How Secure is the Healthcare Network from Insider Attacks? An Audit Guideline for Vulnerability Analysis

Ragib Hasan, Shams Zawoad, Shahid Noor, Md Munirul Haque*, and Darrell Burke
{ragib, zawoad, shaahid}@cis.uab.edu, mhaque@purdue.edu, deburke@uab.edu
University of Alabama at Birmingham, AL 35294, USA
*Purdue University, IN 47907, USA

***Abstract*—The availability of wireless interfaces with the new generation medical devices has spawned numerous opportunities in providing better healthcare support to patients. However, the weaknesses of available wireless communication channels introduce various novel attacks on the medical devices. Since the smart mobile devices, such as smartphones, tablets, laptops are also equipped with the same communication channels (WiFi/Bluetooth), attacks on medical devices can be initiated from a compromised or malware infected mobile device. Attackers can steal confidential medical records from a wireless-enabled medical device. Medical devices or communication channels can also be compromised to feed incorrect medical records to doctors or send life threatening commands to the devices. Moreover, since the compromised mobile devices are already inside the security perimeter of a healthcare network, it is very challenging to block attacks from such compromised mobile devices.**

In this paper, we systematically analyze the novel threats on healthcare devices and networks, which can be initiated from compromised mobile devices. We provide a detail audit guideline to evaluate the security strength of a healthcare network. Based on our proposed guideline, we evaluate the current security state of a large university healthcare facility. We also propose several mitigation strategies to mitigate some of the possible attacks.

I. Introduction

The emergence of wireless-enabled medical devices has created numerous opportunities in providing better support for monitoring and guiding patients' health. Infusion pump, pacemaker, insulin pump, cardiac defibrillators are some examples of wireless-enabled medical devices, which are widely used in patients' healthcare. At the same time, the improvement in smart mobile devices blended with the availability of wireless-enabled medical devices have created a great demand for healthcare applications. According to a research report of ABI, smartphone-based healthcare applications will exceed US$400 million annually by 2016 [1].

However, attackers can access the communication channel used by the wireless-enabled medical devices and perform several types of attacks on them [2], [3], [4], [5]. For example, Radcliffe was able to attack on wireless insulin pumps, pacemakers, and ICDs from half a mile distance [3]. Researchers were also able to successfully compromise an insulin pump and sent lethal doses to the compromised pump from 300 feet distance [4].

Since the smart mobile devices are also equipped with the WiFi/Bluetooth network interfaces and remain *inside* the secure region of the healthcare network, a compromised mobile device can be a very attractive medium to attack on the healthcare infrastructures. It is easy to initiate an attack remotely through malware-infected mobile devices, which are in close proximity to the medical devices. The feasibility of mobile botnet is already proven [6]. Attackers can opportunistically seek for a time to launch an attack that can maximize the havoc on medical devices or patients' health. Collecting electronic medical records (EMR) by sniffing the communication channels can be highly attractive to attackers because of the business value of EMRs. Whereas active attacks, such as sending incorrect medical records or issuing a fatal command to medical devices can jeopardize a patient's life. Such techniques can be used by a murderer to kill someone and it will be very challenging to investigate [7]. Adversaries can launch various targeted attacks using a mobile malware by utilizing various contextual information. Attacks from mobile devices, therefore, are significant and carry a greater risk to patient safety.

Unfortunately, it is very challenging to prevent such a compromised mobile device from penetrating the healthcare network since most of the infected devices are legitimate and permitted to use the communication network. An administrator needs to monitor the environment precisely in order to detect the infected mobile devices. The delay in finding an unusual behavior along with identifying a compromised device might engender serious damage on patients' health. Additionally, most of the medical devices have limited storage, computing power, and battery life. Therefore, it is very challenging to utilize the state-of-the-art anti-virus software or a highly secure encryption algorithm for protecting the communication channel of the medical devices. Instead, it would be better if we implement a framework for securing the network to which those medical devices are connected. Though researchers exposed the weakness of the medical devices by initiating different types of attacks [2], [3], [4], [5] and proposed various possible solutions as countermeasures of those attacks [8], [9], [10], no standards for securing the healthcare network are defined yet.

