2018

A LITERATURE REVIEW ON THE CURRENT STATE OF SECURITY AND PRIVACY OF MEDICAL DEVICES AND SENSORS WITH BLUETOOTH LOW ENERGY

Todd O. Arney
Michigan Technological University, toarney@mtu.edu

A LITERATURE REVIEW ON THE CURRENT STATE OF SECURITY AND PRIVACY OF MEDICAL DEVICES AND SENSORS WITH BLUETOOTH LOW ENERGY

By

Todd O. Arney

A REPORT

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In Medical Informatics

MICHIGAN TECHNOLOGICAL UNIVERSITY

2018

This report has been approved in partial fulfillment of the requirements for the Degree of MASTER OF SCIENCE in Medical Informatics

School of Technology

Report Advisor:	*Dr. Guy Hembroff*
Committee Member:	*Dr. Yu Cai*
Committee Member:	*Dr. Donald Peck*
School Dean:	*Dr. Adrienne Minerick*

Table of Contents

Acknowledgments

I would like to acknowledge my colleagues and mentors Guy Hembroff and Yu Cai for their guidance and advocacy for my continuing pursuit of education.

I'd also like to thank my family for their support and encouragement. It is only with their help that has brought me to where I am at today.

Definitions

Security: A process to help promote privacy through confidentiality, integrity, and availability.

Privacy: Three main canons: Non-intrusion into personal space, non-interference with personal decisions, and control over personal information.

Personal information: Medical and financial related information and data.

Bluetooth Low Energy - wireless communication technology to create wireless personal area networks (WPANs). Formerly known as Bluetooth Smart. Also known as Bluetooth LE, BLE, and BTLE.

Implantable medical devices: The Active Implantable Medical Device (AIMD) Directive 90/385/EEC defines an active implantable medical device as "any active medical device which is intended to be totally or partially introduced, surgically or medically, into the human body or by medical intervention into a natural orifice, and which is intended to remain after the procedure". As one of the highest risk categories of device, they are subject to rigorous regulatory controls both pre- and post-market.[1]

Morbidity: The state of being or incident rate of having a disease, illness, injury, or sickness

List of abbreviations

BLE - Bluetooth Low Energy

CAGR - Compound Annual Growth Rate

EHR - Electronic Health Record

HIPAA - Health Insurance Portability and Accountability Act

IMD - Implantable Medical Device

SCADA - Supervisory control and data acquisition

Abstract

Technology use in healthcare is an integral part of diagnosis and treatment. The use of technology in medical devices and sensors is growing. These devices include implantable medical devices, and consumer health and fitness tracking devices and applications. Bluetooth Low Energy (BLE) is the most commonly used communication method in medical devices and sensors. Security and privacy are important, especially in healthcare technologies that can impact morbidity. There is an increasing need to evaluate the security and privacy of healthcare technology, especially with devices and sensors that use Bluetooth Low Energy due to the increasing prevalence and use of medical devices and sensors. Therefore, more robust security analysis is needed to evaluate security and privacy aspects of medical devices and sensors that use Bluetooth Low Energy.

1 Introduction

In healthcare, medical devices and sensors are used with the intention to improve patients' quality of care. This use ranges from diagnosis to treatment to monitoring to providing life-sustaining medication and services. Examples include wearable devices like Fitbit and heart rate or blood pressure monitors to sophisticated blood glucose monitors, insulin pumps, and implantable cardiac devices.

Medical devices and sensors have become a vital part of healthcare and are used to treat, monitor, and measure a person's health and sometimes used to prevent or cure illness or disease.

Many of these medical devices and sensors use wireless communication for interoperability employing the latest version of Bluetooth called "Bluetooth Low Energy" or simply "BLE." Using BLE for communication provides lower power consumption for devices and therefore substantial battery savings.

With the increased need for healthcare, the need for efficient and cost-effective medical services, and rise in health awareness and home healthcare, the use of BLE medical devices is also increasing.

BLE, as with any wireless communication protocol, has potential security risks that can affect the security of medical devices and can have consequences to patients' privacy ranging from temporary inconvenience to catastrophic failure resulting in death.

There is a need for more rigorous security and vulnerability assessment process for medical devices to promote patient safety and well-being.

2 Background

2.1 Medical devices and sensors in healthcare

Medical professionals rely on a wide range of medical devices and sensors when diagnosing or treating patients. Technology like medical devices and sensors are ideally suited to collect, process, store and respond to the amount of data collected, and through connections to other health information technology, correlated to assist with diagnosis and treatment.

2.2 Medical device and sensors proliferation

The use of medical devices and sensors in healthcare is growing and will continue to grow. The global medical device market is expected to reach an estimated $409.5 billion by 2023, and it is forecast to grow at a CAGR of 4.5% from 2018 to 2023.[2]

According to Berg Insight, in 2016 there were 7.1 million patients worldwide that are remotely monitored using connected medical devices. This number does not include personal health tracking devices. Berg Insight estimates that the number of people remotely monitored will reach 50.2 million by 2021. [3]

The 2018 Bluetooth Market Update states: “Medical grade devices are on a steady climb. Demand for healthcare providers to better administer medication, diagnose injuries, and receive critical updates on their patients’ conditions is driving a 28% CAGR in Bluetooth healthcare wearables over the next five years.” [4]

Tractica predicts that annual wearable device shipments will increase from 85 million units in 2015 to 559.6 million units by 2021, representing a compound annual growth rate (CAGR) of 36.9 percent. [5] ABI Research predicts shipments of just activity trackers will top 87 million in 2021. [6]

Healthcare technology can help to provide solutions to meet this increasing demand. The demand for healthcare has outpaced the supply and has contributed to a corresponding dramatic increase in the costs of healthcare. In this environment, there is a growing need for more efficient and more economical health-related policies, procedures, and practices, and many are looking to technology to help provide solutions.

The current healthcare system has many issues including a large aging population of people (baby boomers) that are now entering the stage where more and more medical resources are needed from a system that is already overtaxed and where healthcare professionals are already struggling to meet the existing workload.

It is estimated that 45% of Americans have at least one chronic condition or illness requiring medical attention and that two-thirds of the population in the United States is overweight or obese which can lead to additional medical issues such as diabetes and heart disease.[7] These issues, along with changes in diet and a more sedentary lifestyle, have contributed to the increased need for healthcare.

