Henry Holben

Dr. White

Rhetoric II

14 April 2016

The Fiend Within Your Wireless Refrigerator: Privacy, Security, and the Internet of Things

Table of Contents

Thesis: Developers working toward the IoT revolution should delay their progress toward high-risk applications, focus on low risk applications, and refine the user privacy agreements of their products.

I. Introduction 1

A. General Overview of Topic 1

B. Statement of Thesis 2

C. Significance of Thesis 2

D. Limitations 2

E. Definitions of Terms 3

F. Organization of Thesis 4

II. Review of Literature 5

A. Introduction 5

B. History of Electronic Hacking and Security 5

1. Hacking 5

2. History of Internet Security 7

3. Modern Threats to Non-IoT Internet Security 7

C. IoT Benefits to User Security 7

D. IoT Hazards to User Security 7

1. The Modern Hacker 7

2. Security Vulnerability Researchers 8

3. Security Concerns 8

E. IoT Hazards to User Privacy 9

1. Security of Privacy 9

2. Conservation of User-Privacy 9

F. Responses made to IoT Security Threats 9

1. Typical Approaches to Security Threats 9

2. Marketing Threats 10

G. Biblical Worldview 10

H. Conclusion 11

III. Argument 11

A. Introduction 11

B. Unacceptability of Risks 12

1. Likelihood of Infiltration 12

2. Risks Compared to Benefits 14 3. Privacy 14 4. Safety 14

C. Developer Motivations 16

D. Endangerment of Non-IoT users 16

E. Recommendations 17

1. Recommendations to Developers 17

2. Recommendations to the United States 20

3. Recommendations to Consumers 21

4. Recommendations to General Public 21

F. Conclusion 22

IV. Works Cited 23

Henry Holben

Dr. White

Rhetoric II

14 April 2016

The Fiend Within Your Wireless Refrigerator: Privacy, Security, and the Internet of Things

Introduction

**General Overview of Topic**

Innovators in the information age are introducing machines and devices that can wirelessly communicate with each other and can be controlled remotely. Such machines allow for massive amounts of data to be gathered almost instantly. The creation of these devices has added a wireless network of appliances to the internet, allowing the connection and the exchange of data between machines to occur online. Technologists often refer to this network as the Internet of Things (IoT) or the Internet of Everything (IoE) and expect that in the future IoT compatibility will continue to become a mainstream feature of most consumer products in a stage of development dubbed *the IoT revolution.* Industries have often found need for machines that can wirelessly communicate and share information, and now product developers have found a place for IoT in the consumer market. Technologists predict that the IoT revolution will lead to changes in the very nature of consumer products and changes in the lifestyles of people using the technology. Technologists differentiate between the networks of IoT devices for Industrial use and the networks of similar devices sold to consumers, calling them the Industrial Internet of things (IIoT); and the Consumer Internet of Things (CIoT) respectively. Industries have found CIoT to be a lucrative market as a wide range of manufactured goods, from communications satellites to industrial equipment to vehicles to appliances to the very clothes consumers wear, can now be integrated with IoT enabled sensors and internet connectivity.

**Statement of Thesis**

Developers working toward the IoT revolution should delay their progress toward high-risk applications, focus on low risk applications, and refine the user privacy agreements of their products.

**Significance of Thesis**

From the early days of telecommunication, the security of information relayed wirelessly has been a major concern for consumers and developers. The threats posed by electronic hackers and cybercriminals have increased steadily with man’s increasing dependence on technology. Historically, cybercriminal hackers known as black-hat hackers have successfully inflicted harm, and stolen identities, and money. With the addition of IoT capabilities to non-informational utilities, black-hats are accumulating a new arsenal of powers. Both the privacy and physical safety of IoT users depend on the security of their Internet-enabled devices. With the expansion of IoT, technologists need to consider the different implications their inventions could have, security and privacy being amongst these implications.

