AFFECTS OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS ON CONSTRAINED SYSTEM BATTERY LIFE: A DESIGN SCIENCE RESEARCH APPROACH

A Dissertation Presented in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Computer Science

By

Nathaniel Triplett

Colorado Technical University

June 2020

Approved by Doctoral Committee:

DocuSigned by:
5E9F70D213D8447...

6/23/2020

Dissertation Chair

Date

DocuSigned by:
Kelly Hughes
A1CE3AB4D72F49A...

6/24/2020

Committee Member

Date

DocuSigned by:
Steven Munkeby
A58B2E80940D440...

6/24/2020

Committee Member

Date

Abstract

Malicious attacks against healthcare providers has become a big business. This is because healthcare information remains viable longer than credit card information and cannot be replaced or reset, like getting a new credit card. Not all medical devices can be protected with an anti-virus or anti-malware program or hide behind a firewall. Implanted and wearable medical device have proprietary operating systems and are classified as constrained systems that make them a challenge for cybersecurity professionals to protect. This design science research examines the feasibility of adding a cryptographic algorithm to an implantable medical device to protect communications between the device and its monitoring station, where one did not previously exist, and the effect on the battery life due to the addition of the new algorithm. The population for this study includes lightweight cryptographic algorithms designed to secure communications between devices. The sample includes four lightweight block ciphers and one lightweight stream cipher that were purposefully selected to ensure diversity across the population. A standard block cipher is also included for representation. The input data were collected from various sources on the Internet and through an interview with the reference device manufacturer. These data were processed through a series of calculations that use an algorithm's gate equivalence measure and the circuit's power per NAND gate shift to determine the additional power consumption attribution for each algorithm in the study. This result is then factored into the power consumption rate prior to the algorithm to calculate the new battery life.

Keywords: …NAND gate, gate equivalent, constrained system, cryptography, lightweight algorithm, power consumption, medical device

Dedication

This dissertation is dedicated to Dr. James R. and Mrs. Christine L. Triplett, Dr. Evelyn Triplett, Dr. Robert F. Triplett, and Dr. Kellie M. Triplett whose legacy I continue, and to my wife, Stephanie, for supporting throughout this journey.

Acknowledgements

I would like to thank the staff and faculty at Colorado Technical University for their guidance and expertise.

Table of Contents

List of Tables

List of Figures

CHAPTER ONE

Cybersecurity is a topic of discussion everywhere. Applying cybersecurity controls to a computerized device such as a computer, tablet, smartphone, or smartwatch provides the benefit of protecting the confidentiality, integrity, and availability of data (Harris & Maymí, 2018). The application of cybersecurity controls is accomplished by closing attack vectors, filtering and integrity checking communications, and monitoring for anomalous behavior. In some instances, authorized data is blocked. In most scenarios, this is not a problem; however, if the device in question is a medical device, interrupted data or a faulty command could lead to a medical emergency. One attack surface that requires a proactive solution is medically implanted and medical wearable devices.

Secure communications between two devices come at a technical cost: power (Almenares, Arias, Marin, Diaz-Sanchez, & Sanchez, 2013). For constrained systems, this technical cost will affect a device's longevity (Batina et al., 2013). For many constrained systems, power usage is not a significant concern as batteries can be recharged or replaced by the user. Implanted medical devices cannot be recharged or have their batteries replaced by the end-user. These constrained systems require surgery to replace when the battery is depleted. Finding a lightweight cryptographic solution could solve the problem of excessive power consumption. This study looked at existing lightweight cryptographic algorithms to identify the technical cost associated with each and whether there is a viable solution.

This chapter starts with a background on the need for research into low power consumption cryptographic algorithms that can be applied to constrained systems. Next, a summary of the conceptual framework, problem statement, research question, and hypothesis are presented to illustrate the gap in current research and how this study fulfills the needs identified.

A list of terms used in this study is presented along with delimitations, limitations, assumptions, and biases to close out the chapter.

Topic Overview/Background

Unsecure communications between devices is an attack vector that malicious actors frequently exploit through man-in-the-middle, replay, and similar attacks (Harris & Maymí, 2018). For most computer systems, intercepting unsecured communications is not a difficult task (Wu & Eagles, 2016). The application of cryptographic algorithms protect the confidentiality and integrity of data as well as provide nonrepudiation (Harris & Maymí, 2018). These algorithms come with a technical cost through power consumption and processing power (Almenares et al., 2013). For constrained systems, this technical cost can be prohibitive (Almenares et al., 2013). Medical wearables and implanted devices fall into this category.

Previous research has briefly addressed lightweight cryptographic algorithms without addressing medical device communications. Analysis has been performed on sensor networks (Al Ameen, Liu, & Kwak, 2012; Choi, Kim, & Chae, 2013; Landsiedel, Wehrle, & Gotz, 2005), smartphones, and Internet of Things devices (Potlapally, Ravi, Raghunathan, & Jha, 2003), which are not classified as constrained systems. Radio-frequency identification (RFID) tags have been studied for secure communications. Radio-frequency identification tags are classified as constrained systems that scavenger power from their environment (Arbit, Livne, Oren, & Wool, 2015; Lohmann, Schneider, & Ruland, 2006; Manjulata, 2014). Radio-frequency identification tags are not within the delimitations of this study. Studies have also looked at the use of lightweight cryptographic algorithms and their power consumption outside of the medical industry (Potlapally et al., 2003; Prasithsangaree & Krishnamurthy, 2003).

Securing communications of medical devices is necessary to protect the patient and the patient’s information. Interception of these communications can lead to the disclosure of personal health information (PHI). As well, unsecure communications can lead to malicious commands sent to a device, causing it to malfunction. In this study, the researcher looks at the viability of securing these communications.

Problem Statement

The problem addressed in this study is the lack of secure communications between medical implanted and medical wearable devices and their base stations (Freedman, 2015; Higgins, 2015; Newman, 2018). Lightweight cryptographic algorithms exist that may provide a solution. While studies have looked at lightweight cryptographic algorithms and their power consumption, these studies do not look at constrained medical devices with a limited power reserve. This lack of research on the effects of power consumption by lightweight cryptographic algorithms demonstrates a gap in the current body of knowledge. The effects on and extent of power consumption by lightweight cryptographic algorithms were examined to determine the feasibility of their application to constrained medical devices.

Purpose Statement

The purpose of this design science research was to examine the extent of power consumption of lightweight cryptographic algorithms and the effect on constrained medical device longevity through an experimental process. Five lightweight cryptographic algorithms have been included in the study that was purposefully selected based on encryption method, block size, key length, and round count. These five algorithms provide a representative sample of the available variations in lightweight cryptography. The variables will include the independent variable gate equivalent and the dependent variable of power consumption.

Research Question

Advances in microcomputers and smart device technology have introduced a security problem (Bazzoli, 2016). This security problem puts user data at risk of loss of integrity and confidentiality. To address this problem and mitigate the risk of data integrity and confidentiality loss, communications between these devices and other devices should be encrypted (Harris & Maymí, 2018). The addition of encryption to a system will cause a subsequent increase in power consumption (Ferrigno, Marano, Paciello, & Pietrosanto, 2005). Because constrained systems have limited power reserves, the addition of encryption will shorten overall battery life. The question is, how much power consumption can be attributed to a lightweight cryptographic algorithm in a constrained device? How much will the battery life be shorted by the introduction of a lightweight encryption algorithm?

Hypotheses

Multiple variables directly affect the power consumption of microcontrollers based on the cryptographic algorithms that could be applied (Batina et al., 2013). This researcher compared both traditional and new, lightweight algorithms to find a viable option for encrypting communications without critically affecting battery life or affecting the reliability of the devices used in the study.

$H1_0$: Lightweight cryptographic algorithms will not reduce the constrained system's battery life to an unacceptable level.

$H1_A$: Lightweight cryptographic algorithms will reduce the constrained system's battery life to an unacceptable level.

$H2_0$: Lightweight algorithms consume power to the extent that will not adversely affect device battery-life of a constrained device, similar to traditional cryptographic algorithms.

$H2_A$: Lightweight algorithms consume power to the extent that will adversely affect device battery-life of a constrained device, similar to traditional cryptographic algorithms.

Conceptual Framework

To thoroughly examine the concept of securing the communications between constrained medical devices and base stations or monitoring devices, it is necessary to look at the factors that make up the conceptual framework. Medical devices provide a challenge to security professionals due to the restrictions that manufacturers face in getting them certified through the United States Food and Drug Agency (FDA; FDA, 2016a). These challenges include proving that new capabilities or features will not adversely affect the patient. New and modified device designs are required to go through extensive testing to ensure patient safety (Ciurana, 2014). Vulnerabilities in medical devices and potential attack vectors include communications, firmware, and data interception (Bazzoli, 2016). Cryptographic algorithms can be utilized to secure communications (Harris & Maymí, 2018). Cryptographic algorithms increase power requirements in computer systems (Batina et al., 2013). Constrained systems such as medical devices can be adversely affected by excessive power consumption. This framework illustrates the bounds of this study to include medical devices, cryptographic algorithms, and the effect of power consumption on the constrained system. Current research addresses individual aspects of this framework but fails to put the pieces together.

Assumptions/Biases

Study assumptions are those facts that are believed without validation (Hathaway, 1995). One such assumption is the population sample chosen accurately represents the overall population and is the best fit for the study. Extensive research has led to the creation of a list of algorithms that are viable candidates for securing communications with minimal power consumption; however, other algorithms may also be suited for this task. A second assumption is the equation selected will accurately demonstrate power consumption of the algorithms chosen for the hardware platform chosen. While equations exist to predict power consumption in electrical circuits (Alioto & Palumbo, 2002; Landsiedel et al., 2005; Lohmann et al., 2006), different circuit architectures require different equations to account for the transistor design and power leakage.

Biases in research exist when the researcher introduces or excludes evidence to follow a single line of thought that proves a theory while not including contradictory evidence (Pannucci & Wilkins, 2011). Bias in research reduces the validity of the study by not presenting all evidence or only the part of the evidence that supports the hypothesis. Through this research, the topic of the feasibility of cryptographic algorithms for constrained systems was examined. The feasibility of one encryption method over another is not analyzed in this research, only the power consumption of the selected algorithms compared to the reference device model. The researcher does not have a stake in either medical device manufacturing or algorithm creation.

Significance of the Study

The feasibility of applying lightweight cryptographic algorithms to constrained medical devices to secure communications between them and the base station or medical terminal used by healthcare providers was examined in this study. Journal articles have mentioned the need without providing a definitive solution. This study will benefit medical device manufacturers, healthcare providers, and patients. Securing these communications will protect patient health information and mitigate a possible attack vector.

Delimitations

Delimitations are boundaries set by the researcher (Simon, 2011). These boundaries include input data, population sample, or limiting the research procedure. Delimitations are necessary to bound or focus the research on a specific location, age range, or timeframe. The delimitations of this study included existing lightweight cryptographic algorithms that were purposefully selected for this study, utilizing mathematical equations, and limiting the comparative analysis to one platform. Additional lightweight algorithms exist that meet the delimitations of this study, but will not be included, as they will not add value to the outcome of the research.

Limitations

Limitations in research are those variables that the researcher has little to no control over (Simon, 2011). The limitations for this research included the availability of data for the lightweight cryptographic algorithms that were analyzed, the use of a mathematical equation vice utilizing electrical measurement devices, and utilizing publicly available device specifications.

Definition of Terms

Several terms were included in this study that may not be familiar to the reader and are explained below.

Constrained device. A constrained device is one that has limitations placed on it by its architecture or environment (Tawalbeh, Hashish, Tawalbeh, & Aldairi, 2017).

Cryptographic algorithm. Cryptographic algorithms are algorithms used for the encryption and decryption of data (Shah & Engineer, 2019).

Gate equivalent. A gate equivalent is the size of the silicone required for an algorithm to perform its function (Rolfes, Poschmann, Leander, & Paar, 2008a).

Internet of Things (IoT). The Internet of Things is all devices that are interconnected on the Internet for communication to perform specific tasks (Tawalbeh et al., 2017).

Radio Frequency Identification (RFID) tags. RFID tags are low power devices that are typically externally powered and authenticate a device or user through a chip that is registered to that device or user (Rushanan, Rubin, Kune, & Swanson, 2014).

General Overview of the Research Design

The research design utilized consisted of a design science approach that calculates the power consumption attributed to an algorithm based on gate equivalence for the algorithm. Each algorithm's gate equivalent was collected from previously published sources. The power consumption calculations took into consideration the transmission packet size and the frequency of transmissions. This additional power consumption was then applied to a reference platform to determine the effects on device power reserve longevity.

Summary of Chapter One

This introduction presented the problem that medical device communications are not secure and the hypothesis that existing cryptographic algorithms can secure these transmissions. Research biases and assumptions have been discussed, and every attempt to mitigate them was performed. Both the research boundaries controlled by the researcher (delimitations) and those not regulated by the researcher (limitations) were discussed that may affect the outcome of the research.

Organization of the Dissertation

This dissertation was separated into six chapters. Chapter 1 of this dissertation introduced the problem of unsecured communications between medical devices and their monitoring stations. Chapter 2 provides a discussion on the previous works around medical device vulnerabilities, challenges faced in securing constrained systems, research performed for securing non-medical devices throughout the Internet of Things, and methodologies for assessing algorithm power consumption. Chapter 3 discusses the research traditions and methods used for this research. As well, Chapter 3 presents the population, the sampling methods, and the analysis that were performed on the sample to identify the effects on power consumption by these algorithms. Chapter 4 includes details of the cryptographic algorithms and the reference platform that was used in the study. In addition, Chapter 4 contains the instrument that was used to take the input of the algorithms and the reference platform to generate the output of power consumption and, ultimately, the new platform battery life with the algorithms applied. Chapter 5 demonstrates the application of the cryptographic algorithms to the reference platform utilizing the instrument presented in Chapter 4. The findings from this design science research are also discussed. Limitations, interpretations, practice implications, and recommendations for future research are presented in Chapter 6.

CHAPTER TWO

Cybersecurity has been in the mass media and the forefront of many corporate executives' minds. One of the industries that have seen the largest impact is the healthcare industry (Angle, 2016; Fu & Blum, 2013; Grau, 2014). Vulnerabilities in workstations, servers, and network equipment are all covered by the standard myriad of patching routines and protective software (Harris & Maymí, 2018). The introduction of interconnected medical devices and other personal electronic devices poses a specific threat since they do not accept the standard anti-virus or intrusion detection software due to constrained resources or proprietary operating systems (Almenares et al., 2013). For this reason, this research will look at the feasibility of adding lightweight cryptographic algorithms to constrained devices such as medical implanted and wearable devices to protect the patient and the patient's information from a malicious actor. This chapter includes how these devices are unique, what challenges are posed to protect them, what vulnerabilities have been discovered and exploited, and what related work exists toward securing these devices.

This chapter starts with the explanation of constrained systems and what sets them apart from other Internet of Things (IoT) devices. Next, an explanation of the risks and compromises that illustrate the importance of establishing cybersecurity controls for these devices. Next is a discussion of previous works that relate to securing constrained devices. This discussion includes different wireless protocols and monitoring techniques that provide limited security to the device. The next section looks at lightweight cryptographic algorithms and what sets them apart from other cryptographic algorithms. Next is an explanation for the assessment of power consumption. Lastly, a brief discussion on the social effects of applying cybersecurity to a medical device and its challenges is presented. This latter section is beyond the scope of this dissertation but should be considered as criteria when planning a modification to a medical device.

Medical Devices and Constrained Systems

As technology has advanced, so has the desire to miniaturize devices for a multitude of uses. Industrial control systems (ICS) is a broad category of automated devices that take input variables and perform a function (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Types of ICS are supervisory control and data acquisition (SCADA) devices and programmable logic controllers (PLC). Medical devices, handheld tools, and SCADA devices, as well as cellular phones and computers, have led to the adoption of a phenomenon known as the Internet of Things (IoT; Suresh, Daniel, V.Parthasarathy, & Aswathy, 2014). The IoT has spread to a wide variety of smart devices from those listed above to refrigerators, home or business security systems, baby monitors, medical equipment, and even vehicles.