As these issues with healthcare continue to gain attention, there is also a rise in healthcare awareness and involvement as an increasing number of stakeholders join the conversation. Individuals, insurance providers, and healthcare organizations are becoming more comfortable with technology and are looking for opportunities to promote self-managed healthcare. Medical devices and sensors using technology provide a way for both clinicians and patients to track everything from quantitative items like number of steps, weight, blood pressure, heart rate, and blood glucose to more qualitative measurements like mood or mental state and sleep quality. Technology is also being adapted and used as an additional channel of patient-doctor communications, telemedicine, keeping track of medical records, and prescription refill requests.

With this attention to health and the rising costs associated with healthcare, technology is providing consumers a cost-effective method to monitor, collect and access their own medical information and provide healthcare providers additional information in their

diagnosis and treatment plans. Along with the increased familiarity and use of mobile and wireless technology, the use of sophisticated and networked home medical devices has increased in recent years. There are several different types of medical devices including consumer grade products like blood pressure monitors, personal fitness tracking, glucose level monitors, wireless weight scales, and wearable devices for monitoring health indicators like Fitbit and Apple Watch. There are also medical grade products called implantable medical devices (IMDs) such as Implantable Cardioverter Defibrillator (ICD) and pacemakers, implantable insulin pumps, and replacement heart implants. A recent report released by Markets and Markets forecasts the global connected medical device market is projected to reach $2.6703 Billion US dollars by 2023 from $763.1 Million US dollars in 2017, at a compound annual growth rate of 23.2% from 2018 to 2023. [8]

With the Affordable Care Act, the HITECH Act, Meaningful Use, and now the Medicare Access and CHIP Reauthorization Act (MACRA), there are now financial incentives for healthcare workers to use health-related information technology (HIT). From healthit.gov:

> The current Centers for Medicare & Medicaid Services (CMS) incentive program that encourages health IT adoption is the Medicare Access and CHIP Reauthorization Act (MACRA), which includes a Quality Payment Program (QPP) with multiple clinician payment tracks. Participation in QPP rewards clinicians' use of certified health IT. [9]

2.3 BLE use in medical devices and sensors

Some of the newest healthcare related systems are wireless devices used in body area networks (BANs) employing Bluetooth Low Energy (BLE). These BLE devices are designed to be low power, efficient and secure for monitoring and wirelessly transmitting vitals such as blood pressure, temperature, and insulin levels. BLE specifically targets the sports and fitness as well as the health and wellness medical industry. [14] BLE offers

prebuilt Health Device Profiles for standardizing communications between BLE health related devices. Some of these prebuilt profiles include:

ECG (heart rate), Blood pressure monitor, Body composition analyzer, Body thermometer, body weight scale, carbon monoxide sensor, cardiovascular fitness and activity monitor, enuresis sensor, fall sensor, gas sensor, glucose meter, independent living activity hub, medication dosing sensor, medication monitor, motion sensor, personal emergency response sensor, and pulse oximeter. [10]

Examples of implantable medical devices include: Implantable cardiac pacemakers, Implantable defibrillators, Implantable nerve stimulators, Bladder stimulators, Diaphragm stimulators, Cochlear implants, Implantable active drug administration devices, Implantable active monitoring devices, Implantable neuro stimulator systems, Implantable infusion pumps, Implantable glucose monitors

One continuous glucose monitor had this to say regarding wireless co-existence and data security:

> The t:slim X2 System is designed to work safely and effectively in the presence of wireless devices typically found at home, work, retail stores, and places of leisure where daily activities occur. See Section 30.11 for more information. The t:slim X2 System is designed to accept BluetoothTM Low Energy (BLE) communication only from a linked Dexcom G5 Mobile Transmitter. BLE communication is not established until you enter the unique Dexcom Transmitter ID into your pump. The t:slim X2 System and system components ensure data security via proprietary means and ensure data integrity using error checking processes, such as cyclic redundancy checks. [11]

Another IMD uses a similar system of an ICD and a "Smart Reader" that uses proprietary communication, then transfers information from the Smart Reader to a smartphone (iPhone or Android) via BLE. This system is called the MyCareLink Smart U.S.

From the website:

> Medtronic makes it easy for heart device patients to stay connected to their doctor. The MyCareLink Smart Monitor for pacemaker patients, including CRT-P, combines a Reader and an app, making this a convenient way to send heart device information remotely to your doctor between clinic visits or whenever you're not feeling well. The app can only be used with a MyCareLink Smart Reader, which is prescribed by the patient's doctor. [12]

Some examples of wearable (Non-implantable) medical devices include:

Fitbit

> Fitbit trackers and watches use Bluetooth Low Energy (BLE) technology to sync with phones, tablets, and certain computers. [13]

Omron blood pressure monitor - this device uses BLE to communicate with a smartphone app to collect and then optionally upload data to other EMR systems.

Smartphones like Apple iPhone use BLE and collect health data. Consider the Apple Health app that collects information such as steps, heart rate, flights of stairs climbed, etc.

Some examples of non-implantable medical devices are some of the many consumer grade devices targeted for sports and health. Two examples taken from the Bluetooth website: [14]

Sports & Fitness

Bluetooth is responsible for enabling wearables like fitness trackers and smart watches that are showing up on wrists everywhere to monitor steps, exercise, activity, and sleep. These devices track fitness levels and athletic performance and use Bluetooth technology to communicate that information in real-time to athletes, coaches, and trainers.

Health & Wellness

Blood glucose monitors, pulse oximeters, asthma inhalers, and other wearable medical devices use Bluetooth technology to help administer medication, diagnose injuries, and transmit critical information securely from patients to providers.

2.4 BLE - general information

Bluetooth is available in two different radio versions: Low Energy (LE) and Basic Rate/Enhanced Data Rate (BR/EDR). Both radio versions operate in the 2.4 GHz ISM band and use frequency hopping spread spectrum (FHSS).

Bluetooth Low Energy (previously known as Bluetooth Smart) is not compatible with Bluetooth Basic Rate (BR) or Bluetooth Enhanced Data Rate (EDR). However, The Bluetooth 4.0 specification allows for devices to implement both LE and BR/EDR systems. Most modern hardware devices and operating systems are Bluetooth dual mode.

In addition to the BR/EDR point-to-point connection method, BLE adds two new network topologies: broadcast and mesh. BLE uses 40 channels (3 advertising and 37 data) with 2 MHz spacing. A BLE device will advertise itself by sending a packet on a minimum of one of the advertising channels at random intervals.

