Nathaly Flores

CYSE 615

Medical

Old Dominion University

Medical

Introduction

The medical field is rapidly adopting wireless technologies, which has led to a raging increase in the installation of medical devices. Unfortunately, attackers are now targeting the industry due to vulnerabilities in these devices. Because Wi-Fi automation is reasonably new in the medical field, deploying wireless devices introduces security gaps. In addition to the possible harm caused by malicious intrusion embedded in wireless devices, there is worry about information heist from devices linked to the building network. Medical devices maintain the risk of an attack, and patches should be created, tested, and installed immediately. The best way for Information Technology officials is to incorporate and maintain robust network authentication and encryption, execute intrusion detection and deterrence systems, and segment networks to safeguard devices and end-users. Information technology supervisors must enforce device administration techniques like executing multi-factor authentication to contain unauthorized admission, deploying details loss prevention software to stop data exfiltration, and employing mobile device encryption software to retain confidentiality and safeguard patients from damage by providently creating security controls for Wi-Fi-enabled networks and medical devices.

Medical records and devices were traditionally connected utilizing physical controls due to their non-electronic ways and the scarcity of network connectivity field (Sansurooah, 2015). Nonetheless, technologies like wireless connections have grown in medical establishments, making technical controls vital as physical controls for securing patient information (Sansurooah, 2015)**.** Clinics and Hospitals now have fifty thousand affiliated medical devices being utilized, with the increasing rate of connecting medical devices growing per bed in the United States (Sansurooah, 2015). Security was newly incorporated into the deployment of medical devices, with the FDA conducting the linked devices in 2005 (Bhatt & Bhatt, 2017). Unfortunately, there have been numerous instances of FDA warnings, device recalls, and documented exploits related to medical device security between 2008 and 2018 (Pandian, Vinayagam, Xu, & Sue, 2020). Given these risks, this essay aspires to summarize the security threats related to Wi-Fi-enabled medical devices and deliver good practices for executing affiliated security controls to safeguard both the devices and the medical data they handle.

Medical security guide

Medical devices support the potential of the Internet of Things (IoT). The medical corporation is awaiting to embrace IoT devices, with an estimated compounded annual growth rate of eleven percent, which could generate $14.7 billion in revenue by 2022 (Minaie, 2013). A recent survey of healthcare IT leaders conducted by (Callisch, 2019) identified EKG/ECG, patient monitoring, and imaging systems as the top three categories of devices to be deployed on the network in the coming years, which will be enabled with WIFI. These devices will perform various functions, including diagnostic and therapeutic treatment, disease detection, and monitoring and maintaining patient health. Furthermore, it states that the market share of these devices will include functionality for maintaining fitness and wellness (Minaie, 2013).

Despite the increasing deployment of wireless medical devices, the healthcare industry must be equipped to address the potential cybersecurity risks associated with the ubiquitous infiltration of connected medical devices. According to the Nyansa, Inc (Callisch, 2019) survey, monitoring and controlling connected medical devices is crucial for ensuring security, but fewer than half of IT departments have implemented such protective measures. The survey also found that:

- 80% of Information Technology professionals analyzed found security and patching amidst the most challenging sites when deploying interconnected medical devices.
- 57% of Information Technology divisions still need to design policies concerning the security risks of wired versus wireless devices.
- Over 50% of Information Technology branches are instructed to sustain biomedical devices but only periodically monitor their routine to ensure proper functionality.

Data security is crucial for accessing sensitive clinical information and patient data in the medical services industry. Automating data management is crucial for efficient decision-making, healthcare information exchange, personalized services based on patient needs, and improved healthcare organization and patient outcomes. Technology is vital in collecting, organizing, storing, retrieving, and sharing medical records among hospital departments and institutions. However, healthcare faces technical, mechanical, ethical, and resource-related barriers, resulting in challenges such as adopting cloud computing and mobile technologies, user errors, increased cyberattacks, health information regulations, and outdated technologies.

Top medical devices

According to Langston, the six most vulnerable medical IoT devices to security risks are Infusion and Insulin Pumps, Smart Pens, Implantable Cardiac Devices, Wireless Vital Monitors, Thermometers and Temperature Sensors, and Security Cameras. Langston also stated that infusion pumps were reported for almost all IoT medical device distribution (Langston, 2019). The National Cybersecurity Center of Excellence (NCCoE) found that wireless infusion pumps are at risk of malicious software attacks, which can bring about for them to break down or perform more distinctly than planned (Khera, 2017). Unfortunately, deploying malicious software safeguards to reduce this vulnerability may impact the pump's performance efficiency (Khera, 2017). Furthermore, wireless infusion pumps are easily compromised because most companies fall through to revising their default passcode during setup, providing direct control over the device and illegal entry to the information repository inside of the device (Khera, 2017). Khera demonstrated that the infusion pump possesses records, including infusion rates, dosages, and other secure health data that a hacker can manipulate and generate to harm the patient's information and to stop this susceptibility from further harming patients' information, a patch must be developed, tried, and remotely deployed to the pump (Kesavadev, Saboo, Krishna, & Krishnan, 2020).