As technology has advanced, so has the desire by certain actors to alter the function or behavior of these devices in a way they were not intended to function. The process of changing devices to function in a way other than their design is known as hacking (FDA, 2016b). Ethical hacking, as used by researchers, allows for the identification of possible vulnerabilities or alternate uses for outdated equipment (TrapX_Labs, 2015). Malicious actors, on the other hand, hack devices to cause a device to malfunction to disrupt its ability to perform its intended function or leverage it to return data that would otherwise not be available.

The security of these devices to prevent tampering has always been a challenge to manufacturers. In many instances, the risk is low enough that security features were not justified. In other cases, there is a risk. The cost or feasibility for implementing security out weighted the risk (Angle, 2016). To understand how to reach these conclusions, the security practitioner must identify critical systems and the impact due to the disruption or destruction of the assets identified. As well, the practitioner must look at the threat, risk, and vulnerability to classify the attack vector (Angle, 2016; Fu & Blum, 2013). Third, the security practitioner must identify possible mitigations for the risk. These risks are all weighed to ascertain if they should be mitigated or not (Angle, 2016). Cost, practicality, impact, probability, and frequency are also factors that must be included when identifying risk mitigation actions (Angle, 2016; Fu & Blum, 2013).

Another challenge is the practicality of implementing security for miniaturized devices. Industrial control system devices come in a variety of shapes and sizes. Industrial Control System devices are used to sense an environmental or system input and perform an action such as opening and closing a valve based on the programmed logic within the device (Nicholson et al., 2012). Industrial control system devices exist in heating and air conditioning systems (HVAC), irrigation systems, and power plants. Supervisory control and data acquisition devices add the ability to report back the input and output variables to a control station. Some medical devices perform in similar ways. Implanted cardioverter defibrillators (ICD) monitor a patient's heart rhythms and provide a shock if the heart rhythm becomes irregular (Ransford et al., 2017). As well, ICDs can record the heart rhythms and shock events for a healthcare professional to download and analyze later.

Many of these devices can be classified as constrained devices or systems. Constrained devices are those that have a limitation that is difficult to or cannot be overcome. Examples of these limits are battery power, where device longevity is limited by battery storage capacity, processing power limits such as those found in miniaturized wearables, or memory or data storage limits based on the design (Igure, Laughter, Williams, & Brown, 2006). Design, practicality, and purpose drive most of these limitations. In the case of wearable and implanted medical devices, the limitation is due to the need for a compact device to prevent patient discomfort.

Medical devices have a unique challenge that other ICS and micro-computers do not: they are subject to rigorous certification by the U.S. Food and Drug Administration (FDA; (FDA, 2016c). This certification process has been bolstered by the requirement for cybersecurity and the protection of patients from malicious actors.(FDA, 2016b). However, one area of the market that has been lacking is the post-market support of these medical devices due to several fundamental challenges in the process (FDA, 2016a; Kramer et al., 2012). First is the fact that the modification of any device from its originally configured and tested form requires it to go through a retest procedure that can be lengthy and costly (Williams & Woodward, 2015; Wu & Eagles, 2016). The manufacturer must prove that the changes to the device will not impact the patient's life (Ciurana, 2014). Another challenge is that by the time many of these devices reach a point where they require an update or security fix, they will have reached their end of usable service. Reaching this point in the product's life means that manufacturers have less incentive to maintain in-use devices and opt for updating those that are still in the supply chain. For this reason, the FDA authored and published a guideline for medical device manufacturers that recommend the incorporation of cybersecurity measures to protect these devices from malicious actors (FDA, 2016c).

Timelines are another area where medical device manufacturers face challenges. Implanted cardioverter defibrillators and other medical devices can take a year or more to design, test, certify, and deliver to the market while cybersecurity vulnerability detection locates them in the wild monthly, weekly, or even daily (Fu & Blum, 2013; Williams & Woodward, 2015). Neglecting to update a device post-sale leads to a device that may start secure but become vulnerable at some point in the development lifecycle. As well, an area that is currently failing the industry is the fact that the FDA database that tracks reported medical device flaws does not accurately monitor for cyber vulnerabilities or device malfunctions due to cyber actions (Fu & Blum, 2013; Kramer et al., 2012). Stale or inaccurate databases lead to misrepresentation of the security and safety of these medical devices to the public and healthcare providers. Cybersecurity needs not only to be included in the development of these medical devices but also updated regularly during the production cycle and the post-market lifespan of the product (FDA, 2016a, 2016c).

This section has illustrated how constrained devices differ from other devices in their construction. As well, the Federal requirements for the manufacturing and approval of a medical device were discussed to show that changes in these devices are not a trivial process. The security of these devices has been and remains a challenge within the medical industry due to their nature and design (FDA, 2016c; Fu & Blum, 2013; Medina, 2013). The next section will discuss risks and compromises to the medical industry and medical implanted and wearable devices.

Medical Device Compromises and Risk Management

The mainstream media frequently reports on compromises to medical systems when they happen. However, research in the same field has seen lesser notoriety. For example, in 2015 a group of researchers examined some standard hospital equipment, such as blood gas analyzers (BGA) and picture archiving and communications systems (PACS), and where able to identify malware that was part of an advanced persistent threat (APT) campaign to gather and exfiltrate medical records (TrapX_Labs, 2015). Malware such as Zeus, Citadel, and Conficker existed on hospital medical devices (Higgins, 2015; Leavitt, 2010). Former Vice-President Dick Cheney found validity in the threat to his ICD while in office and directed his doctor to disable the wireless functionality to prevent possible blackmail or hijacking of the device (Deloitte, 2013; Kloffler & Shaw, 2013; Padmanabhan, 2017).

The realization is that the threats are real even if they have not been acted upon (FDA, 2016b). The reason for this is that many of the medical devices and their corresponding monitoring stations' designs and specifications are freely available on the Internet for hackers and malicious actors to access (Freedman, 2015). As well, due to the design of these devices, they cannot be protected by a firewall or anti-virus/anti-malware software (Grau, 2014). In recent years more considerable emphasis has been put on the insider threat (Verizon, 2019). This concept follows that an authorized user will knowingly or not cause an event that will lead to the compromise of information. Unfortunately, an article published in the Health Data Management journal explained that even after the Health and Human Services Office that enforces HIPAA, there were healthcare providers that failed to take action and adequately secure their internal networks from internal and external cyber threats (Goedert, 2016). Without fully understanding and acknowledging the requirements for the protection of these data, these groups are putting patients and their personal information at risk.

In addition to the U.S. FDA guidelines and recommendations, there is a concern from other groups that focus on cybersecurity. The MITRE Corporation is one such company that looks at improving public and private sector safety and security through extensive analysis and industry best practices. The MITRE Corporation also works directly with the National Institute of Standards and Technology (NIST) when it comes to publishing potential cybersecurity vulnerabilities in the National Vulnerability Database (NVD). Two such contributions relate to vulnerabilities in Medtronic's implanted medical devices that were identified by the FDA and MITRE (FDA, 2019)—assigned a Common Vulnerability Enumeration (CVE) numbers 2019-

6538 and 2019-6540 these two vulnerabilities related to the use of the Conexus telemetry protocol used between the Medtronic device and its monitoring station (FDA, 2016b; MITRE, 2019a, 2019b). These vulnerabilities deal with the lack of encryption use and the possibility that sensitive information could be compromised.

Implantable Cardiac Pacemakers (ICP) are like ICDs, with the exception that they are continually maintaining the heart's rhythm. One such device manufactured by Abbott (formerly St. Jude Medical) had a firmware vulnerability in 2017 that warranted a safety bulletin from the FDA to correct the cybersecurity vulnerability (FDA, 2017). The bulletin stated that while the risk extended to the compromise of patient data and possible tampering of the device, the risk was low, and performing the update could carry more risk than not installing the update.

Another instance is the typical insulin pump that so many diabetics rely on for proper blood sugar levels. According to a study in the Journal of Diabetes Science and Technology (Paul, Kohno, & Klonoff, 2011) identified that insulin pump infusion systems are prone to interference as well as intentional and unintentional communications. The authors also touch on the resource constraint aspect; however, mention that insulin pumps are external to the body and can use rechargeable batteries where internal devices cannot. The authors recommend a monitoring methodology to cybersecurity risks, which is a transference of risk and not a mitigation of the risk.

In a recent journal article in Health Data Management, author Fred Bazzoli (2016) brought to light a problem with the Johnson & Johnson OneTouch Ping infusion pump. However, when confronted, Johnson & Johnson downplayed the vulnerability and stated that the risk was low. However, despite this statement, Johnson & Johnson later provided users and healthcare providers with guidance on how to mitigate the risk until a solution could be implemented (Bazzoli, 2016). In this case, the vulnerability allowed a malicious actor to reprogram the device leading to an unsafe condition for the patient.

The analysis of security and privacy in both SCADA devices and implanted medical devices (IMD) show that vulnerabilities exist. One such article published by Camara, Peris-Lopez, and Tapiador in the *Journal of Biomedical Informatics* looked at the six security properties as they relate to medical devices and how they are threatened (Camara, Peris-Lopez, & E.Tapiador, 2015). The standard confidentiality, integrity, and availability are included, along with authentication, authorization, and non-repudiation. These same findings were related to SCADA devices and networks (Igure et al., 2006). This slightly older article expressed that protocol vulnerabilities were a top-three concern for SCADA networks and created a design challenge. Likewise, Alan Grau published an article in *Electronic Component News* (ECN) that listed a series of possible embedded security controls that would enhance the security of medical devices to include secure firmware, embedded firewalls, event auditing, and reporting, and secure booting (Grau, 2015). Most implanted and wearable devices cannot support this level of technology due to limited resources.

This section illustrated the threats that currently exist for SCADA and medical devices. As well, examples of the real world and perceived threats presented were from the US FDA, MITRE, and medical journals. Abbott, Medtronic, and Johnson & Johnson have all been alerted to vulnerabilities in their medical products (FDA, 2017, 2019). These alerts have led to post-market updates (FDA, 2016a). These post-market updates are reactive, not proactive.

Previous Works Related to Constrained System Security

Several researchers have examined security within constrained systems. In 2017, a group of researchers published an article in the Journal of *Information Assurance and Security* that looked at security within wireless sensor networks (WSN, Tawalbeh et al., 2017). These researchers acknowledged that security came with an operational cost due to the impact on power consumption and restrictions on the computing capacity. The relationship between the triad of security, cost, and performance showed that the balance is difficult to achieve in WSNs. For example, to keep the cost down and performance up, security would suffer. Likewise, to have performance and security, the cost of the product or the cost as it relates to electrical and computing power would adversely affect the device. The representation of this relationship can be expressed in an equation.

$$P * S = C \tag{1}$$

For this logical equation, *P* is power, *S* is security, and *C* is cost.

The researchers presented eight different lightweight algorithms along with their gate equivalents to demonstrate that not all cryptographic algorithms are created equal. Related work also addresses the performance, security, and cost triad (Shah & Engineer, 2019).

Another aspect of constrained systems that researchers have focused on is the current or lack of security measures. The implementation of security happens in one of two basic methods: designed in and bolted on. Bolted on security, as any other bolted on accessory, is never as strong as built-in security (Crain & Bratus, 2015). Bolt-on security is not designed for the specific program or application that it is attached to but instead created to work with a wide range of products (Crain & Bratus, 2015).

Other articles look at power consumption in constrained systems based on the communication method used. Researchers out of the Microsoft Research center in Cambridge looked at Bluetooth Low Energy (BLE), ZigBee, and Adaptive Network Topology (ANT) protocols (Dementyev, Hodges, Taylor, & Smith, 2013). When looking at constrained systems, an important aspect is the power consumption of the protocol used. Adding cryptography to the payload will increase the overall payload size and, subsequently, the power consumption per transmission. As well, an article in the International Journal of Distributed Sensor Networks performed a comparison between ZigBee and ZigBee Pro (Choi et al., 2013). In addition to looking at power consumption, one must examine the effectiveness and security of the protocol. Choosing a protocol that has known weaknesses defeats the purpose of implementing cryptography to protect the communication channel. Protocol selection influences power consumption and should be a deciding factor.

In addition to the protocols of wireless communication, it is necessary to take into consideration the power consumption based on signal strength, transmission distance, and frequency. A study performed in 2012 looked at these factors to find a solution to poor battery life in cell phones (Feng et al., 2012). The results of this study may have come across as rudimentary, but the researchers found that lower signal strength, shorter transmission distances, and cross-layer optimization of the transmission path allowed for lower power consumption (Feng et al., 2012). Although this study was limited to the cellular phone networks that crisscross our nation, they strengthen the foundation for proper product design.

Area type networks come in varying sizes based on the distance required for transmission and the transmission medium. Body Area Networks (BAN) are wireless networks with a distribution limited to the range necessary to reach all areas of the human body (Berhanu, Abie, & Hamdi, 2013; Rushanan et al., 2014). The typical use for a BAN is as a healthcare monitor or fitness tracker since the sensor and the monitor are both worn on the person. This type of network has a limited distance but also a limited set of protections. Despite the limited range of transmission of these networks, they are still vulnerable to attack if communications are not properly protected (Denning et al., 2010). Communication distance in BANs is primarily limited by the transmission distance and not the reception distance. The receiver will pick up anything that can reach the antenna. This arrangement provides a sense of security to the wearer since the transmissions containing personal or health-related data cannot transmit beyond the immediate area of the human body. Al Ameen et al. (2012) discussed that regardless of the limitations posed on the transmission power, its presence makes it vulnerable to eavesdropping attacks. If the transmission payload contains control commands for the medical device, a malicious actor could alter the transmission and replay to the controlled device leading to health problems for the patient.

Several medical device manufacturers and researchers have proposed possible solutions that look at alternate means of securing the medical device. For example, one group looked at using a biometric fingerprint, not a literal fingerprint, based on the patient's EKG or similar metric at the time of the communication as the key or signature that would be factored into the communication stream (Ali, Sivaraman, Ostry, & Jha, 2013; Vishnupriya & Vareed, 2018; Zheng, Fang, Shankaran, & Orgun, 2015). An article published in The Journal of Medical Systems proposed using an anonymous authentication system for securing wireless BANs (WBAN) that was superior in the fact that it addressed the threat of a replay attack (Wu, Zhang, Li, & Shen, 2016). Another group proposed using a biometric hash to secure the transmission (Amin, Islam, Biswas, Khan, & Li, 2015). However, in the latter article, the authors discussed the inherent challenge that this presents due to possible noise or anomalies in the biometric capture. This anomaly represents a unique finding that while the biometric may be consistent in the patient, the point at which sampling occurs could lead to discrepancies. As well, neither of these mechanisms address the adverse effects on power consumption due to the introduction of a cryptographic algorithm on a constrained system.

Monitoring the communications to and from a wearable medical device is another solution. A project called MedMon (short for Medical Monitor) was taken on by a group of researchers from Purdue University and Princeton University (Monaco, 2012; Zhang, Raghunathan, & Jha, 2013). The premise is to monitor the transmissions and warn the user if tampering is detected. The inherent problem is while there is a notification to the patient of the potentially malicious activity; they cannot act to prevent possible harm to themselves. Nor will the notification prevent the hacking of the information or unauthorized access to the device.

With the complications that accompany the manufacturing of medical devices, several groups have proposed integrating security into the design and overall product development lifecycle. The Medical Device Product Development Lifecycle, as explained by Jones and Katzis(2017), consists of five main phases. The first two phases lump the product develop, validate, design, bench test, and redesign together in a cyclic pattern until the device meets the requirements for both safety and healthcare needs. The Medical Device Development (MDD) model goes into further detail with regards to including Federal regulations in the product lifecycle (Medina, 2013).

