Summer 7-5-2016

EVALUATING THE CYBER SECURITY IN THE INTERNET OF THINGS: SMART HOME VULNERABILITIES

Timothy Matthew McGee
United States Military Academy, timothy.mcgee@westpoint.edu

EVALUATING THE CYBER SECURITY IN THE INTERNET OF THINGS: SMART HOME VULNERABILITIES

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

By

Timothy Matthew McGee

Colorado Technical University

June, 2016

Committee

Cynthia Calongne, D.CS, Chair

Bo Sanden, Ph.D., Committee Member

Richard Livingood, Ph.D., Committee Member

5 July 2016

Abstract

The need for advanced cyber security measures and strategies is attributed to modern sophistications of cyber-attacks and intense media attention when attacks and breaches occur. In May 2014, a congressional report suggested that Americans used approximately 500 million Internet-capable devices at home, including, but not limited to Smartphones, tablets, and other Internet-connected devices, which run various unimpeded applications. Owing to this high level of connectivity, our home environment is not immune to the cyber-attack paradigm; rather, the home has evolved to become one of the most influenced markets where the Internet of Things has had extensive surfaces, vectors for attacks, and unanswered security concerns. Thus, the aim of the present research was to investigate behavioral heuristics of the Internet of Things by adopting an exploratory multiple case study approach. A controlled Internet of Things ecosystem was constructed consisting of real-life data observed during a typical life cycle of initial configuration and average use. The information obtained during the course of this study involved the systematic acquisition and analysis of Smart Home ecosystem link-layer protocol data units (PDUs). The methodology employed during this study involved a recursive multiple case study evaluation of the Smart Home ecosystem data-link layer PDUs and aligned the case studies to the existing Intrusion Kill Chain design model. The proposed solution emerging from the case studies builds the appropriate data collection template while concurrently developing a Security as a Service (SECaaS) capability to evaluate collected results.

Keywords: Internet of Things (IoT) Security, Internet of Everything (IoE), Smart Home Security, Smart Home Security Solutions.

Dedication

This study is dedicated to my daughters Leala and Ayan McGee. You remain my motivation in life as you traverse the obstacles life puts in your way. I am grateful for your time, your belief in me, and the unconditional love you have shared as we complete this and many other journeys together. Let this journey represent an area that is possible in your futures, should you so desire.

Acknowledgements

The thought process and the execution of this study necessitated long-term planning and development of tools capable of operating in environments with which I was not always accustomed. Thus, I wish to thank all who have helped me along this journey with revisions, ideas, and the build of the lab. Daniel Poulin volunteered his time to help develop the lab for the Smart Home ecosystem and ensured that the configuration of tools met the requirements of this study. My family has also been a tremendous support structure throughout this endeavor. A special thanks goes to my father, Marvin McGee for dedicating his time to my work and for providing clarity when my thoughts were disarrayed. Thank you dad, and I hope to continue your passion for education in the years to come. To Dr. Cynthia Calongne, I am extremely grateful for the help and guidance you have provided me since 2012. You have been with me from the beginning of my journey and finally to Colorado. Thank you, and I wish you continued success in your career.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

As our world becomes increasingly interconnected, cyber security is expected to increase in prominence. High prevalence of Internet-connected devices has rendered many individuals vulnerable to breaches due to cyber-attacks. The latest generation of electronic devices labeled "smart devices," have increased our abilities to connect to the Internet and this drive is promoted as a means of making life easier and more efficient for the device's owner. Yet, this presumed higher quality of life comes with a trade-off, as it exposes us to significant risks because personal data can be stolen or misappropriated, causing a multitude of problems for the device owner. In particular, the rapid technological advances have not been matched with increased cyber security for the Internet of Things (IoT) devices. The IoT security lag creates an imbalance between technology and available security to satisfy the demands of the current technology. Researchers in the field of IoT note that the current security applications do not consider the advancement of technology or new technology use (Demblewski, 2015). Therefore, as the overall security framework lacks the capability to meet the current demand, millions of private and public individuals, as well as companies, are at risk of invasion or data theft. Such breaches can have adverse financial, economic, and physical consequences. The goal of security frameworks is to identify future security concerns as a means of ensuring that devices are consistently and adequately protected (Demblewski, 2015). In light of the rapidly increasing scope and severity of security threats, future

security structures and IoT security solutions need to be developed dynamically, so that they can evolve to respond to future changes and demands.

Background

Due to the misalignment between rapid technological advances and available security measures, cyberspace has gained national focus and has become increasingly insecure over the past twenty-five years (Mandt, 2015). The chronic lack of security is attributed to the incongruence with which technological advancement are implemented into the devices and services and the corresponding security measures, allowing greater opportunities for attackers to take advantage of the resulting vulnerabilities. Thus, despite the advancements in both technology and security, cybercriminals are still able to manipulate the available technology to meet their needs, resulting in a stalemate between the two sides. Moreover, the "weaker" technologies are more likely to be hacked and breached, allowing attackers to take control of lateral and more secure systems. Attackers are also able to steal/misappropriate data, and cause a variety of damages, not only to the technology and all related components, but to the owner as well, through libel, slander, threats, loss of data, theft, and other risks. In order to mitigate these risks, differing defensive strategies are being developed by cyberspace professionals. These defensive measures are designed to meet the increases in technological vulnerabilities and influence the overall security posture of the emergent technologies. The resulting efforts will make it harder for attackers to access the information within the technology as well as control the technology remotely through unauthorized access. In these initiatives, particular emphasis has been given to cyber-threat intelligence. This information suggests that knowledge must holistically align with the relevant technology's

functionality and its vulnerabilities, as well as viable means of protection. However, efforts made in this domain have yet to yield desirable outcomes, due to the rapid pace of technological advancement (Mandt, 2015). As a result, until technology and security advancements fully align, it is impossible to obtain accurate intelligence based on which vulnerabilities can be detected and evaluated.

Smart technology is also immature, as the current trends in smart technology encompass rapid technological advances. Thus, although smart technology is used by many individuals, it has not yet become conventional and lacks prominent market presence. However, smart technology use is expected to expand tremendously until 2020 (R. Brown, 2015). Although security measures are currently in place, they are not necessarily strong enough to withstand the constant onslaught of the data transmittal that occurs, with exponentially growing nodes always connecting to the Internet (R. Brown, 2015). This increased throughput and growing population of nodes suggest that greater opportunities will exponentially emerge with problems concerning the data organic to smart technology. For example, data can be obtained intentionally or unintentionally without authorization. Smart technological data can serve a more nefarious purpose, subsequently causing a myriad of problems for the data holder. Therefore, it is necessary to ensure that consumers are aware of smart technology vulnerabilities and threats. Being conscious of and resolving the vulnerabilities and threats related to smart technology can be beneficial in the effort to eliminate cyber-crime and reduce the number of cyber-attacks on data comprehensively.

Problem Opportunity Statement

Innovative trends in technology are common occurrence and help advance its usage. For example, cell phones that were once large and clunky have been gradually redesigned as their usage became more prevalent, and are now small and compact. The evolution of telephones has also seen similar trends. As communications evolved beyond wired applications, cordless devices with much longer ranges became available, and many individuals now use the Internet rather than conventional telephone systems. Similarly, vehicles used to be powered by combustion engine and required frequent refueling at petrol stations. Now, it is possible to purchase vehicles that utilize a hybrid of electricity and fuel, allowing the driver to travel further before having to refuel or recharge. On a grander scale, not so long ago, it was impossible to fly across the country; yet, NASA has put a spaceship on the Moon. Thus, limitations are being overcome with advances in science and technology, which are driven by the desire to meet new needs and new demands. In the early 2000s, the Windows phone was in trend, to be replaced by Android, eventually leading to the iPhone. In computers, it was once inconceivable that virtually everyone in the developed world would have a personal computer (PC), yet now most of us have a laptop, as well as a notebook, a netbook, and/or tablets. As this trend shows, devices are getting smaller, faster, and smarter. Most devices can now connect to the Internet without the use of a PC. Amidst all these advancements, security requirements have also increased. However, security improvements have not changed at an equally rapid pace to meet the needs of the technology users. Therefore, smart technology presents increased opportunities for cyber-attacks due to the shortcomings of the currently available security measures. In line with the above, the problem statement

for this study is that consumers are not necessarily aware of vulnerabilities associated with IoT devices despite regularly purchasing smart technology (King, 2015).

Purpose Statement

The purpose of this qualitative exploratory research was to investigate Smart Home technological vulnerabilities within a real life context of the IoT typical usage applications and to characterize this average usage in relation to acceptable and nefarious data behaviors. The contrasted data behavior was subsequently used to illuminate anomalous data link traffic and payloads. Finally, data was collected through measuring Smart Home technology communications in a controlled environment. Current data shows that Smart Home technology owners are not aware of the dangers they face, nor are they cognizant of the extent to which the risks they face stem from ubiquitous technological vulnerabilities (Lemos, 2015). The information obtained in this study involves the systematic acquisition and analysis of Smart Home ecosystem link-layer protocol data units (PDUs).

Research Questions

The present investigation focused on broadening consumer awareness of the security threats and privacy concerns associated with conventional Smart Home web-enabled devices. Thus, as a part of this study, information pertaining to the background of security threats concerning Smart Home technology was obtained through extensive literature review. Therefore, the research questions (RQs) were developed in the context of propositions and were aligned to explore Smart Home technology vulnerabilities and threats. Based on the background information, the following research questions were developed:

RQ1. How secure are Smart Home technology IoT systems, independently?

RQ2. What behavioral data exchange or aggregate device communication occurs between Smart Home objects that effect fundamental security levels?

RQ3. What are the emergent security issues related to Smart Home object behavior that affects personal safety relating to cyber security, resilience to cyber threats, and personally identifiable information from the collection of object usage data?

Propositions

Based on the background information, problem opportunity statement, purpose statement, and research questions, the following propositions can help direct the qualitative focus of the research:

1. It is proposed that Smart Home technology IoT systems are secure only insofar as their owners enable security for these devices, as to be explored given the results of RQ1.

2. It is proposed that Smart Home ecosystem behavioral data exchanges and aggregate communications result in security vulnerabilities, as to be explored given the results of RQ2.

3. It is proposed that confidential information, personally identifiable information, and personal safety are inadequately protected in Smart Home ecosystems, as to be explored given the results of RQ3.

Independent IoT Security. RQ1 is formulated to focus on device-specific Smart Home technology IoT systems for discovering separate areas of vulnerabilities. Independent vulnerabilities stem from isolated devices that are subject to improper configurations, targeted attacks, and unintentional misnomers. Activities of this nature

are often mitigated to an acceptable level through vendor specific remedies though untimely mitigations may pose a residual vulnerability.

Behavioral Heuristics of Aggregated Devices. RQ2 is formulated to focus on inter-device communications that pose vulnerabilities due to a lack of vendor standards. The time associated with remedies which combat aggregate device vulnerabilities is subject to the interests of proprietary market leaders. To foundationally understand sound levels of communication security, vendors typically defer to international security standards to which products must adhere. In this research area, it is established that residual vulnerabilities persist due to a lack of standards and/or noncompliance.

Security of the IoT. RQ3 is formulated to distinguish among three distinct security categories—personal safety, personal cyber security, and personally identifiable information. All three relate to the vulnerabilities at the intersection of the physical domain, the Internet domain, and the Smart Home technology domain (see Figure 1). Within each independent domain, the intersection depicts the device categories that emerge as capabilities shared between the adjacent domains. For example, the single-state devices reside at the intersection of the physical and the Smart Home technology domains, as these require physical proximity to Smart Home technology device to influence personal safety. At the intersection between the physical and the Internet domains reside control platforms, which require external mitigations to address personal cyber security concerns. Finally, multi-state devices with sensory data reside at the intersection of the Smart Home technology and the Internet domains, given that these require advanced external and internal mitigations to address personal cyber security, and

personally identifiable information security concerns. Hence, the IoT capabilities emerge at the intersection of all three domains.

Conceptual Framework

Within organizations, IoT use is expected to increase. Researchers and practitioners perceive IoT as an integrated global network with the constant transmission of information of connection-oriented devices (Boos, Guenter, Grote, & Kinder, 2013; Sundmaeker, Guillemin, Friess, & Woelfflé, 2010). Therefore, the use of Smart Home technology is based on the constant transmittal of data via an integrated global ecosystem. At the same time, threats and vulnerabilities implicit in Smart Home technologies can be examined through human control theories and field theories, which pertain to external and internal threats, respectively (Kalika, Pallud, & Elie-Dit-Cosaque, 2011). The conceptual framework adopted in the present study derives from theoretical perspectives. The major components of this study are physical, the Internet, and Smart Home technology that, while distinct, also overlap. For example, the physical domain overlaps with the Internet due to control platforms, as well as with Smart Home technology due to single-state devices. At the same time, the Internet overlaps with Smart Home technology due to multi-state devices with sensory data. Finally, physical, the Internet, and Smart Home technology domains overlap due to IoT, as shown in Figure 1.

Figure 1. Conceptual Framework.

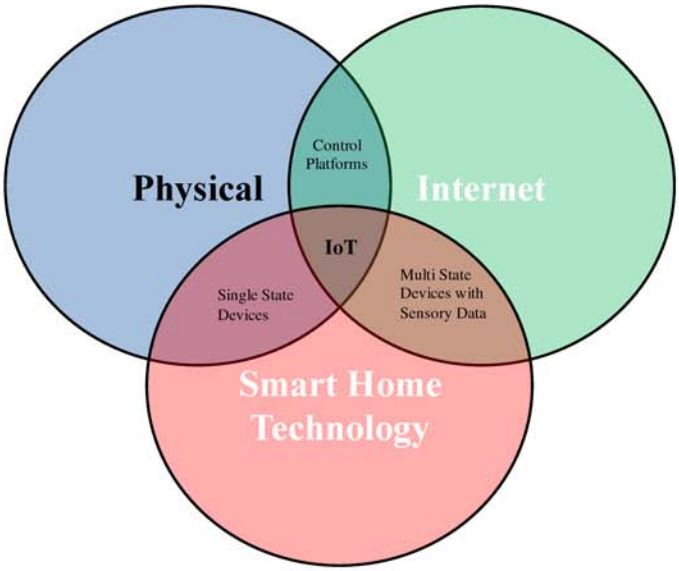

Figure 1. Conceptual Framework. From *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*, paper presented at the European Union Agency for Network and Information Security, by D. Barnard-Wills, Marinos, and Portesi (2014)

Intrusion Kill Chain

The approach to network-based attacks on IoT devices adopted in the present study follows the Lockheed Martin Computer Incident Response Team's (LM-CIRT) adversary focused cyber intrusion process model, "Intrusion Kill Chain" (Hutchins, Cloppert, & Amin, 2011), as shown in Table 1. The Intrusion Kill Chain is an approach that combats specific adversaries by aligning United States Cyber intelligence resources against each phase of the Intrusion Kill Chain. The present study explores the appropriateness of the IoT's relation to the Intrusion Kill Chain during the conduct of RQ3 and the cross case study summarization.

Table 1

Case Study Categorization Analysis; adapted from "Intrusion Kill Chain" (Hutchins et al., 2011)

Phase	Description	Case Study (CS)
Reconnaissance	Research, identification, and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.	CS 1
Weaponization	Coupling a remote access trojan with an exploit into a deliverable payload, typically using an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.	CS 1
Delivery	Transmission of the weapon to the targeted environment.	CS 2
Exploitation	After the weapon is delivered to victim host, exploitation triggers intruders' code	CS 2
Installation	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	CS 2
Command & Control	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel.	CS 3
Actions on Objectives	Intruders take actions to achieve their original objectives and can pinpoint and access critical data	CS 3

Source: Hutchins et al. (2011)

In the context of this study, the Intrusion Kill Chain personifies the anatomy of a cyber intrusion. As discussed in Chapter 3, the case studies conducted as a part of this investigation sought to discover progressively phased indicators of a cyber intrusion. Reconnaissance phase activities are characterized as actor-driven efforts aimed at obtaining generalized information about a potential victim (Hutchins et al., 2011). Information gathering in the reconnaissance phase helps the attacker draw conclusions about the potential victim. Conclusions are drawn to assist in determining whether the victim's technology in use is susceptible to specific attack vectors. The weaponization phase occurs when the attacker customizes attack vectors to achieve desired results. Often, the customization includes the creation of highly specific functions (e.g., through

ruby or python) that force the victim's device to respond in a predetermined sequence. In the delivery phase, the infrastructure is physically connecting the attacker (or attacker's architecture) to the victim (or victim's architecture) and transmits the weaponized function. In this context, exploitation is defined as the successful manipulation of a particular vulnerability using the weaponized function. In the installation phase that follows, the weaponized function calls secondary functions to implant instructions on the victim's device(s). In such an event, infrastructure is established to create communication between the attacker and the victim, which can be linear or obfuscated (the command and control phase). The final phase pertains to the actions the attacker desires to perform on the victim's device(s). Depending on the attacker skill level, the actions that are executed in the objective phase may include sanitation of evidence that any intrusion occurred or may involve sustainment of access through custom encryption tactics.

Assumptions/Biases

As any study of this nature, this research is subject to some assumptions and biases. Specifically, it is assumed that the researcher will remain objective when analyzing subjective data and will assign the same value to all data. The equal data value consideration is assumed because of the need for consistency in analysis. It is further assumed that the researcher will apply consistent methodology when collecting and analyzing the data. This assumption is a necessary prerequisite for all ubiquitous devices. It is also assumed that the use of Smart Home technology will become more prevalent in the future, making security for smart technology even more relevant. The assumption of continued usage of Smart Home technology and consistent market growth is pertinent to the rate of technology advancement and expectations for security.

Significance of the Study

The study is significant to both research and practice, as the results yielded reveal tertiary behavioral device susceptibility to vulnerabilities. For example, the study findings assess and reveal the current level of smart technology vulnerabilities. Consumers and manufacturers can incorporate the conclusions from this study to help build awareness and smart technology usage expectations. Moreover, those involved in developing security measures can respond to the current smart technology vulnerabilities while still meeting the capability requirements users' demand. Aligning the capabilities offered to users and adapting the security requirements to emergent smart technology can mitigate cyber-attacks while remaining consistent for consumer use.

Delimitations

In order to allow the study findings to be interpreted in the correct context, it is essential to state its delimitations explicitly. In the present work, the researcher has elected to focus primarily on smart technology. Restricting the study scope to Smart Home technology allowed addressing one of the most rapidly growing sectors of the technology industry and purchasing trends among technology consumers today. In particular, the researcher has elected to include primarily smart technology that currently connects to the Internet. This narrow focus in terms of the scope and types of technology considered in this study allows the investigation to concentrate on the knowledge of the existence of vulnerabilities relating to smart technology, thus responding to the current demands and trends within the industry. Finally, this knowledge is assessed in relation to the degree of vulnerabilities inherent to smart technology systems.

Limitations

Owing to the narrow scope of the present study, its findings cannot be generalized beyond the types of technologies examined in this work. Thus, the results reported in this thesis will primarily be of value to those that own smart technology. In addition, the researcher must remain aware that the research conducted does not apply to all smart technology users. For instance, some individuals may be highly adept and knowledgeable about their technology, the risks associated, and the vulnerabilities. On the other hand, some smart technology owners may have little to no awareness of risks and/or vulnerabilities. Consumer knowledge level regarding the improvement of associated smart technology security levels can affect the applicable design of related Smart Home ecosystems. However, without a nominal Smart Home ecosystem configuration, it is impossible to gain an accurate and generalizable view of the degree of Smart Home technology vulnerabilities. Thus, this variance of knowledge levels limits the ability of this study to generalize to Smart Home ecosystems beyond a nominal security configuration.

Definition of Terms

The following terms are frequently used in the thesis and are thus defined in the context of the present study:

Smart Home ecosystem. The term Smart Home pertains to a home predominately controlled by technology and embedded sensors. These sensors can be pre-programmed to ensure that certain activities within the home occur at a certain time (such as turning on/off an irrigation system, activating external lighting, or adjusting the thermostat).

Different devices typically connect the Smart Home to the Internet (Gartner & Gartner, 2015).

IoT (Internet of Things). The IoT refers to the ubiquitous array of web-enabled devices that create parallel connection states (Griffin, 2014b). IoT generally provides web access to physical devices that would not typically connect to a logical network.

IoE (Internet of Everything). Similar to the IoT, the IoE refers to the connection of people, things, data, and processes (Cisco_INC., 2016). The IoE incorporates a broader concept of ubiquitous connectivity from the perspective of existing technology. IoE generally provides enhanced web access and capability to physical devices that would typically connect to a logical network.

Cyber attack/cyber intrusion. The essence of a cyber attack/cyber intrusion is based on a purposeful act of aggression whereby an entity develops a payload to breach a logical or trusted boundary. Passing this threshold enables an aggressor to establish a presence in a trusted environment, allowing various actions to be performed in order to achieve a specific objective (Hutchins et al., 2011).

Vulnerability. In the science of computer security, a vulnerability is indicative of a flaw that allows an attacker to reduce a system's general state of security (J. Hughes & Cybenko, 2014).

Threat. Threats represent the intersection of three elements: a system's susceptibility to a configuration flaw, an attacker's access to such flaw, and an attacker's capability and intent to exploit such flaw (J. Hughes & Cybenko, 2014).

General Overview of the Research Design

As a part of the present study, a vulnerability test was performed, which incorporated the theoretical basis of how disparate manufactured systems interconnect. The vulnerability test assisted in meeting the research objectives. In particular, the vulnerability tests pertained to various wireless sensor network (WSN) products, ubiquitous networks, and pervasive computing in the categories of appliances, Smartphones, multimedia systems, lighting, heating, and home alarm systems, as these elements are most pertinent in the systems considered within the Smart Home domain. Devices operating within the Smart Home domain either consume user data or traverse the construct of availability-based systems. The case studies comprising this research were conducted in a controlled environment. The first case study focused on counter-reconnaissance efforts to enhance discovery of possible cyber intrusions relevant to an IoT network, as well as determine the propensity of cyber intrusions to implant into the IoT network. The reconnaissance and discovery efforts helped determine how secure Smart Home technology IoT systems are independent of other connected devices. The second case study focused on the effectiveness of a proposed Debian 7 based (open source Intrusion Detection Software (IDS)) solution. Finally, the aim of the third case study was to explore the IoT object behavior as it applies to the handling of cyber security and safety, resilience to cyber-threats, and personally identifiable information.

