Identifying Opportunities to Compromise Medical Environments

Maureen S. Van Devender
University of South Alabama
mvandevender@southalabama.edu

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

Matt Campbell
University of South Alabama
mattcampbell@southalabama.edu

Michael A. Finan
University of South Alabama
mfinan@health.southalabama.edu

Abstract

The amalgamation of computerized equipment into medical arenas is creating environments that are conducive to security breaches. While previous medical device research has been conducted on medical training equipment, wearable and implantable devices, and on telesurgical systems, there has been minimal research investigating cyber-security vulnerabilities in real-world computer-facilitated surgical environments. The research contribution is an initial empirical analysis of the viability of security vulnerabilities in a computer-facilitated surgical environment. The preliminary results of this investigation generated information that can be used to develop Security Criteria for Integrated Medical Devices.

Keywords

Healthcare informatics, medical device security, cybersecurity, computer-facilitated surgery

Introduction

The rampant amalgamation of technology and healthcare is introducing opportunities for new cyber-attack vectors. Combine this phenomenon with research that indicates that digital evidence, in general, is continuing to integrate and escalate in importance in legal situations, and it is only a matter of time before medical devices are going to be investigated (Berman et al. 2015; McMillan et al. 2013). The proliferation of technology into the healthcare arena is being encouraged by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 which requires the implementation of Electronic Health Records (EHR) for all healthcare providers that participate in Medicare or Medicaid (U. S. Department of Health & Human Service). Complicating matters, the Federal Bureau of Investigation (FBI) predicts that enticing exploitation opportunities will be created in EHR software and medical devices when companies are required to transition to EHR environments (FBI Cyber Division 2014). The FBI report goes on to state that the healthcare industry is not prepared to protect against basic cyber-attacks, much less more sophisticated Advanced Persistent Threats (APTs).

Echoing this idea, a Ponemon Institute (2015) press release reports that criminal attacks in the healthcare industry have increased 125 percent from 2010 to 2015. The press release also emphasizes that most healthcare organizations are not prepared to handle cyber threat environments (Ponemon Institute 2015). Confirmation of this statement is visible in a recent news report where Hollywood Presbyterian Medical Center recently acquiesced to a ransom-wear attack (Mastroianni 2016). A recent article in Bloomberg Businessweek states that it is possible to hack a Hospira drug pump (Reel and Robertson 2015). This activity prompted a warning from the FDA (U.S. Food and Drug Administration 2015a).

Manufacturers are required to report to the FDA all incidents in which a device they manufactured may have contributed to serious injury or death, or has malfunctioned and recurrence on the device or similar devices could contribute to harm or death (U.S. Food and Drug Administration 2016b). The FDA records all reports in the publicly available Manufacturer and User Facility Device Experience (MAUDE) database (U.S. Food and Drug Administration 2016b). Although, the “FDA receives several hundred thousand
Medical Device Reports (MDRs) of suspected device-associated deaths, serious injuries and malfunctions (U.S. Food and Drug Administration 2016b), there is no requirement for timely reporting.

Research has shown that there is significant under reporting and late reporting of MDR incidents (Cooper et al. 2013). Hence, it is realistic to conclude that the MAUDE database does not provide a complete and up-to-date source for analyzing current security problems with medical devices. Furthermore, because cybersecurity risk assessment and adherence to a cybersecurity framework are recommended by the FDA but not required (U.S. Food and Drug Administration 2015b; U.S. Food and Drug Administration 2016a), it is plausible to believe that medical equipment with security vulnerabilities are approved by the FDA for use in hospital settings.

Reports claiming that the healthcare industry is at risk of cyber-attacks, data signifying increased attacks in healthcare environments, and claimed vulnerabilities in specific medical devices prompted the hypothesis that live computer-facilitated surgical environments are at risk of being compromised in healthcare facilities. The hypothesis raises several research questions that need to be explored in order to address the hypothesis:

1. From an open-source intelligence perspective, is it possible to identify plausible points of attack?
2. Is it possible to identify potential attack points by examining an existing footprint?

