Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework

F. Badrouchi, A. Aymond, M. Haerinia, S. Badrouchi, D. F. Selvaraj, K. Tavakolian, P. Ranganathan and Sumathy Eswaran

Abstract Any biomedical device requiring power from a source other than the human body or gravity is considered an active device. Currently available active biomedical devices encompass an enormous variety of technologies, ranging from large imaging machines to miniature implantable stimulators. These devices are vulnerable to cybersecurity threats, especially for devices capable of communication with an internet network. An attack exploiting these vulnerabilities can cause a variety of consequences, including data theft, denial-of-service, and serious patient harm. The chapter provides a comprehensive review of cyberattacks on biomedical devices in a hierarchical layered framework (e.g., sensing, communication, and control) with three specific attacks as case studies: (1) MRI unit-based attack, (2) infusion pump-based attack, and (3) implantable medical device attack.

Keywords Cybersecurity · Biomedical devices · Hierarchical layers

1 Introduction

In fall 2013, a team of elite security researchers known as "white hat hackers" was invited to the Mayo Clinic in Minnesota. They were given 40 different medical devices and told to break into them any way they could in an effort to expose vulnerabilities. The team spent one week analyzing the devices and found that every device had backdoor access points making them vulnerable to unauthorized users. The hackers were able to access the devices' control systems via generic default passwords and unsecured operating systems. After gaining access to the system, the

F. Badrouchi · A. Aymond · M. Haerinia · D. F. Selvaraj · K. Tavakolian · P. Ranganathan (✉)
University of North Dakota (UND), Grand Forks, ND, USA
e-mail: Prakash.ranganathan@und.edu

S. Badrouchi
University of Tunis EL Manar (UTM), Tunis, Tunisia

S. Eswaran
Dr. MGR Educational and Research Institute, Chennai, India

P. Raj et al. (eds.), *Internet of Things Use Cases for the Healthcare Industry*,
https://doi.org/10.1007/978-3-030-37526-3_7

hacker can launch a potentially lethal attack, such as causing a medication infusion pump to over administer medication without alerting staff [1].

Any medical device relying on an external power source is known as an active device [2]. Most modern active medical devices utilize some type of processor or computer to execute preprogrammed commands and to communicate with the hospital's network. These computers, particularly their communication channels, pose a security risk due to insufficient communication restriction, encryption, and monitoring. Once a hacker has accessed the device's processor through these insecure channels, he is able to spread the attack throughout the device's control system, actuators, and potentially out through the communication channels to the rest of the hospital network. The insufficient security protocols for these devices, and for the hospital network in general, are due to many factors, including lack of funding for IT specialists in health care, rapid growth of the variety and number of devices sharing a hospital network, and lack of cybersecurity training for the designers of the medical devices [3].

The main focus of this chapter is the cybersecurity threats on active and connected biomedical devices. As cyberphysical systems, biomedical devices are vulnerable to attack vectors such as eavesdropping, spoofing, and jamming. It is important to understand the interaction between sensors, communication, and computing platform of various medical devices in order to gain insights on how these devices are susceptible to cyberthreats.

A hospital network connects various medical technologies used to provide care to patients, including diagnostic, medication delivery, surgical, and life support equipment. Proper cybersecurity must be maintained to protect patient information and insure its confidentiality from unauthorized access and use. A closer partnership and collaboration is required between multiple entities such as hospitals, vendors of medical devices/equipment, and government agencies to mitigate cyberthreats. The United States Food and Drug Administration (FDA) recently started paying more attention to cybersecurity threats. In 2018, the FDA updated the guidance document entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" which was originally issued in 2014. This document outlines the expectations of new biomedical devices seeking FDA clearance. When comparing the modern cybersecurity demands for insurance companies and financial institutions, the FDA is still behind in making strict regulations controlling connected hospitals and devices [4, 5].

2 Overview of Existing Technologies

Medical devices have many forms and functions in modern health care. Some medical device such as pacemaker is used by an individual, whereas sphygmomanometer or infusion pump is used clinically to assess and treat many people daily. Key security-relevant differences for these device usage scenarios are the amount of personal data stored in the device, sensitivity and quantity of data collected, and type or

specificity of therapy delivered. Large clinical facilities have a much greater risk of information theft-type attack for their electronic medical records and billing info but may have fewer security concerns at the device level than do personal users. Hospital medical devices are de-identified, which lessens the risk of a personally targeted attack. However, personal devices and hospital devices are both susceptible to denial-of-service and improper functioning attacks, which will be elaborated upon later in this chapter. The rest of this chapter will primarily focus on personal medical devices; however, the security topics discussed are also relevant to devices used in a commercial setting.

– Connectivity

Connected medical devices optimize the continuous exchange of information between healthcare providers and the devices in contact with the patient [6]. This communication may occur on wired or wireless networks, or using Near-Field Communication (NFC). Wired networks offer benefits of increased speed and reliability compared to wireless networks; however, the wired networks require that equipment be physically connected and thus cannot be transported freely with the patient throughout the hospital. Wired networks may also be more costly due to the custom designing required to fit the system with the existing hospital infrastructure [7]. Some benefits and architectures of medical device connectivity are presented below.

- Reasons for connectivity
  - Connection of multiple sensors and actuators in body.
  - Record data and transmit to practitioner (e.g., Holter monitor, EEG, EKG).
  - Monitor health status and treat (e.g., artificial pancreas, pacemaker).
  - Storage of personal data for device operation (e.g., patient's goal blood sugar level).
- Various connection capabilities of existing devices are ranked by increasing security concerns:
  - Isolated (no external communication from device),
  - Programmable with wand or physical contact by practitioner,
  - Isolated with sensor,
  - Wirelessly connected,
  - In-home data connection (e.g., nightstand data transfer system),
  - Interoperable network (connection of multiple devices),
  - Interoperable network with sensors, and
  - Smartphone-connected devices.

Some examples of connectivity type based on the class of medical devices are presented in Table 1. In addition, the information on some of the working groups/organizations involved in medical device connectivity and the relevant standards are furnished in Tables 2 and 3, respectively.

Table 1 Examples of connectivity type depending on device class

Class of medical device	Examples	Wiring	Connectivity
Implantable devices	Cardiac defibrillator/Pacemaker	Not wired	Wireless body area network (WBAN)
	Cochlear implant	Not wired	Wireless body area network (WBAN)
	Neurostimulator	Not wired	Wireless body area network (WBAN)
Imaging devices	X-ray scan	Not wired	WLAN-based DDR portable radiography
	CT scan	Not wired	WLAN-based DDR portable radiography
	MRI	Wired	Local area network (LAN)
Medication delivery	Infusion pumps	Not wired	WLAN
	Insulin pumps	Not wired	WLAN
	MEMS piezoelectric micropump	Not wired	PAN–WLAN–WPAN

Table 2 Organizations/working groups involved in medical device connectivity

Organization/Working group	Areas of focus
Association for the Advancement of Medical Instrumentation (AAMI)	Initiatives toward decreasing preventable damage to patients and enhance results when the use of complicated health technology is involved in health care [8]
Health Level 7 (HL7)	Standards and framework for exchanging the electronic health records that supports better clinical practice and health service management [9]
CEN/TC 251	Standards for health information and communication technology (ICT) in the European Union [10]
Personal connected health alliance	Supports a patient-centric strategy to health and wellness improvement through private technology and promotes safe clinical-grade data that changes health behaviors [11]
National Institute of Standards and Technology (US)—Health Information Technology	Promotes point-of-care and personal health environments' device communication by developing and advancing software test tools [12]

Table 3 Standards related to medical device connectivity

Standard	Description
Digital imaging and communications in medicine (DICOM)	It describes medical image formats to guarantee that documents are exchanged for clinical use with the required data quality [13]
ISO/IEEE 11073	Standards addressing communication between external computer systems and medical devices and provide comprehensive electronic data capture of information [14]
ISO/TC 215	Enables compatibility and interoperability between autonomous devices, standardization of information and communication technology (ICT) for health sector [15]

3 Active Medical Devices Cyberattacks

Active medical devices rely on alternative source of power, and some examples include Magnetic Resonance Imaging (MRI) scanners, defibrillators, and infusion pumps. These active devices are often connected to a hospital network which allows communication between the diverse devices on the network, including computers, mobile devices, imaging systems, and medication delivery systems. While this network improves the efficiency and continuity of health care, it also creates significant risks due to insufficient monitoring of the network security. Healthcare IT networks are much more vulnerable than other sectors, such as financial services or insurance companies [3]. One reason for the increased cybersecurity risks of hospital networks is the lack of experienced IT professionals employed in the healthcare sector [16].