Organization of the Dissertation

The present chapter, Chapter 1, served as the introduction to the study. As was stated earlier, the aim of the present investigation was to determine cyber security in the IoT context and evaluate the current use of Smart Home technology. Since Smart Home

technology is becoming more prevalent, it is necessary to dedicate greater efforts into maintaining and/or improving cyber security. As a part of this introductory chapter, the research questions, propositions, limitations, assumptions, and bias were stated, before summarizing information pertinent to the remainder of the thesis. Chapter 2 provides the literature review, focusing on extant studies discussing cyber-attacks, IoT and IoE threats, and vulnerabilities. The methodology utilized for the study is discussed in Chapter 3, elaborating on the concepts behind the study design, thus allowing other researchers to replicate the current research in the future. Chapter 4 provides the study results, which are discussed in relation to the pertinent literature. The final chapter, Chapter 5, provides the conclusion to the study, while also offering recommendations for future activities.

Summary of Chapter 1

The aim of this chapter was to provide a brief overview of the cyber security background, including vulnerabilities, especially in relation to Smart Home technology. As a part of Chapter 1, security threats and privacy concerns inherent in common Smart Home web-enabled devices used by the consumer were also highlighted. The IoT security lag creates an imbalance between technology and the ability of currently available security to satisfy the demands of current technology. This incongruence leaves millions of private and public individuals and companies at risk of invasion or data theft. Yet, available evidence shows that most consumers are unaware of these vulnerabilities. Independent vulnerabilities stem from isolated devices that are subjected to improper configurations, targeted attacks, and unintentional misnomers often mitigated to an acceptable level through vendor specific remedies. However, untimely mitigations may pose a residual vulnerability due to lack of vendor standards or noncompliance. These

issues were the basis for forming the research questions and propositions, addressed in the remainder of this thesis.

The IoT capabilities emerge from the vulnerabilities situated at the intersection of the physical domain, the Internet domain, and the Smart Home technology domain, with some inherent vulnerabilities pertinent to all three domains. In this chapter, evidence was provided, confirming that Smart Home technology vulnerabilities exist. Thus, Smart Home technology is not inherently prepared for potential cyber-attacks, and the common Smart Home technology system is only moderately secure.

As a part of Chapter 1, study limitations, assumptions, and biases were outlined, as these allow interpretation of the findings reported later in this thesis. The chapter's primary importance stems from the delineation of the basic framework for the study, as well as explicating its contribution to the growing field of research.

Chapter 2 is dedicated to the review of pertinent literature, focusing on the sources where personal cyber security in the context of the Internet of Everything (IoE) and the Internet of Things (IoT) are discussed. The aim of the literature review is to identify the gaps in the current knowledge of cyber security, thus confirming the need for the present study, as well as validating further requirements to investigate and assess the possibility of cyber-crimes in the domain of Smart Home technology. The discussions presented in Chapter 2 also highlight the distinction between threats and vulnerabilities, while providing the definition of the nature of both internal and external threats. The CIA Triad is mentioned to establish the foundational work accomplished, which balances efforts for network security. The IoE and the IoT are studied to understand the evolution of ubiquitous computing systems as they relate to the Smart Home ecosystem. Cyber-

crime protection and cyber-crime laws are considered to validate modern challenges as they relate to Smart Home technology vulnerabilities, while also being pertinent to resolving Smart Home technology vulnerabilities. Finally, Chapter 2 closes with a general overview of the case study methodology and a summary of the literature review findings.

CHAPTER 2

Literature Review

Introduction

The purpose of the literature review presented, is to provide information regarding cyber security, the IoT, and Smart Homes. The chapter begins with a discussion of the need for cyber security and provides insight regarding the vulnerabilities within the IoT/the IoE and associated cyber-crimes, including internal and external threats. The chapter also includes a discussion relating to the challenges when cyber-crime warrants further investigations and legal assessments. The literature reviewed in the sections that follow explore the sources that build fundamental cyber security focus, such as the CIA Triad, cyber-crime protection mechanisms, and cyber-crime laws. The different types of Smart Home technology are discussed as well, along with their default vulnerabilities and strategies that can be adopted to resolve them. The chapter closes with a discussion of the chosen research strategy and a summary of the key points.

The Need for Cyber Security

Due to rapid advancements in technology, the need for advanced cyber security has increased dramatically over the last few years, owing to the widespread Internet broadband availability and decreased computing component cost (Mohn, 2015). In October 2015, AT&T reported that, in comparison to 2013, 2014 AT&T networks realized a 62% increase in malicious scanning activity and a 458% increase in vulnerability scans of IoT devices (Krause, 2015). The need for advanced cyber security

is partly attributed to the sophistication of cyber-attacks and intense media attention when attacks and breaches do occur (Dunn Cavelty, 2014). The growing need for advanced cyber security is also related to increased attacker structure and organization when executing cyber intrusions. As a result, cyber-attacks are more costly and much more detrimental to the victims. For example, numerous cyber-attacks have been attempted on the United States' national security, rendering the country vulnerable to domestic and international terrorist threats (Dunn Cavelty, 2014). Other common targets for cyber-attacks include organizations that use, consume, and store sensitive data. Although databases with this type of information are primarily employed in the governmental sector, many are also developed and maintained within the private sector (Bamrara, 2015).

According to Joseph Swedish, President, and CEO of Anthem Inc., a large insurance company, in 2014, a sophisticated cyber-attack on Anthem Blue Cross and Blue Shield affected the private information of approximately 80 million individuals (Swedish, 2015). The cyber-attack compromised current and former members, as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses, and employment information were unlawfully obtained, along with their detailed income data (Swedish, 2015). However, the breach was not reported until early February 2015. According to the reported findings, the cyber-attacks were carried out through stealing the credentials of Anthem employees, which was obtained through a widespread phishing fraud (Balbi, 2015). During the conduct of the breach, personal identifying information was stolen, putting millions at risk of identity theft. Significantly, the Anthem breach was the largest breach reported to date by a healthcare company (Balbi, 2015).

Healthcare companies are not the only targets of sophisticated cyber-attacks. Existing public records proved that cyber-attacks also target large retail companies. For example, in December 2013, Target proved to be vulnerable to sophisticated exploits when the retailer was the victim of two separate cyber-attacks (Weiss & Miller, 2015). The first attack occurred when financial data pertaining to approximately 40 million credit and debit card account numbers were stolen. Less than a month later, in January 2014, Target informed the public that millions of customers' personal information had been stolen. The company also estimated that approximately 70 million individuals could be potential victims (Weiss & Miller, 2015). In October 2015, Target reported that the two data breaches incurred losses of about $248 billion. It is particularly noteworthy that the reported costs were not entirely inclusive. A congressional research service conducted by Weiss and Miller indicated that these costs did not include estimated losses due to a subsequent decline in consumer confidence regarding the handling of their personal data, nor do these costs account for any potential malice, such as damages incurred to consumer credit history (Weiss & Miller, 2015). Finally, the costs related to the Target data breach excluded penalties and/or fines levied by the government (Weiss & Miller, 2015). Significantly, this particular breach has been publicized as one of the largest in the history of the United States. As a result, consumers are increasingly concerned, given the size of the data breach (Weiss & Miller, 2015).

Other concerns relate to the critical infrastructure of the United States. In 2009, researchers established the possibility that the country's enemies could considerably undermine the country's power infrastructure (R. Hughes, 2010). Furthermore, it is anticipated that future wars will take place in cyberspace, which has emerged as a new

battlefield, allowing enemies to attack from any location at any time. Unfortunately, while cyber warfare is gaining in popularity among those aiming to cause harm, public awareness of its extent and devastating consequences are limited. According to R. Hughes (2010), cyber war will be executed through unique cyber-weaponry that will evolve through generations, as will cyber warfare tactics and applications. The author also noted that terrorist groups commonly use attack vectors that maximize damage and avoids directly engaging a formidable adversary.

Cyber-Crime Protection and Laws

Cyber security is not merely a technical issue, but rather involves many diverse legal aspects and frameworks. Therefore, it is necessary for developed countries to assist developing countries in the establishment of strong protections related to cyber-crime (ITU, 2014). At the end of 2006, there were approximately 19 substantive cyber-crime laws and three procedural cyber-crime laws enacted within the United States (Rees, 2006). However, as of 2013, 28 revisions were recommended for laws governing actions attributed to cyber-crimes, or those specifically created to address cyber-crimes (Fischer, 2013). Cyber-crime laws are necessary for a variety of reasons, predating the Internet, and serving many different purposes. However, many laws require revision in order to respond to the rapidly changing circumstances. In particular, amendments and modifications are expected to persist in the future in order to accommodate cyber-crime due to the strong relationship between cyber-crime and social ties. One significant form of cyber-crime, relating to society, is phishing. For example, many phishers are part of an organized group, suggesting that this is becoming organized crime. Available evidence also indicates that organized phisher groups are involved in real-world

relationships through social networks, rather than being members of Internet forums. Moreover, they focus on the use of social engineering, in contrast to malware, to acquire unauthorized information (Leukfeldt, 2014).

Additionally, there is a growing need for cyber security measures. According to a study conducted by the International Telecommunication Union (ITU), information technology systems and the development of Internet services are directly related to cyber security (ITU, 2014). Consequently, for enhancements in cyber security to occur, critical information infrastructures must be protected to increase national security and economic well-being (ITU, 2014). Moreover, to make the Internet safer, it is necessary to align new services and capabilities with government policies (ITU, 2014). Owing to the complexity of cyber-crime, appropriate deterrents are integral to national cyber security and strategies related to protecting the critical information structure. Based on these needs, it is conceivable that cyber security laws can continue to advance proportionally with technology and vulnerabilities (ITU, 2014).

Challenges to Investigating and Assessing Cyber-Crime

The seriousness of cyber-crimes and cyber terrorism is widely recognized. Furthermore, there is a growing consensus that everyone in every sector—both public and private—is affected in some way (Hyman, 2013). Although nations have dedicated significant funds to cyber protection measures, the extent of damage imposed by cyber criminals is difficult to estimate (Hyman, 2013). In addition, no quantifiable metrics presently exist to account for potential cyber-crimes and cyber terrorism attacks that will emerge in the future. According to a study conducted by Symantec Corporation (Hyman, 2013), cyber-crime is estimated to incur $110 billion in costs per year. Yet, McAfee

Incorporation estimated that the actual impact is closer to $1 trillion (Hyman, 2013). Experts at McAfee stated that their assessment was based on financial losses through both malicious and accidental infringement on security (Hyman, 2013). However, McAfee also agreed that there is no definitive way to measure every aspect of data loss. Implied loss due to consumer interpretation of a company's potential lack of security degrades consumer trust, thus, representing one of the most difficult costs to estimate (Hyman, 2013). Irrespective of the type of loss, the disparity between the estimates provided by the two organizations is significant, suggesting the presence of inexplicable barriers to accurate reporting.

In many cases, companies victimized by cyber-crime decide not to report the breach for a variety of reasons, the perceived adverse impact on business operations being the most likely one (Hyman, 2013). Other inhibitions involve reluctance to report the crime to the police. A study conducted by Ernst and Young in 2003 indicated that merely one-quarter of all potential frauds was reported to law enforcement agencies. The survey findings also revealed that only 28% of respondents were satisfied with the investigation results (J. Smith, 2003; R. G. Smith, 2003). In Australia, for example, the following factors were identified as the main inhibitors to reporting cyber-crime to police:

- A belief that the breach was minor and not worthy of police attention
- Concerns regarding potential backlash from consumers
- Concerns related to negative publicity;
- Lack of credible (or any) proof
- Reluctance to prosecute

Other contributing factors were fears of business loss due to electronic systems being down during repairs to security (R. G. Smith, 2003). In some cases, jurisdiction issues impeded the cyber-crime investigation and prosecution of perpetrators. For instance, the Internet provides a platform for international cyber-crime to occur, as the widespread interconnectivity allows the victim to reside in one country while the perpetrator is in another country (R. G. Smith, 2003). Jurisdiction also affects prosecution success, as it introduces unique barriers to logistics and practicalities. For instance, time zone differences often make investigations inconvenient for at least one party involved in investigative activities (R. G. Smith, 2003). Similarly, the need for multilingual translation and interpreters could incur substantial costs, and given that such activities can be time-consuming, they hamper investigation progress. The priorities assigned to different types of crime can also pose a significant barrier to the overall crime investigation. For example, economic cyber-crimes are usually given lower priority relative to violent cyber-crimes (R. G. Smith, 2003). Suspect attribution across an enfranchised domain presents significant issues as well. R. G. Smith (2003) also demonstrated that identity concealment or misrepresentation of self could be conducted utilizing on-line technologies, such as proxies. Identity concealment enables attributable identities to be easily stolen, allowing the e-commerce technologies with public key infrastructures and/or digital signatures to be manipulated (R. G. Smith, 2003). This manipulation can be achieved through providing false documents, supporting alternative identities, rather than true identities. Thus, with seemingly sound identification, it is possible for offenders to register and obtain the public-private key pair (a hallmark of

secure data transfer) using registration authority to access secure transactions (R. G. Smith, 2003).

Threats and Vulnerabilities

The quantity and complexity of advanced persistent threats (APT) or cyber-attacks have dramatically increased in recent years. An APT is a level of persistence in a computing system that allows an attacker at-will access regardless of security constraints (Messmer, 2011). Thus, responding to such threats requires automated solutions that combat APT vulnerabilities in virtually every aspect of our lives. A White House report released in May 2014 suggested that Americans used approximately 500 million Internet-capable devices at home including, but not limited to, Smartphones, tablets, and other Internet-connected devices that run various unimpeded and parallel applications that connect to the web (Wheeler, 2014). Given its high degree of connectivity to the external network, the Smart Home environment is not immune to the paradigm of an APT or cyber-attacks. The home has evolved to become one of the most promising markets for new IoE/IoT developments. It is envisaged that IoE/IoT will embrace technologies emerging in the field of pervasive computing and will offer extensive diversity as it pertains to the types of technology that converge to a single gateway in the home. In 2010, according to the FCC, 78% of Americans used the Internet, and 65% had broadband access at home (Horrigan, 2010). Emergent IoE/IoT devices will sustain exponential growth, as more consumers are made aware of convenience capabilities offered by IoE devices in the home. Consequently, the variety of IoE/IoT devices will eventually create a chasm of unanswered security concerns.

In May 2009, the White House Office of the Press Secretary explained the benefits and dangers of an increasingly connected ubiquitous network, thus highlighting cyber security as an essential aspect of the U.S. economy, national security interests, and the American Military prowess (Theohary & Rollins, 2009). President Obama expressed his concern about the catastrophic effects that a relaxed approach to cyber security could have for the American population. As noted by Theohary and Rollins (2009), "In today's world, acts of terror could come not only from a few extremists in suicide vests but from a few keystrokes on the computer – a weapon of mass disruption" (Theohary & Rollins, 2009, p. 15). The use of "disruption" rather than "destruction" highlights the manner in which the dynamics of terrorism can conceivably effect information networks (Theohary & Rollins, 2009). In making this statement, the president is acknowledging the possibilities of cyber wars and cyber terrorism.

Originally, the utility of control systems, such as those related to IoT security, was limited as their more widespread usage was prevented by the inadequate protocol knowledge by the public. As a result, minimal efforts were made to enhance the security of the control system network, focusing on the physical measures instead (Fenrich, 2007, 2008). Today, this is no longer possible due to the sheer amount of data that is transmitted and stored in such systems, causing most control systems to become connected (always available for data transmission), rather than operating as stand-alone systems (Fenrich, 2007, 2008). Yet, while advantageous, this connectivity increases vulnerabilities and threats. Given that Smart Homes maintain continuous connectivity for home monitoring purposes, the programs required to provide this functionality share similar risks (Fenrich, 2007, 2008).

Control systems manufacturers have become aware of the vulnerabilities and threats they face (Fenrich, 2007, 2008). This discovery prompted the responsible parties to enact different initiatives, which focused on increasing the awareness of the public in regards to the growing prevalence and extent of potential threats. The added focus also meets the purpose of threat mitigating initiatives, e.g., establishing ways to reduce vulnerabilities through different mechanisms, including training programs, awareness and education, and the establishment of security priorities, thus reducing the potential onslaught of threats. The initiatives towards vulnerability and threat mitigations confirm the growing awareness of the fact that issues of this nature can never be fully understood and resolved unless adequate knowledge of the risks imposed by control system usage and capabilities exists. Thus, threats and vulnerabilities can be further categorized as internal and/or external (Fenrich, 2007, 2008).

Internal Threats

Internal threats can be classified as accidental or intentional, whereby the former occur due to a lack of knowledge or inattention (Fenrich, 2007, 2008). Accidental threats are common to complex policies, operations, or lack of data confidentiality. On the other hand, intentional threats are a result of intentional actions, such as data theft (Fenrich, 2007, 2008).

External Threats

In the context of the present study, a web-enabled technology represents a physical product or a device-associated service that consumers use through, or in conjunction with, the World Wide Web (Jones & Schneier, 1995). New web-enabled technology requires the establishment of a baseline level of network security resilience.

External threats arise from the use of malware, or activities of hackers and terrorists. Malware includes items such as spyware, trojans, viruses, and worms. Malware attacks are usually indirect, suggesting that there is no blatant attack on the system, but rather a systematic attack or theft of information. Typically, the goal of malware is to cause communication obstruction, data corruption, installation of backdoors for remote viewing and control, or forced shutdowns, all of which have a negative impact on information systems (Fenrich, 2007, 2008). Hackers are commonly external entities interested in penetrating another system to gain information, intrude on privacy, or gain control of a system. Terrorists, on the other hand, usually target the most critical infrastructure systems, especially those the targeted country requires for operation, such as electricity, water supply, traffic management, and a myriad of other categories of control systems. As a result, this particular threat is a major concern for those that maintain the critical infrastructures, such as governmental agencies and large corporate organizations. The primary difference between hackers and terrorists is that terrorists focus on causing harm to people, whereas hackers aim to disrupt systems or obtain information.

CIA Triad

Establishing the aforementioned security baseline is a critical task that must be completed to meet the needs of consumers and manufacturers alike. For instance, the CIA Triad (Data Confidentiality, Integrity, and Availability) is the basis for fundamental concepts regarding how technology manufacturers balance security for emerging web-enabled technologies. Furthermore, through the CIA Triad, the theoretical design model for balancing baseline network security is established (Ning, Liu, & Yang, 2013). The model can be ascribed to several social theories because of the purpose of network

design. For instance, most networks are used to allow a user faster access to the Internet, while increasing the capacity to accomplish disparate tasks. Therefore, in order to allow technology to improve lives, technology developers must understand not only the associated technology but the people that use it as well (Kleine, 2015).

During the 1980s, the Actor-Network Theory (ANT) was developed (Kleine, 2015). ANT theory focuses on socio-technical systems and the way they are represented as actor networks. These actors include formal/informal processes, technology, and human actions to initiate and complete processes. In addition, for processes to function in the network, they must be involved in some relation with each other, indicating that all processes, technology, and human actions within the network exert a significant influence on one another (Kleine, 2015). The ANT theory is particularly useful in relation to new software. For example, ANT is helpful in analyzing new software user interface actions within networks relating to other actors, whereby it affects the ability of the network to enable or prevent actions taken by other actors (Kleine, 2015). As a result, based on the "actions" of the software, it is reasonably assumed that design intentions do not always correspond to usage outcomes. Therefore, under ANT, "actions" are choices that influence the result in a variety of ways.

The Capability Approach (CA) is another relevant social theory because it describes development in more than economic terms. Its application thus allows human development to have an influence on the design of products and technologies. The co-creator of this approach was the Nobel-prize winning economist Amartya Sen. According to Sen, development is based on the processes involved in establishing and/or expanding real freedoms enjoyed by people (Kleine, 2015). This view suggests that

freedoms are not a prerequisite for a quality of life to be maintained. Therefore, as an actively maintained quality of life is posited to enable people to have enhanced choices, this suggests a link between social theories and network design (Kleine, 2015). The relevance of the CA theory to the technological advances is evident due to the ability of experts to trace the development processes and to examine the manner in which technology influences life. As a result, social theories are useful in the design and development of technology because they are primarily based on a comprehensive socio-technical analysis. Social theories mostly focus on human needs and expectations, while also accounting for constraints imposed by the design. This social theory analysis is useful for identifying design process challenges (Kleine, 2015).

In order to adequately respond to the increasing number of threats and vulnerabilities, many organizations use the CIA Triad. The CIA Triad model is the benchmark against which effectiveness of any given information systems security is measured, in terms of its ability to repel and detect emerging threats and vulnerabilities. Within the Triad, confidentiality focuses on data security and privacy; integrity pertains to maintaining data in its current form, and availability relates to ensuring that the data is provided to and/or is easily obtained by those that need the data (Fenrich, 2007, 2008).

Control systems, as well as Smart Home technologies, utilize the CIA Triad, albeit in reverse order. In this case, availability and integrity are of higher importance than confidentiality. A higher emphasis is placed on availability because the system must always be usable. At the same time, it is assumed that Smart Home technology does not typically have much, if any, sensitive data. Due to the reverse nature of the CIA Triad in this situation, additional issues can arise. Moreover, when Smart Home technology

devices aggregate, the potential exists to perpetuate an environment of highly volatile network vulnerabilities. These diverse network vulnerabilities enable a growing surface upon which a fundamentally different age of cyber security emerges (Roberts, 2014). Now, more than ever, the need for continual testing and patching for vulnerabilities in emerging technologies has become paramount (Protalinski, 2014).

