, IBM's Watson and more sophisticated applications (such as 3D imaging applications), mobile devices could potentially become the primary tools gathering patient medical information. As we discover further in our research, healthcare practitioners prefer to use mobile devices to access patient data faster and with more ease. This could potentially increase the risk of comprising medical and personal information. More devices accessing sensitive patient data wirelessly can lead to an increase in malicious attacks. Wireless traffic was expected to nearly double between 2013 and 2015, propelled by mobile devices, according to Forrester Research's 2013 mobility survey[5]. Currently this trend varies depending on the healthcare institution. Healthcare practitioners already use tablets or smart phones in the healthcare setting; these are currently used to transfer notes or send prescriptions to a personal computer; however, this is only the beginning of what they will be used for in the future.

[4]http://www.epocrates.com/oldsite/statistics/2013%20Epocrates%20Mobile%20Trends%20Report_FINAL.pdf
[5] http://www.forrester.com/Forrsights+Telecom+And+Mobility+Workforce+Survey+Q2+2013/-/E-SUS2191

2.1 Current Mobile Devices Trends in Medical Institutions

During the last few years, mobile devices have spread into the healthcare industry more than ever. These devices have been shown to be beneficial for healthcare practitioners as they can obtain patient information anywhere; in addition they increase communication with other practitioners. In healthcare, mobile technology is successful if it ensures seamless access to information, medical resources and communication at any time and place. Mobile devices have evolved since the early days of the personal digital assistant (PDA) such as Palm, Windows CE, etc., and healthcare practitioners were among the earliest adopters of these devices. Before the universal expansion of EMR/EHR these devices were used primarily as medical libraries, keeping track of appointments, or to store radiology images for patients. At the present time, in a typical healthcare setting, doctors, nurses, and patients constantly use these technologies to access information as hospitals and healthcare systems now integrate these devices into their networks to allow access to patient data. The four market leaders are; Apple's iOS, Google's Android, Research in Motion's Blackberry platforms and Microsoft's Windows OS. In this study we will be using the following definitions in regard to the use of mobile devices in healthcare institutions.

- Mobile Devices: This research will be focused on tablets and smart phones; laptops will be excluded. Most laptops are bulky and require a surface to place them on for effective data entry. This process can place a physical barrier between the doctor and the patient and can prevent effective communication. You can place the tablet on the lap and use it to enter data much like taking notes on a paper chart or clipboard. Furthermore, since the tablet is smaller and lighter

compared to most laptops, it allows providers to interview patients without a large physical barrier, as the laptop can be. As more mobile devices and applications become easier to use, affordable and more powerful, the adaptation to healthcare providers will grow exponentially.

- Healthcare providers: The healthcare providers that were the subject of this study include: physicians, nurses, nursing assistants and medical technicians such as respiratory and physical therapists.
- (BYOD) is short for bring your own device: BYOD refers to those employees who bring their personal computing devices such as smartphones, laptops and tablets to the workplace for use and then connect to the corporate network. This trend is also known as the "consumerization" of Information Technology (IT). This research study focused on tablets and smart phones.
- Consumerization of IT: This is a phrase used to describe the cycle of information technology (IT) emerging in the consumer market, then spreading to business and government organizations, largely because employees are using the popular "consumer market" technologies and devices at home and then introducing them in the workplace.
- EMR/EHR System: An electronic medical record or electronic health record system is a computerized record of a patient's health history, and is usually used in a hospital or outpatient setting, such as a clinic or doctor's office.
- Hospital provided device (HPD): These are electronic devices that are provided by institutions and include tablets and smart phones. These devices are

programmed by the IT department and are prohibited for personal use. In most cases, these devices cannot be removed from the medical institution.