The motivation behind attacks could be stealing data, causing bodily harm, extortion or threat (e.g., cause diabetic coma by hacking insulin pump), and non-malicious (e.g., caused by unintended commands or interference). The attacks have different types including eavesdropping, denial-of-service, power system disruption, physical damage, artificial sensor readings (to cause incorrect therapeutic output), artificial or unauthorized command, and misuse by authorized programmers. To analyze common active medical devices' cyberattacks, the attack points are identified, a review of biomedical cyberattacks is presented in Table 4, and examples of common biomedical devices and related attacks are studied.

The examples of common biomedical devices and related attacks are presented as follows:

(A) **Magnetic Resonance Imaging (MRI)**

During the use of an MRI, a patient's physical safety is breached if a metal object in the treatment room is forcefully pulled toward the MRI's very strong magnetic field. Metal objects can be pulled into the MRI with considerable force, thus breaking the MRI and causing a user to be struck, trapped, or otherwise injured by the metal acting as a projectile. This risk is mitigated by placing metal detectors at the entrance to the

Table 4 A review of biomedical cyberattacks

Security property/attack type	Attack examples	References
Authentication (Spoofing)	Impersonate programmer (in order to alter system programming or internal controls only available to device designer/programmers)	[18–28]
	Impersonate controller/user (in order to spoof system controls normally available to a patient, physician, or technician)	[19–25, 29–36]
	Impersonate the medical device	[24, 31–37]
	Impersonate the external device/receiver	[19, 20, 22, 26, 31, 33–39]
	Other attacks not listed above	[40–42]
	Countermeasures to above attacks	[18, 20, 22–24, 30–34, 39, 41–51]
Integrity (Tampering)	Patient data tampering	[19–21, 25, 33–35, 39, 46, 52, 53]
	Malicious inputs: incorrect sensor data	[18, 20–22, 29, 31, 33–35, 37, 49, 52–55]
	Malicious inputs: jamming	[18, 20, 24, 49]
	Malicious inputs: incorrect control commands	[19, 21, 23–25, 34, 38, 44, 49, 55]
	Modify communications: alter output signal	[20, 22, 33, 46, 48, 49, 56]
	Countermeasures	[20, 23, 24, 31, 33, 43–46, 48, 51, 52, 56]
Non-repudiation (Repudiation)	Delete access logs (hide attack history)	[20, 24, 46, 48]
	Repeated access attempts	[20, 24, 33]
	Devices lacking access logs	[20, 24]
	Countermeasures	[19, 20, 23, 24, 33, 44, 48]

(continued)

Table 4 (continued)

Security property/attack type	Attack examples	References
Confidentiality (Information Disclosure)	Disclose medical information (Data theft)	[19–26, 29–33, 37–39, 46, 52, 54]
	Determine type of device or disclose existence of device (for implanted or non-visible devices)	[20, 23, 31, 34, 52, 54]
	Track the device (for implantable or mobile devices)	[20, 30, 31, 34]
	Eavesdropping	[18, 20, 22–26, 30, 31, 33, 34, 38, 39, 44, 46, 48, 55]
	Countermeasures	[18, 20, 24, 26, 31, 33, 45, 46, 48, 52, 54, 57]
Availability (Denial-of-service)	Drain battery (for mobile or implanted devices)	[20, 23, 24, 26, 29–31, 34, 38, 44, 49, 55]
	Interfere with communication capabilities: electronic attack	[18–20, 24, 26, 29–31, 34, 37, 38, 46]
	Interfere with communication capabilities: physical attack (e.g., Physical destruction of antenna or disconnection from wired network)	[18, 24, 30, 37, 54]
	Flood device with data (jamming)	[18, 20, 30, 33, 44]
	Prevent access by authorized personnel (e.g., Prevent access by physician)	[18, 22, 23, 29, 30, 37, 52]
	Countermeasures	[20, 24, 26, 30–32, 43–45, 49, 55, 58]
Authorization (elevation of privileges)	Reprogram the device	[19–21, 23, 24, 29, 34, 37, 38, 46, 54, 55, 59, 60]
	Update/alter therapy of patient	[18–24, 26, 29–31, 33, 34, 44, 54, 61, 62]
	Maliciously change device functioning (e.g., Too much radiation delivery in imaging device or cause device to shock patient)	[18, 19, 21, 22, 24, 26, 29, 31, 34, 44, 46, 54]
	Turn-off device	[20, 29, 44]
	Countermeasures	[20, 23, 24, 26, 45–47, 49, 50]

MRI room to warn staff of metal objects that must be removed before approaching the MRI machine. A physical safety breach could be enhanced by a hacker if he disables the metal detectors at the entrance to the MRI room [16, 17]. Table 5 represents potential MRI cyberattacks.

(B) **Infusion Pump**

An infusion pump delivers liquid medications to the patient's circulation via an intravenous tube. The pump uses an internal motor to deliver the medications at a controlled rate and pressure as set by the pump control system. These systems include alarms to warn staff of potential physical tampering or complications with the medication delivery. The pumps are often wirelessly connected to the hospital network, thus making them vulnerable to a cyberattack via the infusion pump's communication channels. In the event of an attack, the hacker could cause serious harm to patient or even death by altering the medication delivery schedule and pressure or by halting the medication delivery completely. The hacker could also deactivate the system alarms to prevent intervention by care staff [17]. Following the discovery and publication of several infusion pump vulnerabilities, the FDA has launched an infusion pump improvement initiative which aims to reduce the current security risks present in infusion pumps from many manufacturers by implementing stricter regulations which much be satisfied before new pumps may be sold for use in US healthcare systems [63]. Some manufacturers have begun to implement new technology and control architectures into "smart pumps" which satisfy the new FDA criteria [16]. Table 6 shows potential infusion pump cyberattacks.

(C) **Medical Laboratory**

A crucial component of the modern hospital system is a medical laboratory, which processes biological specimens from patients to provide diagnostic data to medical practitioners. The lab's infrastructure is maintained by the Laboratory Automation System (LAS), which regulates equipment such as refrigerators, fume hoods, biological hazard containment systems, ventilation, and other critical safety equipment. Interruptions to this system, as in the event of a hacker attack, could lead to injury of

Table 5 Potential cyberattacks on MRI [17]

Attacker malicious activity	Consequences
Override magnetic field strength limit	Possible patient tissue burns Possibility of damaging the machine
Disable alarms	Unawareness of dangerous conditions by technician
Reboot the machine	Delete configuration settings
Change information of display	Leads to a technician confusion to follow the protocol
Replace patient's files	Wrongly sent diagnosis to a patient

Table 6 Potential cyberattacks on infusion pump [17]

Attacker malicious activity	Consequences
Alter air purge rate or purge process	Syringe line may contain air during therapy
Disable alarms	Unawareness of dangerous conditions by nurse
Reboot the pump	Delete configuration settings
Change information of display	Leads to a nurse confusion to follow the treatment process
Replace patient's files	Wrongly delivered medication to a patient
Falsifying information on the dosage delivered	The equipment shows that the patient received the required dose, however, he did not

the lab employees, loss of patient's specimens, and delivery of incorrect test results to the practitioners [17]. Table 7 depicts potential medical laboratory cyberattacks.