**Limitations**

To narrow the scope of this thesis from irrelevant research, the following limitations are in effect:

1. This paper is uninterested in economic gains or losses generated by the IoT revolution other than those directly influencing the security of IoT; for example, the unemployment of workers whose jobs have become obsolete, or will become so, due to their replacement by technology is not a security risk and therefore will not be addressed in this paper.

2. This thesis does not address health risks caused by IoT other than the health risks caused by IoT security failures, thus the health risks caused by the existence of IoT itself, psychological risks to individuals and their lifestyles; for example, the soporific effects of technology on users are irrelevant to this thesis’s research.

3. This thesis is unconcerned with IoT information or incidents after 14 April 2016.

**Definitions of Terms**

Because this paper uses some computer jargon the reader may be unfamiliar with, the following glossary of terms is provided.

*Algorithm.* A section of a computer program’s source code that accomplishes a certain required task.

*Black-Hat.* Malevolent internet user who hacks devices on the internet to exploit or injure another user of the internet.

*Code.* Two definitions. a. Instructions given for a computer to follow; b. An encryption.

*Device.* Purpose-built, programable machine with limited functions (Holben).

*Easter Egg.* Discreetly placed algorithm in a computer program.

*Firmware.* “Software kept in semipermanent memory” (Newton and Schoen 545).

*Hacking.* Two definitions a. Use or alteration of a product to function in a manner unexpected by the original manufacturer. b. The infiltration of an electronic system.

*Internet.* Global network of connected computers and devices.

*(IIoT).* IoT systems used particularly in manufacturing and industrial settings.

*(IoT).* The developing network of internet-enabled manufactured goods that do not essentially

require the presence of a computer or internet capabilities to perform their intended functions.

*Reverse Engineering*. “ . . . process of taking the program or product apart, analyzing its makeup, and then putting it back together again. This technique is used in debugging program and in developing products that mimic or improve the original or interface to the original” (Newton, and Schoen 1071).

*Operating System.* “. . .a software program which manages the basic operations of a computer, smartphone, or switch . . . “ (Newton, and Schoen 918).

*Patch.* “A small addition to the original software code, written to bypass or correct a problem in the original code . . . ” (Newton, and Schoen 950).

*PLC.* Programable Logic Controller. “A programable device used for monitoring inputs, and setting outputs to control a machine or process” (Holben).

*Web.* “. . . The universe of accessible information available on many, many computers spread through the world and attached to that gigantic computer network called the

Internet. Global network of connected computers and devices.

*White-Hat.* An individual who hacks or investigates a computer or a program without permission or instruction from the computer or program’s owners, developer(s), etc. and claims innocent or benevolent purposes for doing so.

**Organization of Thesis**

This thesis is organized into the following sections: a table of contents, an introductory section, a review of literature, an argumentative section, and a works cited section. The Table of Contents outlines the structure of the document and provides the page numbers of each part of the thesis. The introductory section includes basic preliminary information the reader will need to comprehend the main body of the thesis. The Review of Literature exposes the findings and arguments of several authors who have previously written about this paper’s topic. The argumentative section of this thesis is designed to persuade the reader of this paper’s thesis statement. The Works Cited page documents the works cited in the paper and accredits the authors as appropriate.

Review of Literature

**Introduction**

While most technologists, developers, technical writers, researchers, and marketers agree that security risks exist in the development of IoT, controversy in the development of IoT security lies in the distinction between the desired responses to threats (Wind River 3). In addition, some researchers have found and continue to find flaws in IoT security systems (Zetter 2-3). Meanwhile, IoT developers persist to hastily release IoT products (Wind River 2).