The Internet of Everything (IoE) and the Internet of Things (IoT)

The phrase "Internet of Things," in the context of industry solutions aimed at greater automation, error reduction, and efficiency improvements, was first introduced in 2000 by the founders of the MIT Auto-ID Center (Gérald, 2010; Sundmaeker et al., 2010). At the time, IoT technologies encompassed simple technologies, e.g., bar codes, smart cards, sensors, voice recognition, biometrics, and since 2003, Radio Frequency Identification (RFID) (Gérald, 2010; Sundmaeker et al., 2010). In September 2003, the Auto-ID Center officially launched the concept of the EPC (Electronic Product Code) network during an EPC Executive Symposium. The EPC's groundbreaking capability introduced a technology infrastructure that served as a tracking mechanism for computers to automatically identify man-made objects while encompassing an entire logistical lifecycle, from plant to distribution centers (Gérald, 2010; Sundmaeker et al., 2010). The Symposium attendees concurred with the view that RFID would become a key enabling technology for economic growth for the next fifty years, inciting a fundamental shift from "computer information processing to computer sensing" (Gérald, 2010, p. 1; Sundmaeker et al., 2010).

IoE and IoT are related to interconnectivity and device intelligence. IoE and IoT will grow in prominence, as future sensory technology will more commonly support IoE

and IoT use case applications. Furthermore, these sensors would be smaller and serve multiple purposes (Noor, 2015). Thus, devices would be more intelligent through deep learning, which is a process that consists of using algorithms designed to allow experience and observations to teach machines. Therefore, it is envisaged that IoE, IoT, and interconnectivity will influence all aspects of daily life. In the business industry, IoE and IoT will be responsible for improved productivity, innovation, and/or economic opportunities, due to lower costs, higher efficiency, and autonomous engagement (Noor, 2015). Overall, through IoE and IoT, connections will be made between people and things, transforming heterogeneous data into data that can be used to assist in creating new ways of completing previously impossible tasks or improving current processes (Noor, 2015).

SmartThings, a sophisticated Smart Home technology company, has developed a platform allowing objects commonly found in homes (such as doors or locks) autonomously to prioritize the usage needs of the owner (Moad, 1997). To establish the SmartThings platform, the owner needs a starter kit (currently retailing at $200) and a Smartphone. The aim of SmartThings is to connect all technologies that should be interconnected (Moad, 1997). Modern ubiquitous device interconnectivity is vastly different from initial Smart Home technology attempts during the 1950s, which failed, in part, due to inadequate technology. SmartThings, noted for its change in the home automation processes, focused on the use of cloud computing to connect to the IoT, thus allowing for remote monitoring and controlling of sophisticated devices using Smartphone applications and cloud technology (Moad, 1997).

It is expected that 11% of homes will have cloud-connected security systems by the end of 2016, increasing to 35% by 2021 (Zalud, 2014). In addition, 13% of homes will have smart thermostats within 2016, increasing to 43% by 2021. An expected 22% of wearable fitness devices will be adopted by the end of 2016, increasing to 43% by 2021 (Zalud, 2014). Despite these expected adoption rates, IoT is currently insufficiently advanced for the related infrastructure to support the increase in the number and type of gadgets available (Zalud, 2014). At the same time, it is envisaged that IoT will extend to other fields, such as home security and automation of devices, including healthcare devices, which will affect the entire Smart Home ecosystem (Zalud, 2014). Thus, IoE, commonly considered IoT, will mature to accommodate a growing number of "Things" (Oriwoh & Conrad, 2015; Oriwoh & Williams, 2014). As a result of this expansion in scope and functionality, IoE and IoT will present global challenges as Smart Home manufacturers out-produce their ability to contain security. Additionally, it is critical to ensure that the devices comprising the IoT ecosystem possess and maintain authentication methods to protect successfully against attacks directed at legacy systems (Beekman & Thompson, 2014; Demblewski, 2015). Fortunately, most authentications occur in proximity to the susceptible device(s). Proximity-based authentication vulnerabilities are easily combated by reducing emanations or beacon power. However, this aspect is most likely not within the scope of control for the homeowner; rather, it is inherent to the specifications set by the manufacturer. Hence, further research is needed to determine if manufacturers even consider this type of threat.

Vulnerabilities and Solutions of IoE and IoT

Some academics believe that IoT began with the concept of distributed computing, leading to enhanced communication technologies. From this relatively simplistic perspective, IoT can be viewed as a means of connecting physical devices to one another, allowing a contextual relationship of services, and establishing a global network of ubiquitous devices (Popescul & Georgescu, 2013). The basis of IoT is the ability to allow many different devices that have different capabilities to sense and communicate with each other (Albert, 2015). Furthermore, as more corporations add IoT to their supply chains, the risks of cyber intrusions will exponentially increase (Krause, 2015). It is thus envisaged that the significance of IoT will substantially increase as more people and companies become technologically grounded. Ultimately, according to some researchers, IoT is based on those non-electronic devices that have been embedded with intelligence (through sensors and other devices) and connectivity capabilities (Ramanathan, 2015). At the same time, IoT is not expected to remain a small component of cyberspace. Rather, it is anticipated to be a dominant factor in the future. Yet, as IoT increases in importance, issues will arise due to trust management—a concept that is presently virtually non-existent in relation to IoT (Ramanathan, 2015).

Concerns about trust, privacy, and security began with the advent of Smartphones. Growing popularity of Smartphone devices prompted privacy and security concerns due to the volume of personal information obtained from, stored on, and shared by the devices and different device apps (Waltzman & Shen, 2015). Private information—social network information, communications, and banking information—was available on the device and was susceptible to hacking or theft. Therefore, as Smartphones can be

connected to the Internet (including wearables), the general security of IoT can be compromised (Waltzman & Shen, 2015). According to Hodgson (2015), IoT advancements will have a significant effect on technology-dense industries—including home security, smart cars, Smart Homes, industrial sensors, mobile devices, and smart cities—because of the diverse concepts defining the purposes and applications of IoT (Hodgson, 2015). Although interconnected devices (such as Smart Home devices) offer significant benefits and are supposedly convenient for users, such devices are also capable of obtaining and storing highly sensitive information about the user (Waltzman & Shen, 2015). Krause (2015) reported that, between 2013 and 2014, the extent of vulnerabilities increased by 62% (Krause, 2015). This upward trend confirms the increased capacity and susceptibility of IoT to the continually emerging exploitation of its data (Popescul & Georgescu, 2013). In the context of corporate IoT, vulnerability scanning surpassed 458% in the same period, and were typically caused by linkages between supply chains and internal business processes (Krause, 2015). According to Hodgson (2015), by 2018, the sensor market will be worth approximately $4 billion, while the value of connected devices will increase to approximately $38.5 billion by 2020 (Hodgson, 2015). The use of sensors is important because they are the necessary component for establishing a relationship between virtual and physical worlds, which allows for reactions from the sensors to the current environment (Popescul & Georgescu, 2013). Therefore, there are multiple opportunities for data collection by companies. Analysis of this information and other collected data allows a detailed profile to be compiled. As a result, those companies that obtain this information can make accurate

forecasts of consumer activity. Many consumers view these analyses as privacy invasive (Waltzman & Shen, 2015).

As IoT is still a relatively new market, the design of IoT devices is likely to present some inherent issues (Hodgson, 2015). Furthermore, IoT offers a new threshold for cyber criminals to attack, which has resulted in a research gap regarding current security framework approaches in relation to technology advancements (Demblewski, 2015). Therefore, policymakers acknowledge possible IoT device implications (Waltzman & Shen, 2015). Issues are also foreseen for the future, as many commercial IoT applications are expected to exist in many new areas (Hodgson, 2015). Thus, policymakers, not only in the United States but also around the world, are developing ways to ensure that privacy and security standards are efficient and are upheld by the companies distributing and/or selling IoT devices. At the same time, policymakers are cautious to ensure that these standards do not impede IoT innovation (Waltzman & Shen, 2015). For example, in 2013, the FTC entered the debate as actions were taken against Trend Net, Inc. In this situation, it was alleged that hackers were able to access the FTC's cameras due to inadequate security. This cyber intrusion led the FTC to establish expectations of the companies offering IoT devices in 2015 (Waltzman & Shen, 2015).

The report generated by the FTC was based on the findings of a 2013 workshop, during which the participants were encouraged to provide feedback with suggestions, along with listing the issues with IoT, and discussing necessary steps to resolve these problems (Waltzman & Shen, 2015). Significantly, the new FTC report considered many of the same privacy principles and recommendations that it had suggested in earlier reports concerning PCs and applied them to IoT devices. The report recommends that

security and privacy be integrated and enhanced through the design of new devices (Waltzman & Shen, 2015).

Thus, it is recommended that IoT device manufacturers conduct a security risk assessment during the design process. Furthermore, the FTC suggested that external vendors that are hired must be able to maintain security, while the company should retain the responsibility for the oversight of the overall security (Waltzman & Shen, 2015). The FTC suggests that data minimization occurs through limitations put in place for obtaining and storing consumer data. However, it is also known that IoT devices allow companies to collect data about consumers, and this practice is considered to be of significant benefit for future business retention (Waltzman & Shen, 2015). Despite the obvious benefits, the FTC cautions that the use of this data may compromise privacy through the accumulation of data, which may encourage hackers to steal the information. Furthermore, the FTC posits that the utilization of this information may compromise privacy because consumers may not anticipate specific uses of their data (Waltzman & Shen, 2015). As a result, the FTC suggested the establishment of specific limits regarding data collection by companies, both sensitive and non-sensitive. It is also important for these companies to destroy data when the data relevancy or need expires (Waltzman & Shen, 2015).

The FTC also recognized the need for consumer disclosure and choice, while acknowledging that this can be challenging in the context of IoT. The obstacle to absolute disclosure of IoT devices is partially due to many devices not containing any form of a user interface (Waltzman & Shen, 2015). This constraint prompted the FTC recommendation that no choice be offered to consumers, provided the use of the information remained consistent with the interaction (Waltzman & Shen, 2015). On the

other hand, if the use of information is inconsistent with the interaction, notification should be provided to consumers, allowing them to choose if and in what manner their data can be utilized. This freedom of choice includes the option to decline participation (Waltzman & Shen, 2015).

Also in 2015, the U.S. Senate Committee on Commerce, Science, and Transportation began discussing IoT issues. In the accompanying hearing, the Committee heard from different experts that provided information regarding various topics. Among the topics was the consideration of how to protect consumer privacy and provide security, while simultaneously establishing a necessary balance of innovation and growth (Waltzman & Shen, 2015). This balance was considered especially important to some experts because it is expected that IoT would benefit retail and industrial industries the most. Furthermore, major concerns were raised regarding security, with one expert arguing that it is necessary to establish necessary security implementation during the design process, as well as during the manufacturing process (Waltzman & Shen, 2015). The FTC also recommends educating consumers about data use, privacy, and security, as well as providing transparency in the applicable industry. Despite these recommendations, the majority of the experts at the hearing did not recommend rushing to regulate IoT (Waltzman & Shen, 2015). In fact, the prevalent view was that consumers and entrepreneurs should have the choice to pursue the path towards IoT, rather than being impeded by regulations imposed by the government. Thus, the hearing attendees acknowledged implications and promise for immense benefits relating to IoT use and installation (Waltzman & Shen, 2015).

In the European Union (EU), IoT privacy and security issues are widely acknowledged, and relevant bodies have worked towards resolving them since 2014. The EU passed Article 29 focusing on data protection, which articulated concerns regarding IoT, akin to the FTC report (Waltzman & Shen, 2015). However, the EU member state representatives are more concerned about user awareness of data collection and processing, as well as the volume of data being collected by IoT devices. Thus, this lack of awareness suggests that there is a significant challenge in demonstrating that there is valid consent by consumers according to laws and regulations in the EU (Waltzman & Shen, 2015). Furthermore, the amount of data collected and its retention could already be leading to violations of laws and regulations within the EU. Thus the EU mandated that IoT data can only be kept for a specified period, typically for as long as necessary for the intended purpose to be accomplished. This restriction implied that secondary repurposing and profiting from data usage statistics that are not related to the original purpose might be in violation of EU laws and regulations due to a lack of consumer consent (Waltzman & Shen, 2015). Therefore, there is immense interest in IoT privacy and security issues, resolutions of which have been guided by FTC reports and Article 29. However, within the EU, Article 29 has a greater impact than the FTC report (Waltzman & Shen, 2015), because the latter focused on best practice recommendations and policies, whereas the former pertains to EU law compliance. Significantly, the FTC did not require regulation of IoT issues through legislation because of the expected rate of technology evolution, implying that any legislation would be premature (Waltzman & Shen, 2015). Ultimately, the FTC report provides a framework for future laws and regulations as well as their enforcement. Thus, companies should follow the FTC report

recommendations, as well as Article 29, to ensure compliance with both the U.S. and EU regulations (Waltzman & Shen, 2015). Because national governmental bodies are increasingly focusing on these issues, cyber-crime related to IoT is an issue that has gained prominence globally (Scott, 2015). However, governments of some countries are taking no efforts to protect their systems and citizens from cyber-attacks enabled by IoT vulnerabilities (Scott, 2015). On the other hand, some businesses require multilayer protection, especially in consideration of IoT payment devices (Scott, 2015).

Some experts recommend prohibiting default passwords because they make it easier for hackers to break into the system. Furthermore, providers and product incorporation must be chosen based on security levels offered (Hodgson, 2015). Industries must consider vulnerabilities, such as increased data collection, which may make them a target for theft. As a result, it is beneficial to increase mobile security and understand the risks inherent in utilizing IoT devices. This risk transference leads to conclusions that wireless networks are the source of the greatest risk (Hodgson, 2015). For example, the first worm—known as the Morris Worm—was created in 1988. As of 2014, cyber-crime has cost more than $400 billion worldwide (Scott, 2015). At the same time, IoT has ethical issues attached to it, namely:

- Ubiquity
- Invisibility
- Ambiguity
- Difficult identification
- Ultra-connectivity
- Autonomous and unpredictable behavior

- Incorporated intelligence
- Difficult to control

Each of these factors has different issues attached to them. For example, as IoT devices decrease in size, they will be less visible, thus masking obtrusiveness. Reduced visibility will allow them to observe interactions without being detected, thus becoming more intrusive to privacy (Popescul & Georgescu, 2013).

However, it is undeniable that the rapid development of IoT will cause a transformation in not only business but private lives as well. Not all consequences can be predicted easily (O'Brien, 2015). This difficulty stems from IoT still being largely undeveloped. It can be expected, however, for IoT to impact product liability (O'Brien, 2015). The newly developed smart devices will have a tremendous effect on the world and IoT in particular. For example, as highlighted by the 2015 FTC report, IoT and smart devices have increased susceptibility to unauthorized access, as well as personal identification/information theft and misuse (O'Brien, 2015). This information can lead to attacks on other systems, such as the Anthem attack. It is also argued that these same risks exist for traditional equipment, such as computers and networks (O'Brien, 2015). Yet, the risks inherent in IoT are much greater than those associated with traditional computers. This perceived risk arises because IoT has evolved into what is currently termed the Internet's third wave (O'Brien, 2015). Through the information gathered and stored in data storage centers, users are vulnerable to identity theft, yet consumers argue that the benefits, such as increased efficiency, outweigh the risks (O'Brien, 2015).

In 2014, Goldman Sachs issued a report suggesting that IoT is adaptable through wearable devices, smart cars, Smart Homes, Smart Cities, and the Industrial Internet.

Furthermore, IoT has been driven by different forces, such as IoT strength, due to decreased costs, the use of Smartphones and increased wireless coverage, revenue generation, and increased productivity, leading to reduced expenses (O'Brien, 2015). The acceptance of IoT was illustrated at the 2015 Consumer Electronics Show, where over 900 technologies were showcased. The number of connectable products increases daily (O'Brien, 2015). Consumers utilize IoT for energy savings and efficiency, as well as to be able to remotely correct problems relating to the home. Thus, presenting an increased opportunity for privacy violations and external/unauthorized interference with the systems (O'Brien, 2015).

The number of vulnerabilities related to IoT devices is especially concerning considering a 2014 Hewlett-Packard report indicating that 70% of devices are vulnerable to external attacks. For instance, in 2014, there was an attack on a German steel plant network (O'Brien, 2015). This cyber intrusion allowed the attackers to control the network externally, preventing a blast furnace from shutting down, which caused significant material damage (O'Brien, 2015). This intrusion is one of only two known cyber-attacks that have caused physical harm. The first attack occurred in Iran's Natard uranium plant through malware execution (O'Brien, 2015).

Other potential vulnerabilities can be found in smart televisions and lateral systems that connect to the associated network (allowing for storing/transmittal of personal information) including:

- The use of IoT devices to attack personal or public networks and/or systems
- Creating physical safety risks by, for example, affecting medical care appliances connected to a home network

Thus, according to the FTC 2015 report, the less expensive smart devices may have increased risks due to lower security standards (O'Brien, 2015). In some cases, these cheaper devices may not offer needed security updates or incorporate other security protection features that may safeguard personal information. As a result, as technology advances further, if corresponding security updates are not available, it is expected that vulnerabilities will increase in the private sector (O'Brien, 2015). Criminal activity can occur through malware that would not leave any apparent traces on the device, leaving consumers unaware of the attack. At the same time, there are concerns relating to issued patches, especially in the context of patch delivery (O'Brien, 2015). Other predictable vulnerabilities from IoT devices pertain to software malfunctions causing damage to property or person, external attacks, and identity theft through misappropriation of personal data. In the business sector, such issues result in product liabilities (O'Brien, 2015).

In 2015, several IoT failures occurred. For example, in April, the wireless hub by Wink failed, whereby all connected devices were disabled. Many potential breaches of security occurred, as a result, increasing vulnerabilities, in particular, those associated with home security systems (O'Brien, 2015). Another failure occurred within Chamberlain and Ooma, caused by compromised IoT devices, disrupting services, potentially affecting consumers' overall security (O'Brien, 2015).

In 2015, the first IoT class action took place due to a report by U.S. Senator Edward Markey. The action involved Toyota, Ford, and GM automobile manufacturers (O'Brien, 2015). The action was prompted by an investigation spearheaded by Markey in response to studies revealing presence of significant IoT vulnerabilities to car systems

that pose significant risks to the safety of drivers. The investigation detailed the following vulnerabilities (O'Brien, 2015):

- Potential privacy intrusions through wireless technologies in the car systems
- Lack of awareness of intrusion possibilities
- Inconsistent, inadequate, and/or haphazard security measures for protection against remote access
- Lack of ability to diagnose or respond to intrusions
- Over-reliance on technology that is not designed for security protections related to IoT devices

Other privacy concerns are raised in relation to navigation systems in automobiles, which could be used to monitor the location of the vehicle, prompting privacy invasions. Thus, owing to the failure of these companies to enhance electronic security, it was argued that the warranties were violated, and the vehicles were defective (O'Brien, 2015).

In other cases, threats have been identified through commercial aircraft safety, considering that many IoT devices onboard an aircraft are connected to the Internet. Thus, the electronics system controlling the aircraft could have unauthorized access opportunities (O'Brien, 2015). Therefore, it is unsurprising that IoT has been argued to pose the highest risks to security, along with de-globalization and supernatural category storms. Part of this risk is due to the number of incidences where automated systems replace humans, allowing for much greater opportunities for unauthorized access to systems (O'Brien, 2015). In this context, IoT device malfunctions are concerning, especially those related to critical infrastructures (O'Brien, 2015).

IoT vulnerabilities pose increased risks to vendors, due to the loss of protection against third-party injury claims (O'Brien, 2015). In fact, many software vendors are unaware of these increased risks relating to product liability exposure due to IoT devices and have not stated provisions in warranty agreements (O'Brien, 2015). Without specific provisions and in the absence of standards for IoT device protections, consumers are not afforded protection relating to IoT device failures (O'Brien, 2015).

Short-term concerns include a lack of standards for IoT devices, which affects all stakeholders of the company. Therefore, IoT companies are vulnerable when incidents occur (O'Brien, 2015). One of the principal arguments generating claims and lawsuits will be a lack of governance by the companies to account for IoT protections, as well as absence or inadequacy of safety standards. Standards are being created by the Institute of Electrical and Electronics Engineers (IEEE) and the International Telecommunications Union (ITU), based on the creation of a threat model for risks. As a part of this initiative, proprietary standards are also being implemented by organizations but are not yet completed (O'Brien, 2015). Yet, it is argued that IoT cannot be 100% secure, despite all regulatory attempts (O'Brien, 2015).

Smart Home Technology

Akin to control systems, Smart Home technology ecosystems involves a diverse array of automation systems. It is now possible to program different electronic equipment (such as a home stereo system) to turn on at a predetermined time. These tasks, once requiring manual completion, can be controlled using a Smartphone that acts as a remote control for the home (Pfledderer, 2015). In 2015, the Smart Home technology was valued at approximately $60 billion. When the Smart Home technology

first emerged, its purpose was to automate routine household tasks. The Smart Home could be programmed to alter the thermostat and thus ensure that the ambient temperature reaches a specific setting at a certain time, turn on electronics remotely, automatically turn on exterior lights (similar to motion detector lights), turn on outside irrigation (such as sprinklers), and other tasks. Today, Smart Home technology has evolved to create one platform, such as an app, to integrate all Smart Home technologies involved. These may include electronics (stereo or television), lights (outside or inside lights), and/or irrigation (Pfledderer, 2015). Wink, for example, was developed by General Electric and Quirky and currently has the capacity to integrate approximately 25 devices with one remote control. According to the company, the purpose of this technology is to solve everyday problems. Most importantly, the technology is adaptable to all needs (Pfledderer, 2015).

Despite the benefits for many users, the Smart Home market is facing some difficulties. Research conducted by the Consumer Electronics Association and Parks Association shows that most consumers (approximately two-thirds) that have broadband access in their households have little or no familiarity with the Smart Home technologies and often do not know where Smart Home technologies can be purchased (Pfledderer, 2015). Therefore, the market has not yet been adapted to the new technologies. Moreover, as the use of this technology becomes more prevalent, new vulnerabilities and opportunities for cyber-crime will emerge (Pfledderer, 2015).