The research contribution is an initial empirical analysis of the viability of exploiting cyber-security vulnerabilities in computer-facilitated surgical environments and to provide a foundation for future work. The paper is structured as follows: Section two discusses relevant medical device research. Section three presents the methodology. Section four presents the results of the research. Section five draws conclusions and presents future work.

Related Works

The continued integration of technology into the medical field coupled with increasing proliferation has stimulated interest in medical security research. Research includes, but is not limited to, the security of medical training devices (Glisson et al. 2015), implantable devices (Rushanan et al. 2014) (Camara et al. 2015) (Malasri and Lan 2009), wearable technology (Li et al. 2013), and telesurgical robots (Bonaci et al. 2015) (Lee and Thuraisingham 2012).

Venkatasubramanian et al., (2012) examine the challenges and research directions in Medical Cyber Physical Systems (MCPS). The authors identify the recent increase in the interoperability of medical devices as providing advantages and improvements in healthcare delivery, while also creating greater attack surfaces. They state that it is essential interoperable medical devices be secure for the primary reasons of their propensity to be deployed in life critical situations and to have access to sensitive health information. The researchers categorize the goals of an attacker as: destroy equipment, disturb operation, reprogram, denial of service, and eavesdrop. They conclude that the domain of MCPS provides a unique set of challenges that are distinct from other cyber physical systems.

Glisson, et al.’s (2015) research in compromising a medical training mannequin demonstrates that it was relatively easy for undergraduate students inexperienced in techniques of security vulnerability exploitation to gain access to a medical device using readily available open-source software. The students were able to exploit vulnerabilities in the network security solution and the network protocol to gain access to the device and to launch a successful denial of service attack. The research provides an initial empirical analysis of the viability of compromising a medical device.

Rushanan, et al. (2014) examine the security vulnerabilities of implantable medical devices (IMDs) and body area networks (BANs). Their research reviews the security goals of confidentiality, integrity and availability that should be maintained through the entire life cycle of the device and a list of specific privacy criteria that should exist on the same timeline. They develop an adversary and a threat model and analyze the vulnerabilities of each security and privacy goal against each threat. The researchers point to the increasing complexity of software coupled with the increase in FDA recalls related to software as evidence of a need for research into improving the trustworthiness and reliability of software in IMDs and BANs. In addition they expose the possibility of Electromagnetic Interference (EMI) attacks and eavesdropping on signals previously thought to be private, indicating a need for more research into security and privacy of
these devices. The authors indicate that limited access to only older devices is a prevalent research obstacle. They advocate the need for researchers to have access to modern medical devices in order to improve research effectiveness.

Camara, et al. (2015) presents a survey of security and privacy challenges with IMDs. The researchers discuss relevant mechanisms proposed to address these issues including their suitability, advantages, and drawbacks. They employ Microsoft’s threat category model of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) to classify the threats. In conclusion, the authors call for interdisciplinary cooperation among researchers to ensure patient safety and privacy and security of data. They further call for users of IMDs to know details about the functioning and possible threats in order to raise security awareness.

Malasri et al. (2009) identify security threats facing wireless implantable devices. They classify wireless implantable devices into three categories: identification, monitoring, and control devices. Identification devices are defined as those used to provide personal information, which are vulnerable to harvesting, tracking, cloning, relay, and physical compromise attacks. The researchers define monitoring devices as those used to provide physiological information about the patient. These are vulnerable to the same attacks as identification devices with the addition of the potential for an attacker to falsify the patient’s identity or generate false patient data. In addition, monitoring devices are vulnerable to denial of service attacks. They define control devices as those capable of modifying the physiological characteristics of a patient. This category includes devices that dispense drugs such as insulin pumps and devices that regulate organs such as pacemakers. Control devices are vulnerable to all the threats faced by monitoring devices. In addition, these devices are vulnerable to wireless reprogramming attacks which have the potential to cause direct harm to a patient. The authors identify relay and physical attacks, denial of service attacks, and wireless reprogramming attacks as open issues requiring more research.