(D) **Heart–Lung Machine**

A heart–lung machine is a device used to maintain an extracorporeal circuit of the patient's blood, called cardiopulmonary bypass. This is necessary during an operation which requires the patient's lungs and heart to be temporarily arrested, such as during a cardiac artery bypass or a lung transplant. While the patient's heart and lungs are nonfunctional, the heart–lung machine draws blood from the body, oxygenates it, and then pumps it back through the patient's circulation. The drug heparin is used to prevent coagulation of the blood as it passes through the machine. Heart–lung machines are critical life support technologies designed for use during difficult and challenging operations. Any alteration to the functioning of the machine poses a significant risk for patient harm or death. If an attacker gains access to the machine through the hospital network, he may cause damage through many different methods. Table 8 explores some possible cyberattacks of the heart–lung machine [17]. Other than studied cases, there are other biomedical devices and systems susceptible to cyberphysical attacks including dialysis machine, medical ventilator, robotic surgical machine, anesthetic machine, active patient monitoring devices, Extracorporeal Membrane Oxygenation (ECMO), medical lasers, Medical Device Data Systems

Table 7 Potential medical laboratory cyberattacks [17]

Attacker malicious activity	Consequences
Block the transfer of information	Critical information are not communicated
Modify test procedures or lab equipment settings	Wrong test results
Corrupt laboratory test results	Makes specialist misdiagnose patient condition and settle on inaccurate treatment choices, recommend an inappropriate medications or direct wrong consideration
Change work orders	Affects patient's treatment

Table 8 Potential heart–lung machine cyberattacks [17]

Attacker malicious activity	Consequences
Alter pump's heparin dosage (excess)	A potential internal bleeding can result from a non-appropriate clot of the blood
Heparin pump shut down	Patient blood clotting possible
Disable alarms	Unawareness of dangerous conditions by technician
Change information of display	Leads to a technician confusion to follow the protocol
Cause random alarms	Leads to a technician confusion to follow the protocol
Reboot the machine	Delete configuration settings

(MDDSs), storage devices for medical images, communications devices for medical images, and Health Electronic Records (HERs).

4 Cyberattack Detection and Prevention

4.1 Medical Device and Hospital Network Cyberattack Anatomy

In order to attack or control a hospital network or medical device, attackers follow an attack procedure composed of five stages [64]:

- Stage 1: Find a target, choose one or more approaches, and then execute attacks, penetrating at least once.
- Stage 2: Gain foothold in a medical device and cautiously seek general information and escalation of privileges. Then begin a lateral movement.
- Stage 3: Continue reconnaissance and identify targets, and move laterally within networks.
- Stage 4: Engage with chosen targets, exfiltrate confidential patient healthcare data and financial records, clean up the artifacts of attack as best as possible, and leave.
- Stage 5: Leave a ransomware tool to run in the network to extort funds directly from the healthcare institution.

Anatomy of medical device and hospital network cyberattack is shown in Fig. 1.

4.2 Tools and Procedures for Detection and Prevention

An effective and efficient cybersecurity plan is necessary for healthcare organizations. According to the Cisco Midyear Cybersecurity Report released in 2016, it takes 100–200 days for an organization to detect possible threats. An effective plan possesses

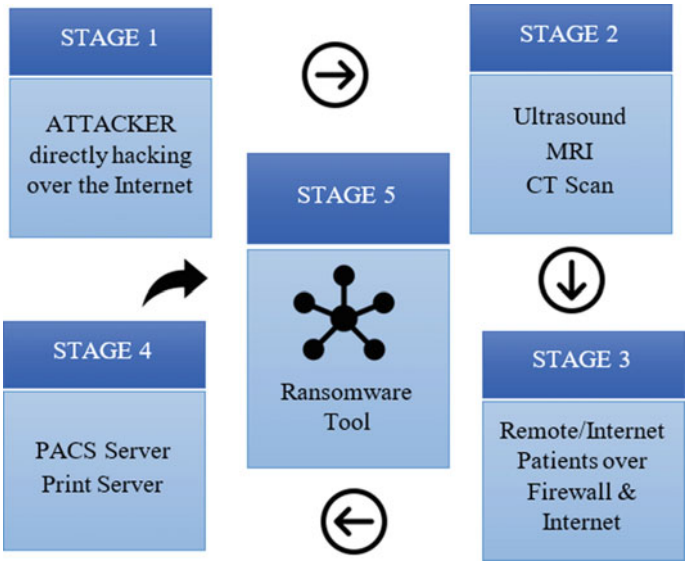

Fig. 1 Medical device and hospital network cyberattack anatomy

strong IT security tools, a strategy to stop emerging threats, and education programs for staff [65]. The robust plan has to secure sensing, control, and communication layers.

The sensing layer of a medical device is responsible for identifying any phenomena in the devices' peripheral and collecting data from the real world. This layer consists of a sensor hub using several transport mechanisms for data flow between sensors and applications [66]. The main attack points for the sensing layer are the sensor's communication with the device and spoofing of the sensor itself to transmit inaccurate sensor information [35, 36, 40, 42, 41, 51]. The sensor link or communication with the device can be secured by encrypting the channel and by maintaining a secure hospital network. Spoofing can be avoided by ensuring proper authentication of the sensor before accepting the data. Many of the novel security approaches for biomedical devices concern body area sensor networks, similar to a local Internet of Things. The main control device on or in the body communicates with several other sensors on the person to establish the network. One current experimental approach to body area network security is to only authenticate sensor nodes within a physical distance from the device to prevent remote attacks. Another method is to use the body's own physiological signals, mainly electrocardiogram (ECG), to generate secure keys.

Wireless connection is the major security concern of the communication layer. Wi-Fi, Bluetooth, and cellular communications may all be victim to eavesdropping, jamming, spoofing, and other remote attacks [38, 20, 33, 18, 24]. Devices should have all unused channels and ports secured to prevent unauthorized access. The network should utilize encryption and firewalls help to secure transmitted data, but these techniques rely on proper maintenance, such as regular password changes

and encryption algorithm updates. Many healthcare facilities lack the financial and technical resources to properly maintain such systems, leaving the hospital network and connected devices vulnerable to attack.

Typically, the control layer falls into four categories [23]:

– Access control based on user's identity to get access.
– Access control based on user's role to decide if he is allowed to access or not.
– Access control based on requesting user's set of attributes to decide if he is allowed to access or not.
– Access control based on a risk adaptive model intended to adapt risk-awareness for making decision.

Risks to the control layer involve denial-of-service and reprogramming, which cause the device to stop functioning or to deliver inappropriate therapy. These attacks can be initiated by spoofing, password tracking, or attacks throughout the healthcare network, and result in unauthorized access to the device controls. A large healthcare team can further complicate security issues, as there are many authorized users which may compromise passwords or the network [29, 22–24, 54].

Prevention of control layer attacks can involve more robust encryption and authentication schemes, as well as practice of proper cybersecurity hygiene, such as updating and securing passwords and maintaining an uncompromised hospital network. Maintaining good cybersecurity practices throughout the network prevents attacker access to the device to prevent the opportunity for a control layer attack.

The cyberattack detection tools can be used to identify rogue access points, hidden networks, and stealth port scans. The common cyberattack detection tools for hospitals and healthcare facilities are given in Table 9. To protect against possible security breaches from inside or outside an organization, suspicious activities should be monitored. Table 10 presents the cyberattack indicators and suspicious behaviors [16].

To effectively detect and prevent the cyberattacks in healthcare organizations, some solutions are provided as follows [65, 67, 16]:

- It is important to discover where sensitive data exists, so it can be protected. A reliable way to protect sensitive data is to classify and modify medical database constantly. The sensitive data is usually in the cloud and on-premises. To reduce

Table 9 Cyberattack detection tools

Cyberattack detection tool	Description and function
Wireshark	A network protocol analyzer provides detailed information about the network
Kismet	A wireless network detector
Net Stumbler	A wireless network detector
Snort	A network intrusion detection system for finding attacks and stealth port scans

Table 10 Cyberattack indicators and suspicious behaviors

Suspicious system behaviors	Suspicious user behaviors
• Unplanned reboots • Very slow performance of CPU • Unusual cycles of CPU • Doubtful configurations/software on a server • Connecting information assurance and cybersecurity (BCS) to an unknown IP • Heavy network traffic • Clearing log files • Unwanted patch modifications	• Continuous logins and logouts • Change of software configuration • Increasing account access rights and privileges • Failed login attempts • Account's connection at non-expected time periods • Creating new user accounts • Asking for information regarding the function of the system

the attack surface, sensitive data in non-production environments should be eliminated. Instead, sensitive data can be replaced with realistic, fictional data for test, development, and market research purposes. Data usage activity across a broad range of data stores should be monitored in the cloud and on-premises including databases, big data platforms, SharePoint portals, and file stores.

- Targeting users with excessive access rights and dormant user accounts is an easy way for attackers to access sensitive data. To reduce the risk of data breach, healthcare organization users who have excessive privileges and deactivated dormant user accounts must be identified and monitored. The unusual password activities must be investigated. The password change of communication network or email can be notified by an email. To avoid these types of attacks, a strong password for email and the communication network must be updated at least every 6 months. The unknown emails should be identified. Phishing emails are growing enormously; therefore, the medical and technical staff need to practice safe email protocol and have to be cautious when clicking on online links from unknown sources and opening email attachments.
- Establishment of an intrusion prevention system to detect potential breaches and halt the attack before the target is reached. Installation of a firewall would aid in isolating threats and preventing the spread of attacks between components of a network. Installation of an appropriate antivirus software is required to prevent network users from accidentally downloading malicious software from websites and to filter phishing emails. The cyberattack detection and prevention tools are shown in Fig. 2.