Research for the securing of constrained systems and devices present several solutions. This section has looked at research into the use of Body Area Network (BAN), Wireless BAN (WBAN), and Wireless Sensor Networks (WSN) protocols for communications with the addition of biometric keys or limited transmission power. As well, protocols such as ZigBee, Bluetooth Low Energy (BLE), and ANT have been researched, looking at their inherent security protocols. As well, off-device monitoring has been researched and implemented, providing the patient with only notification of a problem without resolution. These solutions lack a proactive security stance that patients deserve.

Lightweight Cryptographic Algorithms

One of the challenges that have faced cybersecurity professionals and medical device manufacturers is the use of cryptographic algorithms for securing communications or data without affecting the patient. As previously discussed, one of the challenges to constrained systems and devices is limited power reserves. Adding a cryptographic algorithm to a device translates into more computational cycles, which translate to more power consumed by the system (Batina et al., 2013). Lightweight cryptographic algorithms could ease this burden (Batina et al., 2013).

Cryptographic algorithms fall into one of two categories: stream ciphers and block ciphers. Stream ciphers are those that generate an encryption keystream that consists of a constant stream of characters for encrypting the plaintext (Armknecht & Mikhalev, 2015). Stream ciphers use a starting value referred to as a seed and create a keystream that is used to encrypt one bit at a time until the entire plaintext is encrypted. Although stream ciphers process plaintext quickly, they require a large area in memory to complete this process. The National Institute of Standards and Technology has identified three stream ciphers that might be viable candidates for use in constrained systems (McKay, Bassham, Turan, & Mouha, 2016). A stream cipher keystream is as large as or larger than the plaintext, which will add bloat to the payload and could adversely affect power consumption.

Block ciphers may have less effect on constrained systems than stream ciphers. Block ciphers use a fixed-length key to encrypt blocks of plaintext (Iosifidis & Limniotis, 2016). Block ciphers iteratively encrypt a block of plaintext, start to finish, and then start the next block of text. Block ciphers have been considered better candidates for lightweight algorithms as the key size can be tailored to the expected plaintext size (McKay et al., 2016). As well, block ciphers can utilize separate encryption and decryption algorithms (McKay et al., 2016). One block cipher that is new and requires further investigation is BORON (Bansod, Pisharoty, & Patil, 2017). The one downside to block ciphers is that they are slower than stream ciphers in the encryption and decryption processes.

One other aspect of cryptographic algorithms on systems is the time that it takes to encrypt and decrypt the message. Larger, more complex algorithms, while secure, will add time to the overall process of creating and delivering the message (Almenares et al., 2013). An increase in the processing time will result in additional power consumption. Lightweight algorithms can process a message quicker but are considered less secure and may be deemed unsuitable for many applications.

Lightweight algorithms can have multiple definitions. For this study, the term lightweight algorithms pertain to the algorithm’s power consumption, memory usage, and processor cycles necessary to encrypt or decrypt a given length plaintext. In an article published in 2013 (Batina et al., 2013) a group of researchers built on work from another article published in 2012 (Kerckhof, Durvaux, Hocquet, Bol, & Standaert, 2012) using these criteria for comparing block ciphers and Advanced Encryption Standard (AES) architectures. This study includes the six block ciphers from the older article with a focus on the data and methods presented. The newer article included 11 block ciphers, five of which overlap with the original list. However, based on an article published in 2018 indicated that AES architectures are non-starters in the embedded market due to the high technical cost associated with power consumption, processing cycles, and memory size footprint (Buchanan, Li, & Asif, 2018). For this reason, this study will not consider AES.

Several comparative studies have been performed and published that look at lightweight algorithms. One such article published in the *International Journal of Advanced Computer*

Science and Applications looked at conventional cryptographic algorithms such as Data Encryption Standard (DES), triple-DES (3DES), RSA, and elliptical curve cryptography (ECC, Maqsood, Ahmed, Ali, & Shah, 2017). A similar study looked at these algorithms along with Blowfish and HiSea, which are symmetrical block ciphers (Mushtaq et al., 2017). Another, slightly older, the article looked primarily at ECC as applied to medical devices (Malhotra, Gardner, & Patz, 2007). Additional articles have looked at the lesser-known lightweight algorithms, such as KATAN. These works and the data provided by them form the foundational work for this paper.

When one considers cryptography for mobile devices, they first turn to items of the IoT category, such as a smartphone. However, these are not the only devices to consider. Radio Frequency Identification (RFID) devices are a prime example. In an article published in the International Journal for Information Security, a group of researchers discussed the probability of using public-key cryptography in implementations for RFID devices that would protect the integrity and confidentiality of the information transmitted (Arbit et al., 2015). This implementation looked at a solution known as WIPR (Weizmann-IAIK Public-key for RFID), which relied on a variant of the Rabin algorithm. Another article looked at RFID in sensor networks for device authentication (Manjulata, 2014). Both solutions rely on hardware optimized solution for the cryptography to be successful. In a similar article, Lohmann, Schneider, and Ruland discussed the magnetic field required for a passive RFID smart card to support a level of cryptography that would be considered secure (Lohmann et al., 2006). Their findings showed that for the application to medical devices, the magnetic field strength to support cryptography. However, as pointed out in an article in the Journal of Medical Systems, RFID for patient tracking and association to records is vulnerable to several threats such as interception, interruption, modification, and fabrication (Hawrylak, Schimke, Hale, & Papa, 2012). Successful implementation of these solutions in other IoT devices that, although small in format, have the computational, power, and memory resources to support the larger footprint of the algorithm is possible (Batra, Luhach, & Pathak, 2016).

Other technologies that consist of constrained systems include smart grids, sensor networks, and some payment systems. Smart grids are electrical grids that utilize smart meters to report power utilization for billing (Yan, Chang, & Zhang, 2017). Sensor and acoustic networks use miniaturized monitoring devices that communicate back to a command and control center for the observation of everything from home and business security systems to ocean buoy markers (Peng, Du, Li, & Li, 2016). One of the constraints on sensor networks is the power reserve of the battery. A study conducted in 2010 examined the possibility of extending power reserve life with scavenging technologies (Mikhaylov & Tervonen, 2010). Public transportation systems that are operated by a city or regional transit authority use constrained devices in their pay-to-ride scheme to process payments without requiring cash or credit card transactions (Rupp, Baldimtsi, HinterwΣlder, & Paar, 2015). In each of these cases, the data transferred between the sensor and the monitoring station require protection to provide data integrity and confidentiality.

Algorithms are processes that computers use to accomplish a function. This section discussed the concept of algorithms used in cryptography and the different types that exist. As well, this section discussed the use of cryptography in several applications such as RFID.

Assessing Power Consumption of Algorithms

Analysis of power consumption in computer systems typically looks at the sizing of power supplies or batteries. These analyses look at sustained power and peak power for proper sizing of the power supply and to ensure the safe operation of the device. However, in the case of a constrained system or a system that does not have a constant or rechargeable power supply, the power consumption analysis is designed to predict power reserve longevity.

Power consumption in processors used in everything from PLCs to Itanium class supercomputers all uses a series of transistors to affect an electrical circuit. These transistors are called field-effect transistors (FET) due to the electrical current or signal passes through a varying field that affects the resistance of the circuit (Bi, Shamsi, Yuan, & Jin, 2016). These FETs are also called gates. A series of preprogrammed instructions control these gates and includes adding, compare, in, out, load, and store (Hope, 2018). Each instruction requires a fixed number of gate processes to complete. Likewise, every algorithm utilizes the processor instruction sets to accomplish its tasks. To standardize the effect on the processor and subsequent power consumption, each algorithm uses what is known as a gate equivalence (GE) measure, which equates to the number of gates utilized by the algorithm to complete one function. By identifying the gate power consumption for a given processor, it is possible to predict the aggregate power consumption for a given algorithm based on its gate equivalence.

While computers have been around for several decades, the successful application of miniaturized circuits in the commercial market is relatively new. One of the first studies of measuring power consumption in these circuits included a real-time measurement of power consumption using an iPAQ Personal Digital Assistant (PDA) to test the effects with secure socket layer (SSL, Potlapally et al., 2003). The iPAQ and SSL reached the end of life several years ago. As well, the transistor size, which influences power consumption, in devices had become even smaller since the performance of these tests. Another study that came out around the same time evaluated the effects of RC4 and AES on wireless networks (Prasithsangaree & Krishnamurthy, 2003). This latter study focused on laptops and laptop battery life and not the smaller wearable devices architectures. The results of these studies show one common premise: power consumption and computational processes must be balanced to create a secure device without adversely impacting performance (Ferrigno et al., 2005). The proper balance between performance and power consumption is most important for devices that maintain health and human services.

Several models exist for predicting power consumption. The Accurate Prediction of Power Consumption model, also known as AEON, was proposed in 2005 for predicting power consumption in sensor networks (Landsiedel et al., 2005). However, the basis for this model is on a single type of transistor architecture inherent to sensors. As discussed by Yu Bi et al., there can be significant differences between architectures, such as a complementary metal-oxide-semiconductor (CMOS) and FET (Bi et al., 2016). Additionally, the signal frequency will affect the power consumption of the gate (Alioto & Palumbo, 2002). While one gate type may have a distinct advantage over another at 30 megahertz (MHz), the advantage will lessen or disappear at 1 MHz. This finding indicates that not only architecture but also processor frequency are considerations when designing and evaluating circuits.

In 2008, there were two papers published that addressed both cybersecurity and gate equivalent. Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar published two articles together that discussed the use of RFID and smart cards for the protection of vendor merchandise (Rolfes et al., 2008a) and customer payment cards (Rolfes, Poschmann, Leander, & Paar, 2008b), respectively. In both articles, it was the authors' perspective that for a cryptographic algorithm to be effective, it would require 1,000 GE. This premise can be both a good thing and a bad thing. First, 1,000 GE is a relatively low number for a cryptographic algorithm, which is discussed later in this paper. However, for a constrained system, 1,000 GE could make the difference between security and power reserve longevity.

Assessing power consumption on most electronics requires the use of an amperage meter that is in line with the circuit. However, for small electronics, this may be impractical. This section discussed how power consumption could be calculated based on known device architecture and algorithm behavior. This section also looked at some comparative studies that were performed using handheld devices, such as an iPAQ, to show the effects of cryptography on mobile devices. These studies fall short in direct comparison to the impact on a constrained system.

The Social Effect

The social implications of cybersecurity for medical devices are outside of the scope of this paper; it is still a topic worth mentioning. Adding cryptographic algorithms to a medical device can raise questions for manufacturers, healthcare providers, and patients (Maisel, Paulsen, Hazelett, & Selzman, 2018). Many of the current devices approved by the FDA cannot support the addition of a cryptographic algorithm due to design constraints. The lack of an existing viable product would require millions of dollars in research and development to create a new line of cyber-secure devices that would then have to go through the previously discussed testing requirements. Healthcare providers would have to invest in new equipment to interface with these cyber-secure devices. The addition of these new devices may also require additional training and support from the manufacturer. Likewise, if the cybersecurity solution becomes burdensome on the patient or healthcare provider, it will not be widely accepted (Gonçalves Fontes & José Balloni, 2007; Maisel et al., 2018). An article in the Journal of Medical Devices points out that user awareness of cybersecurity vulnerabilities is relatively low when it comes to such things as their healthcare and medical devices (Aydin & Chouseinoglou, 2013).

Cybersecurity solution integration for medical devices must be such that the patient does not have to perform self-monitoring of the device, and the healthcare provider does not have to worry that the solution will prevent them from being able to care for their patient.

Social acceptance considerations exist when modifying a product such as a medical device that a patient depends on to live. This section discussed how user awareness of cybersecurity vulnerabilities in medical devices is low, and presenting the patient with the option of bolt-on security may be a non-starter.

Conceptual Framework

To understand the feasibility of securing communications between a wearable or implanted medical device, one must first understand the implications of unsecured communications. To make the argument that this is needed is to understand what could happen. Identifying current vulnerabilities and attack vectors, as well as previous successful hacks, will is vital to justify the position that this research is needed and can benefit the community at large (TrapX Labs, 2015). Second, one must understand the process of creating and certifying medical devices. This process is not a simple form of submission or functional test (Ciurana, 2014; FDA, 2016c). Some of these tests can take years and cost tens of thousands of dollars (Ciurana, 2014). Third, identifying lightweight cryptographic algorithms without being insecure is not as hard as it sounds. Several existing algorithm candidates have been identified and are the focus of the research (Batra et al., 2016; Buchanan et al., 2018; Rolfes et al., 2008b). Fourth, taking these candidate algorithms and determining their effects on power consumption is critical to the validity of their use (Batina et al., 2013). These previous two steps will require the identification and use of electrical theory and algorithm science to identify the mechanism that occurs during an algorithm’s execution and how to correlate that to power consumption within the CPU (Texas_Instruments, 1997). Fifth, to determine the effect of power drain on a constrained system, one must first understand what the device limitations are (Batina et al., 2013). Constrained systems are those that have a limitation designed into them for one reason or another. In the case of Implanted Cardioverter Defibrillators (ICD), the battery must be small but contain enough power to allow the device to work for several years. Consultation with the medical device manufacturers is required to understand these limitations and the design basis that drives them (Wu & Eagles, 2016). Lastly, there are several requirements, both government and industry, that dictate communications and cybersecurity (FDA, 2016a, 2016c; Kramer et al., 2012). Figure 1 illustrates this relationship between constrained devices, cybersecurity measures, and the possible attack vectors or vulnerabilities that the lightweight cryptographic algorithms will address.

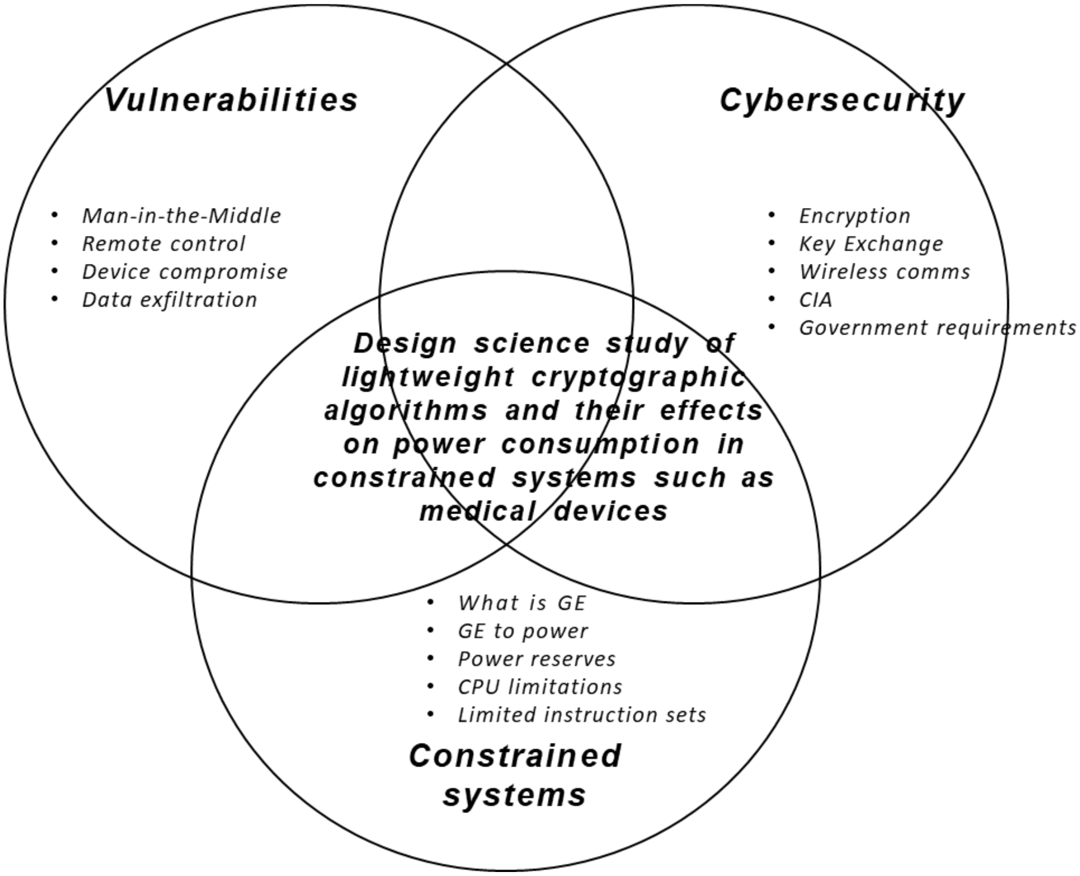

Figure 1. Conceptual Framework for the comparative study of lightweight algorithms for constrained systems.