Li et al. (2013) examine wearable technology, specifically a popular glucose monitoring and insulin delivery system, for security vulnerabilities. With the device user’s manual and publicly available information, the researchers are able to eavesdrop on the communication of the glucose monitoring and insulin delivery system. Furthermore, because there is no encryption used in the communication, they are able to determine the PIN of the device and send packets that could affect the functioning of the device.

Bonaci, et al. (2015) experimentally evaluate the scope and impact of a myriad of potential cyber security threats against the Raven II telesurgical robot, a robot used in research and not approved by the FDA for live surgery. All the threats evaluated are related to intercepting and compromising network communication between the robot and the surgeon console. The researchers are able to successfully breach several elements of the system over a wide attack surface, and present recommendations for securing each. Their purpose is to increase awareness of security issues in cyber physical systems. They further believe that the vulnerabilities identified in their evaluation are not limited to teleoperated surgical robots, but to all teleoperated robots.

Lee and Thuraisingham (Lee and Thuraisingham 2012) at the University of Texas at Dallas (UTD) collaborated with researchers at the University of Washington BioRobotics Lab (BRL) to develop a security enhanced Interoperable Telesurgery Protocol (ITP). ITP defines the structure of communications between surgical robots and controllers, has been adopted by fourteen research groups, and has been used successfully in testing interoperability between the research groups. The researchers enhanced ITP to address the security elements of communication, authentication, authorization, and security policy development and enforcement. They conclude that secure ITP offers a proof of concept and a framework for the development of security appropriate for the rigorous requirements of telesurgery.

Cooper, et al. (2013) conducted a study to evaluate robotic surgery device related complications reported to the FDA. The study compared 12 years of MAUDE data (January 2000 to August 2012) to court records found in LexisNexis (LexisNexis 2016) and PACER (Administrative Office of the U.S. Courts) databases. The results of this study showed there was significant under reporting and late reporting of MDR incidents. Previous medical device research has identified security issues, safety issues, deliberated challenges and proposed solutions. However, there is minimal empirical research investigating cyber-security issues in live computer-facilitated surgical environments. There is also minimal research identifying criteria that can be utilized to mitigate attacks in production environments.
Methodology

Oates (2006) defines a case study based on previous research by Yin (2009) as an "empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." Oates goes on to state that a case study seeks to obtain detailed insight into the object of the investigation. Hence, this research is an exploratory case study that investigates the identification of cyber-security vulnerabilities in production computer-facilitated surgical environments. Any surgical environment could have been chosen for evaluation. As a matter of convenience, a computer-facilitated surgical environment that contained a da Vinci surgical robot at a local medical facility was selected for examination. Robotic surgical systems are one of the most complex medical devices on the market, and they are playing an increasingly important role in surgical procedures. They were used in over 1.75 million procedures in the decade between 2005 and 2015 (Alemzadeh et al. 2015). Intuitive Surgical, Inc., manufacturer of the da Vinci Surgical System reports roughly 652,000 procedures were executed in 2015, up approximately 14 percent from 2014 (Intuitive Surgical 2016b).

The first step was to investigate manufacturer documentation and relevant literature for information on the architecture of the da Vinci surgical robot. Intuitive Surgical, Inc.’s website provides information about the company and the da Vinci Surgical System family of products. A review of the site categories of company, products, training, support, and clinical evidence was conducted to gather information relative to the architecture of the system and the context in which it operates.

The second step examined the functional footprint of a live production system. The robotic surgical environment at a local medical facility was visually inspected. Two surgical nurses on the robotic surgical operating room team and their supervisor assisted with the inspection.

The third step was an investigation to identify the da Vinci operating system. Open-source Intelligence (OSIT) techniques were employed in an attempt to ascertain public information (McKeown et al. 2014). This step in the investigation can be refined into the following steps.

1. Popular search engines were used to conduct an Internet search. The terms provided in Table 1 – Internet Search Terms were used for the initial search.
2. Follow up searches using popular search engines and social media outlets were conducted using additional terms and names discovered in step one.
3. Additional information obtained in step two, such as reference to patent information, was investigated to determine if they were related/relevant to Intuitive Surgical, Inc.