Healthcare settings provide an appropriate platform for the use of mobile devices. Numerous factors have contributed to the popularity of these devices in healthcare, including their relatively low expense, ease of use, and portability. Healthcare institutions divide mobile devices into two categories, Bring-Your-Own-Device (BYOD) and Hospital-Provided-Device (HPD). The federal government supports the concept by producing a Toolkit[6] to support federal agencies implementing BYOD programs. The toolkit is part of the Digital Government Strategy[7], issued by Federal Chief Information Officer (CIO) Steven VanRoekel on May 23, 2012, and provides policies and best practices. By using their own devices employees no longer have to carry two different devices, and no longer have to learn different operating systems for these devices. As we discovered in this research, ease of use can be a major benefit in the adoption of mobile devices. Healthcare practitioners, especially physicians, need to be able to access and search medical information, no matter their location or device brand, or where the data is located. The HPD concept is the costlier of two since a medical institution has to purchase and maintain these devices. In addition to the benefits of using mobile devices there are security concerns, since all medical data are accessed online and are therefore vulnerable. With many healthcare practitioners using their own mobile devices for

[6] https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf
[7] https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

accessing medical and personal patient information, there are concerns regarding regulating their use under the HIPAA, HITECH and Joint Commission policies[8].

Although mobile devices don't store patient data, they display it, so some institutions are installing antivirus and anti-malware software on devices that access their wireless networks. Some healthcare institutions are not aware of the security threats, and do not have the resources to maintain the devices. However, healthcare practitioners are required by law to protect patient medical and personal information.

Every healthcare institution must comply with rules regarding the disposal of medical records, including hardware, software and any devices that can be used to store patient medical and personal information. One common practice among physicians is to text non-encrypted patient medical and personal information to each other even though is against the HIPAA regulations. As one physician describes in a post-survey interview: *"two o'clock in the morning, if I need a consultation from a specialist physician instead of bring the physician in the hospital, I text the results. This is a HIPAA violation but it is a practice that is been done by all residents and physicians because it is a safe time for consultations."* The following figure is a typical diagram of how mobile devices are connected to a medical institution's network (figure 1). Every medical record company has developed its own proprietary application (like Haiku and Canto for Epic EMR). Other companies specialize in providing enterprise mobile management solutions for accessing patient data using mobile devices.