Communication is accomplished with a client-server model through attributes with a Generic Attribute Profile (GATT) that includes unique identifiers for Characteristics, Services, and Descriptors. A characteristic is a data value, a service is a collection of characteristics, and a descriptor is additional information about a characteristic.

In addition to client/server read and write GATT commands, there are server notifications where a characteristic (data value) is sent to a client as it becomes available from the server, and indications which is the same as a notification additionally requiring a client confirmation.

2.5 Healthcare technology security risks

Many consumers and clinicians are eager to adopt and use medical devices and health-related technologies to promote health and wellbeing. However, while technology can help with efficiency and cost issues, there are additional considerations that need to be addressed regarding security and privacy.

Security is defined as a process, not a product, that is used to promote privacy.[15] The three pillars of the security process involved people, processes, and technology. When applying the security process to people, it is training, awareness, and skills that need consideration. Security should also be applied to processes and include management systems, frameworks, best practices, and audits. A technology security process incorporates prevention, detection, monitoring, and response the security threats. It is this technical aspect of security that needs application to medical devices.

Privacy is defined as: non-intrusion into personal space, non-interference with personal decisions, and control over personal information. Personal information is further defined as medical and financial related information and data.

Security is a process and not an end result that is somehow achieved; it is a process that is applied to people, policies, and technology to work towards privacy through confidentiality, integrity and availability. When addressing security and privacy issues in the healthcare field, it is important to understand that in addition to relying on the security of technology to ensure privacy, the potential failure of the security process could result not only in the loss of privacy but could also compromise patient health and safety.

Historically, medical devices and information have been siloed and isolated without the need of interoperability or communication between devices or with a central repository of medical records or information. Medical systems were designed to provide information about the patient or consumer and for patient safety from a medical standpoint (within prescribed limits of medical best practices), not necessarily for cybersecurity - often

lacking methods for monitoring and updating. This is especially true for embedded systems that were traditionally stand alone and not networked. For example, consider modern implantable medical devices like the Implantable Cardioverter Defibrillator that routinely uploads logs to physicians and download new settings and updates. In the past an ICD was a stand-alone embedded device, but today they are sophisticated network connected units that communicate and interoperate with other network devices and technologies.

With this rush for the healthcare industry to adopt technologies, security and privacy issues are often overlooked as new technologies are hurriedly put into place in an attempt to meet the rapid growth and demand on the healthcare system. If security issues are not adequately addressed then there is a possibility of vulnerabilities that can be exploited resulting in risk. Some 94 percent of medical institutions said their organizations have been victims of a cyber-attack, according to the Ponemon Institute.[16]

Moreover, the health sector in 2014 was considered the largest public sector for malicious attack.

Trend Micro's Numaan Huq found that over the past decade, medical organizations make up nearly 30 percent of all observed enterprise hacks Analysis of 10 years of cyber-attack data points to health care as being the industry most breached.[17]. From the report:

> Although retailers have suffered many losses because of data breaches, the most affected industry was actually the healthcare sector, accounting for more than a fourth of all breaches (26.9%) this past decade. The second was the education sector (16.8%) followed by government agencies (15.9%). Retailers only come in fourth place with 12.5%. [17]

2.5.1 High profile cases

There have been several high profile cases involving security issues and medical devices. Take for example the team consisting of researchers from University of Massachusetts at

Amherst and University of Washington in collaboration with Beth Israel Deaconess Hospital and Harvard Medical School that were able to remotely access and disable a cardiac implantable medical device. [18]

Another prominent example of an implantable medical device being hacked is described in the case of a security researcher (and diabetic) hacking his own insulin pump and continuous glucose monitor (CGM) in the paper "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System" [19] The security researchers describes a method for intercepting, decoding, and then changing wireless communications between the Johnson & Johnson insulin pump and the external remote control that would allow for a potentially fatal injection of insulin.

In another example of medical device security issues, a June 2017 report by the Health Care Industry Cybersecurity Task Force, a single piece of legacy technology equipment contained more than 1,400 vulnerabilities. [20]

While the probability of a normal user being unknowingly hacked using the sophisticated methods described in these research papers, it does illustrate that there is a potential issue with the security process on at least some medical devices. It is clear that the use of technology in healthcare is on the rise and that the use of technology includes security and privacy issues that need to be addressed, especially when it pertains to medical devices. The risk of loss of human lives due to security vulnerabilities in medical technology needs to addressed and mitigated.

2.6 Security and privacy in healthcare

Security and privacy in healthcare is important to protect a patient's medical and financial information, but they are especially in healthcare technology that can impact morbidity. Traditionally, security and privacy in healthcare is focused on protecting personally identifiable information or personal health information, rather than addressing a much larger need of promoting the concept of security as a process.

As the name implies, personally identifiable information is any data that can identify a person. Certain information like full name, date of birth, address and biometric data are always considered PII. [21] Personal health information includes anything used in a medical context that can identify patients

HIPAA goes beyond PII security best practices in its requirements for partner organizations. Under the HIPAA privacy rule, health care providers have considerable legal liability for breaches caused by business associates.

There is also a very real threat of PHI being stolen. Medical data is valuable. According to Forbes: [22]

> "On the black market, the going rate for your social security number is 10 cents. Your credit card number is worth 25 cents. But your electronic medical health record (EHR) could be worth hundreds or even thousands of dollars."
>
> “We really need to invest in privacy and security, and also be incredibly transparent with people about what’s being shared with whom, so that they can make the right decisions about what they want to do with their data,” John Moore, medical director at Fitbit (and previously the co-founder and CEO of Twine Health before its recent acquisition), said during the panel.

Side channel attacks use information from a system divulged from the nature of the system rather than a weakness or vulnerability in the system itself. For example: deriving an undisclosed military base from locational data in a fitness app.

Recent months have certainly highlighted data security openings across healthcare, with hospitals and their troves of patient data becoming an increasingly appealing target to hackers.

Consumer fitness and health devices weren’t off the hook either, as Strava’s fitness app was recently shown to not only betray the locations of US military bases and patrol routes, but also allow anyone to de-anonymize user-shared data to reveal names, speeds,

and heart rates. In 2016, Fitbit itself was the target of a cyber attack that collected email address, usernames, and, of note, user GPS data. [23]

With interconnected medical devices and sensors, the concern now includes traditional network security issues include confidentiality, integrity, and availability of data and services. These security issues are detected, prevented, and mitigated with the process of monitoring and response to security threats.