The core focus of our work, which is the threats from infected mobile devices that are inside the security perimeter of a healthcare network, has not been yet explored fully by researchers. In this paper, we take the first step in exploring the threats from a malware infected smart mobile device to medical

devices. We propose a guideline to evaluate the security of existing healthcare networks. Though no real attacks have been yet recorded, we must explore this new threat model to take some early defenses against real attackers.

Contributions: The contributions of this paper are as follows:

- We systematically analyze the threats from compromised mobile devices to healthcare network and devices and present a novel threat model, which can provide future research directions in the healthcare security domain.
- We provide a security audit guideline to evaluate the strength of security of a healthcare network.
- We perform a case study in a large hospital environment and identify several vulnerabilities by following our proposed guideline.
- We present several mitigation strategies to secure the healthcare infrastructures against the possible attacks.

II. Related Work

Researchers observed that medical devices are vulnerable to several types of attacks. Halperin *et al.* were able to perform attacks on the communication channel between a pacemaker and an implantable cardiac defibrillator (ICD) [2]. The attacks were possible since the communication channel was unencrypted. Radcliffe provided a feasibility study on the existing intractable attacks on wireless insulin pumps, pacemakers, and ICDs from a chosen distance of half mile [3]. He succeeded deciphering messages along with accessing the application protocol by applying reverse engineering mechanism on the unencrypted communication channel.

Paul *et al.* identified some security breaches of wireless insulin pump system and proposed mitigation strategies against those threats [8]. Sorber *et al.* explored the security of mobile health (mHealth) systems, where personal mobile devices serve as a gateway between the EMR management system and medical sensor devices [9]. They proposed an architecture – *Amulet*, which ensures privacy and security of mHealth system. Later, Sorber *et al.* proposed Plug-n-Trust (PnT), which can protect confidentiality and integrity of safety-critical medical sensing and data processing on vulnerable mobile phones [11]. They proposed a plug-in smart card that provides a trusted computing environment to keep data safe even on a compromised mobile phone. While their approach allows creating trustworthy applications on mobile devices, they did not consider what would happen if the malware itself would capable of communicating with medical sensor devices.

Secure multiparty computing (SMC) scheme, such as FaeriePlay [12] can also ensure the confidentiality of EMR. SMC systems typically employ garbled Boolean circuits, which hide the computation being executed. While a SMC scheme can be attractive for healthcare applications, evaluating programs as Boolean circuits comes at a high performance cost. Arney *et al.* described some active and passive attack models on Biomedical devices over wireless channel [10]. Goodman *et al.* examined the possibility of homicide and extortion attacks by hacking implantable medical devices [7]. They also pointed out the difficulty of investigating this type of homicide cases.

III. Threat Model

In this section, we present a novel threat model to discuss the possible attacks on healthcare infrastructures from compromised mobile devices.

A. System Model

We present the threat model based on the *Bring Your Own Device* (BYOD) model [13]. Now-a-days, employees are allowed to bring their own mobile devices, such as laptop, smart phone, and tablet computer at their work place. Therefore, a malware infected device, belonging to an employee, now can easily enter into the system and the malware may thus be running inside the security perimeter of the corporation [14]. In a healthcare setting, this will involve mobile devices belonging to a doctor, patient or a visitor who is present inside a healthcare facility or a person's house.

Asset. We consider three assets to model the threats from mobile devices to healthcare: 1) patients' confidential EMR; 2) patient's health; and 3) patients' or medical personnel's location,

Attackers' Capability. We assume that the mobile devices have already been infected by a malware and are connected to the WiFi access point or paired with a Bluetooth-enabled medical equipment. This assumption is fairly common in malware research [15]. In the medical environment, mobile devices, belonging to healthcare personnel or patients, are usually connected with various medical equipment for their own interest (for example, a blood-pressure monitor application for smart mobile devices needs to be paired with a wearable blood pressure monitor). These assumptions are sufficient for DoS attack and to interfere the communication between mobile devices and medical devices. We also assume that attackers are capable of reverse engineering the application protocol of medical devices to learn patient' EMRs as well as sending incorrect signal to medical devices.