Available data indicates that millions of homeowners are embracing Smart Home technology—such as wireless X10, ZigBee, and Z-Wave devices—to enhance flexibility and save time. Smart technology devices include wireless doorbells, appliance controls, wireless smoke detectors, and wireless light switches (Srinivasan, 2012). The acceptance

and use of Smart Home technology is unsurprising considering the role that technology plays in modern society. For example, technology has been developed over recent decades to improve and/or enhance social welfare. Social welfare has realized new ways for interaction to occur between humans and the environment, as well as with those computational things of interest (Mendes, Godina, Rodrigues, Matias, & Catalão, 2015). Recently, technology has been utilized to increase comfort and well-being, as evident in the growing use of social theories in technology design. Energy consumption/reduction monitoring is one of the many ways through which well-being has been enhanced, and this initiative was a result of concerns considering the growing use of resources (Mendes et al., 2015).

According to Mendes et al. (2015), Smart Home technology is a response to four different factors:

- Significant advances in semiconductor technology, which have allowed computing and electronic devices to become an integral part of daily life
- Increased processing power for microcontroller units
- Integration of small sensor nodes that are capable of maintaining data through complex techniques
- Rapid development of wireless technology (Mendes et al., 2015)

Therefore, major market brands are intently focused on making the household products with a frequent turnover more intelligent (e.g., appliances, Smartphones, multimedia systems, lighting, heating, and home alarm systems). One of the enabling communication standards that connect the aforementioned categories of devices is Z-Wave technologies. Z-Wave is a highly compatible wireless technology typically

employed in residential environments for controlling systems, monitoring devices, and reading device statuses (Z-Wave_Alliance, 2015). Despite the potentially positive aspects of greater reliance on technology, homes are left vulnerable through different threats, such as Smart Home technology and mobile device design vulnerabilities (Wright, 2008).

Smart Home Technology Vulnerabilities

Tripwire, a Smart Home security company, has found vulnerabilities in three popular Smart Home hubs—SmartThings, Vera Control, and Wink (Lemos, 2015). Due to these vulnerabilities, Smart Homes are more likely to be targeted by hackers. Web sites of applications designed to be malicious serve as the common vector used by attackers to exploit vulnerabilities and allow unauthorized users to gain control of Smart Home hubs. To determine vulnerabilities, Tripwire has tested the hubs and has uncovered critical flaws. These critical flaws represent vulnerabilities that could provide opportunities for attackers to eavesdrop on communications or even take control of the hub (Lemos, 2015). In November 2014, several common issues were found, such as command injection that would provide root access to the Wink hub. According to Craig Young's research, these vulnerabilities were discovered with little difficulty (Lemos, 2015). The main vulnerabilities in the Wink hub pertained to SQL-injections, which could allow an attacker to issue commands to other smart devices, access unauthorized functions to the hub and wireless network, or even establish and load a backdoor (Lemos, 2015; Microsoft_Security_Bulletin_MS10-089, 2010). Immediately upon discovering the vulnerabilities, Wink repaired the flaws. Vera Control vulnerabilities stem from cross-site request forgery (CSRF) issues. CSRF issues have the potential to allow

nefarious computational instructions to be processed by the hub by permitting an unauthorized user to access a victim's device, or cause the victim to view attacker-controlled Web content, thus providing the attacker with unauthorized access to personal information (Lemos, 2015). As of February 2015, Vera Control had not repaired the issues. However, a minor security issue was found in the SmartThings hub, as it was limited to the potential for eavesdropping in limited situations (Lemos, 2015). SmartThings issued mitigations as a part of a mandatory automatic update for all active hubs, while also allowing inactive hubs to connect to the SmartThings service and receive the update. These types of hubs used in Smart Homes utilize embedded hardware, due to which the built-in security is in most cases inferior to that found in traditional security systems (Lemos, 2015). As a result, there are industry-wide problems caused by low-cost embedded devices. Flaws inherent in these devices demonstrate that any error can cause a significant vulnerability, causing immense damage and/or harm to the system. These hubs lack basic protections provided by most modern operating systems for PCs (Lemos, 2015).

The issues uncovered by Tripwire confirmed the presence of concerns regarding the ability of attackers to control Smart Home functionalities. For example, Smart Home hubs are specifically designed to control different aspects of the home, such as lighting, heating, irrigation, and even locks and cameras (Tripwire Inc., 2015a, 2015b). The issues uncovered by Tripwire were especially concerning because they provided means for successful exploitation, such as allowing hackers to determine when the house is empty (Tripwire Inc., 2015a, 2015b). Consequently, it would be possible to utilize the network to change settings within the Smart Home.

While the use of Smart Home hubs has increased, functionality is still more important than security, which is a common drawback of newer technologies. Young, however, cautioned that, although the current threat is low, it would inevitably increase (Tripwire Inc., 2015a, 2015b). This potential threat will occur because attackers will eventually realize that a significant amount of information can be gained from attacking these hubs (Tripwire Inc., 2015a, 2015b). Therefore, Smart Home hubs can be exploited to decrease security in homes and/or cause physical damage to the home being attacked, or even its occupants. Some Smart Home hubs are particularly vulnerable to executions occurring through exoteric controls, which can allow hackers to hide on the network (Tripwire Inc., 2015a, 2015b).

Risks users are exposed to are also becoming greater, given the increases in IoT and communication abilities related to devices connected to IoT (ConsumerReports, 2015). Yet, these communication abilities offer convenience to consumers. Thus, there must be a balance between practicality and protection, as Smart Home devices have capabilities to send personal data to corporate servers, commonly used in ways that consumers cannot control (ConsumerReports, 2015). Therefore, private information can be collected, combined, and exploited. This aggregation commonly occurs by marketers, but such data can also be stolen (ConsumerReports, 2015). The concerns regarding stolen aggregated private information have led to politicians, such as U.S. Senator Ed Markey, to call for more scrutiny regarding IoT. Markey argued that rules that are strong and can be legally enforced to protect personal information are urgently needed (ConsumerReports, 2015). There were approximately 109 million wearable devices in use globally at the end of 2014. As a result, millions of data items was generated,

confirming that technology is more advanced than current privacy laws (ConsumerReports, 2015).

Smart Home vulnerabilities are a common fear of consumers. According to one study by Veracode, reliance on smart devices increases vulnerabilities. As a part of this investigation, R. Brown (2015) reviewed four manufacturers—Chamberlain, SmartThings, Ubi, and Wink. The devices reviewed were MyQ Garage, MyQ Gateway, home automation hub, voice recognition box, and hub and relay control panel (R. Brown, 2015). The following four categories were employed in the evaluation:

- Potential vulnerabilities implicit in communication between devices and the cloud
- Potential vulnerabilities implicit in communication between the device and the remote control
- Potential vulnerabilities related to the device interfaces
- Potential vulnerabilities pertaining to debugging interfaces, which might allow unauthorized access to commands at the engineering level

The findings revealed that Ubi was the least protected (R. Brown, 2015). Many issues affecting Ubi were identified, such as limited encryption during communications between devices and the cloud, password requirement weaknesses, and few access restrictions to its debugging interface (R. Brown, 2015).

These vulnerabilities through home automation technologies can allow anyone, including those with limited technical abilities, to access properties all over the world. Honeywell, known as one of the biggest U.S. technology manufacturers, has two such flaws. Additionally, it is relatively straightforward to access other users' Honeywell

Tuxedo Touch web interfaces through unauthorized access. As a result, those controlling these interfaces have capabilities to manage the home components that are connected to Honeywell's Tuxedo Touch web (Fox-Brewster, 2015). These flaws could provide an attacker opportunity to control devices or processes, such as security cameras. Other vulnerabilities found in the authentication procedure were significant because there was no requirement for interactions between the attacker and the one being attacked (Fox-Brewster, 2015). The flaws can also be utilized to provide information regarding when homes are unoccupied. Furthermore, attackers can open the locks to the home without authorization and/or change alarm settings. These activities also allow unauthorized users to turn smart hubs into zombies through accessing local area networks (Fox-Brewster, 2015). In other cases, a malicious web page can be used to provide the attacker with complete and total access and control of the system through the exploitation of input validation failures on the web interfaces. Through the exploitation possibilities found, hackers would be able to utilize Smart Home technology vulnerabilities to use the hub for distributed denial of service (DDoS) purposes (Tripwire Inc., 2015a, 2015b). Therefore, as Tripwire shows, due to the serious flaws found in popular systems purchased, homes may be at risk (Moore, 2015). Furthermore, although the threat is low, it is expected to increase as technology becomes more prevalent and more homes become equipped with Smart Home technologies (Moore, 2015). Thus, there are very real risks with numerous points of entry. It is important for vendors to acknowledge these vulnerabilities as well as provide regular updates aimed at mitigating them. Furthermore, consumers need to recognize and understand the risks of Smart Home technology and apply the updates (Moore, 2015).

Extant studies suggest that over 1 billion connected devices used in millions of Smart Homes will have emerged by 2017 (eRadar, 2015); Gartner & Gartner, 2015). However, numerous vulnerabilities exist even in conjunction with single-function devices (such as lights), as well as in fully automated homes (eRadar, 2015; Gartner & Gartner, 2015; Weinberg, Milne, Andonova, & Hajjat, 2015). Therefore, growing evidence of access violations through smart devices to Smart Homes exists.

Currently, no major breach has been attributed to home security or a related automation system; yet, due to the vulnerabilities, the potential exists (Griffin, 2014a). Popular security expos routinely reveal practical research that validates the simplicity involved in comprising basic security measures. For example, researchers have demonstrated the ability to exploit a Samsung smart fridge through an invalid SSL implementation (Venda, 2015). In fact, according to a Hewlett-Packard study, 70% of common IoT devices have different vulnerabilities, such as password weaknesses, lack of communications encryption, and lack of user access permissions (Griffin, 2014a). Other vulnerabilities include potential for cyber intrusions and vulnerable systems, which may allow hackers access because systems are commonly controlled through remote controls (such as a Smartphone app or web portal), enabling criminals to break into Smartphones, and/or tablets in order to steal private and/or corporate data (Griffin, 2014a). These issues increase in scope and prevalence because the devices used in Smart Home technology are non-intelligent and operate individually. As a result, they can be controlled through remote functions. At the same time, since this technology is non-intelligent, they are afforded few authentication mechanisms, if any (Griffin, 2014a).

Moreover, some devices are susceptible to user account resets due to insufficient password and credential complexity in an attempt to retain simplicity for the typical daily user (Neagle, 2015). As technicalities increase, vulnerabilities increase because manufacturers failed to design these devices securely, depending instead on the end user to secure the devices (Neagle, 2015). Thus, in some cases, Smart Home technology can be disabled, allowing criminals time to enter the home, and then re-activate the system. Some higher-end Smart Home products are appropriately focused on security in their designs. This trend is expected to increase as the market and technology mature. However, current IoT security standards continue to be developed and established (Neagle, 2015).

Exploratory Research

The expansion of artificial intelligence (AI) in distributed computing platforms, cloud technologies, ubiquitous devices, and Smart Home ecosystems has evolved the notions of research in the field of computer science to include extended interpretations (Sharoff, 1995). Sharoff's (1995) study is based on the assertion that a paradigm of human-independent intelligent devices fits into philosophical investigations. According to the author, in computer science, philosophical investigations can follow constructs similar to those employed in the cognitive sciences. Marshall and Rossman (1999) concurred with this view, further noting that exploratory research in the fields of cognitive science and computer science helps determine how patterns are interrelated. Ubiquitous devices and distributed computing systems involve many aspects that adapt and learn as they interact and integrate information (Holland, 2006). The concept of information integration of autonomous device interaction beyond human actions is used

in the present study to discover naturalizations that occur and affect vulnerability exposure and cyber security (Schroeder, 2015).

Other theoretical approaches to computer science research relevant to exploratory research include Heidegger's ontological worldview (A. Brown, 2015). Brown suggested that the widespread acceptance of information technology artifacts used in everyday life stems from the seminal concept of existential ontology. In existential Heidegger ontology, phenomenological research is conducted when the aim is to qualify variances in organizational usage. The theoretical basis of Heidegger ontology, as applied to phenomenological research in computer science, is limited to interpretivist and empirical constructivist methods and implicitly demands that data collection involves some human element (A. Brown, 2015). Thus, owing to the use of the Heidegger's ontological research design, in the present study, it was not possible to provide a formulative assessment of interactions between devices and the intuitive operation of the Smart Home ecosystem.

Qualitative exploratory research is particularly useful for the scientific community, as it facilitates conducting formulative research on integral parts of a developing system (Silhavy, Senkerik, Oplatkova, Silhavy, & Prokopova, 2014). In such an approach, data collection occurs through a wide array of systemic methods, including interviews, participant reports, and detailed observations. While human involvement is, as noted above, valuable, the researcher must remain minimally intrusive, to avoid introducing bias in any observable results. Data analysis is equally comprehensive and systemic, whereby the method of analysis follows the nature of the data itself (Waters, n.d.). In addition, by identifying commonalities and correlations in data, common themes

are allowed to emerge. This approach allows the researcher to assign meaning to abstract variables which may or may not qualify as influential factors or essential aspects (Waters, n.d.). The results yielded by qualitative exploratory research can unveil findings and themes that relate to theories presented in empirical studies (Waters, n.d.). The discussion of the findings and emergent themes not only helps elucidate the lived experience but also expands on the themes pertinent to similar contexts described in other sources.

Case Study

Case study approach is adopted when the goal is to conduct an empirical evaluative inquiry into a phenomenon within its real-life context (Creswell, 2013; Merriam, 2009; Simons, 2009; Yin, 2014). Case studies assist in evaluating emergent technologies, due to the implicit assumption of contextual transference and generalization. It is imperative to note that, in the context of the present study, these assumptions were made solely in order to facilitate a high-level functional overview of the particular capabilities of technology, aligned with the described CA theory. The case study construct is significant to emergent technology capabilities as it draws an in-depth singularity of a phenomenon being studied (Simons, 2009). The case study approach, within the scope of emergent technology, helps explore the problems at the juncture of Smart Home security and cyber intrusions, thus illuminating shared characteristics. More specifically, in the present investigation, the case study is designed to provide insight into inherent or overlooked Smart Home security issues, as a means of redrawing generalizations pertinent to personal cyber security. This design framework enhances collective understanding of relative tertiary effects (Merriam, 2009). Yin (2014)

proposed a multiple case sampling procedure that aggressively evaluates cross-case implications by refining initial theories and data collection methods, and subsequently correlating findings with a series of cases (see Figure 2). Figure 2 depicts theory development as the initial step in designing a case study. Once a theory is developed, the researcher proceeds with case selection and defining specific measures in the data collection process. Yin (2014) further explored how the conduct of each case study report should evolve to refine and indicate the extent to which logic is replicated across each case study. If required, the researcher then contrasts the results (represented by the dash red line feedback loop). The steps associated with the depicted feedback process represent a situation where important discovery occurs during the conduct of one of the individual case studies, warranting reconsideration of one or more original theoretical propositions (Yin, 2014). At the end of each case study, individual case reports are written, as this assists in the development of cross-case conclusions and contributes to the quality and comprehensiveness of the final case report.

Figure 2. Multiple Case Study Procedure

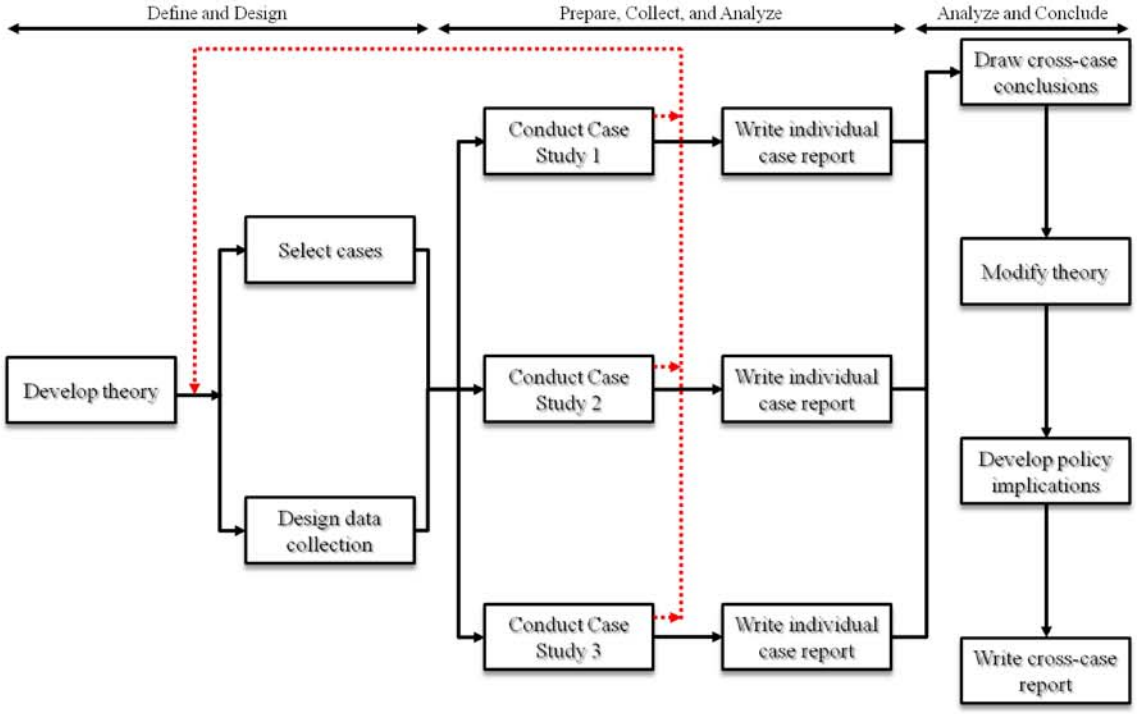

Figure 2. Multiple Case Study Procedure. From *Case study research: Design and methods* (B. Bauhaus Ed., 5th ed.), by R. K. Yin, 2014.

Summary of Literature Review

The review of the pertinent literature presented in this chapter confirmed that cybersecurity efforts regarding IoT security need to be advanced. This advancement is pivotal because cyber-attacks have become more sophisticated and require alignment with the observable experiences within the Smart Home ecosystem (Dunn Cavelty, 2014). It is expected that the need for cyber security will rapidly increase as technologies, ubiquitous devices, means of connecting to the Internet without human involvement, and the sophistication of cyber-attacks continue to advance. In fact, due to the advancements in technology, cyber-attacks have evolved and are expected to escalate into cyber wars. Currently, cyber-attacks are highly organized, causing governments of

many countries to invest extensive funds into the prevention and the mitigation of damage caused by cyber-attacks. The threat of cyber-attacks has increased and has expanded into many different areas. In particular, organizations that handle sensitive data (such as healthcare/insurance agencies and retailers) have become vulnerable, along with users of smart equipment (such as appliances at home that are controlled remotely). Evidence shows that the entire globe has become vulnerable to this threat, and the Smart Home is no exception (Dunn Cavelty, 2014).

The exact cost of cyber-crime is difficult to estimate, not only because some damage cannot be easily quantified, but also because such breaches are insufficiently reported. Problems related to cyber-crime also involve investigation barriers, which commonly enable perpetrators to continue to attack other victims. Due to the immense media attention, fear of negative publicity or consumer backlash remains one of the major investigation barriers (J. Smith, 2003). Inadequate security measures and numerous vulnerabilities are partially the reason that cyber-crime threats exist. Therefore, as technology usage increases, unless the security measures keep the pace, they will become increasingly inadequate. Thus, more attacks will be attempted, many of which will be successful. Common attack attempts using malware are becoming more advanced, more common, and more dangerous.

The focus of the CIA Triad was to provide a framework to balance security and technology advancement. The Triad focuses on benchmarking the effective security measures and eliminating or decreasing risks. Although the Triad has been proven effective, it cannot prevent all attacks, especially as they continue to advance is scope and severity. The Triad, however, remains significant because it focuses on balancing

acceptable levels of data security, accommodations for privacy, obtainable non-repudiation levels, and consistent access (Fenrich, 2007, 2008). The most frequent attacks occur against organizations that store and maintain substantial amounts of sensitive data, including governmental agencies. The Smart Home ecosystem has yet to suffer the same distributed onslaught of cyber intrusions. However, the dynamics and diversity of the technologies introduced to the Smart Home broaden the attack surface and invite the possibilities of complex cyber intrusions. As a result, cyber-attacks threaten the validity and usefulness of the Triad. This threat is especially significant as it is envisaged that Smart Home technology will become widespread.

Smart Home technology is part of IoE and IoT and can be used professionally and personally. The goal of this type of technology is to enhance convenience while reaping positive economic benefits. However, in order for these benefits to be fully realized, cyber security that encapsulates the full extent of IoE and IoT is necessary, because only such a comprehensive approach can assist in protecting all types of smart technology, rather than relying on individualized security for specific products or brands. IoE and IoT represent significant security challenges due to the complexity and diversity of the devices utilized. Therefore, it is evident that some of the seemingly most convenient devices and functionalities (such as the ability to turn the radio/stereo on) may become the prominent focus of targeted cyber intrusions. Victims of such attacks are less likely to notice "insignificant" invasions, just as unnoticed small transactions perpetuate financial crimes, as they are rarely identified, yet, when compiled, manifest in significant invasions. The Smart Home inherits the technology concepts introduced in IoT and IoE. Thus, it is important to be aware of these vulnerabilities, failures in security, and potential

vectors through which cyber-attacks can occur. In this way, security within the larger architecture of the IoT, the IoE, and the Smart Home ecosystem can be increased or improved to protect all users and all data.

CHAPTER 3

Methodology

Overview of the Research

Yin (2014) employed the multiple case study inquiry as a method to evaluate emergent technologies, as described in Chapter 2. This strategy was adopted in the present study. The aim of the qualitative exploratory multiple case study inquiry described in this work was to explore using open source tools and investigate the behavioral heuristics of the Smart Home ecosystem at the data link level, observing frame PDU data for TCP/UDP conversations. This necessitated constructing an IoT ecosystem, comprising of a controlled Smart Home environment, which was observed during a typical life cycle of initial configuration and routine usage tasks, whereby the data collected was subsequently analyzed.