Confientiality of communications and data is achieved through encryption so that the information can only be read be the intended reciever. Integrity of commincations, data and devices assures that no changes have occurred. Resources, data, and devices should also be availabile when requested or needed and resistant to resource depletion.

For example, consider the need for valid data and information from a medical sensor to the accurate diagnoses and treatment of a patient. Without confidentiality that data could be read by a third party and this would violate the principles of privacy. If integrity checks are insufficient then the data could also possibly be intercepted and altered. When demands on device resources such as communication bandwidth are not handled fairly then a rogue device can repeatedly make requests for resources and impact legitimate use.

Neglecting security issues such as confidentiality, integrity and availability has the potential to affect patient morbidity ranging from negligible inconvenience or temporary discomfort to catastrophic resulting in a patient's death. From FDA Postmarket Management of Cybersecurity in Medical Devices: [24]

> Assessing Severity of Patient Harm
>
> Manufacturers should also have a process for assessing the severity of patient harm if the cybersecurity vulnerability were to be exploited. While there are many potentially acceptable approaches for conducting this type of analysis, one such approach may be based on qualitative severity levels as described in

ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application of Risk Management to Medical Devices:

Common Term: Possible Description

Negligible: Inconvenience or temporary discomfort

Minor: Results in temporary injury or impairment not requiring professional medical intervention

Serious: Results in injury or impairment requiring professional medical intervention

Critical: Results in permanent impairment or life-threatening injury

Catastrophic: Results in patient death

3 Problem Statement

There is an increasing need to evaluate the security and privacy of healthcare technology, particularly medical devices and sensors that use BLE. In an ideal world, technology works to make our lives easier and more efficient, and we would not need to be concerned about software bugs, cyber security, system failures, malicious or even unintentional attacks. Communications over both wired and wireless networks would maintain confidentiality, integrity and be available when needed, especially when dealing with personal information and where there is an expectation of privacy.

However, technology develops at a rate faster than our ability to keep up with testing for safety. Coupled with the increase in personal health awareness, healthcare costs, healthcare scope and scale, and the fact that medical information is so distinctly personal information, the security of healthcare-related technology has become an increasingly large target and concern for healthcare workers, security professionals, and everyday people who are the consumers of healthcare-related technology products.

Consider some of the trends in healthcare that show a dramatic increase towards home-based and telemedicine that rely on secure technology for monitoring, data collection and analysis, and medical decision support systems. This increased use of technology has risks not only to financial and medical data, but also directly to a person's welfare, health, and well-being.

Doctors, nurses, clinical staff, healthcare workers are medical experts, not technology experts. Medical professionals already have too much to do, not enough time to do it. Their primary responsibility is to diagnose and treat patients. However, too much of their time is spent dealing with clinical workflow, especially when trying to get data in an electronic health record (EHR) system. This problem is only made worse when medical devices use proprietary software that lacks interoperability and won’t communicate with other systems.

Patients put a considerable amount of trust in physicians and healthcare professionals. Physicians rely on technology to diagnose and treat patients. There is a need to have technology just work and not have to worry about potential privacy issues or spend additional time attempting to mitigate security risks when using technology.

The general public also has a lack of technology and cybersecurity literacy - people do not fully understand the ramifications of technology security or lack thereof. People are willing to accept a loss of privacy in exchange for convenience. This lack of understanding and need for convenience has created a blasé attitude toward security breaches and resulting privacy violations.

From Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices: [25]

> Despite the dangers imposed by cyber-attacks, patients seem to be unaware of their effects as they tend to think about the security of their IMDs as a secondary aspect.

Additionally, patients are often unwilling to implement security procedures for a multitude of reasons including both perceived and actual properties and falls in the realm of Human Computer Interaction (HCI).

From "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," [26]

> "Developing strong technical security defenses is, however, only part of the solution. There is a fundamental gap between developing technical mechanisms that could protect the security of future wireless medical devices if deployed and developing security defenses that will be accepted (even welcomed) by patients, doctors, and other stakeholders."

Not enough attention is given to security and privacy of medical devices and sensors, because it hasn't been needed yet. This is due in part to public misperception and overall publicity of the risks associated with vulnerabilities.

As a comparison, consider automotive safety. By 1965, automobile accidents had become the leading cause of death of Americans under age 44. [27] Yet, there was no public outcry or concern in part due to a lack of visibility. Then automotive safety gained public attention largely because of a book written by (a then unknown lawyer named Ralph Nader) titled: "Unsafe at any speed". [28] Public response to this book was powerful and almost immediate, and by 1966 the Highway Safety Act and the National Traffic and Motor Vehicle Safety Act were passed. Automotive safety had become a national security issue. [29]

Despite so many health-related medical devices and sensors there is little research into the security and safety of these medical technologies that are being so quickly adopted and can so dramatically affect a person's health and safety. Compared to the automotive industry, wearable and implantable medical devices do not receive sufficient testing for security issues.

With the proliferation of medical devices, sensors, and mobile applications we have entered a new area of cybersecurity threats. This new field of "cyber healthcare" and the associated security and privacy issues is more significant to human health, yet the mitigation techniques and solutions are far less researched than the other aspects of healthcare security. Other sectors that have adapoted and integrated technology such as the automotive industry have been recognized as a national safety issue and have standardized. [30]

Currently, the FDA has oversight on medical devices but is not equipped to do extensive testing beyond code review.

The FDA states: [31]

> "Medical device manufacturers and health care facilities should take steps to ensure appropriate safeguards. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance."

However, even if a medical device has software code that is free of defects or bugs, and the device or sensor operates properly, there are very real security concerns that affect security and privacy. Malicious techniques like replay, denial of service, or man in the middle attacks pose a very real threat and warrant more thorough testing.

Due to the fact that BLE uses some of the newest technologies, it is also true that BLE is some of the least tested technology. While the FDA requires unit testing on medical device before approval for use, this testing cannot anticipate new security attacks and methods that are being researched and developed. For example, a recent vulnerability and attack was developed for Bluetooth Classic (called BlueBorne) that gave a malicious entity complete control over a wireless Bluetooth device. [32]

What's been done in the past isn't working in the modern healthcare landscape. Patients and doctors are more technology savvy; historically isolated and embedded systems are now interconnected; everyone is more health conscientious; the cost of healthcare mandates self-managed health solutions, and people are looking toward technology to assist.