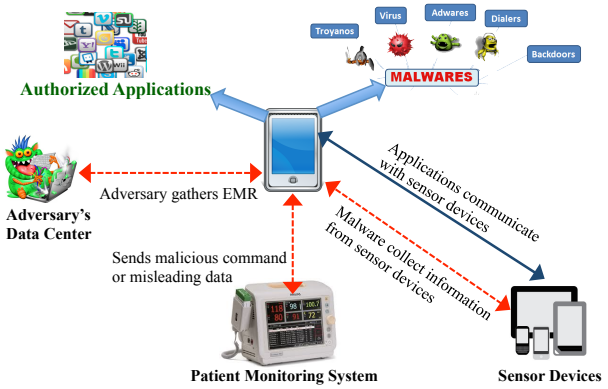

Fig. 1: Attacks on Healthcare Infrastructures and Devices

B. Threat Analysis

The threats on mobile devices can be classified into three main categories: privacy and confidentiality, integrity, and availability. Figure 1 illustrates some possible attacks on healthcare infrastructures initiated by malicious mobile devices.

Privacy and Confidentiality. According to the Health Insurance Portability and Accountability Act (HIPAA) [16], EMRs are private and confidential to the patient. Using mobile devices, an adversary can exploit the available network to gain unauthorized access to EMRs and thus can violate privacy and confidentiality. Below, we present some possible attacks on privacy and confidentiality:

• An adversary can steal a patient's medical records by Man-in-the-middle (MITM) attack on the communication channel. MITM in both Bluetooth and WiFi channel is well explored [17], [18]. For example, to launch a MITM attack in Bluetooth channel, an adversary can create a proxy gateway between two mobile devices connected to each other via bluetooth [19]. This allows the attacker to extract plain-text information from the network traffic as well as the ability to modify a packet in real time. In a medical environment, the devices often communicate with each other using Bluetooth interface and the Bluetooth discoverable option of these devices is often turned on, which makes them vulnerable to this attack. The attacker without the consent of the devices can create a pair between two Bluetooth-enabled devices and listen or modify the confidential information exchanged between them. In this way, the adversary can collect EMRs from malware infected mobile devices of patients, physicians, or patient's visitors without being near to the medical devices in person. With a large number of malware infected mobile devices, an adversary can produce a large-scale dataset of EMR. Publishing the EMR publicly on the Internet will be a serious violation of patients' privacy; especially for celebrities, who do not want to disclose their physical problems.

• To improve patient care, physical security, and management of inventory, WiFi RTLS system is getting widely adopted in healthcare. Therefore, a malware infected mobile device can gather the location of a patient from such location-tagged medical devices. The location of medical personnel can also be exposed if they wear WiFi badges and their smartphones are infected by a malware. As people always tend to keep their smart phone with them, it is possible to track a person's location 24x7 by using a mobile malware.

• For a Bluetooth or WiFi enabled device, the unique 48-bit MAC address of a device is visible to a network packet sniffer. The first 24 bits of the MAC address are reserved as Organizationally Unique Identifier (OUI), which can be used to distinguish different device, such as distinguish between HTC EVO and HTC Hero – the two Android phones from HTC [20]. We argue that it is possible to build a similar type classifier for medical devices to know about the presence of a particular wireless-enabled medical device in a person's body or the surrounding environment. This in turn will expose the disease of that person – a confidential information that the person does not want to share.

Integrity. Below, we describe some attacks that violate the integrity of the communication channel:

• Reverse engineering the application protocol of medical devices can enable an adversary to use a malware infected mobile device to communicate with medical devices and feed incorrect data, e.g., blood pressure or glucose reading. Incorrect data on display devices can lead a doctor to take wrong decision, which can have direct impact on patient's health.