The chosen research approach embodies emergent object behavior present in the Smart Home ecosystem. Case study research brings clarity to complex issues in the field of IoT by extending the real-life experience and situational context, allowing the Smart Home ecosystem to be examined. The case studies discussed here are only limited by lack of understanding; hence, research in the field of Smart Home ecosystems can be expanded to explore applications prominent in the cyber security field. When meeting the aims of the present investigation, the case study approach was preferred to other qualitative research strategies (e.g., experimentation, archival, and historical analysis) because emergent object behavior and vulnerabilities in the Smart Home ecosystem can

be observed in a real life application (Yin, 2014). It is assumed that cyber-attack prevention in the resource-limited home environment is insufficiently combated using conventional tools and applications, such as antivirus software, firewalls, and other security measures (Agapov & Rahman, 2008). Additionally, practitioners in the field of the Smart Home ecosystem development have identified areas of concern regarding privacy and security in IoT (Albert, 2015; Babar, Stango, Prasad, Sen, & Prasad, 2011; R. Brown, 2015; ConsumerReports, 2015; Demblewski, 2015; Neagle, 2015). Privacy and security requirements in Smart Home ecosystem differ tremendously from those pertinent to personal and mobile computing platforms (Albert, 2015; Babar et al., 2011; R. Brown, 2015; ConsumerReports, 2015; Demblewski, 2015; Neagle, 2015). As a part of the present study, a vulnerability test was conducted, involving various wireless sensor network (WSN) products, ubiquitous networks, and pervasive computing in the categories of appliances, Smartphones, multimedia systems, lighting, heating, and home alarm systems, all of which operate within the Smart Home domain. Moreover, devices in the Smart Home domain either consume user data or traverse availability prioritized architecture. The case studies described here were thus conducted in an attempt to demonstrate that the LM-CIRT model can be successfully adopted to mitigate threats in the Smart Home ecosystem. In the present study, it was also employed as a means of performing an effective security assessment, as well as to implement an appropriate threat mitigation in the Smart Home ecosystem (see Figure 5). The case study was conducted in a controlled environment, which contained all of the products in the aforementioned categories, described in more detail later in this chapter.

Research Traditions

The research traditions discussed in Chapter 2 expound upon the nature of exploratory research using a qualitative methodology as applied to Smart Home ecosystems. In this study, exploratory research was based on the premise that a paradigm of human-independent intelligent devices in a Smart Home ecosystem can represent the independent interactions that can be observed from a cognitive notion of object behavior, be it intentional or unintentional. The exploratory research framework meets the objectives of discovering vulnerability exposure and cyber security implications by defining the concepts by which information integration and autonomous device interaction is recorded. In conjunction with the case study, exploratory research declares the autonomy of emergent object behavior present in the Smart Home ecosystem.

Figure 3 depicts a recursive evaluation of the Smart Home ecosystem datalink layer protocol data units from the existing Intrusion Kill Chain design model. The proposed case study framework allows building the appropriate case while concurrently developing the data collection methodology to obtain the anticipated results. Following the logical diagram is shown in Figure 3, the researcher sequentially conducted each case study and compiled individual case study reports. In the next phase, the findings yielded by the case studies were utilized in answering the research questions, as well as to determine appropriateness to the case study framework. The relevance of the findings were used to examine whether the research approach required additional propositions, before reporting the overall results. In the event, the proposition inferred from data collection is inadequate (represented by the red dotted line in the diagram), the researcher must re-evaluate the case study framework and the data collection procedures to identify

potential shortcomings. Once this process is completed, the researcher can resume the case study, employing the modified framework and data collection procedures, summarizing findings pertinent to each case. The researcher then continues to record preliminary cross-case conclusions and proceeds through the case study sequence using the original propositions, the original or modified case study framework, and the original or modified data collection procedures as a guide (represented by the black dotted line). The data obtained through the case studies allow the researcher to validate the data's alignment with the existing theories. In the present study, the case study data was examined in relation to Intrusion Kill Chain Theory (see Table 1), whereby all applicable implications inferred from the data analysis were carefully recorded. Finally, the researcher concluded the reports, detailing all study findings, and summarizing the key findings as relevant to inter-case relationships.

Figure 3. Multiple Case Study Design.

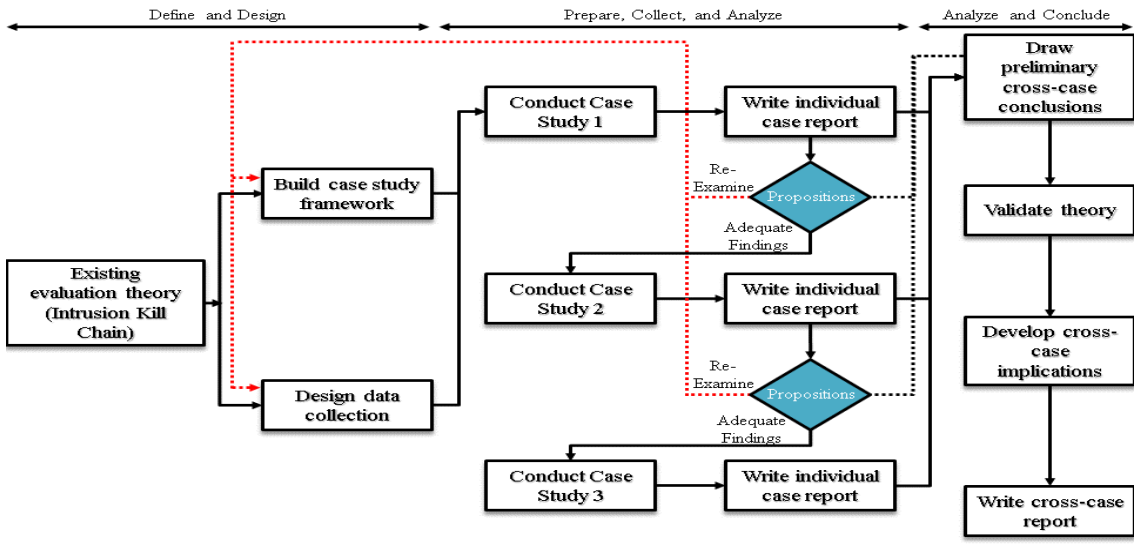

Figure 3. Multiple Case Study Design. From *Case study research: Design and methods* (B. Bauhaus Ed., 5th ed.), by R. K. Yin, 2014.

Research Questions and Propositions

Babar et al. (2011) summarized the potential attacks (see Figure 4) hackers and thieves could perform against the Smart Home ecosystem, including home networking, commercial, mobile, and fixed devices (Babar et al., 2011). However, in their work, the authors focused primarily on hardware-centric mitigations to combat the potential attacks. Moreover, they posited that software could be effective in mitigating potential attacks through cost and power consumption. Empirical evidence suggests that these can be critical factors when applying a software solution exclusively.

Figure 4. IoT device attacks applied to the CIA Triad.

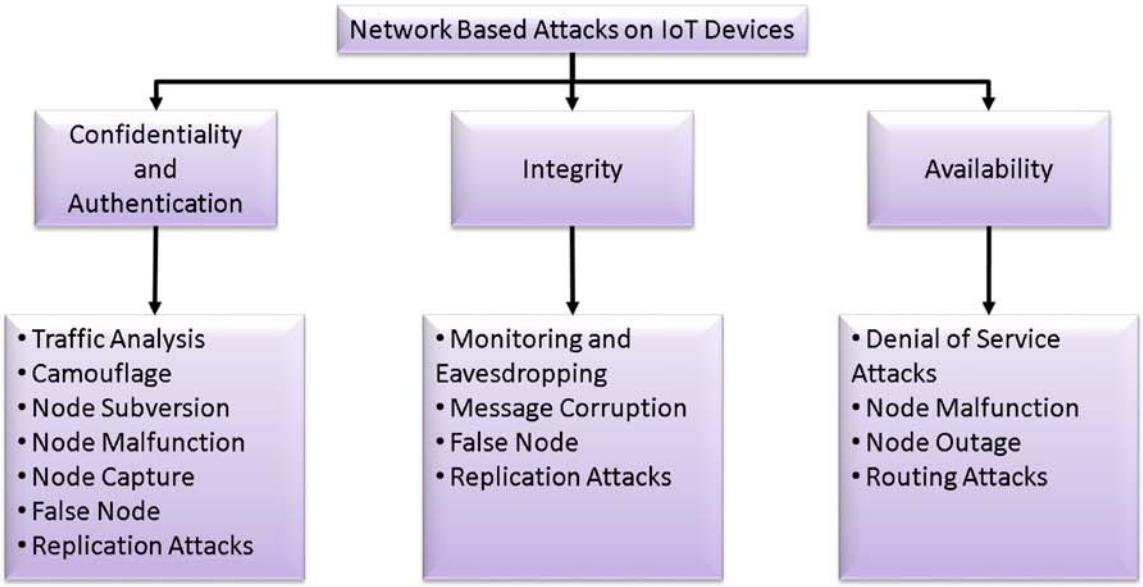

Figure 4. IoT device attacks applied to the CIA Triad. Adapted from *Proposed embedded security framework for Internet of Things (IoT),* by S., Babar, A., Stango, N., Prasad, J., Sen, and R. Prasad, 2011.

Research Design

The multiple case studies conducted as a part of this research were designed to approach, systematically, the high volume of data that was collected during the execution

of this study. This study presents an array of tools available on the Debian 7 platform, which is designed to highlight packet content in transit from a node to an endpoint. The tools available include network vulnerability scans and network forensics tools. This study was conducted using a desktop computer with a Debian 7 based operating system to act as a software-based sensor at the pivotal borders of the Smart Home ecosystem network environment. The first case study was designed to counter attacker-driven reconnaissance efforts. In addition, its aim was to enhance discovery of any existing implants on the Smart Home ecosystem network and/or determine the visibility of common vulnerabilities from internal and external network vantages. The reconnaissance/discovery phase of the Intrusion Kill Chain illuminates a victim's typical device-specific vulnerabilities. Because most Smart Home devices are not purposed to process a broad array of file formats (Abu-Elkheir, Hayajneh, & Ali, 2013; Working_Party, 2010), the weaponization of any payload is limited to execution of system-specific tasks, e.g., firmware upgrades or device health status (Babar et al., 2011). Both reconnaissance/discovery and weaponization evaluation efforts performed as a part of the first case study helped determine how secure Smart Home systems function independently from other devices (aligned with RQ1). The specific goal was to determine confidentiality and authentication susceptibility to cyber intrusions, whereby it was expected that possible vulnerabilities (or threats) would manifest based on each device's response. As previously noted, it was also envisaged that, if the devices outlined in the case study do respond with a positive identification of an exploited vulnerability, the case study data collection process would be revised to allow for a more comprehensive analysis of the suspected node and the endpoint communication

behaviors. The recorded packet capture and sensory data of the first case study were used during the second case study to help filter benign endpoint TCP/UDP conversations that have occurred because of automated node communications. The aim of case study two was to examine the types of behavioral data exchange or aggregate device communication that occur between Smart Home objects and effect fundamental security levels (aligned with RQ2). The objective was to determine node-to-node confidentiality, authentication, and integrity susceptibility to cyber intrusions. During the delivery, exploitation and installation phases of a cyber intrusion, an attacker must be able to manipulate the receiving devices' remote procedure call (RPC or function call) on the receiving device's registry stack (Angelucci, 2014; Babar et al., 2011). A cyber intrusion must also meet acceptable thresholds governed by the device's registry, inject acceptable instructions in the remote device's instruction pointer, have the device execute malicious instructions, and adequately redirect the instruction pointer's anticipated state to an appropriate registry location (Englander, 2009; Raucher, 2015). Tools that are described in detail later in this chapter were employed to illuminate the cyber intrusion process. The procedures required to analyze these processes may expose the possibility of this vulnerability (or threat), provided that actual device complexity exists to respond to RPC instructions, per device or collectively. In an event that the devices outlined in the case study did respond with a positive identification of an exploited vulnerability, the case study design theory was revised to analyze in greater detail the suspected node(s)' endpoint communication behaviors. Moreover, an advanced IDS rule was developed to alert on the observed action. The recorded signature rules, packet capture, or sensory data from the first and second case studies were used to provide a more advanced

signature rule set. The final rule set was evaluated to mitigate the occurrence of false positive or false negative IDS alerts. The effective IDS control state was recorded and used in the third case study to alert and notify of the existence of applicable payloads. Case study three was the culmination of the aforementioned efforts, whereby it incorporated all observations and controls employed in the first and second case study. Its aim was to identify the emergent security issues related to Smart Home object behavior (aligned with RQ3). The case study sought to determine how personal safety relating to cyber security, personal cyber security resilience to cyber-threats, and personally identifiable information relating to undisclosed information collection is impacted in a real life context. The command and control and actions on objective phases of the Intrusion Kill Chain model would typically require the cyber intrusion actor (or function) to create a reliable path to the node it controls. Subsequently, the cyber intruder would relay commands through the victim's architecture, and force the controlled nodes to execute instructions at will (with or without sending an acknowledgment of successful code execution) (Hutchins et al., 2011). The reports generated upon completion of the prior case studies were evaluated in the third case study to determine if the observed conditions aided in the discovery of malicious traffic. This compilation of data included private usage information (or any other privacy information), detailed information about configurations of devices if such data was communicated, their firmware versions, or any other information that would give the attacker useful reconnaissance information.

Sample

The sample, in the context of the present study, pertains to the devices involved in the controlled environment. In other words, it pertains to all devices that can be categorized as Smart Home devices that have the capacity to exhibit behavior beyond the intended design. As devices in a controlled environment, rather than humans, were the object of investigation, this definition of sample is not conventional. In addition, in the controlled environment, controlled refers to the fact that the researcher owns and operates the itemized equipment as an average consumer. Figure depicts the high-level overview of the constructed controlled Smart Home ecosystem. In the controlled environment, the nodes listed in Table 2 were configured as per manufacturer recommendations and were connected accordingly to the Smart Home ecosystem as depicted. Each node can communicate with external addresses either through the Internet Service Provider (ISP) or through the cellular provider's data service. A switch was used to connect additional nodes that span beyond the connections available on the border router. The network traffic sensor (represented by the yellow triangle on the right) for the wired connection uses a hub to expand possible connections between the router and the modem. This hub connection connects to the computer and the network interface card (NIC) was set to passive promiscuous mode in order to minimize interference with routed traffic between the router and the modem. Both the modem and the router were configured as per manufacturer-recommended settings for both wired (represented by the solid green lines) and wireless (represented by the solid red line) connections, as applicable. The network traffic sensor (represented by the yellow triangle on the left) for the wireless connection uses a USB dongle to create a direct link between the PC and sub-1 GHz frequencies,

which is within the Z-Wave frequency range (Z-Wave_Alliance, 2015). The Z-Wave panel was configured by a Vivint technician and was configured to their recommended standards.

Figure 5. Diagram of the Smart Home ecosystem.

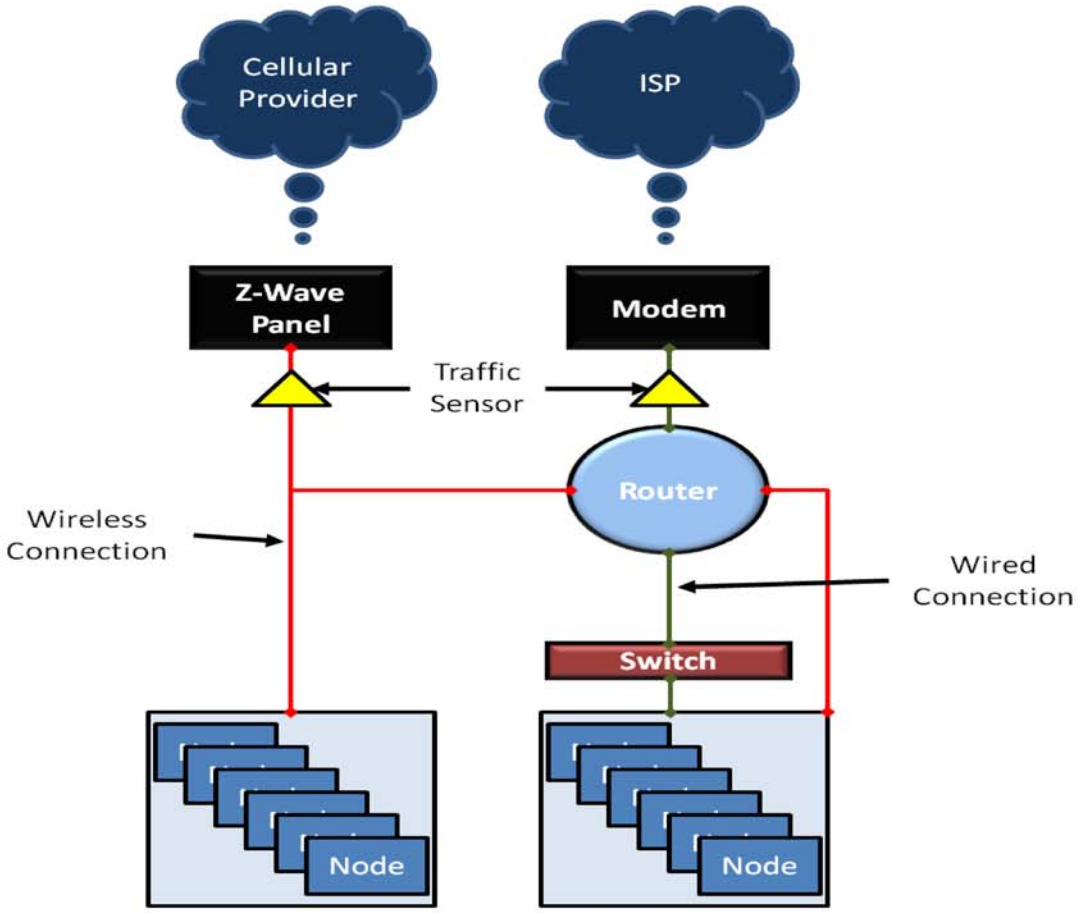

Figure 5. Diagram of the Smart Home ecosystem. Adapted from "Data management for the internet of things: Design primitives and solution," by M., Abu-Elkheir, M., Hayajneh, & N. A. Ali, 2013, *Sensors (Basel), 13*(11), 15582-15612; "Network Challenges for Cyber-Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring," by S., Ali, S. B.,Qaisar, H., Saeed, M. F., Khan, M., Naeem, & Anpalagan, A., 2015, *Sensors (Basel), 15*(4), 7172-7205.

Table 2 provides a list of the nodes in the Smart Home ecosystem that was tested for emergent behavior. The table provides information on the manufacturer, the model

number, and how each appropriate device communicates according to the manufacturer configuration, along with the category (in terms of the typical arrangement in a Smart Home ecosystem).

Table 2

IoT Ecosystem Components

Node	Manufacturer	Model	Communications	Category
Home Router	NETGEAR	R6300v2	Wireless & Wired	Home Infrastructure
Switch	Cisco	Catalyst Express 500	Wired	Home Infrastructure
Modem	NETGEAR	CM400	Wired	Home Infrastructure
Z-Wave Range Extender/Repeater	Aeon Labs Aeotec	DSD37-ZWUS	Z-Wave	Home Infrastructure
Power Line Adapter	NETGEAR	XAV5201	Wireless & Wired	Home Infrastructure
Electronic Deadbolt	Kwikset	910	Z-Wave	Home Security
Wireless Keypad	2GIG Technologies	2GIG-PAD1-345	Z-Wave	Home Security
Door/Window Contact Sensor	2GIG Technologies	2GIG-DW10-345	Z-Wave	Home Security
Wireless Control Panel	2GIG Technologies	2GIG-CNTRL1-345	Z-Wave	Home Security
Takeover Module	2GIG Technologies	2GIG-TAKE-345	Z-Wave	Home Security
Passive infrared motion detector	2GIG Technologies	2GIG-PIR1-345	Z-Wave	Home Security
Smoke/Heat Detector	2GIG Technologies	2GIG-SMKT2-345	Z-Wave	Home Security
Internal GSM Antenna	2GIG Technologies	2GIG-ANT1	Cellular	Home Security
External In-Wall GSM Antenna	2GIG Technologies	2GIG-ANT1X	Cellular	Home Security
AT&T Go-Control Vivint	2GIG Technologies	2GIG-GC3GA-V	Cellular	Home Security
Radio Thermostat	2GIG Technologies	2GIG-Z-CT100	Z-Wave	HVAC
Z-Wave In-Wall On/Off Switch	LEVITON	DZS15-1LW DZC	Z-Wave	lighting
Z-Wave Wireless Lighting Control Dimmer Switch	General Electric	12724	Z-Wave	lighting
Multimedia system	ROKU		Wireless	Multimedia Systems
TV	Sharp	LC-60LE640U	Wireless & Wired	Multimedia Systems
Satellite Receiver	Direct TV	HR44-700	Wireless	Multimedia Systems
Gaming System	PlayStation3	CECH-2501A	Wireless	Multimedia Systems
Computer	Alienware		Wireless & Wired	Multimedia Systems
Network Attached Storage	Seagate	NAS440	Wired	Multimedia Systems
Smart Phone	Samsung	SM-N920V	Wireless & Cellular	Multimedia Systems
Tablet	Samsung	SM-P905V		Multimedia Systems
Multimedia system	ROKU	2710X	Wireless	Multimedia Systems
Computer	Hewlett Packard	ZUA5070D57	USB, Z-Wave, Wireless, & Wired	Multimedia Systems
Sensor Module	Texas Instruments	CC1111EMK	USB & Z-Wave	Test & Evaluation
Sensor Module Programmer	Travis Goodspeed	GoodFET v42 1279	USB & Z-Wave	Test & Evaluation

Instrumentation, Data Collection, and Analysis

The case study instrumentation and data collection plan were designed to facilitate recording as much detail as possible. This not only assisted with the individual and cross-case study analysis but also allowed compiling the final results and reaching study conclusions. The effectiveness of each case study was assessed based on the recommendations made by the authorities in the field of IoT security, specifically the NIST SP 800-53 technical safeguards or countermeasures that, if implemented, could prevent or ameliorate cyber intrusion events (Abrams & Weiss, 2007). Individual case studies are described in detail in the subsequent sections.