**History of Electronic Hacking and Security**

*Hacking*

The first incidents of telecommunication sabotage, hacking, occurred in the early days of the telephone, involving misbehaving telephone operators who pulled practical jokes by misdirecting customers’ calls, spying on conversations, and other such mischiefs (Clarke, Clawson, and Cordell 1). In 1903 a more serious hack interrupted a demonstration by John Ambrose Fleming on a long-range telecommunications system developed by Guglielmo Marconi (New 1). Marconi had boasted his system’s security, hoping that ensuring its security would increase the profits (New 2). The Eastern Telegraph Company, foreseeing that an impregnable system of transmitting electronic systems wirelessly could easily replace the massive cabling telegraph systems they had invested in, hired a magician and telegraph enthusiast named Neville Maskelyne to test Marconi’s system (New 2). Maskelyne transmitted a message several minutes before Marconi’s own scheduled telegraph to Fleming’s audience in which he mockingly accused Marconi of lying about his invention (New 3). Several days later, Makelyne confessed to being the infiltrator and claimed his actions were justified because he had raised public awareness to the system’s vulnerabilities (New 3).

Zuley Clarke, James Clawson, and Maria Cordell report that although the aforementioned incidents are considered early examples of electronic hacking, the term *hacking* was originally coined much later by a 1960s MIT model train enthusiast group (1). The term meant the act of tinkering with an object, pushing its limits or causing it to function in an unprecedented way (Clarke, Clawson, and Cordell 1). The particular group found interest in modifying their trains and afterwards looked to early computer technology as an outlet for their talents (Clarke, Clawson, and Cordell 1). Hacking grew into a subculture of technology enthusiasts that shared a set of ethical values about telecommunications that promoted the thrill of discovery, and innovation, and condemned authoritarianism and repetitive work (Raymond 4-5).

The modern connotations for the word *hacking* developed in the 1980s when some hackers began to utilize their computer skills to commit crimes (Clarke, Clawson, and Cordell 1). Several criminal hacking gangs surfaced; and, in 1986, Congress passed the Federal Computer Fraud and Abuse Act, soon after which numerous cyber criminals were convicted (Clarke, Clawson, and Cordell 2).

History of Internet Security

Internet *s*ecurity has developed primarily through responses made to hacking(*The Washington Post*). As computers became more commonplace the demand for security increased along with the number of entry points for penetration (*The Washington Post*).

*Modern Threats to Non-IoT Internet Security*

Researchers have noted that as more devices are connected to the internet more points of penetration are made available to hackers (*The Washington Post*). In the modern world, so many devices, computers, and users have become connected that many experts consider the internet to be impossible to study thoroughly (*The Washington Post*).

IoT Benefits to User Security

IoT has created devices designed for the improvement of a users security. Because IoT has been implemented in many home automation systems, security systems in those homes may incorporate IoT (Samsung). Some IoT home automation devices can identify when possible points of entry for an intruder are accessible and can notify the owner of any odd activity. (Samsung)

**IoT Benefits to User Safety.**

IoT offers many improvements to the physical safety of its users. IoT devices have been used in Malaysia to most efficiently use the scarce amount of water portioned to rice farming (Kontron 4-5). Several IoT devices have been developed for the medical field, including IoT pacemakers with the ability to wirelessly send heart rate information to a patient’s doctor. (Corman) Military drones can technically be described as IoT devices that defend national security. IoT offers driverless cars which are likely to decrease fatalities in car accidents caused by human error.

**IoT Hazards to User Security**

*The Modern Hacker*

The differing groups of people referred to by the name *hacker* today are often categorized as the traditional hackers, who hold to classic hacker attitudes and enjoy applying their talents as innovators to their chosen fields of work: white-hats, hackers who infiltrate systems and confess to the deed to inform the system’s owner of the vulnerability, or cybercriminal black-hats, *crackers,* who illegally infiltrate computer systems generally working toward destructive ends for personal satisfaction or monetary gain (Garrabrandt, Brian, and Chibizov; Clarke, Clawson, and Cordell 2; Newton and Schoen 221).