<table>
<thead>
<tr>
<th>Step</th>
<th>Search Terms Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Intuitive Surgical, operating system</td>
</tr>
<tr>
<td>2.</td>
<td>Intuitive Surgical, real time operating system</td>
</tr>
<tr>
<td>T</td>
<td>Intuitive Surgical, RTOS</td>
</tr>
</tbody>
</table>

Table 1. Internet Search Terms

Results & Analysis

The first step produced documentation on how the system is constructed, including all of the parts and how they communicate. The da Vinci Surgical System is a robotic surgical system developed by Intuitive Surgical, Inc. The FDA, which regulates the sale of all medical devices in the United States (U.S. Food and Drug Administration 2015c), approved the da Vinci Surgical System for sale in the year 2000. There are four primary components of the da Vinci Surgical System: the surgeon console, patient-side cart, surgical instruments, and vision system (“Intuitive Surgical - da Vinci Surgical System” 2015). The surgeon console is designed for the surgeon to operate from a seated position. It contains a 3D image viewer and handheld master controls that receive the surgeon’s hand movements for translation to movements of the surgical instruments. The patient side cart includes either three or four robotic arms that move in response to the surgeon’s hand control movements. The surgical instruments include a full collection of instruments...
Identifying Opportunities to Compromise da Vinci

available for use in surgical procedures that are connected to the robotic arms and can be exchanged during surgery. The vision system contains a 3D high definition endoscope (flexible tube with camera and light), image processing equipment, and a display that is viewable by operating room personnel (Intuitive Surgical 2016a). The website goes on to state that the vision system equipment is stored in an open cart referred to as the vision cart.

Intuitive Surgical offers a service for remote monitoring of the equipment both during operative procedures and while the equipment is idle (Intuitive Surgical Inc. 2015). This service requires an Internet connection to the device through an Ethernet port or a wireless LAN connection installed on the da Vinci (Intuitive Surgical Inc. 2015). The online information indicates that the Internet connection allows Intuitive Surgical technicians to passively monitor logs and to proactively monitor and review system performance logs for preventative maintenance purposes. The information from the website claims that the da Vinci system does not store any patient data and has no interfaces to other data systems.

The second step investigates a practical implementation of the equipment. A da Vinci Si Surgical Robot, a Stryker high definition camera, a Karl Storz video display system, and an EHR system were observed. As described in the documentation the da Vinci is composed of a surgeon console, a patient-side cart with four robotic arms, and a vision cart which houses the central computer and a viewing monitor. Surgical instruments and an endoscope are attached to the robotic arms as needed for each procedure. The surgeon console and patient side cart are each connected to the central computer via optical fiber cable for video and data communication between the components. The Stryker high definition camera is used when video recording of a surgical procedure is needed, and the Karl Storz video display system is used to present visual displays of data and images from various hospital systems as needed during surgical procedures. Figure 1: Robotic Operating Room Layout, shows the layout of the robotic surgical operating room observed in this investigation.

Figure 1: Robotic Operating Room Layout

A visual inspection of the da Vinci Si Surgical Robot revealed many connectivity options on the back of the da Vinci central computer located in the vision cart. There are three optical fiber ports of which two are in use for connections to the central computer from the surgeon console and the patient-side cart. There is an Ethernet RJ45 port in use that connects to a SonicWALL firewall located at the bottom of the cart through an Unshielded Twisted Pair (UTP) cable. Connected to another port on the firewall is a UTP cable that is rolled up and not connected to anything on the other end. The surgical nurses explained that this would be...
used for software updates and manufacturer monitoring if it were connected to the Internet. There are several video connections available. Two S-video connections are labeled left and right core video. Tip-Ring-Sleeve (TRS) jacks in Red, Green, Blue, and White (RGBW) are labeled as touch screen video, which is a function of the video display mounted on the vision cart. A Digital Visual Interface (DVI) connection is labeled touch screen camera. There are several video output options including one DVI, one composite, one S-Video, and one Serial Digital Interface (SDI), with the composite connection being the only one in use. The touchscreen audio has an undetermined connector type being used, an unused headphone mini-jack, and an unused pair of TRS jacks for audio-input and audio-output. There is a Small Form-Factor Pluggable (SFP) network port in use. There is an unused RS-232 serial port, Video Graphics Array (VGA) port and RJ45 network jack. Lastly, there are three 20-pin circular connectors for power input with two in use. The wireless LAN network interface described in the vendor documentation was not observed. However, no external indicators are necessary for this interface.