Case Study 1

Case study1 data was collected via Wireshark (an open-source packet capture software), which allows for the full packet capture of all TCP/UDP connection sessions through the wired gateway in and out of the Smart Home ecosystem. TCP/UDP traffic was passively observed through the wired gateway using a throwing Star LAN TAP as a passive Ethernet tap. Additionally, Z-Wave traffic was captured with the Texas Instruments CC1111EMK, which allowed the capture of traffic using Z-Force (open source Z-Wave specific traffic capture software, (Fouladi & Ghanoun, 2013)) in the sub-1 GHz frequency range in which Z-Wave traffic operates.

Raw data was analyzed to determine endpoint origins and terminations (see Table 6). The collection of externally viewed conversations assists in the analysis of TCP/UDP traffic viewable from endpoint to endpoint. In this case study, traffic was analyzed to determine the location of the associated node communications. Extensive analysis was also conducted on externally viewed conversations to determine if the traffic can be

monitored from an external source beyond the router. The collection of internally viewed conversations assisted in the evaluation of TCP/UDP traffic communicating laterally with other devices. Analysis of internally viewed conversations allowed identifying nodes or devices that communicate with other internal devices, as well as elucidating the purpose of this exchange. Subsequently, conversations that contain any payload, without regard to purpose or function, were recorded to identify if the observed traffic should be occurring with any external or internal entities. Table 3 displays a coding matrix that helps to summarize sample data that emerged from traffic analysis of external conversations from outside the network, internal to the network, and any associated conversation payloads from outside or within the network. A coding matrix is significant to data collection, as it assists with identifying areas where further research of the observed activity is required.

Table 3

Case Study 1 Data Collection Template

Node	**External Conversations**	**Internal Conversations**	**Payload**
Sample 1	Activity	Activity	Contents Summary

Case Study 2

The data collected through the first case study was analyzed in the second case study in order to develop a custom IoT-focused rule set for the open source Debian 7 based operating system network intrusion detection system (NIDS) solution (SNORT) configured in line with the community rules profile. This analysis helped establish the extent to which behavioral data exchange or aggregate device communication occurs between IoT objects that effect fundamental security levels. Table 4 displays a coding

matrix that summarizes the sample data that emerged from the IDS alerts that were triggered by external conversations from outside the network directed internally, as well as internal conversations from inside the network directed externally. The relevant internal and external conversations were summarized based on general activity, and the activity was matched to the associated IDS configurations. Similar to case study one, the payloads of the internal and external conversations were recorded and further researched. The configuration that triggered the IDS alerts against the associated conversation traffic was also recorded. Table 4 also helps illuminate node activity associations between the scope of visibility of all Smart Home traffic and IDS alert configurations in identifying Smart Home traffic. It is also important to note that traffic observed outbound or inbound to the controlled environment needs to contain acceptable levels of encryption, as traffic that meets this criterion is publicly visible.

Table 4

Case Study 2 Data Collection Template

Node	**Conversation**	**Payload**	**Signature**
Sample 1	Internal or external activity	Contents Summary	SNORT configuration

Case Study 3

The aim of case study three was to identify the emergent security issues related to Smart Home object behavior that affects personal safety relating to cyber security, resilience to cyber-threats, and personally identifiable information (PII) when confidential information is resident in the Smart Home ecosystem. Ultimately, data gathered through case study three facilitated analysis of the IDS configuration to identify internal or external Smart Home conversations. IDS configuration analysis was

conducted to identify internal or external Smart Home encrypted traffic. The IDS configuration analysis also allowed establishing whether the IDS can identify conversations that contain PII in its PDU payload, as well as nodes responding to vulnerability scans. Finally, it enabled the researcher to ascertain if the IDS can control whether Smart Home devices establish point-to-point conversations with internal or external nodes that are transmitting PII or vulnerability data as a payload (see Table 5).

Table 5

Case Study 3 Data Collection Template

Node	**Signature**	**Payload**	**PII**	**Vulnerabilities**	**Controls**
Sample 1	SNORT configuration	Encrypted or Unencrypted	Yes or No	Yes or No	SNORT configuration

Validity and Reliability

The controlled environment is not influenced by researcher's prior knowledge of any vulnerabilities or threats. Moreover, it can be replicated completely, given that the replicated environment acquires the nodes and tools discussed in the earlier parts of this chapter. All sources of data were reported within the constraints of the ethical considerations outlined in the next section. Unaltered and transparent data collection and reporting procedures were pivotal to developing accurate cross-case analysis during the conduct of all three case studies.

Ethical Considerations

Human participation in this research was limited to possible disclosure of information about the researcher's Smart Home ecosystem that could be repurposed nefariously. The potential for exposure also existed as vulnerabilities unique to Smart Home nodes owned by the researcher are discovered. The possible disclosure of other

personally owned wireless networks that are in proximity to the controlled environment presented an additional concern that had to be considered. In order to mitigate the risks of personal information disclosure, appropriate efforts were made to sanitize data collected containing specific individually identifiable information. Vulnerabilities that were discovered, identifying specific nodes, were generalized to the function of the node, as the individual node relates to the overall Smart Home ecosystem. Collateral networks that are in proximity to the controlled environment were identified as a part of the data collection process and were not reported in the final analysis.

Summary of Chapter 3

The methodology chosen for the present study was a deliberate attempt to reconcile an exploratory approach to an emerging technology using case studies. Multiple methods were explored, which could potentially illuminate privacy concerns in the Smart Home ecosystem. This study examined multiple intrusion vectors including wireless technologies and web/IP-based exploits. Yin's (2014) case study construct was adopted to examine the applicability of exploratory research in the context of Smart Home ecosystems. Finally, the work reported here relates to the Lockheed Martin Intrusion Kill Chain to actor-driven intrusions that have possible implications in the Smart Home ecosystem.

CHAPTER 4

Results

Introduction

The Smart Home ecosystem described in Chapter 3 was observed using full data captures (packet captures or PCAPs) from the controlled environment using both a ninja star wiretap and Z-Wave USB dongle, both of which ultimately served as a data collection instrument in the three case studies described in Chapter 3. The PCAP data for the wired network segment was captured using a windows version of Wireshark due to simplicity and system limitations pertinent to network settings and configurations. The PCAP from the Z-Wave network was captured on Kali Linux version 2 using the Z-Wave USB dongle and "Z-Force" (Fouladi & Ghanoun, 2013) in a virtual machine. Both PCAPs were allowed to run while various Z-Wave devices executed tasks within their scope of capability. Additionally, the PCAP collected notional periods where no activity should be occurring. Periods of no activity were significant because the devices in the controlled environment initiated communications with outside sources while no activity in the Smart Home ecosystem was initiated by human activity. This particular activity was closely examined to verify that no privacy information existed in the payload.

This chapter is organized with a brief explanation of the sample demographics of the devices explored in this study followed by the final presentation and discussion of findings. The final presentation and discussion of findings include case study one, which involved a survey of Z-Wave and Ethernet compliant communications, case study two,

which involved the analysis of Z-Wave and Ethernet vulnerabilities observed during the survey, and case study three, which involved the analysis of the Intrusion Kill Chain and a cross-examination of the preceding case studies. The chapter is concluded with a summary of the findings and an introduction to the next chapter.

Sample Demographics

The controlled environment involved devices that were categorized as Smart Home devices. The Smart Home devices evaluated presented the capacity to exhibit emergent object behavior. The study examines not humans but devices in a controlled environment constructed from average consumer Smart Home equipment available on the market in 2015. In the controlled environment, the nodes listed in Table 2 are configured with manufacturer recommended configurations and connected accordingly to the Smart Home ecosystem. Each node was observed communicating with external addresses either through the ISP or through the cellular provider's data service. Network traffic sensors were procured for the conduct of this study for packet capture capability for the single wired connection and for the sub-1GHz frequency Z-Wave connections that occur between the router, modem, and the Z-Wave control panel. The router and the modem were configured with manufacturer recommended configurations for both wired and wireless connections, as applicable. The Z-Wave control panel was configured by a Vivint technician and configured to their recommended standards.

Presentation and Discussion of Findings

RQ1 sought to determine how secure Smart Home technology IoT systems are independently. Because the Smart Home ecosystem designed in the present study

observed object traffic from two methods of communications (Z-Wave and Ethernet), CS1 is further explored from the Z-Wave and Ethernet perspectives.

Z-Wave Compliant Communications (Case Study 1). At a basic level, the Z-Wave network architecture consists of a controller node and a slave node. The controller node acts as the central hub that establishes the unique network identifier, the Home ID, which is repeated in the preamble of a slave node. In the present study, the controller node for the Z-Wave network within the controlled Smart Home ecosystem is the wireless control panel, as described in Table 2. During case study one (henceforth CS1), the controller node was observed initiating transmission to other slave nodes on the network. As explained by McClure et al., (2015), communications from the wireless control panel are typically polling or updating slave nodes for health and maintenance of network routing topologies. Responding to the controller node, as indicated by the Node ID observed during the packet capture, were the slave nodes, also described in Table 2. The slave nodes responded to the solicitations from the control node directly or indirectly from the subsequent re-solicitation from adjacent slave nodes. Similar to IEEE 802.15.4 compliant communications, the Z-Wave nodes observed during CS1 used a mesh-networking model to compensate for a node-to-controller range communication failure, using positive acknowledgment and frame retransmission. It was noted during CS1 that the Z-Wave communication network was self-forming and capable of routing dynamic network topology updates (McClure, Scambray, & Kurtz, 2015). Further research into the Z-Wave structured protocol stack configuration helped elucidate how components relative to each node performed node-to-node and node-to-controller communications. The Z-Wave structured protocol stack is comprised of five layers, namely the physical,

media access control (MAC), transport, network, and the application layer (Fouladi & Ghanoun, 2013; McClure et al., 2015). The physical layer performed physical connectivity tasks associated with channel assignment within the sub-1 GHz radio frequency (RF) modulation and synchronization. The MAC layer of the structured protocol stack displayed the unencrypted Z-Wave Home ID and Node ID. This layer was also capable of preventing collisions using device-specific unique Node ID's and collision avoidance algorithms. The transport layer of the structured protocol stack performed the tasks specific to transmission and reception acknowledgment of frames, as observed during CS1 in the checksum values in the captured frames. The network layer displayed the mesh topology updates and carried out inter-node frame routing, as appropriate, to the device location. The network layer is also responsible for defining and allocating hierarchical device roles in the structured protocol stack, e.g., determining which device is designated as a controller or a slave. The network layer definition and allocation process also associated the device Home ID and Node ID for network route establishment. The network layer definition and allocation functionality are particular security concern given the concept of the Z-Wave node inclusion and exclusion process (McClure et al., 2015). As Z-Wave devices are added to the network, physical access is required to the Z-Wave controller node to initiate the Z-Wave network inclusion/exclusion process. The requirement for physical proximity for an authorized user is essential to maintaining a multifactor security defensive posture for the Z-Wave network. Thus, cyber intruders would have to circumvent physical safeguards in order to include or exclude devices from the network. The last hierarchal tier of the structured protocol stack is the application layer. The application layer brokers the payloads of the

frames received and transmitted. More specifically, the application layer parses and processes payload data, e.g., requests for topology updates and responses to inclusion requests. As a part of CS1, the application layer payload data was closely observed to determine if unencrypted payload contents were routed outside the Z-Wave network via the Ethernet compliant communications. McClure et al., (2015) made specific note that Z-Wave operates at a 3−75-foot range, contingent on the content and type of information required to be transmitted as well as the power source. During the conduct of CS1, the effective distance was not confirmed due to a lack of specialized tools needed to accomplish sub-1 GHz ranging. Nonetheless, it was confirmed that both the control and the slave nodes consistently listen for network topology updates to enhance the meshed infrastructure and further extend the network range, up to four hops (McClure et al., 2015). Range capability of the Z-Wave network is significant to this study, as security implications of specific node-to-node communication may expose pertinent device configuration details that may be of value to an attacker even if located at a considerable distance. It was also observed during CS1 that battery-powered Z-Wave devices were not participants in topology updates to other nodes. As suggested by McClure et al., (2015), battery-powered Z-Wave devices did not participate in forwarding topology changes as a battery conservation strategy (McClure et al., 2015). During the conduct of CS1, the repeater node described in Table 2 was unplugged from the wall and the controller node was observed broadcasting topology updates to the remaining participant nodes. Subsequently, once the repeater node was plugged back into the power source within the timeframe necessary to ensure that the node would not be disassociated from the network, the proper Home ID was broadcasted from the repeater node and the

controller node broadcasted additional topology updates to the remaining participant nodes. As explained by McClure et al., (2015), a Z-Wave node was added to the network through the inclusion process explained above in the application layer portion of the Z-Wave structured protocol stack. The mechanics related to this process include the primary controller associating a Node ID to the device in the range between 1 and 232. Subsequently, Z-Wave nodes continued to use the Node ID value in all transmissions while still assigned within the Z-Wave network. Thus, the Z-Wave network was limited to a maximum of 232 nodes (McClure et al., 2015).

In CS1, the Z-Wave communications, observed using Z-Force, did display the Home ID and Node ID in plain text in the PCAP, as explained above, followed by encrypted payload data. In the context of CS1, externally viewed conversations refer to the computer that was not associated with the Z-Wave Home ID and was able to capture, passively, the traffic from the Z-Wave network. The internal communications were observed in the same manner, focusing on node-to-node specific communications and the content of the conversations. Once any content was discovered from both the external view and the internal view, the traffic behavioral heuristics were generalized to explore the purpose of the conversation, and the results were recorded. Table 6 provides generalized conversations that occurred during the packet capture. The packet capture was terminated after 48 hours. This limitation was imposed to ensure that adequate data would be captured to observe all sequences of communications possible from the participating devices, while also making the data set manageable from the analytical perspective. From the Z-Wave PCAP, the activity of the entire content of the Z-Wave communications could be observed promiscuously, as shown in Table 6.

Table 6

Case Study 1 Data Collection

Node	Externally Viewed Conversations	Internal Viewed Conversations	Payload
Z-Wave Slave Node	Promiscuous Z-Wave sniffing	Home ID and Node ID (Encrypted Payload)	Network topology updates
Z-Wave Slave Node	Promiscuous Z-Wave sniffing	Home ID and Node ID (Encrypted Payload)	Response to control node
Z-Wave Control Node	Promiscuous Z-Wave sniffing	Home ID	Network topology updates
Z-Wave Control Node	Promiscuous Z-Wave sniffing	Home ID	Response solicitation
Z-Wave Control Node	UDP OpenVPN	Encrypted (TLS RSA)	IP Fragmented and Encrypted

Ethernet Compliant Communications (Case Study 1). While the Z-Wave traffic was captured during the execution of CS1, Wireshark was used to capture all Ethernet compliant communications entering and exiting the controlled environment, as explained above. None of the Z-Wave formatted traffic was visible from the wired packet capture; however, traffic originating from the Z-Wave wireless control panel was observed communicating with a Vivint server using an OpenVPN protocol during associated timestamps at which the Z-Wave network traffic was observed. The Vivint server was identified by resolving the IP address captured during the Wireshark analysis of the wired gateway PCAP from an inquiry using a "who.is" search. Additionally, the correlation between the captured Ethernet communications and the observed Z-Wave activity was confirmed through the Internet Protocol (IP) fragmentation that occurred with correlated timestamps between the two network captures. The OpenVPN protocol did encrypt the conversations originating internally to the Z-Wave network. Thus, the theoretical concepts that support how the OpenVPN protocol achieves secure endpoint-to-endpoint conversations is detailed when discussing kernel agnostic tunneling

architectures, UDP/TCP modes, encryption, public/private keys, and payloads later in this chapter. The kernel agnostic tunneling architectures (e.g., TAPs and TUNs) refer to network devices supported entirely in software. OpenVPN is a Secure Socket Layer (SSL)-based Virtual Private Network (VPN) protocol that makes use of the modern Transport Layer Security (TLS) as a method to secure endpoint connections (Crist & Keijser, 2015). The operating system needed to run OpenVPN is agnostic because OpenVPN does not rely on operating system-specific kernel architecture due to the TAP and TUN devices organic to OpenVPN. The TAP and TUN (explained below) devices foster the support for a variety of operating systems, including Linux, Free/Open/NetBSD, Solaris, AIX, Windows, Mac OS, and iOS/Android devices (Crist & Keijser, 2015). However, all aforementioned operating systems still require the installation of client software, which in the case of CS1 was the Z-Wave wireless control panel and the Vivint application installed on the Android device initiating the commands to the Z-Wave network. As a part of CS1, it was also observed that OpenVPN operates using a control channel and a data channel, both of which are encrypted using a custom encryption protocol (easy RSA as observed in CS1, see Table 6). Moreover, all traffic was passed over a single UDP connection using the default OpenVPN protocol and UDP port 1194. The TUN, as referenced above, is an abbreviation for TUNnel. For OpenVPN to function, TUNs create a virtual network layer, with the capability to encapsulate and route layer-3 IP packets (Crist & Keijser, 2015). TAPs, as referenced above, is an abbreviation for a network tap. TAPs perform the task of virtualizing data link layer encapsulation (layer 2) for Ethernet frames, creating network bridges, facilitating collision avoidance and hardware address association (Crist & Keijser, 2015).

OpenVPN uses TAPs and TUNs to process the incoming and outgoing traffic as an application running on the OpenVPN client device. While conducting CS1, it was noted that the encryption protocol OpenVPN was implementing TLS over UDP, as noted in Table 6. TLS is a symmetric encryption technique that employs a uniquely generated key for each session that is negotiated through the control channel during the initiation of the session. TLS also has the organic capability to support identity authentication using public-key cryptography. The public and private key exchange process that occurred during the conduct of CS1 and during the IP fragmented sessions from the OpenVPN protocol took place when the TLS control channel VPN connection was being initiated. Key exchange was also observed during the exchange of new encryption keying material that, according to Crist and Keijser (2015), occurs after a predetermined time lapse. The data channel public and private key exchange process are not negotiated; rather, they are stored in the client and server OpenVPN configuration files (Crist & Keijser, 2015). Finally, the OpenVPN data payloads employ hashing algorithms, such as SHA1, to help ensure the integrity of the packets delivered.

The appropriateness of RQ1 in relation to the first case study and the case study framework establishes that Smart Home ecosystem devices are moderately secure independent of other devices on the network. This assertion is made due to the fact that privacy information is visible using open source tools from a 75 feet standoff distance. Subsequently, the requirement for physical proximity to the Z-Wave controller nodes does help mitigate threat possibilities. The information gathered during CS1 is further evaluated in case study two.

Z-Wave Communications Vulnerabilities (Case Study 2). RQ2 sought to determine what behavioral data exchange or aggregate device communication occurs between Smart Home objects that effect fundamental security levels. Because the Smart Home ecosystem designed in the present study observed object traffic from two methods of communications (Z-Wave and Ethernet), case study two is further explored from the Z-Wave and Ethernet vulnerabilities perspectives. Thus, further research was conducted to explore the vulnerabilities observed during the execution of CS1. As demonstrated in CS1, Z-Force can obtain frame-level visibility of the unencrypted Z-Wave data link, and network layers. An attacker could execute a spoofing attack of an observed Node ID. This would allow the attacker to interact with other nodes over a Z-Wave network without alarming any physical safeguards organic to the Z-Wave network (Fouladi & Ghanoun, 2013). The Z-Wave proprietary protocol does offer an optional security layer, which is implemented at the application layer in the later generations of Z-Wave devices (McClure et al., 2015). However, further security enhancements are subject to cost constraints, and the Z-Wave Alliance has not produced public documentation disclosing security mechanisms employed by Z-Wave devices (McClure et al., 2015). The theoretical concepts that support how Z-Wave traffic employed encryption observed in CS1 revealed that the Z-Wave encryption methods make use of an AES-OFB (Advanced Encryption Standard - Output Feedback Mode) protocol (McClure et al., 2015). The findings reported by Fouladi and Ghanoun (2013) confirm that the protocol implementation of the encryption and authentication methods as used by the Z-Wave AES-OFB is a vulnerability that could allow an attacker to reset the established network key on a target Z-Wave device. This vulnerability arises mainly due to the lack of state

validation in the key exchange protocol handler programmed in the Z-Wave physical device (Fouladi & Ghanoun, 2013).

Because the encryption and authentication methods are vulnerable on the Z-Wave network and the critical node membership information can be observed in plain text (Home ID and Node ID), a Man-in-the-Middle (MitM) attack is possible for the Z-Wave network. The Z-Wave member devices do not validate the identity of the controller, making it possible for valid commands from the controller to be intercepted during the inclusion process with a target device. This vulnerability causes the unassociated Z-Wave device to associate to a malicious Z-Wave controller (McClure et al., 2015).

The encryption and authentication methods also expose the Z-Wave network to attacks due to the lack of confidentiality protection during the Key recovery delivery over the Z-Wave network. The Key recovery key is a well-known character string that was passively observed during the inclusion process in the conduct of case study two (henceforth CS2) while using Z-Force. This key could subsequently be used to decrypt and forge anomalous packets to the Z-Wave network (McClure et al., 2015).

In CS2, the data collected from CS1 was analyzed to develop a custom Smart Home focused rule set from the open source Debian 7 based operating system network intrusion detection system (NIDS) solution (SNORT). SNORT was first configured to alert on all traffic that matched community-rules profiles. The purpose of proposing this tool was to explore the applicability of using SNORT to evaluate Z-Wave packet data. During the execution of CS2, SNORT was unable to parse the PCAP collected during CS1. Thus, the development of a tool was proposed for multi-layer traffic behavioral data exchange and aggregate device communication occurring within a Smart Home

ecosystem. This proposed tool (see Figure 6) would allow timely identification of anomalous objects that effect fundamental levels of security. The proposed solution would also offer a specific emphasis on the plain text observations of CS1.

Figure 6. Proposed framework for a multi-layer traffic analyzer.