As the medical field is using more and more technology, device communication and interoperability is becoming more critical. As this communication and network connectivity is ubiquitous and growing, medical and healthcare technology security and privacy needs to be addressed. We can no longer afford to think of medical devices as isolated and siloed. Health information technology should be viewed holistically and tested as a system, not as individual components.

Other industries, such as automotive, have recently begun to make extensive use of technology and have paid a great deal of attention to security issues and are actively developing and implementing comprehensive testing frameworks. The automotive industry focus on testing is not only advancing the technology itself, it is also promoting sense of priority and security as a required ongoing process.

The increased use of Bluetooth Low Energy medical devices and sensors warrants additional security research and testing. There is an opportunity to be proactive in the security process by establishing a BLE testing lab environment and using existing frameworks and best practices for robust testing of the technology that includes security risk prevention, detection, monitoring, and response.

4 Goals

The goal of this report is to provide a literature review on the current state of security and privacy of medical devices and sensors with Bluetooth Low Energy (BLE).

4.1 General argument

After a review of the available material, the following premises and conclusion are apparent:

- Technology including medical devices and sensors is an integral part of the diagnosis, monitoring, and treatment in healthcare;
- The use of medical devices and sensors in healthcare is growing;
- Bluetooth Low Energy is increasingly being used in medical devices and sensors;
- Security and privacy are important, especially in healthcare technology that can impact morbidity;
- And therefore, there is an increasing need to evaluate the security and privacy of healthcare technology, particularly medical devices and sensors that use BLE.

5 Discussion

There are many security issues with using BLE in medical devices and sensors that could lead to a breach of privacy or even affect patient morbidity.

5.1 BLE use in medical devices and sensors

When medical devices implement a standardized communication method like Bluetooth, there are benefits and risks. The benefits are using an established protocol for exchanging information with other devices that adhere to the same protocol provides compatibility and interoperability. The drawback, however, is that if a vulnerability is found with a method or system that is shared with many devices because of this standardized communication - then all interconnected devices are potentially at risk.

The use of BLE for medical devices and sensor communication is increasing. According to medical device company Orthogonal: "Bluetooth technologies are the most widely used form of medical device connectivity."[33] BLE technologies are designed to work in the medical, healthcare, sports and fitness sector with premade health profiles for use when designing devices.[34] BLE as the name implies also has very low energy consumption (from 1/2 to 1/100th) when compared to Bluetooth BR/EDR, with certain BLE devices lasting 1-2 years on a single 1000mAh battery.[35]

However, despite the publicity and promotion of BLE for medical devices, Bluetooth doesn't work well in implantable devices. This is due to the 2.4GHz frequency range used in Bluetooth, not because of the low power in BLE.[36] From the article:

> Both Bluetooth and Bluetooth Low Energy have limited implantable medical device applications because they use 2.4GHz radio frequency and cannot penetrate well into human tissue.

Additionally, there are potential security issues with the way that BLE devices pair and connect with each other. With BLE there are four modes of authentication that provide

pairing methods and setup BLE connections that are secure. The four modes are: Just Works™, Out of Band (OOB) pairing, Passkey, and Numeric Comparison. However, each of these methods have potential issues that could be exploited.

Just Works™ uses elliptic-curve Diffie-Hellman (ECDH) key exchange providing a secure method of secret key exchange and agreement, but even when using ECDH, there is a possibility of Man in the Middle attacks. From the "Basic Introduction to BLE Security" document [37]

> Just WorksTM:
>
> Once the devices exchange their public keys, the non-initiating device will generate a nonce, which is essentially a random seed value, and then use it to generate a confirmation value Cb. It then sends the Cb along with the nonce to the initiating device. At the same time, the initiating device generates its own nonce and sends it to the non-initiating device. The initiating device then uses the non-initiating device's nonce to generate its own confirmation value Ca which should match Cb. If the confirmation values match, then the connection proceeds.
>
> By virtue of the ECDH key exchange, the Just WorksTM pairing method in LE Secure Connections has substantially more resilience to passive eavesdropping compared to the same method in LE Legacy Connections. However, since this method does not give the user a way to verify the authenticity of the connection, it is still vulnerable to MITM attacks.

Out of band (OOB) pairing is a method whereby the devices do not use Bluetooth at all for pairing, but some other (wireless) connection method for the initial setup and pairing of devices. OOB can provide protection against a potentially malicious third party listening to the pairing process or impersonating a legitimate device to perform a man in the middle (MitM) attack, but only if the (non-Bluetooth) wireless connection is not subject to third-party packet sniffing. [37]

Out of Band (OOB) Pairing:

In OOB pairing, the public keys, nonces and confirmation values are all exchanged via a different wireless technology such as NFC. As in LE Legacy connections, OOB pairing only provides protection from passive eavesdropping and MITM attacks if the OOB channel is secure.

There is also a passkey method where an identical key is manually entered on both devices. The obvious drawback here for medical devices and sensors is the lack of any type of input method or display on the device itself.

Passkey:

In this method, an identical 6 digit number is input into each of the devices. The two devices use this passkey, the public keys they exchanged earlier, and a 128-bit nonce to authenticate the connection. This process is done bit by bit for every bit of the passkey. One device will compute a confirmation value for one bit of the passkey and reveal it to the other device. The other device will then compute its own confirmation value for the first bit of its passkey and reveal it to the first device. This process continues until all the bits of the passkey has been exchanged and verified to match.

Due to the process detailed above, the passkey method for LE Secure Connections is much more resilient to MITM attacks than it is in LE Legacy connections.

Finally, there is the numeric comparison method that uses the same method as Just Works™ but adds an additional confirmation code step at the end for verification. This confirmation code would eliminate a third party posing as a legitimate device, but this method is not well suited for medical devices due to lack of displays.

Numeric Comparison:

> This pairing method follows the exact same procedure as the Just WorksTM pairing method, but adds another step at the end. Once the devices confirm that the confirmation values match, then both devices will independently generate a final 6 digit confirmation value using both of the nonces. They both then display their calculated values to the user. The user then manually checks that both values match and ok's the connection. This extra step allows this pairing method to provide protection from MITM attacks.