Langston stated that smart pens are identified as another attack surface due to the sensitive patient data that can be accessed via the device (Langston, 2019). Doctors utilize these pens to write prescriptions conveyed to pharmacies along with patient information, as stated by Kesavadev (Kesavadev, Saboo, Krishna, & Krishnan, 2020). However, the good news is that the intelligent pen is developed with security in mind. Thus, the solution to fix the susceptibility is simple and can be installed remotely over the network. Kesavadev further elaborates that a researcher from Spirent Security Labs named Saurabh Harit attempted to reverse engineer the smart pen by exploiting network procedures and bypassing the pen's safety inspections and lock-down method (Kesavadev, Saboo, Krishna, & Krishnan, 2020). Through these methods, Harit gained administrative privileges to the device and, eventually, cracked the device encryption to entry to patient medical records on the facility's backend servers. Langston reported that Implantable Cardiac devices are another family of devices vulnerable to attacks. Since 2017, the

FDA has published four statements concerning vulnerabilities in the implantable cardiac devices (Langston, 2019).

Moreover, the University of South Alabama (USA) conducted a research project exhibiting the capability to attack a pacemaker in a patient simulator. The research team warned that such an attack in a live setting could harm the patient (Storm, 2015). Storm suggested brute force overpowering security controls and denial-of-service attacks to affect the embedded device's appropriate functioning negatively. While compromising a medical training simulator may appear effortless, Storm stated that it could damage even patients downstream anticipated incorrectness encountered during medical training.

According to Langston, medical facilities rely on wireless vital monitors, temperature sensors, security cameras, and other IoT devices vulnerable to cyber-attacks (Langston, 2019). Critical wireless transmissions must be encrypted as these devices are connected to the facility's network and may transmit sensitive patient information. Langston illustrated that these devices could be manipulated, giving hackers/attackers entrance to other systems containing sensitive patient information (Langston, 2019). Most healthcare installations lack network partitions of IoT devices from other devices (Williams & McCauley, 2017). For medical facilities to address these problems, networks should be designed to separate IoT devices from sensitive backend systems. Moreover, Langston informed that keeping an inventory of IoT-deployed devices and utilizing manufacturer patches while firmware and software updates are crucial (Langston, 2019).

Williams warned about the breakout of susceptibilities from hidden https tunnels and DNS tunnels, which were not incorporated in Langston's list of the top six weak medical devices (Williams & McCauley, 2017). Hackers/attackers exploit hidden https tunnels to convey sensitive information from the health provider's network and bypass detection like command-and-control communications. As time passes, the encrypted network traffic becomes assistance provider traffic, causing it challenging for the IT team to differentiate between correct or compromised information. On the other hand, hidden DNS tunnels are employed by hackers/attackers to convey health data to the health provider's network and take it out on the acquired nameserver, which the hacker/attacker commands, as described by Craig Sanderson.

How to secure wireless networks

Samsung's 2015 announcement acknowledged that healthcare professionals increasingly adopt wireless technology for treating patients, managing patient records, and tracking assets. Information Technology Administrators in healthcare facilities address wireless susceptibilities and safeguard patient information, and the statement suggested the five best techniques for ensuring wireless networks and devices (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). Samsung suggested the five best methods for ensuring wireless networks and devices safeguard patient information. The first approach was executing authorization entry controls and network encryption to safeguard information transmissions. According to Samsung, weak network entry security can permit crude hackers to enter the facility's wireless network and listen in on information transmissions. Samsung emphasized enforcing robust passwords and employing secure web connections via HTTPS. Specifically, Samsung suggested executing a WPA2-based encryption and authentication framework, supporting device control, and utilizing corporate directory-access procedures to contain information stealing (Islam, Kwak, Kabir, Hossain, & Kwak, 2015).