5 A Hierarchical Layered Framework for Biomedical Devices

Biomedical devices are extremely diverse in complexity, connectivity, and implementation environment. Devices vary from an extremely large, stationary MRI machine

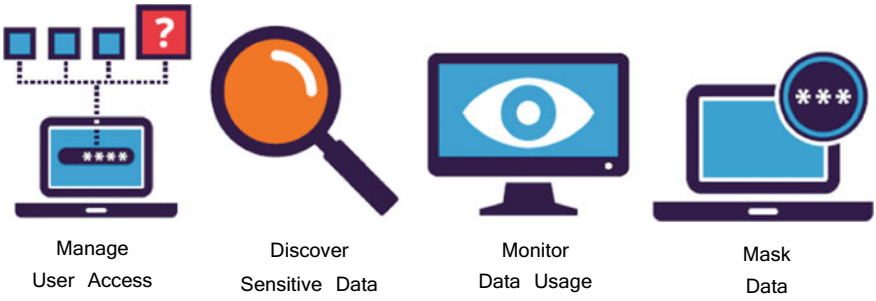

Fig. 2 Cyberattack detection and prevention tools [67]

to a small, implantable stimulator. Previously, in this chapter, cybersecurity topics for biomedical devices have been discussed in general situations to allow the concepts to be applied to as many distinct devices as possible. Three specific examples of biomedical devices are now explored as case studies to further illustrate the cybersecurity concerns of real applications. Three devices considered further are (i) MRI machine, (ii) infusion pump, and (iii) implanted pacemaker. Each of these devices will be examined using a three-layer architecture consisting of sensing, communication, and control layers. The sensing layer includes sensors in communication with the device, which may be internal or external to the device. The communication layer includes the device's communication hardware and software, as well as the networks to which the device is connected. The control layer includes the device hardware and software that handles processing, programming, and device access. The control layer may include cloud processing or other external components.

5.1 Case Study: MRI Unit Cyberattack

MRI units are one of several connected devices that can be attacked by hackers. By gaining access to the MRI unit, hackers can access patient's files and protected information and even change the test procedure and parameters. The attack starts through the communication layer, which is generally the Internet network, and then the hacker can go laterally to gain access to the device's different control layers.

- **Sensing layer attack**:

A hacker can exploit the sensing layer of an MRI unit, for instance, by using metal detectors in the MRI room, a serious physical threat can be created by deactivating these important safety sensors.

- **Communication layer attack**:

The communication is the start point of many attacks on medical devices. The communication layer provides the hacker with access to the system, and from there he

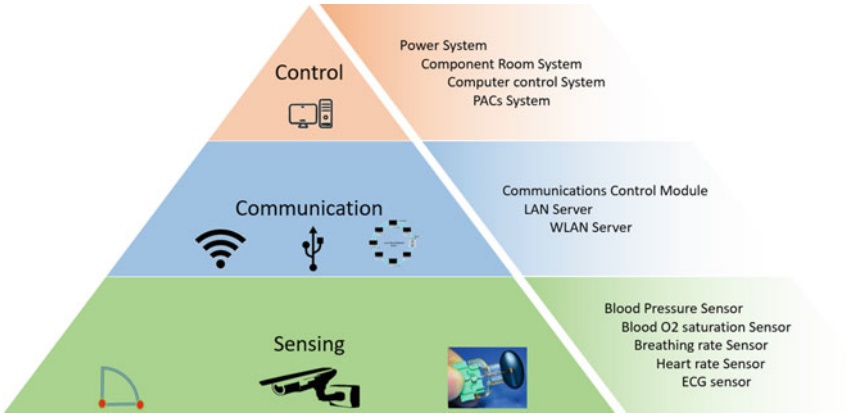

Fig. 3 Three layers in MRI unit

can gain full control of the device. In MRI, one of the communication layer potential attack points is the communication control module. It helps to translate messages between varying wireless communication standards and protocols for retransmission to other devices. The communication system is meant to transmit and/or receive data between physiological sensors, MRI controller, patient monitoring devices, patient entertainment devices, and other computers [68].

- **Control layer**:

The hacker can exploit the computers associated with MRI to change and monitor the operation procedures and parameters as well as MRI system components to cause damage to the equipment. In addition, the attack can reach the Picture Archiving and Communication System (PACS) and gain access to many patients' data.

- **PACS attack**:

The PACS serves to store medical images files such as X-ray, MRI, and CT scan images in Digital Imaging and Communications in Medicine (DICOM) format. It also includes a different type of data, like PDF files, that may be compressed within DICOM files. Hospitals have at least one centralized PACS system connected to all workstations and to the server. If an attacker succeeds to obtain access to the PACS, he can easily spread the malware or gain control to every internal and/or external connected device in the hospital. Figure 3 shows a three-layered framework for an MRI unit.

5.1.1 Attack Overview

In 2015, TRAPX security developed a cybersecurity product and tested it in four US hospitals. The product deploys a shifting minefield of Traps (decoys) and Deception Tokens (lures) that appear identical to the hospital's real IT and IoT assets that no

attacker can avoid [69, 70]. The product decoys were deployed inside the VLANs of the medical device networks and the IT corporate network. After several hours, the decoys were an integrated part of the network and acted as medical devices (from a network perspective). Shortly after, malware touched a medical device decoy and tried injecting malicious files into it. The moment the decoy was touched by the attacker, the platform automatically generated the first high-confidence alert. The alert showed that an MRI device was compromised through an internal IT desktop and then began acting as a staging point that allowed the attacker to execute multiple attacks against the hospital's internal network. The attacker gained medical device's administrator access using a well-known exploit of Windows XP. The attacker used this staging point to run more attacks against the network using the "pass the hash" attack, which leverages the PsExec tool and other malicious payloads [64, 71, 72].

A hacker can gain access to a remote server without requiring, usually mandatory, plaintext passwords. This is possible if the attacker uses the underlying NTLM (Microsoft NT Lan Manager) hash of user's password, and this type of attack is commonly called a pass the hash hacking technique. For systems requiring true authentication, this hacking technique is usually unsuccessful; however, the decoy PACS system used as a trap captured the malicious load to allow the success of the attack. By the second day, a malware was discovered in the PACS trap allowed the company to follow the traces of the attack, detect the origin, and collect its details. The origin of the attack was from a device from a totally different segment of the hospital network. The malware learned the PACS location within the network and attempted to access to the PACS trap by performing pass the hash hacking technique. The trap allowed to detect a hidden malware in the hospital network; however, the attack was unsuccessful on the real PACS but the attacker had the impression that the attack was successful [1, 3, 73]. Table 11 presents the threat behaviors in PACS.

Table 11 Threat behaviors in PACS

Type of file	32-bit portable executable application identified as UPX 0.60-3.x
Application used	The application used the Windows graphical user interface (GUI) subsystem
Attack initiation	The malware virus dropped and executed an UPX packed executable in the user temporary directory
Structure of the attack	The malware virus spread via infected local drives, removable drives, emails, and network shares
Attack execution	The file was a DLL. The DLL was injected into the EXPLORER.EXE process, thereby keeping the malware resident in memory. Part of the medical devices had a mapped network share to a central server where medical files were saved (for instance, medical images). The malware attempted to take advantage of this network share and compromised these servers as well, using the same spreading method. In this case, the malware virus used an administrator account that allowed the attacker to access more medical devices from the same vendor. However, the security program alert allowed the security team to mitigate the attack quickly and avoid any further damage

5.2 Case Study: Infusion Pump Cyberattack

The components of an infusion pump that are relevant to cybersecurity can be classified into three layers: sensing, communication, and control. If an attacker is able to access one of these layers, he may then be able to spread the attack to the other layers. The components of each layer and some possible attack scenarios are given below.

- **Sensing Layer**

The sensing layer of an infusion pump is primarily composed of internal device sensors which monitor pump function and body-worn sensors to detect the patient's vital signs. To ensure accurate delivery of medication, the pump's flow rate and pressure should be monitored by the internal sensors. The patient vital status is monitored by the body sensors to detect any adverse reactions to the delivered medication. The body-worn sensors may communicate with the device controller via wireless or wired link.