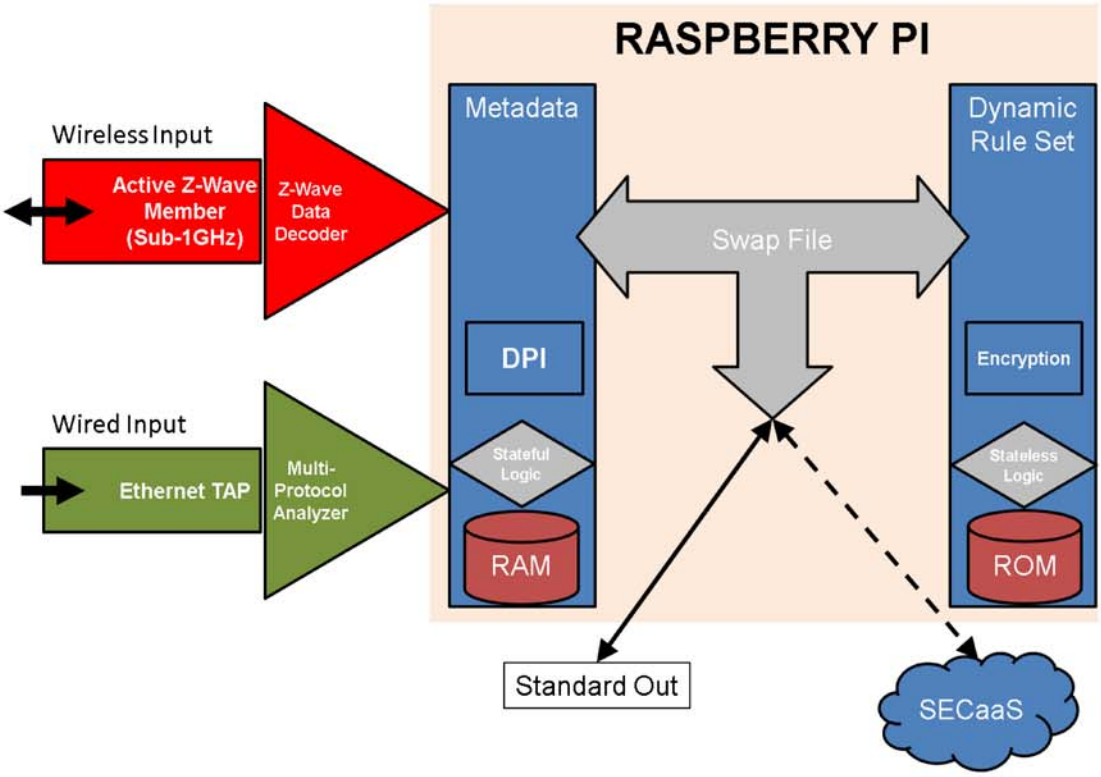

Figure 6. Proposed framework for a multi-layer traffic behavioral data exchange and aggregate device communication analyzer.

Figure 6 depicts the high-level framework of a hardware solution needed for the execution of data analysis for CS2 and case study three. At a basic level, the proposed hardware solution consists of a minimally configured Raspberry-Pi that is capable of collecting and parsing three data input/output (IO) methods. The first IO, depicted in red, would consist of a Z-Wave module capable of associating with the applicable Z-Wave network (Z-Wave IO). The Z-Wave input would have the capacity to parse all layers of

the Z-Wave structured protocol stack and would pass Z-Wave activity along to the metadata function. The Z-Wave output would have the capability to send properly configured control and data channel commands to the Z-Wave network. Overall, the Z-Wave IO would serve the purpose of collecting and locally responding to anomalous events observed of the Z-Wave network. The Ethernet TAP input would have the functionality of collecting Z-Wave conversations that traverse the Ethernet compliant communications to the ISP (see Ethernet traffic sensor shown in Figure 5). Both wired and wireless inputs would need the functionality of a protocol analyzer containing the low-level protocol configurations and would have the capacity to configure the protocol mappings dynamically from the rule sets maintained by a Security as a Service (SECaaS) service provider. The locally configured protocol mappings would contain a list of all known protocol states that is readily accessible from RAM. The metadata function, depicted in blue, would be capable of deep packet inspection (DPI), as well as of decrypting OpenVPN TLS and Z-Wave payload traffic. Here, the stateless logic, depicted in light gray, would be capable of verifying user activity against baseline signatures/heuristics (also called whitelisting). Subsequently, the stateless logic, also depicted in light gray, would be capable of receiving rule set definitions from the dynamic rule set. The dynamic rule set, also depicted in blue, would be a cloud-based solution (SECaaS) that is locally maintained for quick and fail-resistant communications with metadata functions. Lightweight cryptography standards, depicted as encryption, are employed in this solution for ensuring that all Z-Wave IO and Ethernet compliant communications remain resilient to external attacks and intrusions. Lastly, the swap file

is monitored via API locally for user level alerts and via SECaaS for an expeditious analytical response.

The proposed solution will help establish the extent to which behavioral data exchange or aggregate device communication occurs between the IoT objects that effect fundamental security levels. Table 7 summarizes the coding matrix that would notionally be collected from the proposed solution as IDS alerts trigger on external conversations from outside the network directed internally, as well as internal conversations from inside the network directed externally (bidirectional). The relevant conversations were summarized based on the activity and were matched to the proposed IDS solution's alert configuration. Once the Z-Wave Wireless Control Panel initiated conversations, the packet content was analyzed to determine if the Z-Wave network modification request matched the heuristics defined in the dynamic rule set. If the alerts were triggered due to an anomalous device requesting membership to the Z-Wave network, the standard output would notify the user for immediate actions. If the user failed to respond, the SECaaS service provider would have the culpability to address the issue and directly communicate with the Z-Wave network. Table 7 helps illuminate node activity associations between Z-Wave traffic and IDS alert configurations. It is also important to note that traffic observed outbound or inbound in the Smart Home ecosystem is encrypted to meet lightweight cryptography standards for publicly visible traffic.

Table 7

Case Study 2 Data Collection

Node	Conversation	Payload	Signature
Z-Wave Wireless Control Panel	Bidirectional point to point traffic	Encrypted or Unencrypted	Trigger on Unassociated Device requesting Z-Wave membership
Any Z-Wave Device	IP fragmentation	Encrypted or Unencrypted	Trigger on unencrypted traffic

Ethernet Compliant Communications Vulnerabilities (Case Study 2). The control and data channels of the Ethernet compliant communications in/outbound of the Smart Home ecosystem via the ISP (see Figure 7) were encrypted using the UDP OpenVPN protocol, as explained above. As a part of CS2, during the control channel TLS negotiation, configuration information and cipher material exchange processes were observed. This channel was used when the OpenVPN connection was initialized, as shown in Figure 7.

Figure 7. OpenVPN connection initialization.

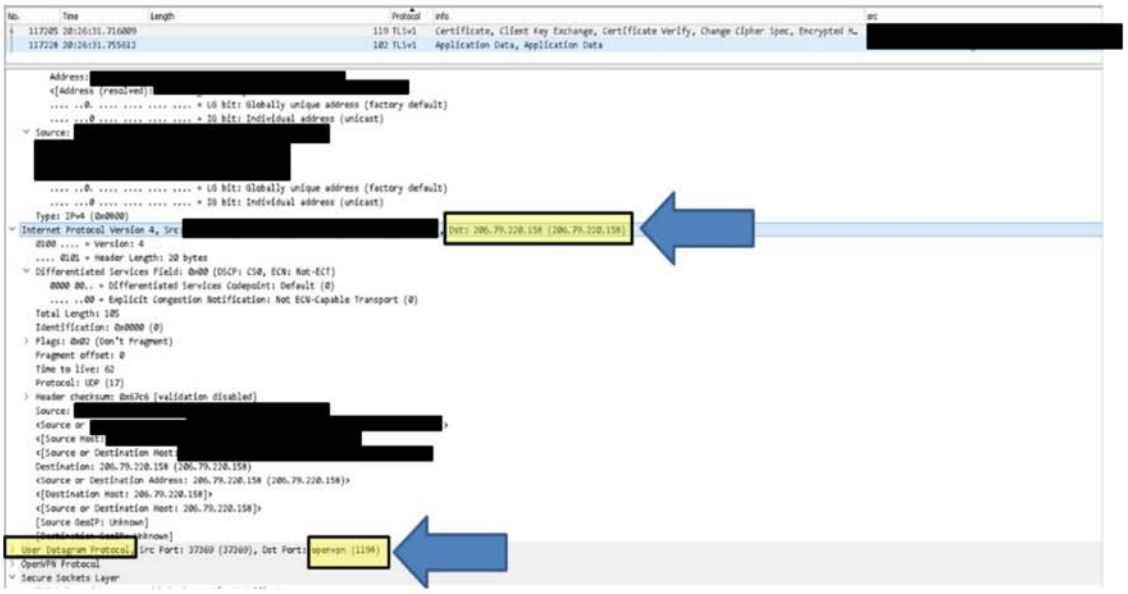

Figure 7. OpenVPN connection initialization captured during Case Study 2.

As observed in CS2, and depicted in Figure 7, if an application or protocol is using UDP for configuration and cipher material negotiation, it is susceptible to message deletion or packet reordering attacks (Crist & Keijser, 2015). The exception to this vulnerability is the pre-shared key point-to-point method using a custom easy RSA key, as explained above. In the case of the OpenVPN conversations that were observed during CS2, only the data channel used this technique. To avoid possible MitM attacks where server impersonation causes client(s) to attempt to connect an adjacent client(s), server certificate verification must be instituted by clients (OpenVPN_Technologies, 2013).

As depicted in Table 7, the "any Z-Wave device" alerts would trigger due to an anomalous device intercepting the Ethernet compliant communications tampering with the IP fragmentation from the ISP network. Subsequently, the standard output would notify the user for immediate actions. If the user failed to respond, the SECaaS service provider would have the capability to address the issue and directly communicate with the Z-Wave network.

The appropriateness of RQ2 in relation to CS2 and the case study framework establishes that Smart Home ecosystem devices are not secure when behavioral data exchange or aggregate device communication occurs between Smart Home objects that effect fundamental security levels. This assertion is made due to the fact the Z-Wave AES-OFB perpetuates a vulnerability that could allow an attacker to reset the negotiated key between a target Z-Wave device and a Z-Wave controller. Furthermore, the requirement for an RSA key, during the OpenVPN conversations is exclusive to the data channel conversations on the Ethernet communications in the Smart Home ecosystem.

The lack of a control channel RSA key subjects Ethernet compliant communications to possible MitM attacks and does not help mitigate threat possibilities. The theoretical concepts supporting how CS2 was executed for both Z-Wave and Ethernet traffic observations prompted the need for the proposed solution, as it helps establish the extent to which behavioral data exchange or aggregate device communication occurs between the IoT objects that influence fundamental security levels. The information gathered during CS2 is further evaluated in case study three.

Kill Chain Analysis (Case Study 3). RQ3 sought to explore the emergent security issues related to Smart Home object behavior that affects personal safety relating to cyber security, resilience to cyber threats, and personally identifiable information from the collection of object usage data. CS1 demonstrated that a cyber intrusion was possible in the Intrusion Kill Chain categories of reconnaissance and weaponization, as shown in Table 1. In previous studies related to Z-Wave security, the researchers demonstrated the effectiveness of using the Z-Force tool to perform actor-driven efforts to discover generalized information about a potential victim (Fouladi & Ghanoun, 2013). The methods proposed by Fouladi and Ghanoun (2013) were replicated during the conduct of this study. The Z-Force tool and the ninja star Ethernet TAP represent reconnaissance phase activities required to arrive at meaningful conclusions about the victim's Z-Wave network. Conclusions are drawn to assist in determining whether the victim's technology in use is susceptible to specific attack vectors. The weaponization phase occurs when the attacker customizes attack vectors, e.g., executes a spoofing attack of an observed Node ID. This would help the attacker's computer to interact with other nodes over a Z-Wave network without alarming any physical safeguards organic to the Z-Wave network.

Because Z-Wave traffic could be observed without the physical access inside the Smart Home ecosystem, attackers could be up to 75 feet away from the home to observe Z-Wave architecture without range-extending wireless tools. This would allow the attacker both standoff distance and the necessary time to construct tools unique to the Z-Wave architecture. The attacker could weaponize packet data that would be capable of executing MitM attacks or key recovery attacks, as described above. Delivery would occur when the infrastructure is physically connecting the attacker (or attacker's architecture) to the victim (or victim's architecture) transmits the weaponized function. The proposed solution outlined above would aid in detecting multi-layer traffic behavioral data exchange and aggregate device communication during the delivery and exploitation, thus illuminating successful manipulation of a particular vulnerability using the weaponized function. Subsequently, the proposed solution will alert, via standard out or via SECaaS, of any weaponized function installs or subsequent calls to implant instructions on the victim's network. The aim of conducting case study three (henceforth CS3), was to identify the emergent security issues related to Smart Home object behavior that adversely affects personal safety relating to cyber security, resilience to cyber threats, and personally identifiable information (PII) when confidential information is resident in the Smart Home ecosystem. During the conduct of CS3, analysis of the IDS configuration based on the solution proposed in CS2 was used to identify internal or external Smart Home conversations. The proposed IDS configuration identified internal and external Smart Home encrypted traffic in the packet payload, as noted in Table 8. The IDS configuration analysis identified conversations that contain PII, along with nodes responding to vulnerability scans. The two main areas of focus for the proposed

solution pertained to the wireless control panel and the Z-Wave member devices, as they communicated externally via the ISP, as shown in Figure 7 and Table 8. Control over the Smart Home devices that establish point-to-point conversations with internal or external nodes that are transmitting PII or vulnerability data as a payload is mitigated by the proposed solution's user and SECaaS alerts. User and SECaaS provider's response to alerts also mitigates risks associated with the attacker infrastructure establishment during the command and control phase and the final phase activities.

Table 8

Case Study 3 Data Collection

Node	**Signature**	**Payload**	**PII**	**Vulnerabilities**	**Controls**
Wireless Control Panel	Trigger on Unassociated Device requesting Z-Wave membership	Unencrypted	Yes	Yes	User verification of activity
Any Z-Wave device	Trigger on unencrypted traffic	Encrypted	yes	yes	User verification of activity

The appropriateness of RQ3 in relation to CS3 and the case study framework establishes that Smart Home ecosystem presents emergent security issues related to Smart Home object behavior that concerns personal safety relating to cyber security, resilience to cyber threats, and personally identifiable information. This assertion is made due to personally identifiable information traversing internal and external to the Smart home ecosystem in plain text. The use of the proposed solution does help mitigate associated threats identified in RQ3.

Summary of Findings

When interpreting the findings yielded by the present study, it is essential to acknowledge their lack of generalizability to every Smart Home ecosystem configuration, Smart Home device, or ISP communications with the Smart Home ecosystem. The research conducted in this study presented the analysis of CS1, CS2, and CS3. CS1 presented the analysis of Z-Wave and Ethernet compliant communications. The analysis of CS1 involved the passive capture of Z-Wave and Ethernet compliant communications and the presentation and further research of the observations. CS2 presented the analysis of Z-Wave and Ethernet vulnerabilities using SNORT. The Z-Wave and Ethernet vulnerabilities were not fully explored due to a capability gap, which identified that accurate correlation between the captured Ethernet communications and the observed Z-Wave activity is not currently possible without the proposed solution. In addition, it should be emphasized that the proposed tool designed for deep packet inspection capable of decrypting OpenVPN TLS and Z-Wave payload traffic would follow the logic described above and would be capable of verifying user activity against white-listed baseline signatures/heuristics. CS3 presented the analysis of the Intrusion Kill Chain and a cross-examination of the preceding case studies. CS3 also investigated the practical use of the proposed solution as an effort to mitigate the transmission of PII or vulnerability specific data in/outbound to the Smart Home ecosystem. Chapter 5 presents conclusions drawn from the data presented in chapter 4. The present study offers viable solutions and recommendations for enhanced security practices in the use of Smart Home technology.

CHAPTER 5

Findings and Conclusion

Smart Home ecosystems are seen as the next step in the computing age evolution. Owing to their reliance on platforms that integrate and aggregate ubiquitous sensors and devices with a variety of communication protocols, Smart Home ecosystems are empowered by cloud technology and make the devices consumers use on a daily basis more intelligent and thus more beneficial. In the Smart Home, the resident is safer due to on-demand communications to local emergency responders, the mobility-impaired individuals are more independent, and countless others are expected to benefit from the almost limitless possibilities that will likely emerge as the technology becomes more widespread. However, as modern society progresses technologically, so do the ability of those who wish to perpetuate harm, to steal, or to exploit the innocent. The aim of the present study was to explore the current vulnerabilities in the emerging Smart Home ecosystem and identify patterns cyber attackers would exploit to inflict nefarious actions. The case studies presented in this thesis were designed and conducted in order to evaluate the Smart Home ecosystem by applying two prominent methods of inter- and intra-communication technologies—Ethernet compliant communications and Z-Wave compliant communications.

The problem this study sought to address is the gap in knowledge consumers have concerning vulnerabilities within IoT devices given recent trends of accelerated and the regular purchase of smart technology. This study offered a qualitative exploratory

research with the purpose of investigating Smart Home technology vulnerabilities within a real life context of the IoT typical usage applications. Moreover, this study was purposed to characterize average Smart Home device usage in contrast to acceptable and nefarious data heuristic behaviors. Subsequently, SNORT and the proposed solution contrasted data behavior and illuminated anomalous datalink traffic and payloads. Finally, real-time Smart Home traffic was evaluated for the propensity to be vulnerable and disclose personally identifiable information (PII) through exploring current and proposed solutions in a controlled Smart Home ecosystem environment. The information obtained during the course of this study involved the systematic acquisition and analysis of Smart Home ecosystem link-layer PDUs. The methodology employed during this study involved a recursive multiple case study evaluation of the Smart Home ecosystem data-link layer PDUs and aligned the case studies to the existing Intrusion Kill Chain design model. The proposed solution emerging from the case studies builds the appropriate data collection template while concurrently developing a SECaaS capability to evaluate collected results. The ethical implications during the conduct of this study involved limited human participation. The only exception was the possible disclosure of information about the researcher's Smart Home ecosystem that could be repurposed nefariously. To mitigate the possibilities of personal information disclosure, appropriate efforts were made to mask the data collected containing specific ISP information. The vulnerabilities discovered were generalized to the function of the specific node as the individual node relates to the overall Smart Home ecosystem. Collateral networks were discovered in proximity to the controlled environment. However, the collateral networks

were not reported in the final analysis of the data, as the collateral networks did not impede any instruments used in the conduct of this study.

Chapter 5 presents the conclusions from the as appropriate to the conduct of all three case studies. The findings and conclusions present solutions to mitigate Smart Home technology vulnerabilities discovered during the conduct of this study, the limitations of the study, the implications for practice, the implications inferred from the conduct of this study, and the recommendations for future research. Finally, this chapter is surmised with the overall generalizations found during the conduct of this study.

The sensors used to control smart technology gather data. It is thus advised that users seek the necessary information regarding the types of data the devices used in the context of a Smart Home ecosystem generates (Widman, 2015). Because of increased risks of unauthorized access, users need to consider sensor orientation when sensors are utilized in the home. According to Widman (2015), it was possible to monitor homes remotely through video cameras already installed in the home. In fact, in this study, the author assessed ten security systems, reporting that all tested systems were affected by this particular issue. Not only was it possible to watch the home, but also obtain information as to whether or not the home was vacant. Therefore, users need to amplify the security features of the devices. In fact, the insecure defaults of the systems are considered one of the major problems related to these devices. As a result, default passwords need to be changed and the new ones made sufficiently strong by using lower and upper case letters, numbers, and symbols to increase security. Keeping networks separate is an adequate resolution to protect personal data on phones and PCs. In addition, each network should have a separate password to protect the connected home

devices from hackers in the event of an intrusion (Widman, 2015). Furthermore, network segmentation is necessary. Another useful option is to hide the network or make it invisible to allow the associated Wi-Fi network to be discovered by automatic searching. As a result of this configuration, in order to use this network, users would be required to know the name, enhancing security. As mentioned above, other threats originate outside the proximity of the home, typically from open ports in the IP construct (Kong, Tian, Pan, Liu, & Wu, 2013). Remote communication channels are established between remote maintenance servers and the devices in the home, allowing the consumer, the Smart Home service provider, and the Smart Home manufacturers, but also potential attackers, to communicate with the specific devices. The most obvious solution to this issue is to turn off the communication channels. Unfortunately, it is presently possible to manipulate communication channels to an attacker's desired state. Additionally, users are typically limited to reduced functionalities when devices are powered off. There are other solutions to this problem, such as re-sequencing of the more common ports (obfuscation) to other ports and/or creating a pseudo port-based encryption at the point of entry for the device/home (Agrawal & Sohi, 2012). In simple terms, re-sequencing will deny a straight-line communication channel to a consumer’s devices/home. Finally, as with all devices that communicate across networks, a so-called zero-day threat is always present (Bambauer, 2013). These are unforeseen threats, for which no solution can be provided in advance. While this deficiency is inevitable, whenever issues emerge, there are learning opportunities that help advance the given field. Thus, networks are still thriving and are overcoming threats and vulnerabilities by quickly identifying emergent issues and researching the solution.

Limitations of the Study

The study conducted cannot be generalized to all that own technology because it did not include all types of technology. As executed, this study is generalized only to those that own smart technology that is similar to the devices evaluated. The study also accounts for the generalization of the knowledge level of those that own smart technology by fully explaining the specific tools required to address the full potential and implications existent given multiple proprietary vulnerabilities. The generalization of the knowledge level is done to acknowledge the existence of tools that can circumvent encryption levels that are beyond the capacity of the researcher's equipment available to conduct this study. Thus, the vulnerabilities discovered, the systems used, and the tools incorporated in this study are limited to a moderately capable desktop computer running Windows 10 and the tools required to observe traffic on the networks falling within the scope of this study.

Implications for Practice

The NIST standards and guidelines offer potential approaches to mitigating security and privacy concerns in the IoT (Hogan & Newton, 2015). NIST validates the requirements for the solution proposed in this study by offering the challenge of developing lightweight cryptography standards that meet the demands of the IoT hardware constraints (Hogan & Newton, 2015). NIST guidelines emphasize the importance of security and privacy in the IoT and differentiate their unique requirements from traditional hardware and software designs for desktop/server environments. It is also postulated that advanced cryptography would be the most effective means of enhancing the security posture of Smart Home ecosystems. Given a sufficiently strong

encryption sequence, interconnected device communication, and susceptible systems, internal Smart Home device Z-Wave and Ethernet traffic would become exponentially more resilient to external attacks and intrusions.