Considering all 4 methods for use in medical devices and sensors, there is no ideal choice. OOB paring requires additional wireless communication channels and therefore additional circuitry, power consumption, and expense to the device. Passkey and Numeric comparison methods require user input and output on the device making it impractical for medical equipment. This leaves the Just Works™ method for pairing which is potentially vulnerable to MitM attacks. [37]. From the "A Basic Introduction to BLE Security" document on "Practical Considerations Concerning BLE Pairing Methods:"

> Therefore it is reasonable to assume that most devices will use the passkey method or Just WorksTM, which means that most devices will have some degree of vulnerability. Designers working on products with high-security requirements, such as medical devices, should consider other wireless protocols if OOB pairing or Numeric Comparison cannot be implemented in their designs.

5.1.1 BLE security risks

There are currently many security risks associated with Bluetooth Low Energy. Some of these risks include Man in the Middle (MitM) attacks, replay attacks, and network communication decryption.

Many devices do not properly implement BLE link layer encryption. A recent survey found that 8 of 10 devices did not implement proper BLE encryption.[38][39]

Even with encryption, many BLE devices are still susceptible to Man in the Middle (MitM) attacks where a malicious third party impersonates a legitimate device and can intercept and decrypt BLE network traffic.[40] MitM attacks can include Denial of Service (DoS) attacks making resources unavailable, spoofing data values, capturing data, or even taking control of devices.

There are several software packages available that can be used to perform MitM attacks on BLE, and there are additional tools to scan, capture, process and transmit BLE packets. For this paper, the focus is on open source software packages that can be run on low cost hardware and open source Linux systems.

BLE MitM software tools:

GATTattacker - The tool creates exact copy of attacked device in Bluetooth layer, and then tricks mobile application to interpret its broadcasts and connect to it instead the original device. At the same time, it keeps active connection to the device, and forwards to it the data exchanged with mobile application. In this way, acting as “Man-in-the-Middle,” it is possible to intercept and/or modify the transmitted requests and responses. [41]

BTLEjuice - BtleJuice is a complete framework to perform Man-in-the-Middle attacks on Bluetooth Smart devices (also known as Bluetooth Low Energy). It is composed of: an interception core, an interception proxy, a dedicated web interface, Python and Node.js bindings. BtleJuice is composed of two main components: an interception proxy and a core. These two components are required to run on independent machines in order to operate simultaneously two Bluetooth 4.0+ adapters.[42]

Additional BLE software tools:

hcitool - hcitool is used to configure Bluetooth connections and send some special command to Bluetooth devices. [43]

BLEah - A BLE scanner for "smart" devices hacking based on the bluepy library. [44]

gatttool - Writing and transmitting BLE data and attributes can be accomplished using gatttool. [45]

pygatt - Python wrapper for gatttool.[46]

CrackLE - crackle cracks Bluetooth Smart (BLE) encryption. It exploits a flaw in the pairing mechanism that leaves all communications vulnerable to decryption by passive eavesdroppers.[47]

Wireshark: Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.[48]

BLE hardware tools:

Capturing raw BLE wireless packets for reconnaissance could be accomplished using Wireshark BLE header dissector and an open source hardware BLE device like Ubertooth One.

Ubertooth One: Project Ubertooth is an open source wireless development platform suitable for Bluetooth experimentation. Ubertooth ships with a capable BLE (Bluetooth Smart) sniffer and can sniff some data from Basic Rate (BR) Bluetooth Classic connections.[49]

Devices also need to be have BLE available. A popular USB component to add BLE are USB dongles based on the CSR 8510 chip made by Qualcomm.[50]

5.1.2 BLE security risk mitigation

Medical devices and sensors like most any other technology, have the ability to accept inputs and provide outputs and should have the capability to be monitored and updated

through a communication channel. These are all potential attack vectors that can be vulnerable to exploits and present risks.

The current security testing as outlined in the FDA guidance for medical devices and sensors is not adequate. Medical devices can pass FDA guidelines while still not following the security process of prevention, detection, and constant monitoring and response to threats with updates to prevent issues in the future. This is because the FDA guidance is for code review and checks for bugs in software. This type of review doesn't account for different types of attacks listed below: [51]

Information harvesting - data is collected during network transit.

Tracking the patient - using information such as GPS to monitor a persons movements and identify physical locations.

Impersonation (MitM) - A malicious user places themselves in the middle of communication between two other devices, impersonating a legitimate device then intercepting and redirecting information to the intended device.

Relaying attacks - similar to a MitM attack, a malicious user has access to both the legitimate sender and receiver and can collect information from the sender and relay that information to the receiver at a distance.

Privilege escalation: Hack one hospital device, now have gained a foothold to hack other devices.

Backdoor: hack one controller device to insert a backdoor on every medical device it updates.

Replay attack: where data is captured and replayed with or without modification.

Denial of service (DoS): make the devices unavailable for legitimate use by depleting resources.

Wireless decryption: capturing enough wireless data to detect patterns and decrypt sensitive data.

Many of these type of attacks can be mitigated by properly implementing strong session key exchange encryption and/or using an out of band (OOB) session key exchange where the key is transferred by another (secure) means outside of Bluetooth.

There is additional security auditing that needs to be done on medical devices and sensors. Fortunately, there are cybersecurity frameworks provided by NIST and HITRUST that outlines additional steps to improve the security process.

Recently, three frameworks have been developed to address cybersecurity risks and vulnerabilities: the Food and Drug Administration (FDA) guidance and recommendations, the Health Information Trust Alliance Cybersecurity Framework (HITRUST CSF), and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The FDA and HITRUST frameworks address medical devices and healthcare specifically.

FDA - In December 2016, the FDA released a document that contains the guidance and recommendations for “managing postmarket cybersecurity vulnerabilities for marked and distributed medical devices.” Additionally, there is an FDA guidance for “Radio Frequency Wireless Technology in Medical Devices” issues in August 2013.

HITRUST - HITRUST has developed a healthcare-specific security and privacy framework (the HITRUST CSF). “HITRUST CSF provides organizations with the needed structure relating to information security tailored to the healthcare industry.”

NIST - The NIST Cybersecurity Framework - “This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.”