• An adversary can exploit an insecure communication channel to send malicious/incorrect commands to control devices through a malware infected mobile device. A malicious command to a implantable defibrillator, pacemaker, or an infusion pump can be life threatening for a patient, such as sending a command of lethal dose to the patient's insulin pump or stop command to a pacemaker.

Availability. We discuss some possible attacks on the availability of the wireless medical devices below:

• The vulnerability of WiFi/Bluetooth channels against DoS attack is a serious bottleneck to ensure the availability of the medical devices. Researchers showed that the IEEE802.11 standard [21], which is used in the WiFi channel is prone to DoS attack [22]. An attacker can launch DoS attack on WiFi-enabled medical devices from a mobile device where both devices use the same WiFi network. We confirm that it is possible to launch a DoS attack on the WiFi and Bluetooth channel by Android smartphones. In our experiment, we knew the external IP of a WiFi-enabled device and we were able to send a burst of packet to that device from an Android phone, which made the target-device unavailable for a time being.

• Moyers *et al.* showed that it is possible to launch a battery exhaustion or resource depletion attack on mobile devices through Bluetooth/WiFi channel [23]. The wireless-enabled implantable medical devices are generally battery powered and a similar attack on such devices is also possible, which can make the devices unavailable.

Localized Targeted Attack. Localized targeted attacks can fall into any of the three categories mentioned above. An attacker can place an intelligent malware in the smart mobile devices, which remains dormant, but whenever the person carrying such malware-infected mobile device enters into a certain location, the malware will be activated. In this way, an adversary can target a hospital to bring down their reputation by triggering the malware whenever owners of the malware infected devices come to that particular hospital.

IV. Security Audit

A. Audit Guideline

In this section, we provide an auditing process to determine how secure the healthcare network and medical records are in a hospital environment.

R.1 *Resistance to Denial of Service (DoS) Attack:* There are several tools to identify whether the network can stand against DoS attack. We suggest using tools both for smart phones and laptop computers.

dSploit is a proven penetration testing tool for the Android operating system [24]. If the WiFi network of a healthcare facility is not resistant to DoS attack, it is possible to completely block a medical device from using the WiFi network by following the script injection technique of *dSploit*.

Low Orbit Ion Cannon (*LOIC*) [25], [26] can block the target device by sending large streams of UDP, TCP, or HTTP request. Knowing the IP address of a medical device is enough for an attacker to perform the DOS attack using this tool. It is also possible to remotely run the tool using Internet relay chat (IRC) protocol. In that case, the remote mobile device will be served as the botnet.

aircrack-ng [27] and *mdk3-v6* [28] can make it possible to check whether a healthcare network is susceptible to DoS attack. To use aircrack-ng, we first need to set the WiFi interface of a device into monitoring mode and generate some arbitrary packets using *mdk3-v6*. If the MAC address of the access point or the IP of a medical device is known, we can send the generated packets to the targeted IPs. If the network is resistant to DoS attack, we will not notice any time out while pinging the targeted IPs.

R.2 *Resistance to WiFi Password Cracking:* Revealing the password of WiFi network can make the attack on privacy, integrity, and availability easier. *FeedingBottle* can be used to crack the WiFi password [29]. The tool requires a file, where all the possible combinations of passwords are stored. If the WiFi network of a hospital is not secure, *FeedingBottle* can reveal the password of the network using this file.

ReveLA WiFi is an android-based application to check the security of WiFi networks and recover passwords [30]. If the WiFi network is insecure, the tool marks the network as vulnerable and can identify the password.

R.3 *Resistance to ARP Poisoning Attack:* A network susceptible to ARP poisoning attack means attackers can forward the network packets to their desired destination before the packets reach the original gateway. To ensure the privacy and integrity of medical records, we need to make sure that a healthcare network is secure against this attack.