Summary of Literature Review

Medical wearable and implanted devices pose a challenge to the healthcare industry from several angles. The cybersecurity angle is a difficult nut to crack. This chapter started with a discussion on what constrained systems are and the challenges they pose to manufacturers (Nicholson et al., 2012). Next, the cybersecurity challenges and possible attack vectors were discussed to understand better what must be protected and the impact of a successful attack (FDA, 2016b). Previous works were presented to show that although studies and research exists, it does not answer the question of applicability to medical devices. One of the major challenges for the implementation of security on constrained systems is the impact on power consumption. Power consumption can be predicted by equations that were presented based on the platform and the algorithm's characteristics (Landsiedel et al., 2005; Potlapally et al., 2003). Identifying cryptographic algorithms with minimal power requirements is necessary to properly secure communications and protect patients and their data (Shah & Engineer, 2019). Currently published research looks at many IoT devices, but not the applicability of lightweight cryptographic algorithms for medical devices to protect patients and their information.

The application of existing lightweight cryptographic algorithms is the focus of this dissertation. Chapter 3 includes a discussion of the research tradition and method that were used to perform a comparative analysis of the selected algorithms. In addition, Chapter 3 consists of the explanation of the population and sampling process that was used to select the algorithms included in the study. These algorithms are discussed in further detail in the Instrumentation section. Data collection and analysis for this study will also be addressed toward the end of Chapter 3.

CHAPTER THREE

The problem statement for this research was that implanted and wearable medical devices do not use cryptography to secure wireless communications putting the patient and healthcare provider at risk of cyberattack (Angle, 2016). Malicious cyber-attacks occur daily (Fu & Blum, 2013; Higgins, 2015). Attacks against the healthcare industry have become more prevalent because the data exfiltrated remain viable longer than financial data (Leavitt, 2010). Securing devices that connect to healthcare provider networks provides an additional layer of protection for the patient and provider alike.

The purpose of this study was to analyze the power consumption related to lightweight cryptographic algorithms when applied to an implanted medical device (IMD) and the subsequent effect on battery life to identify if battery longevity was reduced to the point that jeopardizes patient health. Cyber-attack vectors include medical devices and healthcare provider networks (Leavitt, 2010). Standard cybersecurity practices focus on the network but not the implantable and wearable devices. Cybersecurity measures must be implemented to protect the patient and their personal health information (PHI).

This chapter includes the research tradition and method that was implemented for this research. This chapter also consists of the population and sample size included in the study, as well as how the sample size was determined. A brief discussion will follow that included reasoning for the research method, data validity, and reliability, and ethical considerations.

Research Tradition

Research methodologies fall into three main categories; qualitative, quantitative, and mixed (Bryman, 2006). A fourth methodology is design science (Hevner, March, Park, & Ram, 2004). The purpose of a research methodology is to guide what type of data to be collected, the mechanism for collecting the data, how the data is analyzed, and what the output of the analysis will detail. This study used design science research that will include the collection and analysis of encryption algorithm characteristics and evaluation of the resultant data to evaluate the feasibility of using encryption algorithms in constrained systems. Design science research provides the empirical data collection and analysis required to assess and compare the numeric outcomes of an algorithm's power consumption (Wieringa, 2016).

Qualitative and mixed-method research will not be used in this study. These methods utilize in part or whole surveys and interviews that are presented to participants for an understanding of a phenomenon or behavior that is being studied (Yilmaz, 2013). The quantitative method was used to perform the calculations and comparative analysis of the encryption algorithms in the study (Yilmaz, 2013). This study analyzed power consumption attributed to cryptographic algorithms when applied to an implanted medical device. This analysis included design considerations and design effects due to the algorithms.

The purpose of the research design was to identify the variables in the research, identify their relationship, and identify the procedures utilized for data collection and analysis (Bryman, 2006). Selecting a research design provides the researcher with a framework to perform the research while ensuring that the problem statement is clear and concise, the data are chosen appropriately, and the data with its analysis align to the problem statement (Creswell & Creswell, 2018). Data that does not align to answer the research question will not provide benefit to the research.

Design science research is a methodology that looks at processes and artifacts (Wieringa, 2016). New product or process development is not the sole focus of design science. Design science also includes process and artifact improvements to existing designs based on new information or application, as well as advancements in technologies (Wieringa, 2016). According to Hevner (2004), design science involves seven guidelines that researchers must follow to validate its use.

1. The research must be relevant to the current time and scenario.
2. The research output must create or modify an artifact involved in the research to develop a solution to the problem identified.
3. The design artifact must be rigorously tested and proven.
4. Contributions to the body of knowledge must be verifiable.
5. The method used to evaluate the design must be rigorous in construction and evaluation.
6. The search process to identify, evaluate, and design a solution to the problem must be reachable.
7. The research must be effectively communicated in a technical and managerial manner.

The research in this study followed the design science guidelines in the following ways. The problem statement is relevant to current cybersecurity risks associated with medical implanted devices. The output from this study showed, or not that lightweight cryptographic algorithms can be utilized in medical implanted devices without compromising battery life. The evaluation method for the power consumption of the algorithms in the study was backed by tested and proven electrical theory. The research contained in this study was verifiable and repeatable. The research utilized the rigorous design considerations involved in selecting and evaluating algorithm power consumption. The analysis included available means found throughout the cybersecurity and electrical engineering fields. The results of this study included a communication method easily understandable and effectively conveyed to technical and managerial persons.

In a recent study published in the International Journal of Advanced Computer Science and Applications (Maqsood et al., 2017) utilized a design science analysis of algorithms. This analysis focused on the performance attributes of different symmetric and asymmetric algorithms on non-constrained systems. The performance measures included encryption/decryption time, key exchange time, and key generation time of six different algorithms as they were applied to securing constrained systems. A similar study examined 12 cryptographic algorithms for relative power consumption, encryption/decryption performance, and dependencies as they apply to IoT devices (Shah & Engineer, 2019). Similar to the study proposed in this paper, the previous two studies leave a gap in the body of knowledge as it applies to constrained systems and power consumption related to the encryption/decryption process. The gap of power consumption compared to cryptography in constrained systems is where this design science research study will focus.

Research Question

Advances in microcomputers and smart device technology have introduced a security problem (Bazzoli, 2016). This security problem puts user data at risk of loss of integrity and confidentiality. To address this problem and mitigate the risk of data integrity and confidentiality loss, communications between these devices and other devices should be encrypted (Harris & Maymí, 2018). The addition of encryption to a system will cause a subsequent increase in power consumption (Ferrigno et al., 2005). Because constrained systems have limited power reserves, the addition of encryption will shorten overall battery life. The question is, how much power consumption can be attributed to a lightweight cryptographic algorithm in a constrained device?

How much will the battery life be shorted by the introduction of a lightweight encryption algorithm?

Hypothesis

Multiple variables directly affect the power consumption of microcontrollers based on the cryptographic algorithms that could be applied (Batina et al., 2013). It was this researcher's goal to compare both traditional and new, lightweight algorithms to find a viable option for encrypting communications without critically affecting battery life or affecting the reliability of the devices used in the study.

$H1_0$: Lightweight cryptographic algorithms will not reduce the constrained system's battery life to an unacceptable level.

$H1_A$: Lightweight cryptographic algorithms will reduce the constrained system's battery life to an unacceptable level.

$H2_0$: Lightweight algorithms consume power to the extent that will not adversely affect device battery-life of a constrained device, similar to traditional cryptographic algorithms.

$H2_A$: Lightweight algorithms consume power to the extent that will adversely affect device battery-life of a constrained device, similar to traditional cryptographic algorithms.

Research Design

The research design for this study was design science research. Design science research is a two-part methodology that looks at both the process and the artifact of an identified problem (Hevner et al., 2004). Design science is not limited to a new product or process creation but can also be used for the analysis of a design problem that leads to a change in either the process or artifact. This design science study examined the relationship and to what extent the addition of a cryptographic algorithm had on the power reserves of a constrained system. This relationship deals with the independent variable of the algorithm and the dependent variable of the power consumption. The research for this study included five different cryptographic algorithms that were selected based on their key size, block size, round count, and encryption process and provide a representative sample of the population of lightweight algorithms that are available. This diversity sample is adequate to demonstrate the power consumption of lightweight algorithms and their effect on the battery life of constrained systems. Data for the algorithms selected in the population sample was utilized in a formula that calculated the power required to encrypt a standard plaintext that is typically transmitted by the IMD to its monitoring station. The published life expectancy of an IMD can range from 7 to 11 years. The next step of the research was to gather the number of transmissions made by the IMD per month and calculate the power consumed attributed to the algorithms per quarter. This consumption rate was then added to the normal extrapolated power consumption rate to identify the new battery depletion time. An acceptable longevity time was established and compared to the new depletion time to determine the impact of introducing the algorithm and viability of the solution.

Population and Sample

The population of a group is the aggregate number of those objects that satisfy a specific criterion (Adam, n.d.). Cryptographic algorithms are classified into two main categories: block and stream. Block ciphers process a block of data based on the key length during the encryption process. While this key length is fixed for a given version of the algorithm, different versions of the algorithm can utilize different key lengths. Block ciphers also declare a block size of the plaintext message that is processed at a time. If the plaintext message is longer then the block size, then it is fragmented for encryption and later reassembled. Stream ciphers utilize a continuous stream key and process the plaintext message in a constant process. The stream cipher key must be equal to or greater than the plaintext being encrypted (Harris & Maymí, 2018). Both block and stream ciphers can perform multiple rounds, or repeated encryption processes to strengthen the encryption process. The longer the key, or the more rounds that are processed, the more power that the algorithm consumes. An additional characteristic of cryptographic algorithms is the number of resources required. Lightweight algorithms are those that utilize less processing power, less memory, have a smaller footprint (also known as gate equivalence), or use smaller keys or blocks for the encryption/decryption process (Rolfes et al., 2008a). In the case of the latter, lightweight algorithms are considered inadequate for systems that require a high level of security. For constrained systems, lightweight cryptography is adequate to secure the device without monopolizing the device’s resources (Rolfes et al., 2008a). The population for this study was cryptographic algorithms identified as lightweight due to block size, key length, or gate equivalence.

A sample is a portion of a population that can be considered to be representative of the whole (Adam, n.d.). The size of the sample will vary from study to study depending on the number of variants that are being represented within the population (Adam, n.d.). The subject of this research was the cryptographic algorithms classified as lightweight encryption/decryption algorithms. The selection of these algorithms was based on the amount of information available on the Internet that supports the inclusion and validity of the algorithm. Five algorithms were included in this study that represents different algorithm architecture types based on key lengths, stream vs. block cipher, and the number of rounds performed by the algorithm to encrypt the plaintext. Only lightweight algorithms were considered for this study due to the minimal resource requirements they have compared to their full-size counterparts. Lightweight refers to the algorithm’s footprint and gate equivalent, which are the two factors that relate to power consumption (Batina et al., 2013). Based on the plaintext payload, some algorithms have a key length or encryption mechanism that results in a bloated ciphertext payload leading to excessive power consumption. For example, an encryption algorithm that has a block size of 1024 bits will produce a ciphertext that is a multiple of 1024 bits in length. If the plaintext is only 250 bits long, the ciphertext will have 774 bits of bloated space. This translates to unnecessary power consumption.

Sampling Procedure

Sampling is the process of selecting a sub-group of the population (CIRT, n.d.). The procedure by which a sample is determined is based on the randomness of the sample. The randomness is a controllable variable by the researcher (Pell Institute, 2020). Sampling can be categorized into two main categories: probability and non-probability. Probability sampling involves randomness while non-probability does not. Non-probability sampling is a controlled method of sampling based on requirements established by the researcher. Diversity sampling is a form of non-probability sampling and ensures that all variants within the population are equally represented (Creswell & Creswell, 2018). This study used diversity sampling.

The objects in this study were lightweight cryptographic algorithms. These algorithms presented multiple characteristics that make them unique. These algorithms were categorized as either stream ciphers or block ciphers. Block ciphers utilize blocks and keys of different sizes based on the variant of the algorithm. Both block and stream ciphers can be performed more than once on the same plaintext to increase their strength (Harris & Maymí, 2018). This repeated process is called a round. The number of rounds performed by an algorithm is determined by its design. All these variables factor into the weight of an algorithm. The algorithms chosen for this study provided a representative sample of the variants that existed within the cryptographic space. While there is a multitude of algorithms and variants in use, including all algorithms in this study would result in redundant work and dilution to the actual focus of this study. The Pell

Institute (Pell Institute, 2020) provided guidance on sample size for research where there is no clear delineation in the required sample size and precision of the study is up to the researcher. Four questions the researcher must answer are (a) how precisely do you want to be, (b) how sure do you want to be of your answer, (c) how much variation is there in the population you are studying, and (d) how small of an effect do you want to be able to identify. This design science research examined only one contributor to power consumption in the constrained system, that attributed to a cryptographic algorithm. The addition of more algorithms to this study would not have increased the precision of the research nor account for the additional variance that would provide value without distracting from the research question.

Instrumentation

The instrument used the algorithm block size and gate equivalent, and the reference device's battery size and power per 1,000 gate equivalents as inputs. Calculations, as discussed in Chapter 4 that make up the instrument, were performed on each of the algorithms. The output was the power consumption rate for each algorithm and a projected new battery-life based on that consumption rate (see Chapter 4).

Validity

Research validity was evaluated in four different areas (Webster, n.d.). External validity looked at if the research can be applied to other forms, times, or populations outside of the sample set. The external validity of the study was determined viable as the analysis presented in this study can be used against other algorithms to identify the power consumption related to them performing their function. Internal validity looked at if the test objectives in the test are both related and causal. The internal validity of this study was determined sound as the increase in gate equivalents in an algorithm directly correlated or was causal to the rise in power consumption and was supported by the equation used. Construct validity asked if the subject of the study was measured. In this study, the end goal was to evaluate the power consumption of algorithms and compare this to the power reserves on a constrained system or device to determine if the addition of the algorithm would deplete the power reserve at an unacceptable rate making the device unusable. Therefore, construct validity was determined sound. The last of these validity checks is the Statistical Conclusion validity. This validity check addressed whether the variables are related. The gate equivalent for an algorithm was related to the power consumption of the algorithm, and therefore, the statistical conclusion was sound.

The validity and reliability of the data in the gate equivalents of the cryptographic algorithms chosen were established through the support of multiple sources that provided the same values.

Reliability

Research reliability is the ability to perform a test more than once and receive the same results each time with the same given data (Dudovskiy, 2019). There are four types of research reliability: test-retest, parallel forms, inter-rater, and internal consistency (Dudovskiy, 2019). The test-retest reliability assumes the same instrument is used to study a phenomenon, and the same results are received (Dudovskiy, 2019). Parallel test reliability uses more than one instrument to study a single phenomenon, and the same results are obtained (Dudovskiy, 2019). Inter-rater reliability uses more than one researcher who uses the same instrument and gets the same results (Dudovskiy, 2019). Internal consistency reliability is used to compare subjects to find the extent of similarity (Dudovskiy, 2019). This study utilized test-retest reliability, which provided a consistent output based on the inputs. This process was repeatable.

Data Collection

The collection of data for a study will vary based on the intent of the study, the sampling method and population, the research tradition and method, and the data source. The research performed to determine the effects of cryptographic algorithms on constrained systems included data from the internet. These data included previous analysis into gate equivalents of algorithms and the correlation of gate equivalents to power consumption. Where possible, multiple sources were used to corroborate the values for each algorithm. These data were then inserted into a table along with any caveats. A single algorithm can have multiple versions based on key length, block size, and round count. These variables were discussed for each algorithm, and the variant with the least gate equivalent, satisfying the lightweight requirement, was used for the study to illustrate that lightweight algorithms can provide security with minimal impact to device battery life.