Threats to the sensing layer are loss of sensor function and delivery of incorrect sensor data to the control layer. These attacks may cause the device to deliver inappropriate treatment or to cease treatment altogether. The sensors may be vulnerable to physical or electronic attacks, either of which can modify the sensor data before it is sent to the control layer.

- **Communication Layer**

The communication layer of the infusion pump includes wireless communication with the hospital network and possibly with body-worn sensors. The wireless hospital network allows healthcare providers to communicate with the device to schedule and monitor patient treatment. The hospital network also includes many connected computers, mobile devices, and biomedical devices, forming an Internet of things [74].

The most common attack point for an infusion pump is through the communication layer. The wireless connection is often weakly secured, and the passwords and security that are used may not be adequately updated [74]. Threats to the communication layer include eavesdropping, theft of protected health information, and execution of unauthorized commands.

- **Control Layer**

The device control layer for the infusion pump is an embedded system, onboard firmware and software, and online programming and updates. Loss of function of the infusion pump may occur in a non-attack scenario if a software or firmware update is interrupted or if exposure to harmful conditions (such as a strong MRI magnetic field) causes loss of data on the embedded system.

A common attack point for the control layer is through downloaded updates. If the updates are modified by an attacker, the pump's functioning may be maliciously altered. Inappropriate updates may also cause denial-of-service attacks, such as battery drainage or lockout of authorized personnel [74]. Figure 4 represents three layers

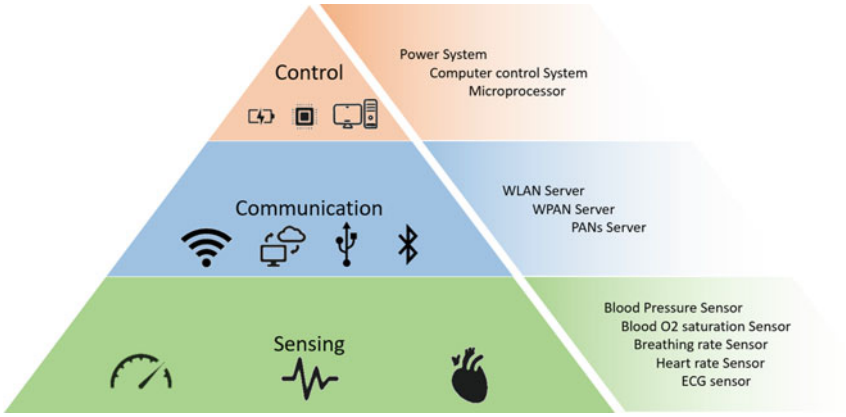

Fig. 4 Three layers in infusion pump

in infusion pump.

- **Attack Overview**

Concern about infusion pump performance and potential malfunction has been growing in recent years, prompting notices by the United States Food and Drug Administration (FDA) to pump manufacturers [63] and the creation of the FDA infusion pump improvement initiative [63]. The lack of continuous monitoring of pump performance after its implementation in the clinical setting is the central issue of the FDA communications. It is likely that some of the malfunctions are due to cyberattacks, but many clinical systems lack the resources to detect such an attack [75]. Because the devices are not adequately monitored by the manufacturer after implementation, their malfunctions may go undetected or undiagnosed [63].

In July 2015, the FDA issued a safety communication, warning healthcare teams that security vulnerabilities had been identified in certain Hospira Symbiq and LifeCare infusion pump models [76]. These vulnerabilities allowed the pump system to be remotely accessed through the hospital's wireless network via the system's communication layer [75]. The attacker could then gain access to the control layer to deliver inappropriate medication dosage or launch a denial-of-service attack [76]. The vulnerabilities in the device were not identified by the manufacturer, but rather by an independent hacker who reported the flaws to the United States Department of Homeland Security (DHS) [77], which then issued a statement about the security vulnerabilities [78]. Although no known attacks were launched on the devices, the affected pump models were pulled from market citing issues unrelated to cybersecurity after the FDA safety communication [76]; however, an unknown number of affected pump models remained in use and were still available from third-party retailers [79]. The DHS Advisory identified several security flaws in the pump devices, including failure to close unused ports (FTP and telnet ports), continued use of a default manufacturer password on port 8443, communication keys stored in plain text on the device, absence of authorization checking on the device, as well as other

Table 12 Cyber threats in infusion pump

Method of attack entry	Attacker gains remote access to the pump via the hospital network, which could be compromised through unsecured emails, etc. Hospira pump shipped with default password that went unchanged in many hospitals
Device vulnerabilities [78]	• Stack-based buffer overflow (can be exploited to execute attack code) • Improper authorization • Insufficient verification of data authenticity (device accepts updates without requiring authentication) • Default hard-coded password • Clear text storage of vital information • Poor key management (private keys and certificates stored on device) • Use of vulnerable software (versions of AppWeb) • Uncontrolled resource consumption (requires manual reboots)
Attack types	Reprogram device, denial-of-service, eavesdrop, track device
Attack outcome	No reported attacks actually occurred. In the event of a real attack, reprogramming the device to inappropriately deliver or withhold medication could lead to patient injury or death. Other attacks include eavesdropping to steal private health information, denial-of-service or jamming to make pump nonfunctional, or tracking the device within the hospital network to track the patient

vulnerabilities [75, 79, 76, 77]. Table 12 presents threat behaviors in infusion pump. Figures 5 and 6 represent network diagram of an MRI unit and an infusion pump, respectively.

5.3 Case Study: Implantable Medical Device Cyberattack

Implantable Medical Devices (IMDs) are used for diagnostic, monitoring, and therapeutic purposes. IMDs should be not only robust and effective but also secure and safe. Since the patient's life is depended on these electronic devices, only the authorized medical personnel should have access to the devices. There are several types of attacks reported by users and hospitals such as theft of protected health information and execution of fraudulent device commands. In this section, control, communication, and sensing layers in IMDs are studied and potential threats in the access schemes are presented to prevent unauthorized access.

The IMD access control schemes are divided into four categories including the access control architecture, the communication channel security keys type, the access control logic, and the access control channel [23].