Ettercap [31] uses the attacker's MAC address to alter the ARP cache of the victim's device. All the packets from the victim's device first come to the attacker before going to the intended destination. However, if the network is secure, it will block the fake routing advertisement message from *Ettercap*.

WiFiKill is an android-based tool to assess the resistance of a WiFi network against ARP poisoning attack [32]. This tool can deceive the medical devices to consider an android phone as the WiFi router by spoofing ARP replies.

DroidSheep [33] can make a android phone acting as a router and intercepting all the network traffic. On the other hand, *DroidSheep Guard* can monitor the Androids ARP-table and can detect ARP-Spoofing on the network launched by DroidSheep or other ARP spoofing tools [34].

R.4 *Resistance to Reverse Engineering Attack:* By reverse engineering application protocol, an attacker can break the privacy and integrity of medical record. In order to know the application protocol, attackers need to decrypt the application data packets. Using the following tools, we can determine whether a network is resistant to reverse engineering attack.

Reaver can be used to check the resistance of a WiFi network against reverse engineering attack [35]. This tool collects UV

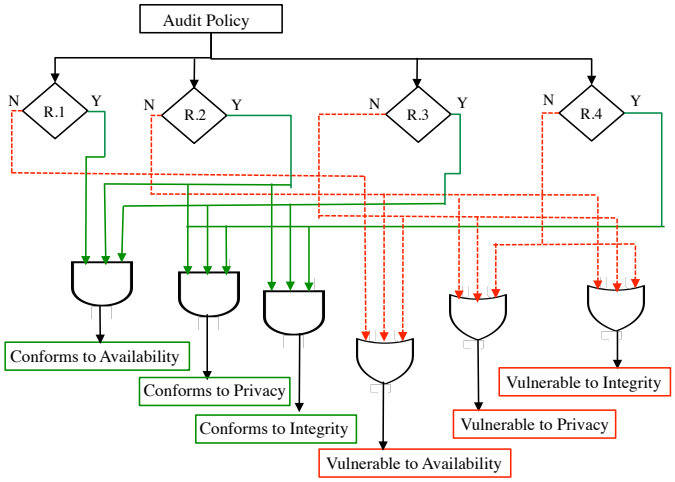

Fig. 2: Process Flow for Security Audit

packets from the network and if the network is not secured, it can decrypt application data-packets after collecting sufficient amount of UV packets.

SSLStip can also verify the security of data packets [36]. This tool first collects data packets by spoofing gateway MAC address and generates a file, which has all the collected data. If the network is not secured, this tool can decrypt the meaning of the captured data.

Assessment Decision. Based on the aforementioned audit criteria, we derive an assessment decision strategy, which is illustrated in Figure 2. According to the decision strategy, if a network is resistant to denial of service attack (R.1), WiFi password cracking (R.2), and ARP poisoning attack (R.3), the network conforms to availability. Failure to conform any of the three policies means that the network is vulnerable to availability. Similarly, if a healthcare network is protected against WiFi password cracking (R.2), and ARP poisoning attack (R.3), and Reverse Engineering Attack (R.4), the network can ensure privacy and integrity of medical record. Failure to protect either of these three attacks indicates that the network is vulnerable to privacy and integrity.

B. Evaluation of a Healthcare Facility

According to the proposed auditing procedure, we explored the current security state of the University of Alabama at Birmingham Hospital — a large university healthcare facility. To avoid any unwanted incident, the security assessment was conducted in a network infrastructure prepared by Health System Information Services (HSIS) lab that was similar to the actual hospital network. Result of the audit is summarized in Table I, which indicates several vulnerabilities in the ongoing usage model for medical devices.

Current Security Measures. The hospital implemented following schemes to ensure the security of the wireless enabled medical devices.

- The hospital maintains one dedicated WiFi network for medical devices and another WiFi network for medical personnel. This scheme can help to avoid any intrusion in WiFi network of medical devices from malware infected mobile devices.