Jajodia, Noel, and O'Berry (2005) recommended that security installers disable port forwarding to reduce alarm system susceptibility (Jajodia, Noel, & O'Berry, 2005). Concurring with this view, some authors argue that port forwarding is not needed because it exposes vulnerabilities unnecessarily. Jajodia et al. (2005) also recommended installing a virtual private network (VPN), which provides users with secure, encrypted tunnels (Jajodia et al., 2005). These tunnels allow the user to visit the desired site safely and securely. Many experts also recommend that the home PC have a separate network than the connected devices in the Smart Home. It is expected that home security and automation systems will experience more vulnerabilities due to the migration from IPv4 to IPv6. The purpose of these protocols is to carry communications in the form of Internet traffic from endpoint to endpoint. With the emergence of IPv6, ubiquitous devices can be interconnected conveniently from endpoint to endpoint, increasing Smart Home mainstream applicability. Given IPv6's greater address space, ubiquitous devices can possess unique IPv6 address and subsequently configure themselves automatically when connected to an IPv6 network using dynamic address auto-configuration protocols (Liu, Yang, Chen, & Pan, 2014). Therefore, those planning the use of Smart Home technology need to be aware of hacking concerns as well. Although each Smart Home technology uses similar concepts, each of these systems has the same type of architecture, resulting in similar vulnerabilities. According to one hacker (King, 2015), the firmware is considered the brains of a device. Firmware is instrumental in remotely pointing the

device to an update provided by a hacker. Cyber intrusions that are extensive enough to manipulate device firmware allow the hacker to compromise the device without the victim being aware of such an intrusion, causing the device to be useless to the victim; such approaches are often referred to as a rootkit. Some Smart Home manufacturers insist that vulnerabilities be part of the design. These same manufacturers argue that consumers wanted the vulnerabilities to remain to run custom scripts and plug-ins. Other IoT vendors have products with built-in security bugs that are similar. Therefore, these exposures can be combated by simply requiring that manufacturers install security compliant firmware, while also mandating verification of application codes. These security considerations are important in light of the fact that there are 25 vulnerabilities in a common device, causing approximately 75% of those presently in use to be vulnerable to hacking at any given moment (King, 2015).

It is debatable whether or not the market is prepared to defend devices using the necessary resources or should apply similar (or the same) safeguards and standards used with computers (Bartik, 2015). These issues pertain to all types of smart technology and are not unique to Smart Homes. However, the connected house is expected to become the norm, as technology continues to advance to provide smarter capabilities. The mainstream is embracing Smart Home technology. For instance, according to one survey, by 2019, over two-thirds of consumers will purchase smart devices. Although no standard security recommendations presently exist as the Smart Home technology is new, protection can be attained by utilizing solutions for security issues. For example, security can be improved using password manager software and mobile data security. Once these solutions are leveraged, greater involvement in the groundwork security is expected,

benefitting the future users by protecting their privacy. The obvious strategy is to password-protect devices, as this assists in preventing tracking (Hill, 2012). Another effective option is to encrypt devices. Encryption is essential because it has been argued that Smart Home technology mirrors the capabilities of a tiny computer (Widman, 2015). Moreover, according to Hewlett-Packard, many of the currently available home security systems are particularly vulnerable to eavesdropping on communications.

Implications of Study and Recommendations for Future Research

Many of the vulnerabilities confirmed in this study have been discovered in previous practitioner demonstrations. However, little information exists exploring the consolidated risks that emerge when proprietary system interact with one another with little to no security standards for communications. Currently, there are no off the shelf devices that offer the level of analytics needed to combat active cyberspace security events. Furthermore, the resource constrained consumer technologies or the Smart home ecosystem, lacks both the infrastructure and architecture to prevent active cyberspace security events. This study explored and proposed the development of a system that has the capability to learn Smart home ecosystem baseline configurations. The hardware based solution outlined and recommended in this study requires future attention as it would present an appropriate level of visibility to detect and alert Smart Home users of the occurrence of rogue nodes and anomalous devices. Ideally, a hybrid of a hardware/software/cloud-based solution would offer behavioral heuristics analysis, using checksums similar to the TCP protocol, that is continuously monitored by a SECaaS provider. The system solution outlined and proposed in this study should be aligned at the gateways of the Smart Home Ecosystem to alert and identify success and failure of

node member authentication to the Z-Wave network. Future research should include methods that can be employed to adequate encryption home ID visibility, whereas traffic transmitted in the sub-1GHz frequency range is not readily observed using conventional tools e.g. protocol analyzers Wireshark and Z-Force. Future research should include the testing of encryption strength of traffic that goes to the ethernet compliant networks from the Z-Wave wireless gateway. Future research should include a quantitative assessment of the systems mentioned in this study of how many consumers understand security implications contained within this study. This would determine if the systems in use from various Smart Home providers have inherent vulnerabilities or flaws that expose consumers to unacceptable levels where PII concerns are not mitigated, and vulnerabilities are not mitigated.

Conclusion

IoT expands the reach of technology and provides the means for the physical world to derive its characteristics from the cyberspace domain. Smart Home technology is merely a subset of the IoT, as it is currently limited to the items that make life at home more intelligent. The IoT and IoE make the world more communal and our interactions with it more intelligent, while also rendering the tasks we are required to perform on a daily basis more receptive to human behavioral heuristics. The ever-growing security concerns are not a phenomenon that can be ignored in the home. Solutions to the security implication in the home require innovative thinking, more collaborative development, and combative complacency that postures future generations in an Internet where everything personal and vulnerable is preserved from cyber incursions.

References

Abrams, M., & Weiss, J. (2007). *Bellingham control system cyber security case study*. Retrieved from http://csrc.nist.gov

Abu-Elkheir, M., Hayajneh, M., & Ali, N. A. (2013). Data management for the internet of things: Design primitives and solution. *Sensors (Basel), 13*(11), 15582-15612. doi:10.3390/s131115582

Agapov, V., & Rahman, S. M. (2008, December). *11th international conference on exploring wireless device driver vulnerabilities.* Paper presented at the Computer and Information Technology, Khulna. doi: 10.1109/ICCITECHN.2008.4803130

Agrawal, S., & Sohi, B. S. (2012). Feature optimization and performance evaluation of machine learning algorithms for identification of P2P traffic. *Journal of Advances in Information Technology, 3*(2), 107-114. doi:10.4304/jait.3.2.107-114

Albert, M. (2015). Seven things to know about the internet of things. *Modern machine shop, 88*, 74-81. Retrieved from http://www.mmsonline.com/articles/7-things-to-know-about-the-internet-of-things-and-industry-40

Angelucci, T. (2014, July). Embedded systems and the internet of things – what's under the hood? *RTC, the magazine of record for the embedded open systems industry,* 1-4.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (IOT). *ResearhGate*, 1-5.

Balbi, A. (2015). Massive cyber attack at anthem. *Strategic Finance, 97*(3), 11.

Bambauer, D. E. (2013). Ghost in the network. *University of Pennsylvania Law Review, 162*, 1011.

Bamrara, A. (2015). Evaluating database security and cyber attacks: a relational approach. *The Journal of Internet Banking and Commerce, 20*(2), 1-8. doi:10.4172/1204-5357.1000115

Barnard-Wills, D., Marinos, L., & Portesi, S. (2014). *Threat landscape and good practice guide for smart home and converged media.* Paper presented at the European Union Agency for Network and Information Security. Retrieved from www.enisa.europa.eu.

Bartik, C. (2015). *Emerging smart technology and its security vulnerabilities | CloudEntr.* Retrieved from http://www.social-peek.com

Beekman, J., & Thompson, C. (2014). Breaking cell phone authentication: vulnerabilities in AKA, IMS and android. Retrieved from http://www.cs.berkeley.edu

Boos, D., Guenter, H., Grote, G., & Kinder, K. (2013). Controllable accountabilities: The internet of things and its challenges for organisations. *Behaviour & Information Technology, 32*(5), 449-467.

Brown, A. (2015). *Rethinking information systems research methods with Heidegger's Ontology*. Paper presented at the European Conference on Research Methodology for Business and Management Studies e-Learning, London, UK.

Brown, R. (2015). Study highlights security vulnerabilities in the smart home. *CNet*. Retrieved from http://www.cnet.com/news

Cisco Inc. (2016, June). Internet of everything. Retrieved from https://newsroom.cisco.com/ioe

ConsumerReports (2015, April). In the privacy of your own home. *ConsumerReports* Retrieved from http://www.consumerreports.org/cro/magazine

eRadar (2015). The Convenience of Smart Home Automation Could Compromise Security. *SoftLayer*. Retrieved from http://www.eradar.eu/convenience-smart-home-automation-compromise-security/

Creswell, J. W. (2013). *Qualitative inquiry and research design: choosing among five approaches* (B. Bauhaus Ed. Third ed.). 2455 Teller Road Thousand Oaks, CA 91320: SAGE Publications, Inc.

Crist, E. F., & Keijser, J. J. (2015). *Mastering OpenVPN*. Birmingham B3 2PB, UK: Packt Publishing Ltd.

Demblewski, M. (2015). *Security frameworks for machine-to-machine devices and networks*. (3726428 Ph.D.), Nova Southeastern University, Ann Arbor. ProQuest Dissertations & Theses Global database.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science And Engineering Ethics, 20*, 701-715. doi:10.1007/s11948-014-9551-y

Englander, I. (2009). *The architecture of computer hardware, systems software, & networking* (Fourth Edition ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Fenrich, K. (2007). *Securing your control system.* Paper presented at the 50th Annual ISA. POWID Symposium Controls & Instrumentation Conference, Pittsburgh, Pennsylvania. Retrieved from http://www.isa.org

Fenrich, K. (2008). Securing your control system: the 'CIA triad' is a widely used benchmark for evaluating information system security effectiveness. *POWER ENGINEERING, 112*(2), 1-5. Retrieved from http://www.power-eng.com

Fischer, E. A. (2013). *Federal laws relating to cybersecurity: Overview and discussion of proposed revisions*. (R42114). Retrieved from https://www.fas.org/sgp/crs/natsec/R42114.pdf.

Fouladi, B., & Ghanoun, S. (2013). Security evaluation of the Z-Wave wireless protocol. *Black hat USA, 24*, 1-2.

Fox-Brewster, T. (2015, July). Vulnerability warning: hackers can haunt homes hitting horrible honeywell security holes. *Forbes Magazine,* 1-2.

Gartner, R. M., & Gartner, J. R. (2015, March). Gartner says smart cities will use 1.1 billion connected things in 2015. *Gartner*. Retrieved from http://www.gartner.com/newsroom/id/3008917

Gérald, S. (2010). The internet of things: between the revolution of the internet and the metamorphosis of objects. *Forum American Bar Association*. Retrieved from http://cordis.europa.eu

Griffin, J. (2014a). Experts discuss the unintended security vulnerabilities of connected home alarm and automation systems. *Security Info Watch*. Retrieved from http://www.securityinfowatch.com

Griffin, J. (2014b). Unsecured smart home systems leave homeowners, enterprises vulnerable. *SecurityInfoWatch.com*. Retrieved from http://www.securityinfowatch.com

Hill, K. (2012). 10 Incredibly simple things you should be doing to protect your privacy. *Forbes Magazine*. Retrieved from http://www.forbes.com

Hodgson, K. (2015). The Internet of [Security] Things. *SDM: Security Distributing & Marketing, 45*, 54-72.

Hogan, M., & Newton, E. (2015). *Supplemental information for the report on strategic US government engagement in international standardization to achieve US objectives for cybersecurity*. Retrieved from http://csrc.nist.gov/publications

Holland, J. H. (2006). Studying complex adaptive systems. *Journal of Systems Science and Complexity, 19*(1), 1-8. doi:10.1007/s11424-006-0001-z

Horrigan, J. B. (2010). *Broadband adoption and use in America*. Federal Communications Commission.

Hughes, J., & Cybenko, G. (2014). *Three tenets for secure cyber-physical system design and assessment*. Paper presented at the SPIE Defense+ Security. doi: 10.1117/12.2053933

Hughes, R. (2010). A treaty for cyberspace. *International Affairs, 86*(2), 523-541.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Retrieved from 6th Annual International Conference on Information Warfare & Security: http://www.lockheedmartin.com

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM, 56*(3), 18-20. doi:10.1145/2428556.2428563

ITU. (2014). *Understanding cybercrime: Phenomena, challenges and legal response*. ITU Retrieved from http://www.itu.int/ITU-D

Jajodia, S., Noel, S., & O'Berry, B. (2005). Topological analysis of network attack Vulnerability. In V. Kumar, J. Srivastava, & A. Lazarevic (Eds.), *Managing Cyber Threats: Issues, Approaches, and Challenges* (pp. 247-266). Boston, MA: Springer US.

Jones, M. F., & Schneier, B. (1995). *Securing the World Wide Web: Smart tokens and their implementation.* Paper presented at the Fourth International World Wide Web Conference, Boston, MA.

Kalika, M., Pallud, J., & Elie-Dit-Cosaque, C. (2011). The influence of individual, contextual, and social factors on perceived behavioral control of information technology: A field theory Approach. *Journal of Management Information Systems, 28*(3), 201-234. doi:10.2753/MIS0742-1222280306

King, S. (2015). How vulnerable are smart-home systems? *Netswitch technology management*. Retrieved from https://www.netswitch.net

Kleine, D. (2015). The value of social theories for global computing. *Communications of the ACM, 58*(9), 31-33. doi:10.1145/2804246

Kong, D., Tian, D., Pan, Q., Liu, P., & Wu, D. (2013). Semantic aware attribution analysis of remote exploits. *Security & Communication Networks, 6*(7), 818-832. doi:10.1002/sec.613

Krause, R. (2015, October 14, 2015). Internet of Things hikes security risk, says AT&T. *Investors Business Daily.* Retrieved from http://www.forensicmag.com

Lemos, R. (2015). Hubs driving smart homes are vulnerable, security firm finds. *eWeek.* Retrieved from: http://www.eweek.com

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime, 17*, 231-249. doi:10.1007/s12117-014-9229-5

Liu, Z., Yang, H., Chen, G., & Pan, Y. (2014). *Context-aware semantic infrastructure for IPv6-based Smart Home.* Paper presented at the 2014 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC-14).

Mandt, E. J. (2015). *On integrating cyber intelligence analysis and active cyber defense operations.* (Master of Science Capstone Project), Utica College, ProQuest Dissertations Publishing. (1598438)

McClure, S., Scambray, J., & Kurtz, G. (2015). *Hacking exposed: network security secrets and solutions* (Third Edition ed. Vol. 6). New York: McGraw-Hill/Osborne New York.

Mendes, T., Godina, R., Rodrigues, E., Matias, J., & Catalão, J. (2015). Smart Home communication technologies and applications: wireless protocol assessment for home area network resources. *Energies, 8*(7), 7279-7311. doi:10.3390/en8077279

Merriam, S. B. (2009). *Qualitative research: a guide to design and implementation* (Second ed.). 989 Market Street, San Francisco, CA 94103: Jossey-Bass.

Messmer, E. (2011). What is an 'Advanced Persistent Threat,' anyway? *Network World, 28*(3), 15-16.

Microsoft_Security_Bulletin_MS10-089. (2010). vulnerabilities in forefront unified access gateway (UAG) could allow elevation of privilege (2316074). *Security TechCenter.* Retrieved from https://technet.microsoft.com

Moad, J. (1997). At your service. *PC Week, 184*, 131&134. Retrieved from http://connection.ebscohost.com

Mohn, E. (2015). Internet of Things (pp. 1-2). Ipswich, Massachusetts: Salem Press.

Moore, M. (2015). Beware – your smart home might be a massive security risk. *Tech Week Europe.* Retrieved from http://www.techweekeurope.co.uk

Neagle, C. (2015, April). Smart Home hacking is easier than you think. *Network World.* Retrieved from http://www.networkworld.com

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer, 46*(4), 46-53. doi:10.1109/mc.2013.74

Noor, A. K. (2015). The connected life: The Internet of Everything coming to a building near you. *Mechanical Engineering, 137*, 36-41.

O'Brien, H. M. (2015). *The Internet of Things and the inevitable collision with products liability* part 2: one step closer (Vol. 35, pp. 6-12). Mondaq.com (UK): Product Liability, Technology and electronic products.

OpenVPN_Technologies, I. (2013). *OpenVPN howto*. Retrieved from https://openvpn.net

Oriwoh, E., & Conrad, M. (2015). 'Things' in the Internet of Things: Towards a definition. *International Journal of Internet of Things, 4*(1), 1-5.

Oriwoh, E., & Williams, G. (2014). *Internet of Things: the argument for smart forensics*. Paper presented at the Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. https://www.researchgate.net

Pfledderer, S. (2015). SMART MOVES. Home automation technology is on the rise, bringing opportunities for landscape companies. *Landscape Management, 54*(5), 34-36.

Popescul, D., & Georgescu, M. (2013). Internet of Things: Some ethical issues. *Annals of Economics & Public Administration, 13*, 208-214.

Protalinski, E. (2014). NPD: US homes now hold over 500m Internet-connected devices with apps, at an average of 5.7 per household. *The Next Web, Inc., 2015*(February 6). Retrieved from http://thenextweb.com

Ramanathan, A. (2015). *A multi-level trust management scheme for the Internet of Things*. (Master of Science in Computer Science Thesis), University of Nevada, University of Nevada, Las Vegas. Retrieved from http://digitalscholarship.unlv.edu/thesesdissertations/2417

Raucher, A. (2015). Taking an end-to-end approach to IoT security. Retrieved from http://www.techdesignforums.com

Rees, A. (2006). *Cybercrime: Laws of the United States*. www.qcert.org: Q-CERT Retrieved from http://www.qcert.org

Roberts, P. (2014). Breaking and entering: "Smart" Homes easy targets for hacking | the security ledger. *The Security Ledger, 2014*. Retrieved from https://securityledger.com

Schroeder, M. J. (2015). Towards Cyber-Phenomenology: Aesthetics and natural computing in multi-level information systems *Recent Advances in Natural Computing* (Vol. 9, pp. 69-86). Springer, Japan.

Scott, N. (2015). Cyber Crime: 10 Things every leader should know. *Director,* 69, 68-72. Retrieved from http://www.director.co.uk

Sharoff, S. (1995). Philosophy and cognitive science. *Stanford Humanities Review: Constructions of the Mind, 4*(2), 1-7. Retrieved from http://web.stanford.edu

Silhavy, R., Senkerik, R., Oplatkova, Z. K., Silhavy, P., & Prokopova, Z. (2014). *Modern trends and techniques in computer science*. 3rd Computer Science On-line Conference 2014 (CSOC 2014): Springer International Publishing.

Simons, H. (2009). *Case study research in practice*. University of Southampton, UK: SAGE Publications Ltd.

Smith, J. (2003). Fraud: the unmanaged risk. 8th global survey. *Ernst & Young Forensic Services. Biennial Global Survey (8th edition)*. Retrieved from https://www.whistleblowing.com.au

Smith, R. G. (2003). Investigating cybercrime: Barriers and solutions. *Retrieved July, 3*, 2007. Retrieved from http://www.aic.gov.au

Srinivasan, V. (2012). *Non-Invasive sensor solutions for activity recognition in Smart Homes.* (3507085), University of Virginia, Ann Arbor. ProQuest Dissertations & Theses Global database.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). *Vision and challenges for realising the Internet of Things*. Luxembourg: Publications Office of the European Union: European Union.

Swedish, J. (2015, January). [Anthem was the victim of a sophisticated cyber attack – Important message from Joseph Swedish, President and CEO].

Theohary, C. A., & Rollins, J. (2009). *Cybersecurity: Current legislation, executive branch initiatives, and options for congress*. (Congressional Report No. R40836). Washington DC: Library of Congress Congressional Research Service. Retrieved from http://assets.opencrs.com

Tripwire Inc. (2015a). Tripwire uncovers significant security flaws in popular Smart Home automation hubs. *Business Wire.* August 3, 2015. Retrieved from http://www.tripwire.com

Tripwire Inc. (2015b). Zero-Day vulnerabilities in Smart Home automation hubs. *Information Security Buzz*. Retrieved from http://www.informationsecuritybuzz.com

Venda, P. (2015, August). Hacking DEFCON 23's IoT village Samsung fridge. *Pen Test PartnersHome.* August 18, 2015. Retrieved from https://www.pentestpartners.com

Waltzman, H. W., & Shen, L. (2015). The Internet of Things. *Intellectual Property & Technology Law Journal, 27*, 19-21. Retrieved from https://www.mayerbrown.com

Waters, J. (n.d.). Phenomenological research guidelines. Retrieved from https://www.capilanou.ca

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624. Retrieved from http://www.sciencedirect.com

Weiss, E. N., & Miller, R. S. (2015). *The target and other financial data breaches: frequently asked questions*. (R43496). www.crs.gov Retrieved from https://www.fas.org

Wheeler, T. (2014). *Tenth broadband progress notice of inquiry*. (GN Docket No. 14-126). Washington, D.C. Retrieved from https://apps.fcc.gov

Widman, J. (2015). How to keep your connected home safe: 7 security steps you can take. *Network World*. Retrieved from http://www.techhive.com

Working Party (2010). *Opinion on the Industry proposal for a privacy and data protection Impact Assessment Framework for RFID Applications*. Brussels, Belgium: Data Protection Working Party. Retrived from: http://www.dataprotection.ro/servlet/ViewDocument?id=722

Wright, D. (2008). Alternative futures: AmI scenarios and minority report. *Futures, 40*, 473-488. doi:10.1016/j.futures.2007.10.006

Yin, R. K. (2014). *Case study research: Design and methods* (B. Bauhaus Ed. Fifth edition ed.). Thousand Oaks, California 91320: Sage publications.

Z-Wave_Alliance. (2015). About Z-Wave technology. Retrieved from http://z-wavealliance.org

Zalud, B. (2014). Beyond the hype: wicked or wickedly, a good internet of things impacts smart home, appliances. *Appliance Design, 62*, 28-33. Retrieved from http://www.sdmmag.com