According to the Health Care Industry Cybersecurity Task Force for the Department of Health and Human Services (HHS) in a June 2017 report to Congress on Improving

Cybersecurity in the Health Care Industry, “Healthcare cybersecurity is in critical condition.”[52]

> “The report makes clear that there are many steps which public and private partners must take to continue this progress. An important first step is to leverage the work HITRUST has done in developing a healthcare-specific security and privacy framework (the HITRUST CSF) and fully support the work the Healthcare and Public Health Sector Coordinating Council (HPH-SCC) has completed (with HITRUST) in developing a healthcare-specific implementation guide of the NIST Framework,” the organization stated.

5.1.3 BLE additional testing

Additionally, a BLE testing environment could be developed using low cost and open source hardware and software.

This testing environment would follow FDA guidance and the NIST and HITRUST cybersecurity frameworks.

While these frameworks provide a very comprehensive overview of cybersecurity and methods to meet compliance requirements, there is still a need to develop standardized security testing (and possibly even certification) for medical devices and sensors. This paper will propose a practical and low-cost BLE experimental setup that fits within the framework, guidance, and recommendations set forth by the FDA , HITRUST and NIST organizations.

6 Conclusions

Technology including medical devices and sensors that use BLE is an integral part of the diagnosis and treatment in healthcare, and the use of medical devices and sensors in healthcare is growing.

Security and privacy are important, especially when dealing with personal information and with healthcare technology that can impact morbidity.

Medical devices and sensors using BLE need improved comprehensive security testing to ensure the security, privacy, health, safety, and well-being of patients. Testing is also needed for the clinical trust and acceptance for use, and to promote interoperability, efficiency and cost savings.

More could be done about the security of BLE medical devices and sensors including more definitive testing on BLE devices, development of a testing environment for evaluating BLE hardware and software with procedures that fit within FDA guidance and also the HITRUST and NIST cybersecurity frameworks.

6.1 Future work

There are many additional areas of BLE security and privacy research that could be explored. Two areas are developing a BLE testing environment lab setup and understanding how BLE security analysis fits into recently developed cybersecurity frameworks and guidance for medical devices.

6.1.1 Testing environment

Future work could include designing and implementing a low-cost testing environment using commercial off the shelf components and open source software to perform security testing and vulnerability assessment on BLE systems.

An example testing environment might include hardware components such as:

Raspberry Pi - The Raspberry Pi is a tiny and affordable computer that you can use to learn programming through fun, practical projects.[53]

Ubertooth One - Project Ubertooth is an open source wireless development platform suitable for Bluetooth experimentation. Ubertooth ships with a capable BLE (Bluetooth Smart) sniffer and can sniff some data from Basic Rate (BR) Bluetooth Classic connections. [49]

There are also many opensource operating systems and software packages designed for security analysis. This software includes:

Kali Linux - an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. [54]

Wireshark. [48]

GATTattacker .[41]

BTLEjuice [42]

Frameworks and guidance

The FDA guidance for managing cybersecurity vulnerabilities in medical devices, the HITRUST and NIST cybersecurity frameworks are complex documents meant to encompass many different scenarios of devices, vulnerabilities, attacks and other situations.

A practical guide could be constructed specifically for testing BLE medical devices and sensors that maps to these frameworks and guidance. This would both promote the proposed testbed and leverage the work already done by HITRUST, NIST and the FDA.

7 References

[1] "Active Implantable | Medical Devices | BSI America - BSI Group." https://www.bsigroup.com/en-US/medical-devices/Technologies/Active-Implantable-Medical-Devices/. Accessed 12 Jul. 2018.

[2] "Global Medical Device Market 2018 with Forecasts to 2023 - Driven by ...." 23 Apr. 2018, https://www.prnewswire.com/news-releases/global-medical-device-market-2018-with-forecasts-to-2023---driven-by-healthcare-expenditure--technological-development--aging-population--chronic-diseases-300634442.html. Accessed 30 Jun. 2018.

[3] "mHealth and Home Monitoring - Berg Insight." http://www.berginsight.com/reportpdf/productsheet/bi-mhealth8-ps.pdf. Accessed 30 Jun. 2018.

[4] "Bluetooth Market Update 2018 | Bluetooth Technology Website." https://www.bluetooth.com/markets/market-report. Accessed 11 Jul. 2018.

[5] "Tractica | MobiHealthNews." https://www.mobihealthnews.com/tag/tractica. Accessed 12 Jul. 2018.

[6] "Activity Tracker Market to Top 87 Million by 2021 with ABI Research ...." 22 Feb. 2016, https://www.abiresearch.com/press/activity-tracker-market-top-87-million-2021-abi-re/. Accessed 12 Jul. 2018.

[7]"The Growing Burden of Chronic Disease in America - Jstor." https://www.jstor.org/stable/20056677. Accessed 12 Jul. 2018.

[8] "Medical Device Connectivity Market 2018 - Global Forecast to 2023." 24 May. 2018, https://globenewswire.com/news-release/2018/05/24/1511322/0/en/Medical-Device-Connectivity-Market-2018-Global-Forecast-to-2023.html. Accessed 12 Jul. 2018.

[9] "Meaningful Use and MACRA | HealthIT.gov." 16 Mar. 2018, https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use-and-macra. Accessed 12 Jul. 2018.

[10] "Health Device Profile | Bluetooth Technology Website." https://www.bluetooth.com/specifications/assigned-numbers/health-device-profile. Accessed 12 Jul. 2018.

[11] "t:slim X2 ™ Insulin Pump w/ Dexcom G6 CGM - Get Started!." https://www.tandemdiabetes.com/products/t-slim-x2-insulin-pump. Accessed 12 Jul. 2018.

[12] "MyCareLink Smart U.S. - Medtronic." http://www.medtronic.com/us-en/mobileapps/patient-caregiver/mycarelink-smart-us.html. Accessed 12 Jul. 2018.

[13] "Fitbit Help - How do Fitbit devices sync their data?." 22 May. 2018, https://help.fitbit.com/articles/en_US/Help_article/1877. Accessed 12 Jul. 2018.

[14] "Connected Device | Bluetooth Technology Website." https://www.bluetooth.com/markets/connected-device. Accessed 12 Jul. 2018.

[15] "Essays: The Process of Security - Schneier on Security." https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html. Accessed 12 Jul. 2018.

[16] "Health Care Cyberthreat Report: Widespread ... - SANS Institute." https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735. Accessed 12 Jul. 2018.