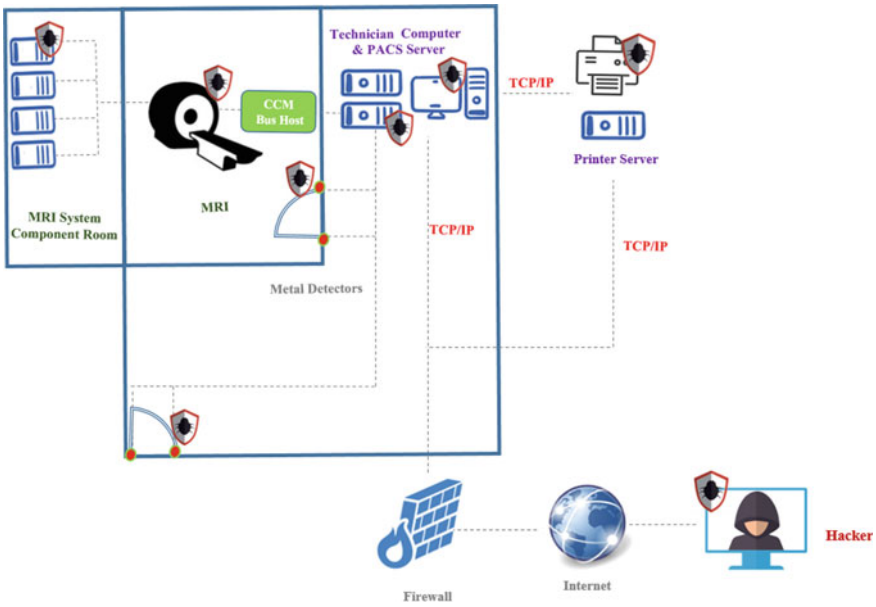

Fig. 5 Network diagram of an MRI unit

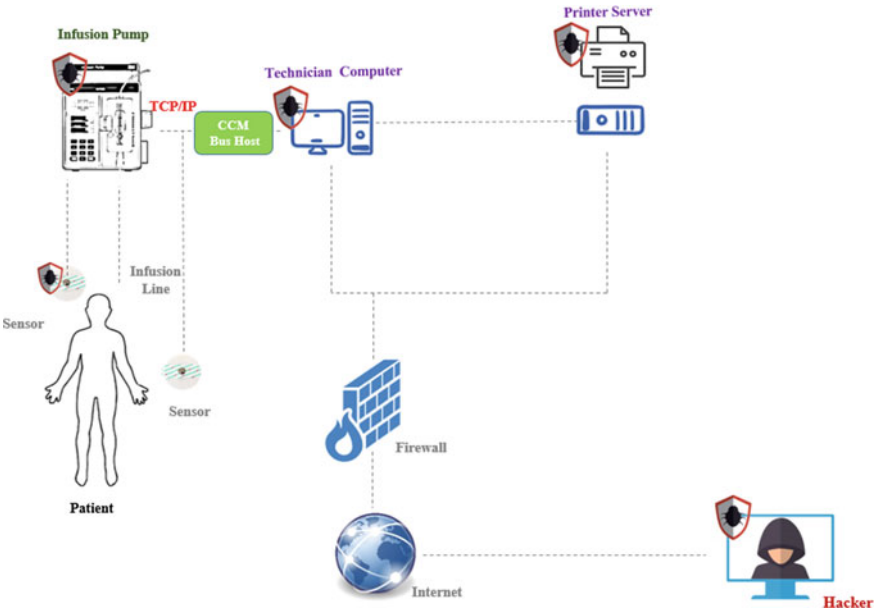

Fig. 6 Network diagram of an infusion pump

- **Control Layer**

Access Control Architecture: The authorized person is able to communicate with IMD directly and indirectly. In the case that user connects to IMD via a proxy device (indirect control), the user is able to specify proxy parameters [23].

Type of Keys: The preloaded permanent keys and the temporary keys generated from a certain source can be used to have direct and indirect access control [23].

Access Control Channel: The access control panel can be managed by ordinary activities such as human muscle motions and sound/video [23].

Access Control Logic: The logic of IMD access control using temporary and permanent keys is different. Access control logic is the key matching for the permanent keys and the access control logic for temporary keys is defined by the properties of the physical channel [26].

- **Communication Layer**

The other layer is communication. It is mandatory to study safety and protection conditions and risks to the Wireless Body Area Network (WBAN) communication structure [52].

The communication design in WBANs system has three levels as follows:

Intra-WBAN communication, the signals measured by sensors will be received by a personnel server (PS) acting as an entrance. The PS sends the collected data to the next level.

Inter-WBAN communication, the second tier is like a bridge between the PS and the user via Access Points (APs) that are accounted as a key component of the communication network.

Beyond-WBAN Communication, in this level, the medical history and specific profile of the patients are accommodated; therefore, a medical environment database is a necessity. It is worth mentioning the personal server in first level can directly connect to the third level of network via General Packet Radio Service (GPRS) or broadband cellular networks.

There are two modes of inter-WBAN communication, infrastructure-based mode communication and ad hoc-based mode communication. The infrastructure-based mode communication is used for most of the WBAN applications and provides better security than ad hoc-based mode communication and also performs like a database server. Although the ad hoc architecture setup is bigger, it promotes motion across much bigger areas [52].

5.3.1 Sensing Layer

The sensors are embedded in sensing layer. The aim of the sensing layer of implantable medical devices is to identify phenomena in human body and obtain data [66]. It is worth mentioning that the locations of sensors are not fixed because the body changes position [52]. Figure 7 depicts three layers in implantable medical devices.

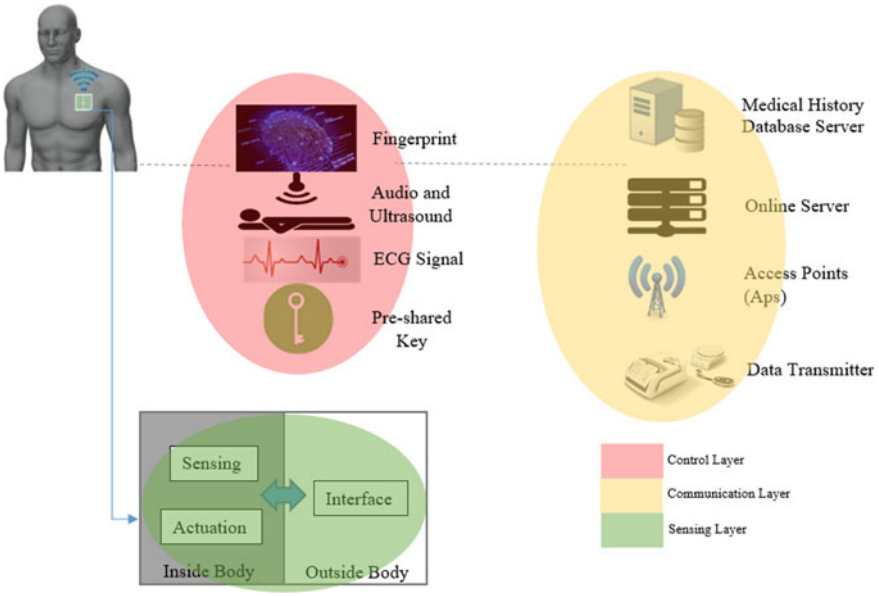

Fig. 7 Control, communication, and sensing layers in IMDs

5.3.2 Attack Overview

A new generation of pacemakers is equipped with wireless technologies to help cardiologists monitor how well the devices are functioning. There is a growing interest in using wireless systems for medical implants for data communication and in charging batteries of medical implants using Wireless Power Transfer (WPT) [80, 81]. Developing medical implants such as the pacemaker with wireless capabilities increases vulnerability to hacking attacks. The hacking attack of pacemakers was reported by the US Food and Drug Administration (FDA) in 2012. According to this report, in some cases the batteries in pacemakers were prematurely drained and in some others the devices were forced to excite the heart at deadly speeds [82]. In this case, the attack occurred in communication layer. To avoid these types of attacks, the patients are required to update their devices' firmware. The update can be done by trained medical staff and there is no need for any invasive surgery. Pacemakers with a remote monitoring unit last longer, have better battery life, have fewer inappropriate shocks and malfunctions, and have improved overall health management [82].

There was another alert issued by FDA regarding safety communication of implantable cardiac devices including Medtronic's Implantable Cardioverter Defibrillators (ICDs) and Cardiac Resynchronization Therapy Defibrillators (CRT-Ds). This FDA communication alerts users to the security vulnerabilities present due to communication between various components of these systems, including the implanted device itself, the home monitoring and data transmission stations, and

Table 13 Potential Implantable Medical Devices (IMDs) cyberattacks

Malicious hacker activity	Consequences
Manipulating access control of an affected product	The attacker is able to inject, modify, and intercept data within the telemetry communication [84]
Connecting to communication protocol	The attacker can change memory in the implanted cardiac device [84]
Having access to external controller unit of IMD	The attacker can reprogram the medical implants [85]
Connecting to medical history database server	The attacker can steal confidential information of the patients
Having access to the sensing layer	The unauthorized personnel are able to monitoring information collected by the sensors and manipulate data from sensors [86]
Controlling power range of transmitter in case that it is used for wireless power transfer (WPT)	The attacker can damage or burn the medical implants

programming devices in the clinic. The manipulation of cardiac device configured by clinic programmers is to be considered an attack in control layer [83].

The Medtronic Conexus Radio Frequency Telemetry Protocol is released by CISA in 2019 [84]. This protocol allows the Medtronic cardiac devices to wirelessly communicate between the implanted device, clinic-based programming and data-display stations, Medtronic-operated programming and update stations, and home data collection stations. Beyond safety features in the current Medtronic's implantable cardiac devices, multiple research teams are developing novel authentication and encryption strategies to improve robustness of medical device cybersecurity. The potential cyberattacks against Implantable Medical Devices (IMDs) are presented in Table 13.

6 Conclusion

A three-layered hierarchical framework categorizing the attack vectors of biomedical devices was discussed. Specifically, how the isolation of sensing, communication, and control layer framework in three medical devices as use cases: MRI unit, infusion pump, and implantable medical devices will help in mitigating the cyberattack vectors was presented. A review of several literatures on possible cyber threats that can occur in biomedical devices was detailed in this chapter. Such a framework will help provide some isolation and lead time to thwart attacks, and enable in implementation of cybersecurity policies in the intrusion detection systems or firewall units in healthcare organizations.