Data Analysis

The instrument used the algorithm block size and gate equivalent, and the reference device's battery size and power per 1,000 gate equivalents as inputs. Calculations, as discussed in Chapter 4 that makes up the instrument, were performed on each of the algorithms. The output was the power consumption rate for each algorithm and a projected new battery-life based on that consumption rate. A simple comparative analysis characterized the output and illustrated the algorithm's effects on battery life. The current state was no algorithm applied to the reference device with an end (new) state having an algorithm applied.

Ethical Considerations

This research included the evaluation and comparison of cryptographic algorithms. These cryptographic algorithms were freely available to the public without licensing requirements. Cryptographic algorithms are not human or animal. Informed consent was not required for their use.

The platform that was used as a reference model of the constrained system is an implanted cardioverter defibrillator. The manufacturer was contacted for additional information specific to the reference device used in the study. The manufacturer name and device model number were not disclosed in this research at the request of the manufacturer. This information was available through online or publicly available sources.

Written by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in 1979, The Belmont Report provides protection for humans that participate in biological and behavioral research (HHS, 2016). To increase the scope of research protections, the Department of Homeland Security released the Menlo Report in 2012 (DHS, 2012). The scope change includes communications and information technology data that is collected for this research. Neither the Belmont Report nor the Menlo Report was applicable as there are no human participants in this research.

Summary of Chapter Three

This study used the gate equivalent of the selected algorithms to determine the power consumption of each by an implanted medical device. This power consumption was then used to determine the effects on the battery life of the device. This analysis was used to determine if the addition of the algorithms will shorten the life of the device to the point that is not feasible or will show that the addition may reduce the device longevity, but still be within the limits of usability. In the next chapter, the algorithms, reference platform, and the instrument are discussed in detail.

CHAPTER FOUR

Threats to people and their everyday lives lead to the discovery of new attack vectors not previously realized. In recent years a shift in malicious activity has targeted medical devices as ingress to healthcare provider networks (Al Ameen et al., 2012; TrapX_Labs, 2015; Wu & Eagles, 2016; Zhang et al., 2013) and to compromise personal healthcare information (Leavitt, 2010; Williams & Woodward, 2015). Protecting the data transmitted between devices and their monitoring stations can be accomplished through encryption of the data while in transit. Cryptographic algorithms used for encrypting data perform processes in addition to those of the normal device processes. These new processes consume power. The model presented will determine the amount of power attributed to lightweight cryptographic algorithms and the effects on a constrained device's battery life.

The Algorithms

This study included data retrieved from the internet of characteristics of the algorithms examined in the study. These characteristics include key length, block size, round count, footprint size, and gate equivalent where available. These data were used to calculate the power consumption of each algorithm when applied to the base system. These algorithms were not executed as part of the study.

Present, Tiny Encryption Algorithm (TEA), Katan, and High Security and Lightweight (HIGHT) are lightweight block ciphers that were selected to represent block ciphers of differing block sizes or key lengths.

Present has two variants that utilize either 80-bit or 128-bit key lengths, an 80-bit block size, a round count of 31, and uses substitution-permutation network (SPN) for the encryption/decryption process (Bogdanov et al., 2007; Rolfes et al., 2008a). Created by the Orange Labs, Ruhr University Bochum, and the Technical University of Denmark in 2007, Present is an algorithm that was developed to be a lightweight and highly efficient cryptographic algorithm for RFID applications (Bogdanov et al., 2007).

Tiny Encryption Algorithm (TEA) has only one variant with a 128-bit key length, 64-bit block size, a round count of 64, and uses the Feistel method for encryption/decryption (Alizadeh, Hassan, Zamani, Karamizadeh, & Ghazizadeh, 2013). Created by two crypto-analysts from the Cambridge Computer Laboratory in 1994, TEA was initially designed to replace DES (Data Encryption Standard) in computer systems (Alizadeh et al., 2013; Wheeler & Needham, n.d.) and has more recently been proposed for use in RFID systems (Alizadeh et al., 2013).

The High Security and Lightweight (HIGHT) algorithm has only one variant with 128-bit key length, 64-bit block size, a round count of 32, and uses the Feistel method for encryption/decryption (Alizadeh et al., 2013). HIGHT has been proposed for use in RFID systems and sensor networks, as well as hardware implementations in FPGA devices (Hong et al., 2006).

Katan, unlike the previous three candidates, offers three variants that differ based on block size vice key length. Katan offers 80-bit key length; 32-, 48-, or 64-bit block size; a round count of 254; and uses the Feistel method for encryption/decryption (Alizadeh et al., 2013). Like HIGHT, Katan is optimized for use in hardware implementations (Batina et al., 2013).

Advanced Encryption Standard (AES) is currently the industry standard block cipher that is used in non-constrained systems for securing sensitive data (Prasithsangaree & Krishnamurthy, 2003) and is included for reference to demonstrate the need for lightweight algorithms. AES utilizes a 128-bit block size; 128-, 192-, 256-bit key lengths; and is considered a heavy algorithm due to the complexity of the algorithm (Manjulata, 2014).

Table 1

Block Encryption Algorithm Specifications

Algorithm	Block Size (in bits)	Key Length	Round count	Encryption mechanism
Present	80	80, 128	31	SPN
TEA	64	128	64	Feistel
HIGHT	64	128	32	Feistel
Katan	32,48,64	80	254	Feistel
AES	128	128,192,256	10,12,14	Rijndael

Trivium is a lightweight, hardware optimized stream cipher chosen to represent other stream ciphers available. Trivium utilizes an 80-bit key length and an 80-bit initialization vector (IV) to generate a 288-bit internal state (Canni`ere & Preneel, 2012). This internal state initiation process is utilized to generate the keystream as opposed to having a defined key, such as is used by block ciphers (Canni`ere & Preneel, 2012).

The Platform

The platform that the algorithms were tested against was the specification of an implanted cardioverter defibrillator (ICD). Justification for using the specification of the device instead of an actual device was this study would be performing calculations about previously collected data from external sources instead of directly collecting measurements from the device. The device specifications were obtained through publicly available product guides and verified through manufacturer discussions. The portions of the device specifications that provided the most insight into the device's constraints were battery capacity, circuit architecture, transmission frequency, and plaintext payload size. Plaintext payload size multiplied by transmission frequency with and without cryptography was used for the comparison. The current device design utilizes a 1,000 milliamp-hours (mAh) battery. In contrast, a smartphone contains a 3,000 mAh battery, and a smartwatch uses a 300 mAh battery. In both cases, the battery must be recharged regularly, depending on use. ICD batteries cannot be recharged and are expected to last 5 to 11 years. This battery operates both the device's microprocessor that monitors and tracks the heartbeat and provides the electrical shock to stabilize the heartbeat, if necessary.

These data were utilized in a series of mathematical equations to determine the power consumption contribution for an encryption event. The independent variable for this equation was the gate equivalent for the algorithm, and the dependent variable was the power consumption attributed to the algorithm. As the gate equivalent increased, the power consumption increased — the opposite was not true.

The Instrumentation

There are four components to power consumption in a circuit: leakage, transient, static, and dynamic power consumption (Texas Instruments, 1997). Static power consumption happens in all circuits and is based on the components used in the circuit design (Texas Instruments, 1997). Dynamic power consumption is attributed to two components of power consumption: transient power consumption and capacitive-load power consumption (Texas Instruments, 1997). Transient, or short-circuit, power consumption exists when a transistor changes state from on to off or vice versa. Capacitive-load power consumption is power consumption based on switching frequency. Dynamic power consumption equals transient power consumption plus capacitive-load power consumption. Therefore, assessing the contribution to the power consumption of a cryptographic algorithm was a measure of dynamic power consumption.

The manufacturer provides data on its website, as well as during a telephone conversation for the reference platform that was used. The data retrieved from the manufacturer website that was utilized in this research was the advertised device longevity based on the percentage of pacing the device provides. This was in the form of the product specification pamphlet. The pamphlet stated that that the device longevity is 11 years with 0% pacing and 8 years with 100% pacing. The data retrieved during the phone conversation with the manufacturer included estimations of power consumption per gate equivalence, message size and frequency, and the device battery capacity. The manufacturer confirmed that the device utilized a low standby power CMOS transistor that was 32nm in size. This transistor is rated at 77.7716 pW per NAND gate event according to a study in the International Journal of Engineering and Technical Research (RajaSekhar & Reddy, 2015) and confirmed by the manufacturer. These data were retrieved and utilized to determine the average power consumption rate for the device platform. The device's battery rating was provided in amp-hours, 1Ah, and was divided by the shortest expected longevity duration, 8 years, to ensure the most restrictive value was used.

To determine power consumption for the algorithm, several aspects must be accounted for. The manufacturer was contacted to provide payload size and frequency of transmission, as these values are not on the manufacturer's web site. Data collection for each algorithm in the study included the algorithm's gate equivalent. Gate equivalent is a standard of measure for algorithms for comparison and indicates an equivalent measure for the algorithm through its process to encrypt/decrypt a payload equivalent to its minimum block size through X number of NAND gates. With these data, the power consumption attributed to the algorithm was calculated.

$$\frac{\text{Plaintextsize}}{\text{blocksize}} = \text{Blocks per transmission} \tag{2}$$

$$\frac{\text{Total blocks} * \text{Algorithm GE}}{1000} = \text{Total GE(x1000)} \tag{3}$$

$$Total\ GE * \text{Power per GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = \frac{\mu Ah}{qtr} \tag{4}$$

$$\frac{\mu Ah}{qtr} * 4 = \frac{\mu Ah}{yr} \tag{5}$$

The last portion of this process was to take the device base power consumption and add the algorithm attributed power consumption to calculate a new annual power consumption rating. The new yearly power consumption rate was then divided into the battery amp-hour capacity for the new battery life of the device.

$$Algorithm\ \mu Ah + Device\ \mu Ah = new\ yearly\ power\ consumption \tag{6}$$

$$\frac{Battery\ capacity}{Yearly\ power\ consumption} = Device\ battery\ life \tag{7}$$

These calculations were performed for each of the algorithms in the study, and a table was populated for value comparison. From a design science perspective, the effects of the algorithm on device longevity were examined to determine the viability of adding the algorithm. The IEEE P485 standard states a 10-15% design margin in battery capacity (IEEE, 2011). However, the manufacturer of the device used as the reference model stated that a 5% increase in power consumption would be acceptable. If the algorithm reduced battery life to less than 5% of its initial longevity, then the addition of the algorithm was determined viable. If greater than 5%, then the addition was detrimental to the life expectancy of the device.

Summary of Chapter Four

This design science research evaluated the power consumption of select cryptographic algorithms and the effect on implanted medical device battery-life. The intent of this research to show that the addition of a lightweight cryptographic algorithm to a constrained system such as an implanted cardioverter defibrillator would have minimal effect on the battery life of the device. Chapter 4 included discussion on the algorithms that were evaluated, the test platform they were applied to, and the method used to calculate the effects. Chapter 5 put this model to practice, providing the results of applying the selected algorithms to the test platform.

CHAPTER FIVE

Cryptographic algorithms are used throughout the computer world to protect data from unauthorized changes and disclosure (Harris & Maymí, 2018). Cryptography comes at a price in the form of additional processor cycles that result in increased power consumption, latency, and reduced throughput (Batina et al., 2013). For constrained systems, this extra overhead could shorten a device's longevity or feasibility for its intended purpose. The purpose of this study and the instrument introduced in Chapter 4 was to evaluate lightweight cryptographic algorithms against the reference architecture of an implantable cardioverter defibrillator, which has a non-replaceable, non-rechargeable battery. Theoretical application of the selected algorithms to the processes of this device provided a new power consumption rate and device longevity.

This study was performed by executing a series of equations to identify the power consumption contribution when a lightweight cryptographic algorithm is applied to a reference platform where cryptography was not initially present. This process started with identifying the specifications of the reference device and its battery capacity, which was determined to be 1 Ah. The reference device has an 8-11-year life expectancy according to the manufacturer's published literature and confirmed during a phone discussion. The most restrictive time of 8 years was chosen for the study. Dividing the battery capacity by the longevity provided an annual power consumption of 125 mAh/year. Next, the reference device communication sessions were identified and determined to consist of a three-message event. The first message was the device interrogation that returned a 256-bit message. The second message was the patient data, which includes the pacing events and device parameters, and the return was a maximum of 150 kilobytes. The third message was a command message to the device, which was 256 bits in size. Next, the gate equivalence for each of the algorithms selected for the study was identified. This gate equivalence is a unit of measure that is used to compare algorithms and was used in this study to calculate power consumption. The messages were aggregated, divided by the algorithm block size, and then multiplied by the gate equivalence to determine the gate events the communication session would require. The reference device power consumption per gate event was identified and validated with the manufacturer. This value was then multiplied by the number of gate events for each algorithm to determine the power consumption for each communication session. This calculated value only accounts for the dynamic power consumed. To calculate the total power, the dynamic power, which accounts for 80% of the total power, was multiplied by 1.25 to determine the total power consumption per session. Since these communications sessions take place on a quarterly basis when the patient visits their doctor, the calculated power consumption per session was multiplied by four to achieve an annual power consumption. For each algorithm, this annual power consumption was added to the initially computed power consumption of the reference device without cryptography to determine the new annual power consumption rate. Finally, the new yearly power consumption rate was divided into the reference device battery capacity to calculate the new device longevity and compared to the 8-year value of no cryptography present to determine if the algorithm is viable or not. The threshold was set at a reduction in device longevity of no more than 5% by the manufacturer. These calculations were discussed in detail in Chapter 4.

Description of the Study Sample

This study included a population of lightweight cryptographic algorithms. Cryptographic algorithms that are identified as lightweight include those with relatively small key lengths, block sizes, or round counts (Rolfes et al., 2008b). The selected sample represented the population and included variables such as block size, key length, round count, cryptographic method, and encryption/decryption process. According to the Pell Institute (2017), the researcher should decide the sample size based on four factors, including precision, certainty, variations, and effect size. The algorithms selected for this study provided the necessary coverage for the variations in the population, such as not to overwhelm the point, a satisfactory level of certainty, and adequate data points to provide a level of precision. The effect size will vary based on the representation in the sample, which provided justification for the inclusion of a full-size algorithm in the study for reference.

Results

Implantable cardioverter defibrillators (ICD) are microcomputers with very specialized functionality. These devices provide monitoring of heart rhythms, recording for future diagnostics, and stimulation when necessary (Manolis, Maounis, Koulouris, & Vassilikos, 2017). While the monitoring and recording of heart rhythms is a continuous process performed by these devices, the stimulation, also known as cardio resynchronization therapy (CRT), varies based on the needs of the patient. Because of this, most manufacturers of ICD provide a range for device longevity. Studies have shown that while manufacturers indicate between 5 and 11 years or more for some devices, there is a small percentage of patients that require a high level of CRT, leading to premature device battery failure in as little as 36 months (Manolis et al., 2017). While this is less than ideal, it is essential to point out that the battery life of these devices is not a given and anything that significantly reduces the battery life should be avoided.

For the purpose of this study, a commonly utilized ICD from a reputable manufacturer acted as the platform. This manufacturer requested that its name and product name be excluded from the study.

This manufacturer publishes the specifications for its device on its website and claims that with minimal pacing required, the device battery will last 11 years. This number drops to 8 years, with 100% ventricle pace, ventricle sense, and inhibit (VVI) action from stabilizing the heart rhythm.

As previously discussed in Chapter 4, there are four significant parts that account for the power consumption in a circuit: leakage, short-circuit, static and dynamic, also called switching, power (Yadav, 2014). Leakage and static power are the least significant contributors accounting for approximately five percent of the power consumption in a transistor (Yadav, 2014). Short-circuit power is that power which is consumed when a transistor is switching and accounts for approximately 15% of the power consumption (Yadav, 2014). Dynamic power is by far the largest attributor of power consumption at 80% (Yadav, 2014) and was the characteristic by which power consumption in the circuit was based. The instrument only calculated the expected dynamic power consumption, and as such, the resultant power consumption rate was multiplied by 1.25 to account for the static power and leakage values.