The first suggested control by Samsung guards information transmissions and contains hackers from operating the installation network to venture attacks against medical devices for patient care. Samsung's second-best approach suggests containing malicious attacks. Managers execute wireless intrusion detection and precluding systems, including wireless intrusion prevention systems (WIPS), which aid in catching rogue entrance pinpoints and safeguard against Denial of Service and Man-in-the-Middle attacks (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). Samsung's third proposal concentrates on network architecture and the significance of helpful network segregation. The statement recognizes that personal devices demand IT officials split them from hospital-managed devices and Wi-Fi utilizing separate SSIDs and appoint Bring Your Device (BYOD) Wi-Fi network entry and security procedures. The report also emphasizes the necessity of operating network segregation for internal access between divisions founded on functions and obligations. Additionally, the statement advises procedure orders demanding Virtual Private Network (VPN) utilized when accessing sensitive information on an external network while off-premises (Islam, Kwak, Kabir, Hossain, & Kwak, 2015).

The fourth proposal by Samsung underscored the significance of executing controls for mobile device management. The announcement stated that patient forms are more valuable to hackers than credit card numbers due to the information's volume and specificity, social security numbers, address information, and financial data (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). Samsung's proposal safeguarding against unauthorized access, the statement advised executing multi-factor authentication, deploying information loss prevention (DLP) software to control information breakout, and utilizing mobile device encryption software like Samsung Knox receptacle to guarantee confidentiality (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). Finally, the fifth proposal by Samsung highlighted the usefulness of a Wi-Fi-certified computer kit with an industry-recognized identification of interoperable, specifically for shared computers.

Conclusion

The healthcare enterprise vigorously embraces wireless technologies, and the number of medical devices linked to the internet is increasing. Unfortunately, this trend also makes the industry an appealing target for hackers aiming to exploit device exposures. Although wireless medical devices are useful for healthcare professionals and patients, they present security susceptibilities compromising patient information's confidentiality and integrity. Furthermore, these susceptibilities also pose a threat of physical harm to patients. For example, attackers could meddle with the correct functioning of an implant device, like a wireless infusion pump, by manipulating susceptibilities and throwing a Denial-of-Service attack.

The deployment of Wi-Fi-enabled medical devices in the healthcare business is a relatively new outcome that presents security gaps. As a result, there are worries about the security of patients, which has led the FDA to urge boosted security controls, specifically for implant devices. In addition to situations about implant devices, there is a threat of information theft from hacked devices. IT administrators must design, test, and deploy software patches to confound these safety susceptibilities. To discourse confidentiality and integrity problems, IT administrators must follow the best techniques, executing robust network authentication and encryption, deploying intrusion detection and precluding systems, and architecting networks to execute device and end-user segmentation. Device control procedures should also be executed, like implementing multi-factor authentication, deploying information failure prevention software to contain information outbreaks, and utilizing mobile device encryption software to retain confidentiality. Healthcare professionals must heed security's most valuable techniques to ensure the resumed usefulness of wireless medical devices. By identifying and managing threats to patient health records and medical devices, they can take coordinated measures to mitigate security risks. However, the most critical priority is safeguarding patients from harm by proactively executing security controls for Wi-Fi-enabled networks and medical devices.

Works Cited

Bhatt, Y., & Bhatt, C. (2017). Internet of Things in HealthCare. *SpringerLink*.

Callisch, D. (2019, February 11). *New Healthcare IT Survey Reveals How Harnessing New Digital Technologies, IoT Systems and Device Data Are Reshaping Industry Priorities*. Retrieved from BioSpace: https://www.biospace.com/article/releases/new-healthcare-it-survey-reveals-how-harnessing-new-digital-technologies-iot-systems-and-device-data-are-reshaping-industry-priorities/?s=105

Islam, S. M., Kwak, D., Kabir, M., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE*.

Kesavadev, J., Saboo, B., Krishna, M. B., & Krishnan, G. (2020). Evolution of Insulin Delivery Devices: From Syringes, Pens, and Pumps to DIY Artificial Pancreas. *SpringerLink*.

Khera, M. (2017). Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications. *Special Section: Cybersecurity for Diabetes Devices*.

Langston, F. (2019, October 31). *Top 6 Hackable Medical IoT Devices*. Retrieved from Critical Insight: https://www.criticalinsight.com/resources/news/article/top-6-hackable-medical-iot-devices

Minaie, A. (2013). Application of Wireless Sensor Networks in Health Care System. *2013 ASEE Annual Conference & Exposition*.

Pandian, G., Vinayagam, V., Xu, B., & Sue, M. (2020). Security Challenges of IoT and Medical Devices in Healthcare. *Taylor&Francis Group*, 20.

Sansurooah, K. (2015). Security risks of medical devices in wireless environments. *ECU*.

Storm, D. (2015, September 8). *Researchers hack a pacemaker, kill a man(nequin)* . Retrieved from ComputerWorld: https://www.computerworld.com/article/2981527/researchers-hack-a-pacemaker-kill-a-man-nequin.html

Williams, P. A., & McCauley, V. (2017). Always connected: The security challenges of the healthcare Internet of Things . *IEEE*.