References

1. Robertson J, Reel M (2015) It's way too easy to hack the hospital. Wired. http://www.bloomberg.com/features/2015-hospital-hack/
2. Schich A (2019) Active medical devices. https://www.med-cert.com/en_certification/en_medical-device/
3. TrapX Labs (2015) Anatomy of an attack medjack (Medical Device Hijack), pp 1–39
4. U.S. Food and Drug Administration (2014) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff (Document Issued on: October 2, 2014), FDA Guide, p 6
5. FDA (2014) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff. FDA Guide, p 6
6. Witonsky P (2012) Leveraging EHR investments through medical device connectivity. Healthc Financ Manage 66(8):50–3
7. Brookstone A (2011) Pros and Cons of wireless and local networks. http://www.americanehr.com/blog/2011/08/the-pros-and-cons-of-wireless-and-local-networks/
8. Meldrum SJ (1979) Association for the advancement of medical instrumentation 14th annual meeting. J Med Eng Technol 3(5):259
9. Health Level Seven International (2014) Health Level Seven International: tools & resources. http://www.hl7.org/participate/toolsandresources.cfm
10. CEN/CT, "CEN/TC 251," (2015) European Committee for Standardization. http://cimlaboratory.com/
11. Personal Connected Health Alliance, "Personal Connected Health Alliance," (2018). http://www.pchalliance.org/
12. Brien GO, Brien GO, Edwards S (2017) Securing wireless infusion pumps in healthcare delivery organizations, p 354
13. Rodrigues JJPC, Sendra Compte S, de la Torra Diez I (2016) Digital imaging and communications in medicine. In: e-Health Systems, pp 53–74
14. IEEE 11073-10207-2017—IEEE Health informatics—Point-of-care medical device communication. IEEE Standards Association. https://standards.ieee.org/standard/11073-10207-2017.html
15. ISO, "ISO/TC 215 Health informatics," (1998). https://www.iso.org/committee/54960.html
16. Ayala L (2016) Cybersecurity for hospitals and healthcare facilities
17. Archibold RC (2001) Hospital details failures leading to M.R.I. fatality. The NewYork Times. http://www.nytimes.com/2001/08/22/nyregion/hospital-details-failures-leading-to-mri-fatality.html?src=pm
18. Challa S, Wazid M, Das AK, Khan MK (2018) Authentication protocols for implantable medical devices: taxonomy, analysis and future directions. IEEE Consum Electron Mag 7(1)
19. Wu F, Eagles S (2016) Cybersecurity for medical device manufacturers: ensuring safety and functionality. Biomed Instrum Technol 50(1)
20. Camara C, Peris-Lopez P, Tapiador JE (2015) Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Informat 55
21. Klonoff DC (2015) Cybersecurity for connected diabetes devices. J Diabetes Sci Technol 9(5)
22. Zheng G, Zhang G, Yang W, Valli R, Shankaran R, Orgun MA (2018) From WannaCry to WannaDie: security trade-offs and design for implantable medical devices. In: 2017 17th international symposium communication informative technology ISC 2017, vol 2018-Janua, pp 1–5
23. Wu L, Du X, Guizani M, Mohamed A (2017) Access control schemes for implantable medical devices: a survey. IEEE Internet Things J
24. Ellouze N, Rekhis S, Boudriga N, Allouche M (2017) Cardiac implantable medical devices forensics: postmortem analysis of lethal attacks scenarios. Digit Investig
25. Zheng G et al (2019) A critical analysis of ecg-based key distribution for securing wearable and implantable medical devices. IEEE Sens J 19(3):1186–1198

26. Rekhis S, Boudriga N, Ellouze N (2017) Securing implantable medical devices against cyberspace attacks. In: 2017 2nd international conference anti-cyber crimes, ICACC 2017, pp 187–192
27. Pycroft L, Aziz TZ (2018) Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Expert Rev Med Devices 15(6):403–406
28. Mcdonald KA, Security CI, Clinic M, Wirth A, Architect DH (2018) The intersection of patient safety and medical device cybersecurity
29. Pycroft L et al (2016) Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg 92
30. Altawy R, Youssef AM (2016) Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices. IEEE Access 4
31. Hasan R, Zawoad S, Noor S, Haque MM, Burke D (2016) How secure is the healthcare network from insider attacks? An audit guideline for vulnerability analysis. In: Proceedings—international computer software and applications conference
32. Meng W, Li W, Wang Y, Au MH (2018) Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Future Generat Comput Syst
33. Kompara M, Hölbl M (2018) Survey on security in intra-body area network communication. Ad Hoc Netw 70
34. Arney D, Venkatasubramanian KK, Sokolsky O, Lee I (2011) Biomedical devices and systems security. In: Proceedings of the annual international conference of the IEEE engineering in medicine and biology society, EMBS
35. Williams PAH, Woodward AJ (2015) Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices Evidence Res 8
36. Ali B, Awad AI (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors (Switzerland)
37. Stine I, Rice M, Dunlap S, Pecarina J (2017) A cyber risk scoring system for medical devices. Int J Crit Infrastruct Prot
38. Kramer DB, Fu K (2017) Cybersecurity concerns and medical devices lessons from a pacemaker advisory. JAMA J Am Med Assoc
39. Lee M, Lee K, Shim J, Cho SJ, Choi J (2017) Security threat on wearable services: empirical study using a commercial smartband. In: 2016 IEEE international conference on consumer electronics-Asia, ICCE-Asia 2016
40. Jagannathan S, Sorini A (2016) Self-authentication in medical device software: an approach to include cybersecurity in legacy medical devices. In: ISPCE 2016—proceedings: IEEE symposium on product compliance engineering
41. Pozzobon O, Canzian L, Danieletto M, Chiara AD (2010) Anti-spoofing and open GNSS signal authentication with signal authentication sequences. In: Programme and abstract book—5th ESA workshop on satellite navigation technologies and European workshop on GNSS Signals and signal processing, NAVITEC 2010
42. Salem A, Zaidan D, Swidan A, Saifan R (2016) Analysis of strong password using keystroke dynamics authentication in touch screen devices. In: Proceedings—2016 cybersecurity and cyberforensics conference, CCC 2016
43. Anderson S, Williams T (2018) Cybersecurity and medical devices: are the ISO/IEC 80001-2-2 technical controls up to the challenge? Comput Stand Interfaces
44. Kulac S, Sazli MH, Ilk HG (2018) External relaying based security solutions for wireless implantable medical devices: a review. In: Proceedings of the 2018 11th IFIP wireless and mobile networking conference, WMNC 2018
45. Gao Y, Liu W (2015) A security routing model based on trust for medical sensor networks. In: Proceedings of 2015 IEEE international conference communication software networks, ICCSN 2015, pp 405–408
46. Wazid M, Das AK, Kumar N, Conti M, Vasilakos AV (2018) A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE J Biomed Heal Informat 22(4):1299–1300

47. Das AK, Wazid M, Kumar N, Khan MK, Choo KKR, Park YH (2018) Design of secure and lightweight authentication protocol for wearable devices environment. IEEE J Biomed Heal Informat
48. Challa S et al (2018) An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Comput Electr Eng 69:534–554
49. Ellouze N, Rekhis S, Boudriga N, Allouche M (2018) Powerless security for cardiac implantable medical devices: use of wireless identification and sensing platform. J Netw Comput Appl
50. Paliokas I, Tsoniotis N, Votis K, Tzovaras D (2019) A blockchain platform in connected medical-device environments: trustworthy technology to guard against cyberthreats. IEEE Consum Electron Mag 8(4):50–55
51. BSI (2019) Multi-part Document BS EN 419251—security requirements for device for authentication. The British Standards Institution. https://landingpage.bsigroup.com/LandingPage/Series?UPI=BS EN 419251
52. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2017) Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt Informat J 18(2)
53. Kohli S, Exploring cyber security vulnerabilities in the age of IoT. Cyber Security Threats, IGI Global, 1609–1623
54. Xu J, Venkatasubramanian KK, Sfyrla V (2016) A methodology for systematic attack trees generation for interoperable medical devices. In: 10th annual international systems conference, SysCon 2016—Proceedings
55. Mosenia A, Jha NK (2018) OpSecure: a secure unidirectional optical channel for implantable medical devices. IEEE Trans Multi Scale Comput Syst 4(3):410–419
56. Mikson C, Hammargren L, Strunk E (2017) Medical devices and data: protecting patients and their PHI
57. Alabdulatif A, Khalil I, Yi X, Guizani M (2019) Secure edge of things for smart healthcare surveillance framework. IEEE Access
58. Chizari H, Lupu EC (2019) Extracting randomness from the trend of IPI for cryptographic operators in implantable medical devices. IEEE Trans Dependable Secur Comput
59. Gaukstern E, Krishnan S (2018) Cybersecurity threats targeting networked critical medical devices. In: ASEE IL-IN section conference, vol 2
60. Owens B (2016) Stronger rules needed for medical device cybersecurity. Lancet 387(10026):1364
61. Slotwiner D (2019) Editorial commentary: cybersecurity of cardiac implantable electronic devices—role of the clinician. Trends Cardiovasc Med
62. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF (2018) Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians. Hear Rhythm
63. FDA (2014) Infusion pumps—infusion pump improvement initiative
64. Trapx B (2018) MEDJACK.4 medical device Hijacking, pp 1–29
65. Sabio R (2017) 5 ways to detect a cyber attack. Huffpost. https://www.huffingtonpost.ca/2017/01/30/detect-cyber-attack_n_13880814.html
66. Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS (2018) A survey on sensor-based threats to
67. Anand K (2016) Healthcare cyber security and compliance guide. Imperva
68. Brown MJ, Herrera B (2013) Method and apparatus for MRI compatible communications. US20140275970A1
69. Tomlinson K (2017) The lurker in your MRI machine wants money, not your life. Archer Energy Solutions LLC. https://archerint.com/the-lurker-in-your-mri-machine-wants-money-not-your-life/
70. TrapX (2019) The most effective solution for advanced breach detection. https://trapx.com/product/
71. Ewaida B (2010) Pass-the-hash attacks: tools and mitigation, p 53
72. Jadeja N, Parmar V (2016) Implementation and mitigation of various tools for pass the hash attack. Proc Comput Sci