To calculate the average power consumption of the device as illustrated in Chapter 4, the battery capacity of the device (1 Ah) was converted to milliamp hours, divided by the number of years of advertised device longevity, and then converted to microamp hours.

$$\frac{1\,Ah}{8 years} * 1{,}000 = 125\,mAh/yr = 125{,}000\mu Ah \tag{8}$$

This calculation demonstrated that an ICD device with 1Ah battery capacity with 8-year longevity consumes 125,000 µAh per year. This power consumption includes the monitoring and pacing actions listed above, as well as communications between the device and its monitoring station.

The reference platform consisted of a complementary metal-oxide-semiconductor (CMOS) processor and 48 KB of RAM. This processor utilizes a 32nm architecture with a reduced instruction set to minimize the power requirements and footprint within the device. The device was designed with an expected 3-hour communication session when first initialized and one hour of communications per year spread across four quarterly doctor visits. Each of these quarterly visits consists of a series of transmissions that includes device identification, download of patient data, and an adjustment to the operational configuration of the device, also called a command signal, if necessary, as shown in Figure 2. Each communication begins with a handshake between the device and the monitoring station that is not encrypted. All transmissions after this initial handshake are encrypted. The device identification includes a packet that is 32 bytes or 256 bits in size. The patient's downloaded data will vary based on the pacing settings of the device and the number of events the patient experiences. This value can be as little as 0 bytes if no pacing events take place and up to the size of the external memory, which is 1 MB in size. However, the average message size is between 75 and 150 KB, according to the manufacturer. For the purpose of this study, the message size of 150 KB, or 1,200 Kb or 1,228,800 bits, were used. Adjustment of settings is performed by uploading a configuration file to the device that is 256 bits.

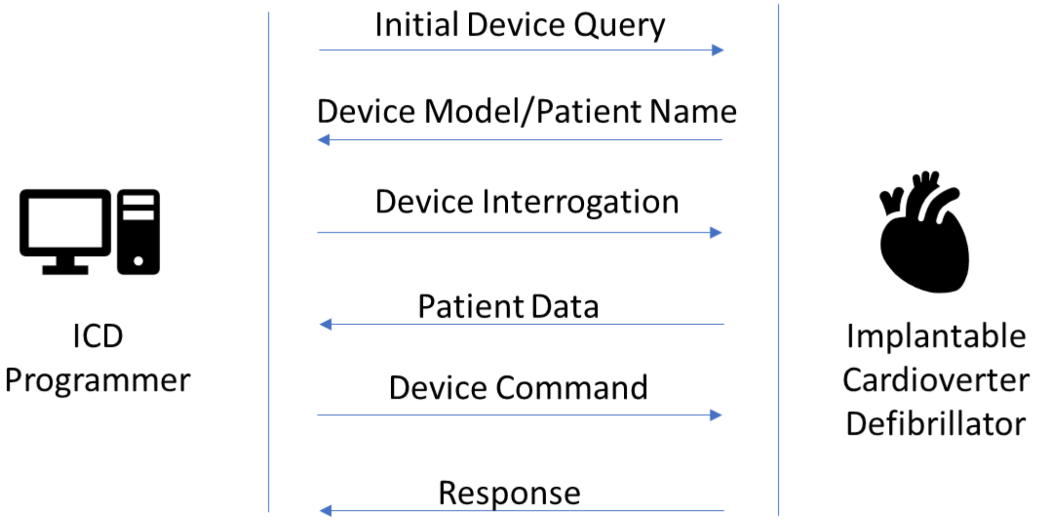

Figure 2. Transmission sequence between ICD and ICD Programmer.

Cryptographic algorithms perform a series of actions on data to convert it from plaintext to ciphertext and back to plaintext. These actions include OR, XOR, and AND (Shah & Engineer, 2019). Each of these actions can be equivocally compared by their relative operations when compared to a two-input NAND gate (Rolfes et al., 2008b). This value is called gate equivalents and is calculated by dividing the area of silicone required of the algorithm by that of a standard NAND gate (Rolfes et al., 2008b). Table 2 lists the published gate equivalents for the algorithms that are included in this study.

Table 2

Encryption Algorithm Gate Equivalents

Algorithm	Block Size (in bits)	Key Length	Round count	Gate Equivalent	Reference
Present	80	80	31	1,570	(Rolfes et al., 2008b)
TEA	64	128	64	2,100	(Bogdanov et al., 2007)
HIGHT	64	128	32	3,048	(Hong et al., 2006)
Katan	32	80	254	802	(Armknecht & Mikhalev, 2015)
AES	128	128	10	3,400	(Hong et al., 2006)

Trivium	8	80	--	2,952	(Canni`ere & Preneel, 2012; Good & Benaissa, n.d.)

As previously discussed, the session setup and handshake are not encrypted; only the message payload is encrypted. For each of these payload and algorithm combinations, the resultant ciphertext payload must be rounded up to the next full block size. For example, for a 256-bit plaintext and an 80-bit block size, the ciphertext is 256/80 = 3.2, rounded up to 4, 4×80 = 320 bits. Therefore, the new ciphertext payload is a minimum of 320 bits. This same derived multiple was subsequently used to calculate the power consumption for the algorithm used for its block size. For the previous example, an algorithm with an 80-bit block size and 1,000 gate equivalents will consume power equivalent to 4,000 gate equivalents for the reference circuit.

Present Device ID Message $$\frac{256\ bits}{80bits/block} = 4\ blocks \tag{9}$$

Patient Data $$\frac{1{,}228{,}800\ bits}{80bits/block} = 15{,}360\ blocks$$

Command Signal $$\frac{256\ bits}{80bits/block} = 4\ blocks$$

Total Gate $$\frac{(4 + 15{,}360 + 4) * 1{,}570\ GE/block}{1000} = 24{,}127.76\ \mathrm{GE}$$

TEA Device ID Message $$\frac{256\ bits}{64bits/block} = 4\ blocks \tag{10}$$

Patient Data $$\frac{1{,}228{,}800\ bits}{64bits/block} = 19{,}200\ blocks$$

Command Signal $$\frac{256\ bits}{64bits/block} = 4\ blocks$$

Total Gate $$\frac{(4 + 19{,}208 + 4) * 2{,}100\ GE/block}{1000} = 40{,}336.8\ \text{GE}$$

HIGHT

Device ID Message $$\frac{256\ bits}{64bits/block} = 4\ blocks \tag{11}$$

Patient Data $$\frac{1{,}228{,}800\ bits}{64bits/block} = 19{,}200\ blocks$$

Command Signal $$\frac{256\ bits}{64bits/block} = 4\ blocks$$

Total Gate $$\frac{(4 + 19{,}208 + 4) * 3048\ GE/block}{1000} = 58{,}545.984\ \text{GE}$$

Katan

Device ID Message $$\frac{256\ bits}{32bits/block} = 8\ blocks \tag{12}$$

Patient Data $$\frac{1{,}228{,}800\ bits}{32bits/block} = 38{,}400\ blocks$$

Command Signal $$\frac{256\ bits}{32bits/block} = 8\ blocks$$

Total Gate $$\frac{(8 + 34{,}800 + 8) * 802\ GE/block}{1000} = 30{,}809.632\ \text{GE}$$

AES

Device ID Message $$\frac{256\ bits}{128bits/block} = 2\ blocks \tag{13}$$

Patient Data $$\frac{1{,}228{,}800\ bits}{128bits/block} = 9{,}600\ blocks$$

Command Signal $$\frac{256\ bits}{128bits/block} = 2\ blocks$$

	Total Gate	$\frac{(2+9{,}600+2)*3{,}400\ GE/block}{1000}=32{,}653.6\ \mathrm{GE}$	
Trivium	Device ID Message	$\frac{256\ bits}{8bits/block}=\ 16\ blocks$	(14)
	Patient Data	$\frac{1{,}228{,}800\ bits}{8bits/block}=\ 15{,}360\ blocks$	
	Command Signal	$\frac{256\ bits}{8bits/block}=\ 16\ blocks$	
	Total Gate	$\frac{(16+153{,}600+16)*2{,}952\ GE/block}{1000}=453{,}521.664\ \mathrm{GE}$	

Table 3

Plaintext Gate Equivalents Footprint

Algorithm	Block Size (in bits)	Gate Equivalent (GE)	Device Identification (256 bits)	Patient Data (1,228,800 bits)	Command Signal (256 bits)	Total Blocks	Total Gates (x1000)
			Blocks	Blocks	Blocks	Blocks	GE
Present	80	1,570	4	15,360	4	15,368	24,127.8
TEA	64	2,100	4	19,200	4	19,208	40,336.8
HIGHT	64	3,048	4	19,200	4	19,208	58,546
Katan	32	802	8	38,400	8	38,416	30,809.6
AES	128	3,400	2	9,600	2	9,604	32,653.6
Trivium	8	2,952	16	153,600	16	153,632	453,521.7

The reference architecture was an implantable cardioverter defibrillator (ICD). This device utilizes a 32nm transistor that is rated at 77.7716 pW per NAND gate equivalent. This translates to 77.7716 nW, or 77.7716 nAh at 1v, per 1000 gate equivalents. Table 3 listed the resultant 1,000 gate equivalents for each of the algorithms per quarterly visit to a doctor. This value was multiplied by the processor power per 1,000 gate equivalents to calculate the quarterly dynamic power consumption. To account for the four types of power consumption in a circuit, the calculated power for the total gate equivalents was multiplied by 1.25, then divided by 1,000 to output the value in micro Amp-hours. To calculate the annual power consumption, the quarterly calculated value was multiplied by four. Based on this process, Table 4 lists the resultant power consumption for each algorithm.

Present

$$24{,}127.8\,GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 2{,}345.57\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} \tag{15}$$

$$2345.57\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} * 4\,\frac{\mathrm{qtr}}{\mathrm{yr}} = 9{,}382.29\,\frac{\mu\mathrm{Ah}}{\mathrm{yr}}$$

TEA

$$40{,}336.8\,GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 3{,}921.32\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} \tag{16}$$

$$3{,}921.32\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} * 4\,\frac{\mathrm{qtr}}{\mathrm{yr}} = 15{,}685.29\,\frac{\mu\mathrm{Ah}}{\mathrm{yr}}$$

HIGHT

$$58{,}546\,GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 5{,}691.52\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} \tag{17}$$

$$5{,}691.52\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} * 4\,\frac{\mathrm{qtr}}{\mathrm{yr}} = 22{,}766.08\,\frac{\mu\mathrm{Ah}}{\mathrm{yr}}$$

Katan

$$30{,}809.6\,GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 2{,}995.14\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} \tag{18}$$

$$2995.14\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} * 4\,\frac{\mathrm{qtr}}{\mathrm{yr}} = 11{,}980.56\,\frac{\mu\mathrm{Ah}}{\mathrm{yr}}$$

AES

$$32{,}653.6\,GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 3{,}174.4\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} \tag{19}$$

$$3{,}174.4\,\frac{\mu\mathrm{Ah}}{\mathrm{qtr}} * 4\,\frac{\mathrm{qtr}}{\mathrm{yr}} = 12{,}697.61\,\frac{\mu\mathrm{Ah}}{\mathrm{yr}}$$

Trivium $$453{,}521.7GE * \frac{77.7716pAh}{GE} * \frac{\mu Ah}{1{,}000{,}000pAh} * 1.25 = 44{,}088.89 \frac{\mu\text{Ah}}{\text{qtr}} \qquad (20)$$

$$44{,}088.89 \frac{\mu\text{Ah}}{\text{qtr}} * 4 \frac{\text{qtr}}{\text{yr}} = 176{,}355.54 \frac{\mu\text{Ah}}{\text{yr}}$$

Table 4

Encryption Algorithm Power Consumption

Algorithm	Block Size (in bits)	Gate Equivalent (GE)	Total Gates (x1000)	Power Per Qtr (μAh)	Power Per Yr (μAh)
Present	80	1,570	24,127.8	2,345.6	9,382.3
TEA	64	2,100	40,336.8	3,921.3	15,685.3
HIGHT	64	3,048	58,546	5,691.5	22,766.1
Katan	32	802	30,809.6	2,995.1	11,980.6
AES	128	3,400	32,653.6	3,174.4	12,697.6
Trivium	8	2,952	453,521.7	44,088.9	176,355.5

The final phase was to combine the yearly power consumption rates to ascertain a new annual rate. This new rate was then divided into the battery capacity to find the new device longevity. As stated in Chapter 4, a design margin of 5% will determine if the addition of the cryptographic algorithm was feasible or detrimental to the device longevity. As the initial device longevity was stated at 8 years, the new longevity threshold is 7.6 years.

Present
$$9{,}382.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} + 125{,}000\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 134{,}382.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} \tag{21}$$

$$1{,}000{,}000\mathrm{\mu Ah}/134{,}382.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 7.44yr$$

TEA
$$15{,}685.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} + 125{,}000\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 140{,}685.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} \tag{22}$$

$$1{,}000{,}000\mathrm{\mu Ah}/140{,}685.3\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 7.108yr$$

HIGHT
$$22{,}766.1\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} + 125{,}000\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 147{,}766.1\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} \tag{23}$$

$$1{,}000{,}000\mathrm{\mu Ah}/147{,}766.1\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 6.767yr$$

Katan
$$11{,}980.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} + 125{,}000\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 136{,}980.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} \tag{24}$$

$$1{,}000{,}000\mathrm{\mu Ah}/136{,}980.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 7.300yr$$

AES
$$12{,}697.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} + 125{,}000\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 137{,}697.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} \tag{25}$$

$$1{,}000{,}000\mathrm{\mu Ah}/137{,}697.6\,\frac{\mathrm{\mu Ah}}{\mathrm{yr}} = 7.262yr$$

Trivium $$176{,}355.5\frac{\mu\text{Ah}}{\text{yr}} + 125{,}000\frac{\mu\text{Ah}}{\text{yr}} = 301{,}355.5\frac{\mu\text{Ah}}{\text{yr}} \quad (26)$$

$$1{,}000{,}000\mu\text{Ah}/301{,}355.5\frac{\mu\text{Ah}}{\text{yr}} = 3.318yr$$

Table 5

Power Consumption with Cryptographic Algorithm

Algorithm	Block Size (in bits)	Gate Equivalent (GE)	Algorithm Power (μAh)	Total Annual Power	New Device Longevity
Present	80	1,570	9,382.3	134,382.3	7.44
TEA	64	2,100	15,685.3	140,685.3	7.11
HIGHT	64	3,048	22,766.1	147,766.1	6.77
Katan	32	802	11,980.6	136,980.6	7.30
AES	128	3,400	12,697.6	137,697.6	7.26
Trivium	8	2,952	176,355.5	301,355.5	3.32

Discussion of Study Findings

The introduction of a cryptographic algorithm to an existing design where no cryptography existed adds overhead to the device that the manufacturer did not plan for. The values in Table 5 show that this introduction and the impact that it has on the reference platform. Of the six algorithms in the study, none of them resulted in a newly calculated device longevity of greater than 7.6 years, which is the acceptable level of impact, as stated by the manufacturer. If the design margin of 10% was utilized according to the IEEE P485 standard, the new threshold would be at 7.2 years. Present, Katan and AES resulted in calculated device longevity of fewer than 7.6 years and greater than 7.2 years, indicating that they would be viable candidates for encryption if the IEEE standard design margin were followed. TEA, Hight, and Trivium all resulted in calculated device longevity of fewer than 7.2 years, meaning they would not be viable candidates even if the IEEE standard were utilized for the acceptance criterium. Trivium resulted in an impact that reduced device longevity to less than half the original value showing that this stream cipher contributed overhead is excessive.