Criteria	Ensure	Test Tool	Results
Resistant to DoS	Availability	LOIC	Failed
		aircrack-ng, mdk-v6	Failed
		dSploit	Failed
Resistant to WiFi password cracking	Privacy, Integrity, Availability	Feeding-Bottle	Passed
Resistant to ARP poisoning attack	Privacy, Integrity, Availability	EtterCap	Failed
		WiFiKill	Passed
Resistant to reverse engineering attack	Privacy, Integrity	Reaver	Passed
		SSLStrip	Passed

TABLE I: Audit Result

• The hospital uses Secured Socket Layer (SSL) as a means of communication standard between the central patient monitoring or EMR management system. The SSL technology can ensure the integrity and authenticity of data which traverse through a SSL-enabled communication channel.

• We run *Reaver* for 2 hours in the hospital environment and collected UV packets to break the password. However, due the security measure taken by the hospital environment, it alters the channel every couple of minutes and therefore, it is not possible to decrypt the UV packets.

Vulnerabilities and Possible Attack Scenarios. Two different networks for medical devices and smart mobile devices can secure the system against integrity violation, even though it is possible to attack on privacy and availability. We explored that it is possible to sniff different types of packets without connecting to the WiFi network. We were able to identify the MAC and IP address of the surrounding devices and the wireless access points from the broadcast packets. We could launch a DoS attack by masquerading the IP address. By analyzing the MAC address, we can also identify the type of a medical device and thus can determine a person's confidential health condition.

In the hospital, there were general purpose pumping machines, which transmit patients' health condition to the central monitoring system. We identified that the pumping machines are vulnerable to DoS attack though they communicate with the monitoring system through a SSL-enabled channel. Hence, the system complies with the *R.4* property but does not comply with the R.1 property of Section IV-A. Moreover, since the gateway IP address is hard-coded in the device, it is not possible to prevent jamming the IP without updating the firmware.

We found that the vital sign monitor system of the hospital communicate with the central EMR system over WiFi and transmits confidential EMR and login credentials of medical personnel without using SSL protocol. Using a packet sniffer, we were able to get the Address Resolution Protocol (ARP) packets from the channel. By ARP spoofing, we could launch a MITM attack and identify all the data packets sent for the EMR system [31]. The vital sign system uses WEP and WiFi Protected Access 2 (WPA2) encryption scheme. It is possible to decipher the WEP encryption and identify the EMR from the WiFi communication channel [37]. Besides the EMR, login credentials of medical personnel can be exposed in the same way. If the login credentials are exposed, an adversary can gather anyone's confidential medical records.

Our survey confirms our original arguments regarding the safety of WiFi and Bluetooth enabled medical devices. The vulnerabilities we exposed show that such devices are prone to different types of attacks from mobile malware.

V. Defense Mechanisms

Efficient Anti-Malware and DoS Blocker. A robust anti-malware scheme can reduce the risk of many possible attacks that we present in the threat model. With the presence of a strong anti-malware, an adversary cannot use a malware as a proxy to trigger an attack; the adversary needs to be located inside the healthcare network coverage area and must be connected with the network, which will make it more difficult to launch an attack. However, the traditional signature based malware detection schemes are not efficient for smart mobile devices due to the resource constraint. To overcome the resource constraint on the mobile devices, researchers proposed cloud based anti-malware architectures [38].

Researchers proposed several schemes to protect DoS attack in IEEE 802.11 network protocol [39]. However, the feasibility of such solutions is still unexplored. The response time to detect and block DoS attack is extremely crucial for medical devices since a very short period of unavailability for some devices can jeopardize a patient's life.

Network Anomaly-based Intrusion Detection. Kim *et al.* proposed a malware detection technique based on the anomaly in battery usage at the presence of a malware [40]. Similarly, from the anomalous network usage, we can identify a malware. A mobile device first needs to identify its normal network usage pattern using a machine learning scheme. An intrusion detection module will then raise alarm whenever the network usage deviates from the known pattern. However, due to the resource constraints, we can choose a certain interval or random interval to trigger the module. For example, before reading data from display devices, physicians can run this module to make sure whether the data is coming from the actual sensor device or a malware. The anomalous behavior in network usage can also be used to detect and block DoS and RD attack.