Atop the vision cart behind the da Vinci video display is a high definition camera that can be used to record the surgical procedure. It is a Stryker model 240-050-88 (Stryker). This device has many connection ports on the back. The base communication module on the rear lower left contains the following ports: 1 Personal System 2 (PS2) mouse, 1 PS2 keyboard, 4 Universal Serial Bus (USB), 1 RJ45, 1 parallel, 1 VGA, 1 RS-232 serial, 1 audio microphone and speaker. Built into the back plain in the upper right is a plethora of video input/outputs including a camera port, audio input/output, video input/output, and coaxial composite in/out. There are 6 interface card slots in the lower right. Two of them have cards in them. One has two DVI ports, and the other has three IEEE 1394 high-performance serial bus ports. A DVD burner and high definition screen are located on the front of the device. A search of the vendor’s website was unsuccessful in revealing when the Stryker model number 240-050-88 was manufactured. A patent number on the back of the device was used in an Internet search. The exploration revealed a U. S. patent that was issued in 2004 (Chang et al. 2004).

Two desktop computers were observed in the operating room. One is the user interface to the Karl Storz Video Display system. This system controls three video display monitors around the room. It interfaces with the various hospital systems to provide access to data and images from these systems for display on the monitors around the surgical room. For example, x-rays from the hospital Picture Archiving and Communication System (PACS) can be displayed during surgery. The second desktop computer is an interface to the hospital EHR system. It is noted that this computer’s operating system is Microsoft Windows XP. USB ports were observed on both computers. Located behind the operating table is a wheeled anesthesia console that is not part of this investigation.

A visual examination of the operating room revealed several potential security vulnerabilities, such as exposed USB ports, potential Internet connectivity, an out of support operating system, and minimal physical access restrictions. The visual examination revealed at least nine exposed USB ports. Active USB ports inherently trust connected storage mediums. Stuxnet, a worm that infected one of Iran’s nuclear facilities, is suspected of being transferred to air-gapped computers via a USB drive (Kushner 2013). Hence, USB devices can be used to install malicious software on devices that contain active USB ports. Complicating matters, the evolution of USB attacks has resulted in modified firmware (Goodin 2014). The firmware on a USB device can be manipulated by an attacker allowing them to take surreptitious actions against the host computer including injecting malicious scripts and capturing data (Goodin 2014). This type of attack has been labeled as a BadUSB attack (Goodin 2014). These types of attacks are plausible if an infected USB device were inserted into an active USB port in the operating room.

The Stryker high definition camera contains two IEEE 1394 ports. NIST published a security vulnerability summary due to a design flaw in the specification for 1394 that allows for an attacker to gain read and write access to sensitive memory on the host device (US-CERT/NIST 2008). The vulnerability appears to have been corrected with an update to the specification in 2008 (IEEE 2008). It is unclear which version of the IEEE 1394 specification is used on this device. Because the patent for the Stryker device was issued in 2004 (Chang et al. 2004), it is possible that the vulnerable specification is employed.

Ethernet is an IEEE standard for Local Area Network (LAN) connectivity. LAN access presents two points of attack. The first potential point of attack comes from another device that is connected to the network. The second potential point of attack comes when a LAN has access to a Wide Area Network (WAN), primarily the Internet. In the implementation observed, an Ethernet cable was not connected to a LAN or WAN. However, it is possible that this connection is used when the vendor applies updates and downloads...
performance logs from the system. The wireless LAN connection described in the vendor literature is another point of attack. Hence, it is possible for an implementation of the da Vinci Surgical Robot to have an active Internet connection at all times via a wireless connection. A wired or wireless connection to the Internet provides a potential attack vector for the injection of malicious software and/or the exfiltration of sensitive data.