Table 6

Device Longevity

No encryption	Present	TEA	HIGHT	Katan	AES	Trivium
8 Years	7.44	7.11	6.77	7.30	7.26	3.32
100%	93.00%	88.88%	84.63%	91.25%	90.75%	41.50%

One interesting aspect of this study was that the results were not entirely as predicted. The application of a stream cipher to the reference model was initially analyzed as not a good fit due to the expected overhead that the stream cipher format is not lightweight in nature. This characteristic was realized by the reduction in device longevity of approximately 58%, which was well above the acceptable design margin. AES, on the other hand, was expected to result in a much higher overhead than what was observed. This lower overhead can be attributed to its large block size compared to the other algorithms in the study. The overall results showed that due to the tight design constraints placed on the reference device by the manufacturer, none of the selected algorithms in the study met the design goal of less than 5% reduction in device longevity when the algorithm was applied.

Chapter Summary

Performing design science research on an existing platform by introducing an independent variable, the cryptographic algorithm, where there was not one previously allowed the researcher to observe the effects of such variables on the power consumption of the constrained device. In Chapter 5, this effect was applied, observed, and recorded, showing that while minimal in its design, the cryptographic algorithm can have a noticeable impact on constrained systems. Chapter 6 will include a discussion on how this research can be applied to the healthcare and medical device manufacturing fields, possible follow on research, and limitations encountered during the study.

CHAPTER SIX

The protection of electronic data, both in motion and at rest, is a priority of cybersecurity professionals. For data in motion, cryptographic algorithms are utilized to encrypt the plaintext message to protect its confidentiality (Harris & Maymi, 2018). For the healthcare industry and their patients, the protection of medical devices can mean the difference between life and death. As well, medical information retains its value to a malicious actor longer than credit card information (Leavitt, 2010). The problem addressed in this study was the lack of secure communications between medical implanted and wearable devices and their base stations (Freedman, 2015; Higgins, 2015; Newman, 2018). The purpose of this design science research was to examine the extent of power consumption of lightweight cryptographic algorithms and the effect on constrained medical device longevity through an experimental process.

Chapter 5 included the calculations and representation of the power consumption overhead due to the addition of cryptographic algorithms to a constrained device. This contribution was expected to show that the lightweight algorithms would provide minimal impact to battery-life while the full-size block and the selected stream ciphers would exceed the overhead tolerance of five percent as specified by the manufacturer. However, minimal effects on battery life with the addition of cryptography were not the case as all selected algorithms for this study exceed the set tolerance.

Limitations of Study Findings

As discussed in Chapter 1, limitations are variables in a research study that is out of the control of the researcher (Simon, 2011). The limitations for this research included the lack of published information for implantable cardioverter defibrillators, protection of intellectual property regarding device specifications, and a global pandemic that impacted manufacturer response time. The published data of the device used as the reference device included a sales pamphlet that includes capabilities, settings, voltages, and longevity of the implantable cardioverter defibrillator. However, neither this pamphlet nor any other source included the processor architecture, NAND switching power consumption, or message sizes. The manufacturer provided or confirmed initial assumptions about the reference device but would not provide specific details to protect the intellectual property.

To acquire this information and use it in this study, the researcher signed a Confidential Disclosure Agreement. This agreement prevents the disclosure of specifications that can lead to compromise of the device or disclosure of specifications that would compromise the intellectual property of the manufacturer. Additionally, the manufacturer requested that the company name and device name be withheld from the study for confidentiality reasons.

Interpretation of Study Findings

This study utilized calculations to identify the contribution or impact that the addition of a cryptographic algorithm to a platform that did not previously support would have on battery life and device longevity. A total of six cryptographic algorithms were selected that included four lightweight block ciphers, one standard block cipher, and one lightweight stream cipher. The initial assertion was that standard block ciphers and all stream ciphers would introduce excessive overhead on power consumption and were added for reference and support of this claim. The study findings illustrated that while the claim for the excess nature to power consumption for the stream cipher was proven by reducing battery life by more than half (58.5%), the standard block cipher had as little impact to battery life as did the lightweight block ciphers (9.25%). This illustrates that for these conditions, lighter is not always better.

The four lightweight block ciphers included in this study (Present, TEA, HIGHT, and Katan) reduced battery life by 7% to 17.37%. According to the IEEE P485 standard, a 10% design margin would have allowed Present and Katan to be introduced to the device without exceeding the design margin, while TEA and HIGHT would have exceeded the design margin. The manufacturer specified that only a 5% design margin was permitted, more restrictive than the IEEE standard. This resulted in all four of the lightweight block algorithms being deemed unsuitable for use.

The study findings illustrate that while there is a contribution in power consumption due to the addition of cryptographic algorithms, these contributions are kept to a minimum due to the periodicity with which they are utilized by the device. This is a manufacturing design constraint on the use of the cryptographic algorithm by the manufacturer to limit the impact to battery life and extend device longevity, according to the manufacturer. By limiting the frequency of transmission to once a quarter when the patient has follow-up visits with their doctor and minimizing the transmission size to only what is necessary, the manufacturer can limit the power consumption impact to the device. With that being the case, even with minimal frequency of transmissions that would utilize the cryptography, the power consumption was calculated to be more than the manufacturer allowed. In discussions with the manufacturer, it was noted that every design consideration is made to prolong battery life. The inclusion of a cryptographic algorithm would be contrary to that.

Practice Implications of Study Findings

This design science research study has proven several considerations for the manufacturing of constrained medical devices, such as implantable cardioverter-defibrillators. With the current battery technology that utilizes a lithium silver battery (Boriani, Merino, Wright, Gadler, Schaer, & Landolina, 2018), there is a limit to the storage capacity of an implanted medical device battery due to the design size limit (Mallela, Ilankumaran, & Rao, 2004). The average implantable cardioverter defibrillator is 2” x 2” x ¼” in size, and half of this volume is consumed by the battery (Mallela, Ilankumaran, & Rao, 2004). Lithium batteries of this size are limited to approximately 1W of capacity (Boriani et al., 2018). If the battery were larger to support increased longevity, the volume and weight of the device would increase, making it uncomfortable to the patient (Fornell, 2015). As well, current implanted medical device batteries cannot be recharged, so the device must be surgically replaced (Vintges, 2012). Adding additional overhead, such as cryptographic algorithms, will adversely impact battery longevity based on current implanted medical device design (Almenares et al., 2013). One major takeaway is that battery technologies for these devices must advance if a manufacturer wants to include the additional overhead of cryptography (Vintges, 2012). A second takeaway is that despite being classified as lightweight algorithms, the selected algorithms in this study contribute overhead that is still too costly of an impact on battery longevity. The manufacturer set a 5% limit on battery life, and all candidates in the research exceeded that threshold.

Recommendations for Further Research

Continued research of lightweight cryptographic algorithms is necessary to fill gaps for constrained devices. Constrained devices such as implanted medical devices present a unique challenge to cybersecurity professionals due to limited overhead tolerance and limited device serviceability (Bazzoli, 2016; Freedman, 2015; Grau, 2015). Cryptography does not have to be implemented in software (Harris & Maymi, 2016) but can be handled by hardware specifically designed for the task. These devices currently exist in server and workstation computers in the form of expansion cards or onboard chipsets (Brecht, 2015). However, these devices consume large amounts of power and can generate excessive amounts of heat (Batina et al., 2013). This makes them unsuitable for use in implanted medical devices (Ciurana, 2014). Additional design science research to miniaturize these devices, control their power consumption, and minimize their heat generation would be a persuasive topic to advance the protection of medical devices. Design science research concerning battery technologies or power scavenging technologies would benefit this area of study. Battery technology advancements to increase storage capacity while maintaining a small form factor will go a long way to support implanted medical devices. Recharging of these batteries through power scavenging or inductive charging technologies could provide a method to prolong device longevity and increase overhead tolerance for additional capabilities.

Encryption is not the only solution for the protection of data in motion. In large enterprise networks, the use of secure tunnels between sites provides a layer of protection to the data that traverses the link (Harris & Maymi, 2016). Secure tunnels use protocols to secure the communications between two sites, such as secure socket tunneling protocol (SSTP), point-to-point tunneling protocol (PPTP), and internet protocol security (IPSec; Harris & Maymi, 2016). The mechanism used to secure the communication path varies depending on the tunneling protocol. Power consumption for each protocol will vary, as well. Research on the use and power consumption of a tunneling protocol for constrained medical devices could present an alternative to the examined encryption solutions.

Conclusion

The research question proposed in this study was in two parts: how much power consumption can be attributed to a lightweight cryptographic algorithm in a constrained device and how much will the battery life be shorted by the introduction of a lightweight encryption algorithm? This design science research study analyzed power consumption contributions due to the addition to cryptographic algorithms to implanted medical devices that did not previously include cryptography. The results of this study calculated this contribution. They demonstrated that cryptography contributions to power consumption result in a higher than allowable impact to battery-life through a series of calculations. This study utilized calculations to determine the algorithm effects instead of direct measurements due to the lack of availability of the reference medical device.

The values of interest consisted of the battery capacity, device longevity, communication session frequency, message size per session, and power consumed per gate event within the reference device. These values were identified as 1 Ah battery capacity, 8-year device longevity, quarterly communication session frequency, 1,229,312-bit message size, and 77.7716 pAh per NAND gate event by the manufacturer, respectively. For the selected algorithms, the units of interest included the block size and the gate equivalence. These values varied for each algorithm and were listed in Table 1. The algorithms that were chosen to represent lightweight block ciphers consisted of Present, HIGHT, TEA, and Katan. As well, AES, a standard block cipher, was included for reference to evaluate if lightweight algorithms were lower on power consumption than a standard block cipher. Trivium, a lightweight stream cipher, was included for comparison.

A series of calculations were performed on each algorithm. These equations were used to determine the power consumption and new device longevity of the reference device when applying the algorithms. The initial device longevity was determined to be 8 years by the manufacturer's published data and confirmed with the manufacturer during a phone conversation. The calculated new device longevity was shown in Table 6. The results illustrated that at the current battery capacity of 1 Ah, the calculated device longevity dropped to between 7.44 years and 6.77 years for the lightweight block ciphers, AES calculated device longevity was at 7.26 years. Trivium reduced device longevity to 3.32 years. The manufacturer dictated a 5% reduction in device longevity limit, which results in 7.6 years. The conclusion is that, of the selected algorithms for the given reference device, none of the algorithms in this study were deemed viable solutions without causing an unacceptable impact on device longevity.

Two hypotheses were presented, along with their null. Hypothesis $H1_0$ stated lightweight cryptographic algorithms would not reduce the constrained system's battery life to an unacceptable level. This hypothesis was proven false due to the reference device's battery-life was calculated to fall below the acceptable level, as stated by the manufacturer. The null hypothesis was accepted that battery-life was reduced to an unacceptable level. Hypothesis $H2_0$ stated lightweight algorithms consume power to the extent that will not adversely affect device battery-life of a constrained device, similar to traditional cryptographic algorithms. This hypothesis was proven false with the demonstration that AES, a full-size cryptographic algorithm, was calculated to consume only 2.25% more power than the Present algorithm and 6.12% less than the HIGHT algorithm placing it in the middle of the selected algorithms for power consumption.

The current body of literature contains a gap that this study was intended to address; the effects of applying a cryptographic algorithm to a constrained medical device that currently does not incorporate cryptography. The United States Food and Drug Agency (FDA) has issued advisories to medical device manufacturers stating the importance of adding cryptography to protect the patient and their data (FDA, 2016c) and the need for firmware updates to address vulnerabilities (FDA, 2017). Journal articles have discussed the need for cryptography in medical devices (Angle, 2016; Bazzoli, 2016; Deloitte, 2013; Freedman, 2015; Fu & Blum, 2013), as well as what the characteristics these algorithms should possess to minimize the impact on medical device resources (Batina et al., 2013). Several articles have been written that align the use of lightweight algorithms in constrained devices such as RFID cards (Mojtaba et al., 2013; Lohmann et al., 2006) and sensor networks (Ameen et al., 2012; Ali et al., 2013), but not medical devices.

This study presented four crucial takeaways. First, for the given battery capacity, the addition of a cryptographic algorithm presents excessive overhead. If the battery capacity were increased, then the effects would be less impactful. Second, lightweight cryptographic algorithms are classified as lightweight because they use smaller keys or block sizes, but this does not translate to less power consumption. Third, current studies and publications are lacking on the topic of cryptography applied to medical implanted devices. Lastly, the need for cryptography is one of protection; both for the patient and the healthcare provider. This protection cannot come at a risk to the patient by decreasing the medical device longevity, performance, or reliability.

REFERENCES

Adam, H. M. (n.d.). Research population. Retrieved from https://www.academia.edu/5563491/Research_Population

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93-101. doi:10.1007/s10916-010-9449-4

Ali, S. T., Sivaraman, V., Ostry, D., & Jha, S. (2013). *Securing data provenance in body area networks using lightweight wireless link fingerprints*. Paper presented at the Proceedings of the 3rd international workshop on Trustworthy embedded devices, Berlin, Germany. http://citeseerx.ist.psu.edu/viewdoc/download?doi:10.1.1.677.7663&rep=rep1&type=pdf

Alioto, M., & Palumbo, G. (2002). NAND/NORAdiabatic gates: Power consumption evaluation and comparison versus the fan-In. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, 9*.

Alizadeh, M., Hassan, W. H., Zamani, M., Karamizadeh, S., & Ghazizadeh, E. (2013). Implementation and evaluation of lightweight encryption algorithms suitable for RFID. *Journal of Next Generation Information Technology, 4,* 13.

Almenares, F., Arias, P., Marin, A., Diaz-Sanchez, D., & Sanchez, R. (2013). Overhead of using secure wireless communications in mobile computing. *IEEE Transactions on Consumer Electronics, 59*(2), 335-342. doi:10.1109/TCE.2013.6531115

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Li, X. (2015). Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems. *Journal of Medical Systems, 39*(11), 140. doi:10.1007/s10916-015-0318-z

Angle, J. (2016). Medical devices: Managing the risk. *National Cybersecurity Institute Journal*, 31-37.

Arbit, A., Livne, Y., Oren, Y., & Wool, A. (2015). Implementing public-key cryptography on passive RFID tags is practical. *International Journal of Information Security, 14*, 85-99. doi:10.1007/s10207-014-0236-y

Armknecht, F., & Mikhalev, V. (2015). *On lightweight stream ciphers with shorter internal states.* Paper presented at the International Workshop on Fast Software Encryption, Berlin, Heidelberg.

Aydin, O. M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal of Medical Systems, 37*(6), 9984. doi:10.1007/s10916-013-9984-x

Bansod, G., Pisharoty, N., & Patil, A. (2017). BORON: an ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology & Electronic Engineering, 18*(3), 317-331. doi:10.1631/FITEE.1500415

Batina, L., Das, A., Ege, B., Kavun, E. B., Mentens, N., Paar, C., . . . Yalcın, T. (2013, 2013). Dietary recommendations for lightweight block ciphers: Power, energy and area analysis of recently developed architectures. Retrieved from https://www.esat.kuleuven.be/cosic/publications/article-2341.pdf

Batra, I., Luhach, A. K., & Pathak, N. (2016). *Research and analysis of lightweight cryptographic solutions for internet of things*. Paper presented at the Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India. https://dl.acm.org/doi/10.1145/2905055.2905229

Bazzoli, F. (2016). Medical device dangers: Little progress in plugging security gaps, even as hackers threaten. *Health Data Management, 24*(7), 20-23.

Berhanu, Y., Abie, H., & Hamdi, M. (2013). *A testbed for adaptive security for IoT in eHealth*. Paper presented at the Proceedings of the International Workshop on Adaptive Security, Zurich, Switzerland. https://dl.acm.org/doi/abs/10.1145/2523501.2523506

Bi, Y., Shamsi, K., Yuan, J.-S., & Jin, Y. (2016). More than moore in security: Emerging device based low-power differentiate power analysis countermeasures. *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-16)*, 467-470.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., . . . Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. Retrieved from http://www.lightweightcrypto.org/present/present_ches2007.pdf

Boriani, G., Merino, J., Wright, D. J., Gadler, F., Schaer, B., & Landolina, M. (2018). Battery longevity of implantable cardioverter-defibrillators and cardiac resynchronization therapy defibrillators: technical, clinical and economic aspects. An expert review paper from EHRA. *European Society of Cardiology, 20*, 16.