Power Efficient Encryption & Authentication Schemes. Manufacturers often skip strong encryption schemes to minimize power consumption and cost; sometimes even there is no encryption for the low-powered smart devices. The two recent incidents of medical device hacking provide proof of such vulnerability [3], [4]. Since many medical devices are battery powered, we need to focus on finding low power consuming, strong encryption and authentication schemes.

For implantable devices, we need more power efficient strategy because it is not possible to change the battery of these devices frequently. Researchers accomplished several successful attacks on the WEP encryption scheme of WiFi [41], [37]. WPA2 is still considered as secured encryption scheme for WiFi channel, but not all the medical devices are using this encryption due to the power constraint.

Threat	Consequence	Mitigation Strategy
Sniffing confidential data from the WiFi or Bluetooth communication channel	Breach of confidential medical record, patient location, and health condition.	Low power consuming, strong encryption scheme and network anomaly based intrusion detection
Sending malicious command from mobile devices to medical devices.	A lethal dose to a insulin pump or a stop command to a pacemaker, killing the patient.	Low power consuming, strong authentication scheme.
Sending misleading information from the mobile devices to the display.	Misguide the doctor to take appropriate decision.	Low power consuming, strong authentication scheme and network anomaly based intrusion detection.
Launching a DoS and RD attack from mobile devices making it unavailable.	Unavailability of critical medical devices can be fatal.	Network and battery usage anomaly based efficient DoS and RD blocker for low-powered medical devices.
Battery exhaustion attack by keeping the communication channel busy.	Can kill patients who use pacemaker or defibrillators.	Network anomaly based intrusion detection.

TABLE II: Overview of threats on health-care infrastructures from mobile device, consequences, and mitigation strategies

VI. Conclusion

The new generation wireless-enabled medical devices and smart mobile devices open numerous opportunities for the healthcare sector. Unfortunately, a malicious individual can exploit the vulnerability of the communication channels and launch different attacks on the healthcare infrastructures using mobile devices. In this paper, we explored some possible attacks from mobile devices to healthcare infrastructures considering the mobile devices are inside the security perimeter of the healthcare facility's network. We proposed a security audit guideline for WiFi networks to assess the security strength of a network. We also propose a set of mitigation strategies to defend against the attacks. In the future, our goal is to provide the audit guideline for Bluetooth networks. We will also design and develop the proposed network anomaly-based anti-malware and DoS blocker system.

Acknowledgment

This research was supported by the National Science Foundation under the CAREER Award CNS-1351038 and a UAB CAS Interdisciplinary Grant.

References

[1] ABI Research, "Smartphone health applications will exceed $400 million annually by 2016," https://goo.gl/7FOUyy, November 2011.

[2] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Security and Privacy*, 2008, pp. 129–142.

[3] M. Hunter, "Can wireless medical devices be hacked?" http://goo.gl/U6eD6V, 2011.

[4] BioSpace, "Hacker shows off lethal attack by controlling wireless medical device," http://goo.gl/Q80I9D, 2012.

[5] N. Paul, "Insulin pump security and reliability: Past, present, and future," *Oak Ridge National Laboratory JDRF meeting*, April 2010.

[6] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating bluetooth as a medium for botnet command and control," in *proceedings of the 7th Conference on Detection of Intrusions and Malware & Vulnerability Assessment DIMVA*, 2010.

[7] M. Goodman, "Who does the autopsy? criminal implications of implantable medical devices," in *USENIX HealthSec*, 2011, pp. 4–4.

[8] N. Paul, T. Kohno, and D. Klonoff, "A review of the security of insulin pump infusion systems." *Journal of diabetes science and technology*, vol. 5, no. 6, p. 1557, 2011.