Windows XP on the EHR system computer presents another vulnerability. Support for Windows XP was ended by Microsoft in April 2014 (Microsoft 2014). Accordingly, no security updates are provided by Microsoft. This leaves the operating system vulnerable to malicious software attacks. In addition, software programs running on Windows XP may not be updated by respective vendors creating additional security vulnerabilities.

Lastly, physical security could be tightened in the environment. Enhanced physical security controls would minimize unauthorized access to the equipment. Enhanced monitoring software could minimize the possibility of unintentional individual system and overall operating room compromises as well.

The manufacturer does not identify the operating system used in the da Vinci Surgical Robot. Hence, the third step seeks to identify the operating system of the da Vinci. While recent research indicates that Open-Source Intelligence (OSINT) search behaviors, procedures, and practices are still being refined, it does indicate that these techniques are being used in a variety of online investigations (McKeown et al. 2014). The third step used OSINT to determine the operating system used by the da Vinci. The preliminary investigation focused on search engines and social media outlets to acquire publicly available information. To investigate this issue, search engines were used to identify companies that listed Intuitive Surgical as a client. Publicly available search engines were then utilized to cross reference identified companies with products and employees of Intuitive. At this point, cross reference searches were conducted with the previous results and surgical patents. The investigation revealed information that suggests the operating system is or has possibly been at some point in time a specific Real Time Operating System (RTOS). It also revealed two robotic surgical related patents that were applied for in 2009 and 2010 and assigned to Intuitive Surgical in 2015 (O’Grady et al. 2015; Zhao et al. 2015).

The preliminary results of this investigation produced data that can be used in the development of Security Criteria for Integrated Medical Devices (SCIMD). The primary data suggest that network connections, live ports, operating system vulnerabilities, and physical access should be considered when securing robotic operating room environments.

Conclusions and Future Work

The reality is that computer-facilitated surgical environments are complex atmospheres that will continue to be integrated into the medical field. Open-source analysis reveals that data can be acquired from the Internet that can be used to identify plausible points of attack. On-site analysis identified network vulnerabilities, general access vulnerabilities, and open-source opportunities to acquire relevant data. In this particular scenario, the LAN capabilities provided potential attack vectors from local and Internet-connected devices. In addition, open USB ports and antiquated operating systems provide additional paths for compromising devices. The OSINT investigation indicates that the operating system could be an RTOS. The data collected from the on-site analysis identified several potential points of attack. Hence, the initial analysis supports the hypothesis that live computer-facilitated surgical environments are at risk of being compromised in healthcare facilities. The preliminary investigation contributes to the development of SCIMD.

Future research will expand the criteria that can be used to mitigate an attack in computer-facilitated environments. This will necessitate the examination of a variety of medical environments, such as hospitals, outpatient medical facilities, doctors’ offices, and simulation labs to identify and refine the criteria needed to secure a variety of medical environments. In conjunction, research should also investigate reverse engineering medical equipment in computer-facilitated surgical environments to discover security vulnerabilities, identify relevant residual data that is present after interactions and establish forensic procedures for investigating medical equipment. Further research will investigate potential security vulnerabilities inherent in RTOSs and identify design considerations that can mitigate these vulnerabilities. Building on this line of thought, future research will identify performance problems with medical equipment that could be indicative of a cyber-attack. These problems will be translated into practical
exercises that can be used to train medical professionals to detect performance problems with medical equipment that could be indicative of a cyber-attack.

References


O'Grady, P., McDowall, I., and Hoffman, B. D. 2015. "Imaging mode blooming suppression." USA.


Zhao, T., Zhao, W., Hoffman, B. D., Nowlin, W. C., and Hui, H. 2015. "Efficient vision and kinematic data fusion for robotic surgical instruments and other applications." USA.