[17] "Follow the Data: Dissecting Data Breaches and ... - Trend Micro." 22 Sep. 2015, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data. Accessed 12 Jul. 2018.

[18] "Defcon: Excuse me while I turn off your pacemaker | VentureBeat." 8 Aug. 2008, https://venturebeat.com/2008/08/08/defcon-excuse-me-while-i-turn-off-your-pacemaker/. Accessed 12 Jul. 2018.

[19] "BH11-Hacking Medical Devices-Radcliffe - Media.blackhat.com…." https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Accessed 12 Jul. 2018.

[20] "Report on Improving Cybersecurity in the Health Care Industry." 2 Jun. 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Accessed 12 Jul. 2018.

[21] "Personally Identifiable Information: HIPAA Best Practices - Virtru." 20 May. 2016, https://www.virtru.com/blog/personally-identifiable-information-hipaa/. Accessed 12 Jul. 2018.

[22] "Your Electronic Medical Records Could Be Worth $1000 To Hackers." 14 Apr. 2017, https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/. Accessed 12 Jul. 2018.

[23] "Fitbit, UnitedHealth, Empatica heads discuss data privacy challenges ...." 10 Apr. 2018, https://www.mobihealthnews.com/content/fitbit-unitedhealth-empatica-heads-discuss-data-privacy-challenges-wearables. Accessed 12 Jul. 2018.

[24] "Postmarket Management of Cybersecurity in Medical Devices - FDA." 28 Dec. 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed 12 Jul. 2018.

[25] "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey ...." https://ieeexplore.ieee.org/document/7393449. Accessed 12 Jul. 2018.

[26] "Patients, Pacemakers, and Implantable Defibrillators: Human Values ...." http://dub.uw.edu/djangosite/media/papers/denning-CHI10-authors-version.pdf. Accessed 12 Jul. 2018.

[27] "National Traffic and Motor Vehicle Safety Act | United States [1966 ...." https://www.britannica.com/topic/National-Traffic-and-Motor-Vehicle-Safety-Act. Accessed 12 Jul. 2018.

[28] "Unsafe at Any Speed - Wikipedia." https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed. Accessed 12 Jul. 2018.

[29] "Understanding the National Highway Traffic Safety Administration ...." 31 Jan. 2017, https://www.transportation.gov/transition/understanding-national-highway-traffic-safety-administration-nhtsa. Accessed 12 Jul. 2018.

[30] Transactions of the National Safety Council, Forty-First Annual Safety Congress, Chicago, IL, 1953.

[31] "Medical Devices - FDA." https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm. Accessed 12 Jul. 2018.

[32] "BlueBorne Information from the Research Team - Armis Labs." https://www.armis.com/blueborne/. Accessed 12 Jul. 2018.

[33] "Bluetooth-Enabled Medical Devices - Orthogonal.io." http://orthogonal.io/articles/developing-bluetooth-enabled-medical-devices/. Accessed 12 Jul. 2018.

[34] "Health Device Profile | Bluetooth Technology Website." https://www.bluetooth.com/specifications/assigned-numbers/health-device-profile. Accessed 12 Jul. 2018.

[35] "The Hitchhikers Guide to iBeacon Hardware: A ... - Aislelabs." 4 May. 2015, https://www.aislelabs.com/reports/beacon-guide/. Accessed 12 Jul. 2018.

[36] "When Is Bluetooth LE Useful in Medical Devices? | MDDI Online." 12 May. 2015, https://www.mddionline.com/when-bluetooth-le-useful-medical-devices. Accessed 12 Jul. 2018.

[37] "A Basic Introduction to BLE Security - Wireless - eewiki." 25 Oct. 2016, https://eewiki.net/display/Wireless/A+Basic+Introduction+to+BLE+Security. Accessed 12 Jul. 2018.

[38] "Hacking challenge: steal a car! - Black Hat." https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf. Accessed 12 Jul. 2018.

[39] "GATTack.io." https://gattack.io/. Accessed 12 Jul. 2018.

[40] "an active man-in-the-middle attack on bluetooth smart ... - WIT Press." https://www.witpress.com/Secure/ejournals/papers/SSE080202f.pdf. Accessed 12 Jul. 2018.

[41] "FAQ · securing/gattacker Wiki · GitHub." https://github.com/securing/gattacker/wiki/FAQ. Accessed 12 Jul. 2018.

[42] "GitHub - DigitalSecurity/btlejuice: BtleJuice Bluetooth Smart (LE) Man ...." https://github.com/DigitalSecurity/btlejuice. Accessed 12 Jul. 2018.

[43] "hcitool - configure Bluetooth connections - Linux Man Pages (1)." https://www.systutorials.com/docs/linux/man/1-hcitool/. Accessed 12 Jul. 2018.

[44] "GitHub - evilsocket/bleah: A BLE scanner for "smart" devices hacking.." https://github.com/evilsocket/bleah. Accessed 12 Jul. 2018.

[45] "Get Started with Bluetooth Low Energy on Linux · Jared Wolff." 14 Apr. 2014, https://www.jaredwolff.com/blog/get-started-with-bluetooth-low-energy/. Accessed 12 Jul. 2018.

[46] "GitHub - peplin/pygatt: Python wrapper for gatttool (from BlueZ) and ...." https://github.com/peplin/pygatt. Accessed 12 Jul. 2018.

[47] "crackle, crack Bluetooth Smart (BLE) encryption." 24 Apr. 2014, https://lacklustre.net/projects/crackle/. Accessed 12 Jul. 2018.

[48] "Wireshark · Go Deep.." https://www.wireshark.org/. Accessed 12 Jul. 2018.

[49] "Project Ubertooth - Home." http://ubertooth.sourceforge.net/. Accessed 12 Jul. 2018.

[50] "CSR8510 | Qualcomm." https://www.qualcomm.com/products/csr8510. Accessed 12 Jul. 2018.

[51] AlTawy, Riham, and Amr M. Youssef. "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices." IEEE Access 4 (2016): 959-979.

[52] "Report on Improving Cybersecurity in the Health Care Industry." 2 Jun. 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Accessed 12 Jul. 2018.

[53] "The Official Raspberry Pi Projects Book." 3 Mar. 2015, https://www.raspberrypi.org/magpi-issues/Projects_Book_v1.pdf. Accessed 12 Jul. 2018.

[54] "Kali Linux." https://www.kali.org/. Accessed 12 Jul. 2018.