[8] http://www.jointcommission.org/standards_information/standards.aspx

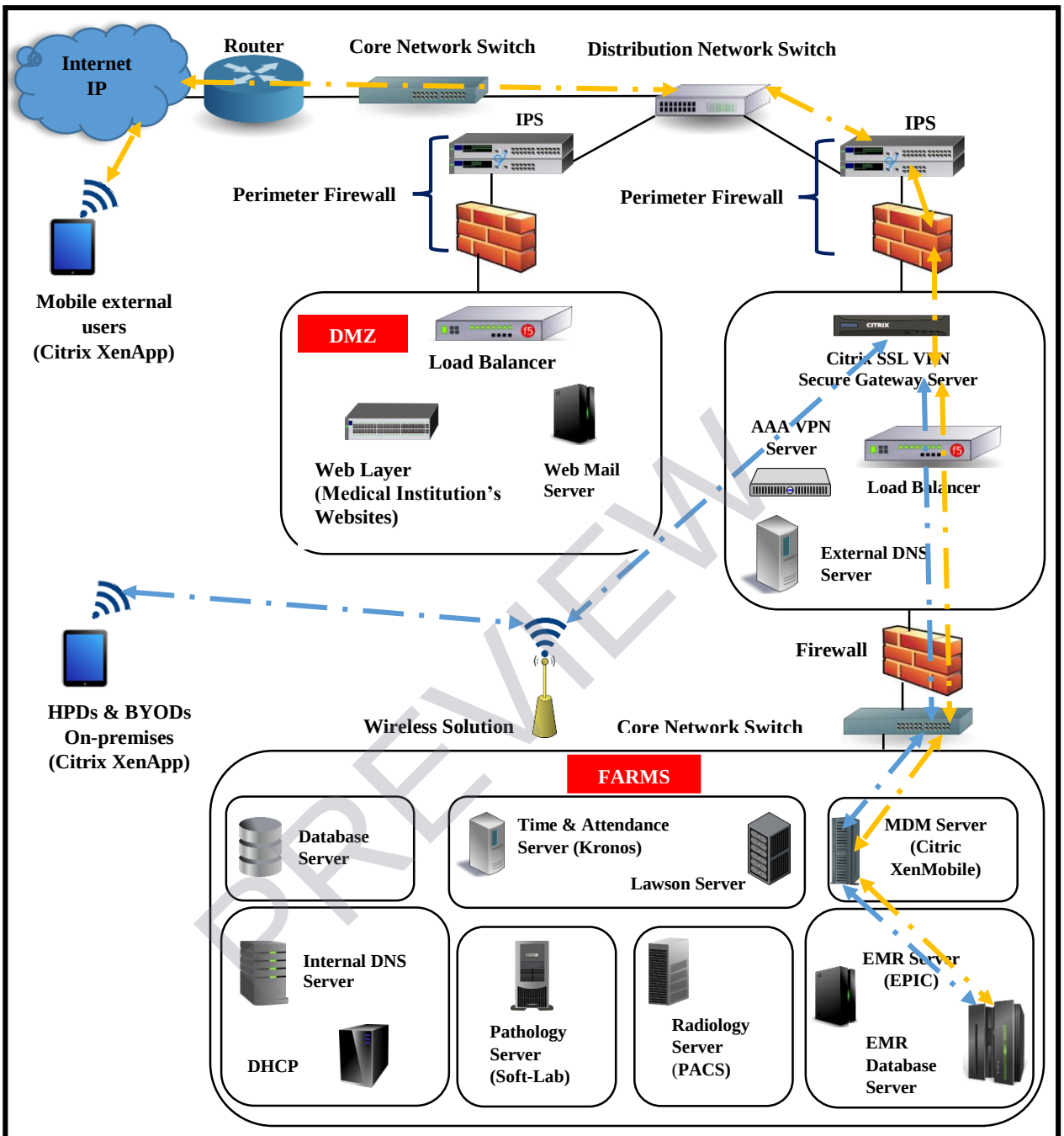

Figure 1: An illustration of how mobile devices access EMR in a medical institution.
***On-premises mobile devices using Citrix XenApp (HPDs-BYODS)**
****Mobile external users using Citrix XenApp**

Definitions for Figure 1

- **Internet Protocol (IP):** The IP is a unique identifying number (address) for each computer by which data can be sent from one computer address to another via the Internet. *"Every host and router on Internet has an IP address that can be used in the source address and destination address field of IP packets."* [115].
- **Transport Layer Security (TLS) protocol, and Secure Sockets Layer (SSL) protocol**: Are used to provide secure communication between a browser and server.
- **Router:** This device connects computers to the Internet. *"A router acts as a dispatcher, choosing the best path for information to travel so it's received quickly.*[9]*"*
- **Network Switch**: *"A switch serves as a controller, enabling networked devices to talk to each other efficiently"*[10] According to Cisco there are 3 layers in the hierarchical network model; core, distribution and access. The core network switch transfers large numbers of packets as fast as possible. The distribution switch controls the access of data to the core, and the access switch brings local users into the network.
- **Perimeter Firewall:** This filter controls/inspects incoming and outgoing network traffic. The perimeter firewall resides in the perimeter which is protected by the perimeter switch and IPS. [115]

[9]http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html
[10]http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html

- **Intrusion Prevention Systems (IPS):** The IPS monitors the network for malicious activities (detects, prevents, identifies, and logs information about malicious activity). The IPS and perimeter firewall stand as the first defense of the medical institution's environment. *"IPS has the ability to block traffic by discarding packets as well as simply detecting suspicious traffic."*[21]
- **Load Balancer:** This distributes data evenly across a computer network preventing it from becoming overwhelmed.[11] [115]
- **Application layer:** This is a layer in the Open Systems Interconnection (OSI) seven layer model and in the Transmission Control Protocol/Internet Protocol (TCP/IP). The application layer provides services like simple mail transfer protocol (SMTP), file transfer, web surfing, network data sharing, etc. [115]
- **Wireless solution:** This is a device that connects users who have no physical wired connection between sender and receiver (wireless routers).
- **Demilitarized Zone (DMZ):** The DMZ, or network perimeter, contains servers, routers, and switches that preserve security by preventing the medical institution's network from being exposed on the Internet. "*Short for demilitarized zone, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies."*[12]

[11] https://f5.com/resources/white-papers/load-balancing-101-nuts-and-bolts
[12] http://www.webopedia.com/TERM/D/DMZ.html