Brecht, D. (2015). Tales from the Crypt: Hardware vs. Software. *Infosecurity*.

Bryman, A. (2006). Integrating quantitative and qualitative research: how is it done? *Qualitative Research*, *6*(1), 17.

Buchanan, W. J., Li, S., & Asif, R. (2018). Lightweight cryptography methods. *Journal of Cyber Security Technology, 1*, 187-201. https://doi.org/10.1080/23742917.2017.1384917

Camara, C., Peris-Lopez, P., & E.Tapiador, J. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics, 55*, 18. https://doi.org/10.1016/j.jbi.2015.04.007

Canni`ere, C. D., & Preneel, B. (2012). Trivium specifications. *ECRYPT: eSTREAM Portfolio*. Retrieved from https://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf

Choi, K., Kim, M., & Chae, K. (2013). Secure and lightweight key distribution with ZigBee Pro for ubiquitous sSensor networks. *International Journal of Distributed Sensor Networks, 9*(7), 608380. doi:10.1155/2013/608380

CIRT. (n.d.). Sampling methods. Retrieved from https://cirt.gcu.edu/research/developmentresources/research_ready/quantresearch/sample_meth

Ciurana, J. (2014). Designing, prototyping and manufacturing medical devices: an overview. *International Journal of Computer Integrated Manufacturing*, 901-918.

Crain, J. A., & Bratus, S. (2015). Bolt-on security extensions for industrial control system protocols: A case study of DNP3 SAv5. *IEEE Security & Privacy, 13*(3), 74-79. doi:10.1109/MSP.2015.47

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Los Angeles: Sage.

Deloitte. (2013). Networked medical device cybersecurity and patient safety. Retrieved from http://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/center-for-health-solutions-networked-medical-device-cybersecurity-and-patient-safety.html

Dementyev, A., Hodges, S., Taylor, S., & Smith, J. (2013). Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. *Wireless Symposium (IWS), 2013 IEEE International*, 1-4.

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. (2010). *Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA. http://dmrussell.net/CHI2010/docs/p917.pdf

DHS. (2012). *The Menlo Report: Ethical principles guiding information and communication technology research*. Retrieved from https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

Dudovskiy, J. (2019). Research reliability. Retrieved from https://research-methodology.net/research-methodology/reliability-validity-and-repeatability/research-reliability/

FDA, U. S. (2016a). *Postmarket management of cybersecurity in medical devices* Retrieved from https://www.fda.gov/media/95862/download.

FDA, U. S. (2016b). *Cybersecurity*. Retrieved from http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

FDA, U. S. (2016c). *FDA outlines cybersecurity recommendations for medical device manufacturers*. Retrieved from http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm.

FDA, U. S. (2017). *Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers: FDA safety communication*. Retrieved from https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals.

FDA, U. S. (2019). *Cybersecurity vulnerabilities affecting Medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication*. Retrieved from https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm633960.htm.

Feng, D., Jiang, C., Lim, G., Cimini, L. J., Feng, G., & Li, G. Y. (2012). A survey of energy-efficient wireless communications. *IEEE Communications Surveys & Tutorials*, 167-178.

Ferrigno, L., Marano, S., Paciello, V., & Pietrosanto, A. (2005, 18-20 July 2005). *Balancing computational and transmission power consumption in wireless image sensor networks.* Paper presented at the IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems, 2005.

Fornell, D. (2015). Advances in Implantable Cardioverter Defibrillator Technology. *Diagnostic and Interventional Cardiology*.

Freedman, A. (2015). Implantable devices: Medical devices open to cyber threats. Retrieved from http://www.riskandinsurance.com/implantable-devices-medical-devices-open-to-cyber-threats/

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 35-37.

Goedert, J. (2016). Multitude of medical devices pose hacking threats for providers. *Health Data Management*.

Gonçalves Fontes, E. L., & José Balloni, A. (2007). Security In information systems: Sociotechnical aspects. In T. Sobh (Ed.), *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering* (pp. 163-166). Dordrecht: Springer Netherlands.

Good, T., & Benaissa, M. (n.d.). Hardware performance of eStream phase-III stream cipher candidates. Retrieved from https://www.ecrypt.eu.org/stream/docs/hardware.pdf

Grau, A. (2014). Security requirements for medical device--What's really needed? *Medical Design News*.

Grau, A. (2015). Securing medical devices, solving the challenge of the weakest link. *ECN*.

Halperin, D., Clark, S. S., Fu, K., Heydt-Benjamin, T. S., Defend, B., Kohno, T., . . . Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. Retrieved from https://www.secure-medicine.org/hubfs/public/publications/icd-study.pdf

Harris, S., & Maymí, F. (2018). *CISSP all-in-one exam guide, Eighth edition*. New York: McGraw-Hill Education.

Hathaway, R. (1995). Assumptions underlying quantitative and qualitative research: Implications for institutional research. *Research in Higher Education, 36*, 28.

Hawrylak, P. J., Schimke, N., Hale, J., & Papa, M. (2012). Security risks associated with radio frequency identification in medical environments. *Journal of Medical Systems, 36*.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information system research. *MIS*, *28*(1), 32.

HHS. (2016). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. Retrieved from https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Higgins, K. J. (2015). Hospital medical devices used as weapons In cyberattacks. Retrieved from http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.-S., . . . Chee, S. (2006). *HIGHT: A new block cipher suitable for low-resource device*. Paper presented at the International Association for Cryptologic Research. https://link.springer.com/content/pdf/10.1007%2F11894063_4.pdf

Hope, C. (2018, 11/13/2018). Instruction set. *Computer Hope*. Retrieved from https://www.computerhope.com/jargon/i/instset.htm

IEEE. (2011). 485-2010 - IEEE recommended practice for sizing lead-acid batteries for stationary applications. Retrieved from https://ieeexplore.ieee.org/document/5751584

Igure, V. M., Laughter, S. A., Williams, R. D., & Brown, C. L. (2006). Security issues in SCADA networks. *Computers & Security*, 498-506.

Iosifidis, E., & Limniotis, K. (2016). *A study of lightweight block ciphers in TLS: The case of Speck*. Paper presented at the Proceedings of the 20th Pan-Hellenic Conference on Informatics, Patras, Greece. https://dl.acm.org/doi/10.1145/3003733.3003794

Jones, R. W., & Katzis, K. (2017). Cybersecurity and the medical device product development lifecycle. *ICIMTH*.

Kerckhof, S., Durvaux, F., Hocquet, C., Bol, D., & Standaert, F.-X. (2012). *Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint*. Paper presented at the 14th international conference on Cryptographic Hardware and Embedded Systems, Belgium.

Kloffler, D., & Shaw, A. (2013). Dick Cheney feared assassination via medical device hacking: 'I was aware of the danger'. Retrieved from http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance. *PLoS ONE, 7*(7), 7. https://doi.org/10.1371/journal.pone.0040200

Landsiedel, O., Wehrle, K., & Gotz, S. (2005). Accurate prediction of power consumption in sensor networks. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi:10.1.1.112.6036&rep=rep1&type=pdf

Leavitt, N. (2010). Researchers fight to keep implanted medical devices safe from hackers. Retrieved from https://www.hh.se/download/18.3e02b8a112e11a6f45a8000589/1341267677424/5+Security+in+Embedded+Computing.pdf

Lohmann, T., Schneider, M., & Ruland, C. (2006). Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags *International Federation for Information Processing*, 278–288.

Maisel, W. H., Paulsen, J. E., Hazelett, M. B., & Selzman, K. A. (2018). Striking the right balance when addressing cybersecurity vulnerabilities. *Heart Rythm, 15*(7), 2. https://doi.org/10.1016/j.hrthm.2018.05.002

Malhotra, K., Gardner, S., & Patz, R. (2007). *Implementation of elliptic-curve cryptography on mobile healthcare devices.* Paper presented at the Proceedings of the 2007 IEEE International Conference on Networking, Sensing and Control, London.

Mallela, V. S., Ilankumaran, V., & Rao, N. S. (2004). Trends in Cardiac Pacemaker Batteries. *Indian Pacing Electrophysiol Journal*, 4(4), 12.

Manjulata, A. K. (2014). Survey on lightweight primitives and protocols for RFID in wireless sensor networks. *International Journal of Communication Networks and Information Security, 6*, 29-43.

Manolis, A. S., Maounis, T., Koulouris, S., & Vassilikos, V. (2017). “Real life” longevity of implantable cardioverter-defibrillator devices. *Clinical Cardiology, 40*(9), 6.

Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications, 8*(6), 7.

McKay, K. A., Bassham, L., Turan, M. S., & Mouha, N. (2016). *Report on lightweight cryptography*. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

Medina, L. A. (2013). Supporting medical device development: a standard product design process model. *Journal of Engineering Design*, *24*(2), 83-119.

Mikhaylov, K., & Tervonen, J. (2010). *Optimization of microcontroller hardware parameters for Wireless Sensor Network node power consumption and lifetime improvement*: IEEE.

MITRE. (2019a). CVE-2019-6538 *National Vulnerability Database.* Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2019-6538

MITRE. (2019b). CVE-2019-6540. *National Vulnerability Database.* Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2019-6540

Monaco, A. (2012). Keeping hackers out of implanted medical devices. Retrieved from http://theinstitute.ieee.org/technology-focus/technology-topic/keeping-hackers-out-of-implanted-medical-devices

Mushtaq, M. F., Jamel, S., Disina, A. H., A.Pindar, Z., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications, 8*(11), 12.

Newman, L. H. (2018). A new pacemaker hack puts malware directly on the device. Retrieved from https://www.wired.com/story/pacemaker-hack-malware-black-hat/?verso=true

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, 418-436.

Padmanabhan, P. (2017). A major medical device maker's unique approach to data security. *CIO*.

Pannucci, C. J., & Wilkins, E. G. (2011). Identifying and avoiding bias in research. *Plastic and reconstructive surgery, 126*(2).

Paul, N., Kohno, T., & Klonoff, D. C. (2011). A review of the security of insulin pump infusion systems. *Journal of Diabetes Science and Technology, 5*(6), 6.

Pell_Institute. (2020). Determine appropriate sample size. Retrieved from http://toolkit.pellinstitute.org/evaluation-guide/collect-data/determine-appropriate-sample-size/

Peng, C., Du, X., Li, K., & Li, M. (2016). An ultra-lightweight encryption scheme in underwater acoustic networks. *Journal of Sensors, 2016*, 10. doi:10.1155/2016/8763528

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2003). *Analyzing the energy consumption of security protocols*. Paper presented at the Proceedings of the 2003 international symposium on Low power electronics and design, Seoul, Korea. https://dl.acm.org/citation.cfm?id=871518

Prasithsangaree, P., & Krishnamurthy, P. (2003). *Analysis of energy consumption of RC4 and AES algorithms in wireless LANs.* Paper presented at the GLOBECOM '03. IEEE Global Telecommunications Conference (IEEE Cat. No.03CH37489).

RajaSekhar, M., & Reddy, P. S. (2015). Modelling and design solutions for NANO- CMOS using predictive technology. *International Journal of Engineering and Technical Research (IJETR), 3*(6), 3.

Ransford, B., Kramer, D. B., Foo Kune, D., Auto de Medeiros, J., Yan, C., Xu, W., . . . Fu, K. (2017). Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing And Clinical Electrophysiology: PACE, 40*(8), 913-917. doi:10.1111/pace.13102

Rolfes, C., Poschmann, A., Leander, G., & Paar, C. (2008a). *Security for 1000 gate equivalents*. Retrieved from https://pdfs.semanticscholar.org/8a06/a4ad4efe60f3a9c9640fa82b5b1ccde7caa6.pdf

Rolfes, C., Poschmann, A., Leander, G., & Paar, C. (2008b). *Ultra-lightweight implementations for smart devices – Security for 1000 gate equivalents*. Paper presented at the Smart Card Research and Advanced Applications, Berlin, Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-540-85893-5_7.pdf

Rupp, A., Baldimtsi, F., HinterwΣlder, G., & Paar, C. (2015). Cryptographic theory meets practice: Efficient and privacy-preserving payments for public transport. *ACM Trans. Inf. Syst. Secur., 17*(3), 1-31. doi:10.1145/2699904

Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014, 18-21 May 2014). *SoK: Security and privacy in implantable medical devices and body area networks.* Paper presented at the 2014 IEEE Symposium on Security and Privacy.

Shah, A., & Engineer, M. (2019). *A survey of lightweight cryptographic algorithms for IoT-based applications*. Paper presented at the Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing, Singapore. https://www.researchgate.net/profile/Ankit_Shah37/publication/329072888_A_Survey_of_Lightweight_Cryptographic_Algorithms_for_IoT-Based_Applications_Proceedings_of_ICSICCS-2018/links/5c4f029c458515a4c745e441/A-Survey-of-Lightweight-Cryptographic-Algorithms-for-IoT-Based-Applications-Proceedings-of-ICSICCS-2018.pdf

Simon, M. (2011). *Dissertation and scholarly research: Recipes for success*. Seattle: Dissertation Success, LLC.

Suresh, P., Daniel, J. V., V.Parthasarathy, & Aswathy, R. H. (2014). *A state of the art review on the Internet of Things (IoT)* Paper presented at the International Conference on Science, Engineering and Management Research.

Tawalbeh, H., Hashish, S., Tawalbeh, L., & Aldairi, A. (2017). Security in wireless sensor networks using lightweight cryptography. *Journal of Information Assurance and Security, 12*, 118-123.

Texas_Instruments. (1997). CMOS power consumption and Cpd calculation. Retrieved from http://www.ti.com/lit/an/scaa035b/scaa035b.pdf

TrapX_Labs. (2015). *Anatomy of an attack: Medjack [medical device hijack]*. Retrieved from http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf?aliId=1006644

Verizon. (2019). Insider threat report. *Insider Threat.* Retrieved from https://enterprise.verizon.com/resources/reports/insider-threat-report/

Vishnupriya, T. H., & Vareed, J. (2018, 20-21 April 2018). *Cryptographic method to provide confidentiality and integrity in implantable medical devices.* Paper presented at the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT).

Webster. (n.d.). Research methods. Retrieved from http://faculty.webster.edu/woolflm/statmethods.html

Wheeler, D. J., & Needham, R. M. (n.d.). TEA, a tiny encryption algorithm. Retrieved from https://www.movable-type.co.uk/scripts/tea.pdf

Wieringa, R. J. (2016). Design science research methods and writing research papers. Retrieved from https://wwwhome.ewi.utwente.nl/~roelw/DSM180minutes.pdf

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.), 8*, 305-316. doi:10.2147/MDER.S50048

Wu, F., & Eagles, S. (2016). Cybersecurity for medical device manufacturers: Ensuring safety and functionality. *Biomedical Instrumentation & Technology, 50*(1), 12.

Wu, L., Zhang, Y., Li, L., & Shen, J. (2016). Efficient and anonymous authentication scheme for wireless body area networks. *Journal of Medical Systems, 40*(134), 13.

Yadav, A. (2014). Power consumption at circuit or logic level in circuit. Retrieved from https://www.slideshare.net/AnilYadav55/power-estimation-by-anil-kr-yadav?from_action=save

Yan, L., Chang, Y., & Zhang, S. (2017). A lightweight authentication and key agreement scheme for smart grid. *International Journal of Distributed Sensor Networks, 13*(2), 1550147717694173. doi:10.1177/1550147717694173

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 15.

Zhang, M., Raghunathan, A., & Jha, N. K. (2013). MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Transactions on Biomedical Circuits and Systems*, *7*(6), 871-881. doi:10.1109/TBCAS.2013.2245664

Zheng, G., Fang, G., Shankaran, R., & Orgun, M. A. (2015). Encryption for implantable medical devices using modified one-time pads. *IEEE Access, 3*, 825-836. doi:10.1109/ACCESS.2015.2445336