*Security Vulnerability Researchers*

Unlike black hat cybercriminals, who illegally investigate source code or insert any destructive viruses, security vulnerability researchers typically find a weakness within particular software or firmware and announce the weakness online or in public, often causing panic amongst consumers of the product with the exposed flaw (Garrabrandt, Brian, and Chibizov). Such researchers often expose such flaws as a method of developing a reputation amongst developers at the expense of the reputation of the product and security developers of the exposed product (Garrabrandt, Brian, and Chibizov).

*Security Concerns*

It takes little experience, time or resources for a computer novice to become capable of causing damage by hacking (Garrabrandt, Brian, and Chibizov). A lot of material for hackers is available online (Garrabrandt, Brian, and Chibizov). This material is often blatantly easy to use for destructive ends.

**IoT Hazards to User Privacy**

*Security of Privacy*

With the risks of one’s computer being hacked comes the risk of one’s personal information being leaked or stolen. IoT’s effectiveness as a data collector has raised some concerns with researchers. Data collected by IoT is susceptible to hackers. Consumer information has been valuable enough as a target for hackers in the past. In a future where IoT devices continuously gather data on their owners, theft of information will only become easier and more commonplace.

*Conservation of User-Privacy*

User privacy agreements on products often give companies the right to gather data about their users. IoT under those same circumstances will allow companies to gather data about consumers much quicker (Garrabrandt, Brian, and Chibizov).

**Responses made to IoT Security Threats**

*Typical Approaches to Security Threats*

Historically, most security protocols have typically been developed, starting as security built into a particular program at its earliest launch and have been patched and updated as needs arise; when a bug is found or exploited, companies are forced to release a software patch as quickly as possible (Garrabrandt, Brian, and Chibizov).

*Marketing Threats*

Another difficulty in the development of IoT is that security cannot be easily marketed (Garrabrandt, Brian, and Chibizov). Consumers generally assume security to be guaranteed in the products they buy (Garrabrandt, Brian, and Chibizov). Because there is more hype amongst consumers for devices that can wirelessly communicate with the internet and little hype for security, IoT can be more easily marketed than the security it requires (Garrabrandt, Brian, and Chibizov). However, by marketing security, software developers often simply dare hackers to try and crack their products’ security (Garrabrandt, Brian, and Chibizov). Some black-hats take this as a challenge and often prove, for the sake of proving, that security software can be compromised easily by one with sufficient skill (Garrabrandt, Brian, and Chibizov).

**Biblical Worldview**

IoT is an ingenious application of man’s desire to create and innovate; however, just like man, IoT is flawed but may yet be improved. IoT can be viewed as a result of the creation and fall of man as described in the Bible. Just as man may be redeemed through the grace of Christ, so might man’s flaws in man’s inventions be improved and remedied: “Then God said, ‘Let us make man in our image, after our likeness“ (*The Holy Bible: English Standard Version,* Gen. 1.26). Man, made in God’s image, possesses a limited reflection of God’s infinite creative power and ingenuity.

This creativity is evident in humanity’s technological advances and improvements to such advancements. IoT likewise exhibits man’s desire to create, to fill the earth and subdue it.

Problems concerning the security of consumers’ privacy arising with the technology of IoT are a direct consequence of man’s moral depravity. In a perfect world, security and privacy vulnerabilities in IoT would not be problematic. In such a world there would be no just reason for users to hide anything and no just reason to investigate or injure another user. But man as he is, is hasty, reckless, secretive, indulgent, evil and ignorant. Man is sinful; likewise, his ability to create has been perverted. The Internet of Things will present many flaws, all resulting from man’s impatience to improve his standard of living.

**Conclusion**

The literature pertaining to IoT as a whole agrees that the poor security of IoT is a serious threat to the wellbeing of its users. Authors disagree as to what the correct method for addressing IoT issues is. Despite the rising awareness of IoT’s security risks, many authors are concerned that IoT development as a whole still prioritizes the release of new products over the refining of old products.