73. Perez R (2017) Article 29 Working Party still not happy with Windows 10 privacy controls. Haymarket Media, Inc. http://www.scmagazine.com/home/security-news/privacy-compliance/article-29-working-party-still-not-happy-with-windows-10-privacy-controls/
74. O'Brien G, Edwards S, Littlefield K, McNab N, Wang S, Zheng K (2018) Securing wireless infusion pumps in healthcare delivery organizations
75. CISA (2013) Hospira Symbiq infusion system. Biomed Saf Stand 43(18):144
76. FDA (2017) LifeCare PCA3 and PCA5 infusion pump systems by Hospira: FDA safety communication—security vulnerabilities. https://wayback.archive-it.org/7993/20170112164109/http:/www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm446828.htm
77. Thomson I (2015) This hospital drug pump can be hacked over a network—and the US FDA is freaking out. Register. https://www.theregister.co.uk/2015/08/01/fda_hospitals_hospira_pump_hacks/
78. CISA (2015) Hospira Plum A+ and Plum A+3 Infusion systems. Biomed Saf Stand 45(8):60–61
79. Stanley N, Coderre M (2016) An introduction to medical device cyber security a European perspective. Healthc Inf Manag Syst Soc
80. Shadid R, Haerinia M, Sayan R, Noghanian S (2018) Hybrid inductive power transfer and wireless antenna system for biomedical implanted devices. Prog Electromagn Res C 88(June):77–88
81. Haerinia M (2018) Modeling and simulation of inductive-based wireless power transmission systems. In: Olfa K (eds) Energy harvesting for wireless sensor networks: technology, components and system design, 1st edn., De Gruyter: Berlin, Germany; Boston, MA, USA, pp 197–220
82. Alpine Security (2019) Most dangerous hacked medical devices. https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices
83. US FDA (2019) Cybersecurity vulnerabilities affecting medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication
84. Department of Homeland Security (2019) Medtronic conexus radio frequency telemetry protocol
85. P. S. Development (2011) Integrated circuits for implantable medical devices
86. Cichonski J (2019) Security for IOT sensor building management systems case study

Foued Badrouchi is currently a Ph.D. candidate at the University of North Dakota (UND), Grand Forks, North Dakota, USA. He received his B.Sc and M.Sc. degree in Petroleum engineering from Boumerdes University (UMBB), Algeria, in 2015. He is currently an Instructor and Teaching Assistant at the Department of Petroleum Engineering. He is also a Lab Manager and serves as the President of the Society of Petroleum Engineers UND student chapter. He is also named as Technical Advisor for a Petroleum Cybernetics graduate program in Algeria. He is part of a team focusing on kidney transplantation amelioration. His research interest includes Petroleum Engineering, machine learning, biomedical engineering, and kidney transplantation.

Abby Aymond is a Master of Biomedical Engineering student at the University of North Dakota (UND). Her thesis focus is the development of an electronic device to monitor and analyze cardiovascular signals in the user's home environment. She received a Bachelor of Science in electrical engineering with a focus in biomedical engineering from UND.

Mohammad Haerinia received his B.Sc. and M.Sc. degree in Electrical Engineering. Currently, he is researching at the University of North Dakota, ND, the USA in the field of Biomedical Engineering. His research interest includes wireless power transfer (WPT), WPT for medical devices, design of the implantable antenna, and applied electromagnetics. He is a member of IEEE-Eta Kappa Nu (IEEE-HKN), the honor society of IEEE. He serves as a Reviewer for

Institution of Engineering and Technology (IET) Journals (Power Electronics, Electronics Letters and Microwaves, Antennas & Propagation), and also IEEE Journals (Antennas and Wireless Propagation Letters, Antennas and Propagation Magazine).

Samarra Badrouchi is a graduate student at the Medical School of Tunis, Tunisia. She is currently completing her residency in Nephrology at the Internal Medicine and Nephrology Department, Charles Nicolle's Hospital, Tunisia. She worked for one year as an intern in different departments in the hospitals of Tunis and worked one year as a volunteer in the Endocrinology Department in the Tunisian Institute of Nutrition. She succeeded in the national exam of specialization in medicine. She is currently working on her Medical Doctor degree (Ph.D.) and she is the head of a research team focusing on studying and ameliorating the Kidney Transplantation Experience using Machine Learning. Her research interests include dialysis, kidney transplantation, and the use of artificial intelligence in the medical field.

Daisy Flora Selvaraj is currently a postdoctoral research fellow at the University of North Dakota (UND), Grand Forks, North Dakota, USA. She received her B.E degree in Electrical and Electronics Engineering from Bharathidasan University, India, in 1999 and the M.E degree in High Voltage Engineering from Anna University, India, in 2008 and the Ph.D. degree in Electrical engineering from Visvesvaraya Technological University (VTU), Belgaum, India in 2018. From 2013 to 2017, she was a Senior Research Fellow at R&D Management Division of Central Power Research Institute, Bengaluru. Her research interest includes smart grid, data analytics, cyberphysical systems, control algorithms for smart grid, condition monitoring of power apparatus, and machine learning algorithms.

Kouhyar Tavakolian joined the Electrical Engineering department in March 2014. Prior to joining UND, he was a postdoctoral fellow at ECE department at the University of British Columbia, Vancouver, Canada for 2 years. He received his B.Sc. in Biomedical Engineering from Tehran Polytechnic in 2000, M.Sc. degree in Bioelectrical Engineering from Electrical Engineering department at the University of Tehran in 2003, and another M.Sc. degree in Computer Science from University of Northern British Columbia, Canada in 2005. His particular interest is in biological signal and image processing, biomedical instrumentation, and noninvasive cardiology technologies, and he has published more than a hundred journal, conference proceedings, patents, and book chapters in these fields.

Prakash Ranganathan is currently an Assistant Professor of Electrical Engineering and also serving as the Research Director for Data Energy Cyber and Systems (DECS) Laboratory at the University of North Dakota (UND). His research areas include operations research, smart grid, data mining, and cybersecurity. He is a senior IEEE member and member of Research Institute for Autonomous Systems (RIAS), a center for advancing autonomous systems, data, and cybersecurity research. He also plays a leadership role in cyber educational initiatives for the North Dakota University System (NDUS). He is a recipient of the College of Engineering and Mines (CEM)'s Dean's Outstanding Faculty Award; North Dakota Spirit Faculty Achievement Award from UND Alumni Foundation recognizing his significant contribution in teaching, research, and service and a Public Scholar Award from Center for Community Engagement. He earned his Ph.D. in Software Engineering from North Dakota State University (NDSU). He also plays a mentorship role for several native American students and tribal college faculty across the tribal reservations in the State of North Dakota.

Sumathy Eswaran is currently a professor of Computer Science and Dean at Dr. MGR Educational and Research Institute, India. She holds rich experience of 15 years from Industry and 15 years in academics. She has 30+ publications. Her interest is in data management, data sciences, and education management.