[9] J. Sorber, M. Shin, R. Peterson, C. Cornelius, S. Mare, A. Prasad, Z. Marois, E. Smithayer, and D. Kotz, "An Amulet for Trustworthy Wearable mHealth," in *HotMobile*, 2012.

[10] D. Arney, K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Biomedical devices and systems security," in *IEEE EMBC*. IEEE, pp. 2376–2379.

[11] J. M. Sorber, M. Shin, R. Peterson, and D. Kotz, "Plug-n-trust: practical trusted sensing for mhealth," in *MobiSys*. ACM, 2012, pp. 309–322.

[12] A. Iliev and S. W. Smith, "Small, stupid, and scalable: secure computing with faerieplay," in *ACM STC*, 2010, pp. 41–52.

[13] BCS - The Chartered Institute for IT, *Mobile Computing: Securing Your Workforce*. British Informatics Society Ltd, 2011.

[14] K. Barr, P. Bungale, S. Deasy, V. Gyuris, P. Hung, C. Newell, H. Tuch, and B. Zoppis, "The vmware mobile virtualization platform: is that a hypervisor in your pocket?" *ACM SIGOPS Operating System Review*, vol. 44, no. 4, pp. 124–135, 2010.

[15] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security*, 2011.

[16] www.hhs.gov, "Health Information Privacy," http://goo.gl/XsQYv1.

[17] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures," *IEEE Transaction on Wireless Communication*, vol. 9, no. 1, pp. 384–392, 2010.

[18] H. Hwang, G. Jung, K. Sohn, and S. Park, "A study on mitm vulnerability in wireless network using 802.1 x and eap," in *IEEE ICISS*, 2008.

[19] "Proxying Bluetooth devices for security analysis using btproxy," https://goo.gl/EXHJmb.

[20] www.enterasys.com, http://bit.ly/lzuteW.

[21] IEEE, "Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Standard 802.11, 1999 Edition*, 1999.

[22] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *proceedings of USENIX Security*, 2003, pp. 15–28.

[23] B. Moyers, J. Dunning, R. Marchany, and J. Tront, "Effects of Wi-Fi and Bluetooth battery exhaustion attacks on mobile devices," in *IEEE HICSS*, 2010, pp. 1–9.

[24] "dSploit," http://dsploit.net/, last accessed December 04, 2015.

[25] GooglePlay, "Low orbit ion cannon (LOIC)," https://goo.gl/uWRrQj.

[26] sourceforge.com, "LOIC - low orbit ion cannon," http://sourceforge.net/projects/loic/.

[27] "Aircrack," http://www.aircrack-ng.org/.

[28] "ASPj's WiFi Page," http://aspj.aircrack-ng.org/.

[29] "FeedingBottle," http://goo.gl/C7PimN.

[30] revela wifi, "ReveLA WIFI:Reveal the password of any WiFi network," http://revela-wifi.en.uptodown.com/android.

[31] Ettercap, http://ettercap.sourceforge.net/.

[32] "WiFiKill," http://goo.gl/1ydKm.

[33] code.google.com, "droidsheep," https://code.google.com/p/droidsheep/.

[34] droidsheep.de, "DroidSheep Guard," http://droidsheep.de/?page_id=265.

[35] code.google.com, "Reaver open source," http://goo.gl/6EmyU.

[36] www.crack wifi.com, "Using sslstrip for a man in the middle attack over https (SSL), and arpspoof hack paypal," http://goo.gl/1uLqZ3.

[37] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," in *NDSS*, 2001, pp. 17–22.

[38] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid android: versatile protection for smartphones," in *ACSAC*, 2010.

[39] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks," *Comp. Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[40] H. Kim, J. Smith, and K. Shin, "Detecting energy-greedy anomalies and mobile malware variants," in *MobiSys*. ACM, 2008, pp. 239–252.

[41] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *MobiCom*. ACM, 2001, pp. 180–189.