Argument

**Introduction**

The failure to sufficiently address faults in the new information age technology of IoT will jeopardize the privacy and the security of its users. As items such as smart watches, smart lightbulbs, even smart refrigerators hit the consumer market, the implementation challenges and the connectivity of those same consumer goods will make way for black-hat hackers to acquire private information and to gain control of the goods.

Developers working toward the IoT revolution should delay their progress toward high-risk applications, focus on low risk applications, and refine the user privacy agreements of their products. Although developers are aware of the risks involved with early IoT devices, their responses to these threats have been unsatisfactory. The technology is developing faster than its protection protocols; and if proper precautions are not taken, consumer and industrial utilities alike will be extremely vulnerable to cyberattacks and the mass-hysteria that is certain to follow.

**Unacceptability of Risks**

*Likelihood of Infiltration*

Imagine a future in which all of one’s utilities are interconnected. Every aspect of a modern day is synchronized. The car has already started and warmed the interior when the businessperson steps out the door one cold morning in January. Smart houses, smart appliances, and IoT home automation systems make life at home more comfortable and convenient. The IoT revolution has produced such items as smart lightbulbs, smart lawn sprinklers, and smart refrigerators. IoT has even been extended to cities, creating smart cities. Businesses employ IoT to better gather data, increase profits, decrease production costs, pin-point inefficiencies, and detect machine failures long before they ever happen; driverless cars save hundreds of lives; wireless drones spare soldiers’ lives; IoT pacemakers relay patient information directly to their doctors—and all through the power of the internet. On a macroeconomic scale, IoT is paving the way for information to be gathered, processed, and put to use within seconds, leading to a decrease in production costs of nearly all industries. The global internet as a whole is now able to effectively and quickly gather information about everything mankind has imbedded with a sensor and given internet capabilities.

However, a darker side of the ever-helpful internet exists. Those same sensors in the home are gathering data on their users: data which companies are using to better advertise products to those same users and the consumers are naively accepting the privacy agreements that permit this breach in their privacy. In other words, the modern household has been bugged, devices are leaking information to the outside world, and the homeowners themselves have placed the sensors. In addition to the developers who spy on buyers legally, IoT has made access to smart cars, smart homes, smart cities, smart drones, smart pacemakers, etc., open to criminal hackers. And while the world’s devices are getting smarter, they are entrusted with tasks they are not ready to protect against hackers. Thus, IoT in its current state presents huge risks to the consumers who buy them, and, by extension, to the general public that surrounds them. Nevertheless, developers continue to add more IoT features to their devices. Now stop imagining. IoT is here. Welcome to the future!

More devices empowered with internet connection means more openings available for hackers to infiltrate. The IoT revolution is creating these openings at a dangerously fast rate. Additionally, IoT developers are releasing IoT security systems and, consequentially, are creating a greater demand for hackers in the criminal world. Despite the security threats, a vast portion of consumers are unaware that the danger exists. Most security experts agree that no system is truly non-hackable. The abundance of motivations for cybercrime is ever-growing. The internet has made petty thievery, murder, terrorism, and simply wrecking havoc available to anyone with an interest in cybercrime. In fact, hacking is not difficult. Security researchers have shown time and time again that anyone with the time and money to learn some basic skills and install the right tools on his or her computer can cause serious problems on the internet. Although no computer system is impenetrable, or can be expected to be so, IoT in its current state presents dangers too significant to be permitted.

Risks Compared to Benefits

Although IoT threatens user security and privacy, it also offers improvements to it. To judge whether IoT bears a significant risk to the user, both the risks and improvements need to be compared. One such example, IoT smart home security systems allow houses to detect when doors or windows are open and can relay this information directly to the owner. However being an internet device such security systems can be deactivated via hacking, making burglary a simple matter of breaking in and out of the formerly “smart” building. IoT devices offer consumers improvements and risks in their security, and as a consequence, in their safety and privacy. However, when the risks and improvements are weighed, the threats far outweigh the improvements.

*Privacy*

IoT devices add impermissible risks to user privacy. By default, IoT devices are enabled with sensors to efficiently gather information. In IIoT, producers of a certain good use these sensors to quickly examine their efficiencies, possible defects, etc. On the consumer market these devices allow users’ machines to detect when they are needed or to act autonomously. However, not all of the data gathered benefits the consumer. Often developers use IoT devices to gather information about the buyer. Doing so allows the product’s service developers to better advertise to the consumer. In addition, the numerous sensors added by home automation systems are used to collect large amounts of data which in turn are sent to the automation system’s main computer.

The following quote describes a process IoT devices use to communicate with other devices. This process could prove useful to hackers wishing to find information about another’s system, as there own IoT devices have the power to detect similar devices.

The numerous IoT devices provide a variety of services that are discoverable utilizing known techniques including domain name service based service discovery (DNS-SD). DNS-SD does enable an IoT client device to query other IoT devices to discover the services that are available, but the existing framework for clients to query other IoT devices produces broad searches that result in many responses from the other IoT devices. In addition, a querying device often times must establish a session with a responder device to retrieve more information about the services provided by the responder. And if the services are not of interest to the querying device, the querying device must disconnect and continue the discovery process. Thus, existing service discovery methodologies are prone to overly broad responses that increase network traffic and may cause substantial delays. “(Researchers Submit Patent Application, 'Enhanced DNS-Based Service Discovery in an Internet of Things (IoT) Environment', for Approval (USPTO 20150341446).”

The user’s computer will access data gathered by the user’s other devices to learn about its user. The information will be gathered for the purpose of better serving the user; but in the event of hacking, the information could easily fall into the wrong hands.

*Safety*

The vulnerabilities in any IoT devices threaten the physical safety of their users. Some computerized cars have been proven to be vulnerable to cyberattacks. Car computers in many modern cars are used to relay the information from the driver to the vehicle, and many of these cars are given internet capabilities. Having infiltrated a vehicle, security researchers testing the dangers of car security have been able to disengage the breaks, take control of the steering, and cause the airbags to deploy, amongst other tricks. In the hands of a cybercriminal, these hacks could easily prove deadly to a driver, to anyone sharing the road with an infiltrated vehicle, and to any pedestrians nearby. In little time, IoT will allow driverless cars to communicate with each other, establish obstacles, etc. Although this improvement will prevent many accidents the risk of car hacking will increase.

**Developer Motivations**

Developers have several motivations to create IoT related features in their products while not strengthening security to an appropriate level. Currently, several developer companies are competing to become the leading developer of IoT products. Historically, developers having secured themselves as the recognized leading developer of a particular kind of good have had great success coming near to a monopoly on that good. Second, unlike security, the hype already built in IoT smart products makes IoT enabled devices easy to market to consumers. Third, innovators such as people working on IoT often consider themselves pioneers of technology. Innovators such as those are more interested in having their name become associated with some valued technology rather than becoming yet another faceless refiner of the age-old practice of security. Thus developers have more motivation to upgrade the features of their product, such as IoT rather than to upgrade their security.

**Endangerment of Non-IoT users**

Even people abstaining from usage of IoT will be endangered by the consumers of the technology. A hacker having gained control of a driverless car could not only use that vehicle to harm the passengers but also other people on or near the same road. Infiltrators will be empowered to shut down or manipulate IIoT industrial equipment, allowing a hacker to cause city blackouts or to use factory equipment for other destructive purposes. Perhaps the most extreme example in the modern age, hacked military drones could be used to attack civilians.

**Recommendations**

*Recommendations to Developers*

History has shown the necessity for caution in the development of new technology. The Wright brothers are prime examples of cautious innovators. Orville and Wilbur Wright made numerous test flights on man-sized kites before they ever attempted to build and fly the airplane. The Wrights took careful steps to Kitty Hawk even while other pioneers of aviation, such as Samuel Langley, rushed (and failed) to solve the problem of flight (Engel, Dixon, and Jackson, 64-67). The Wrights were saddened by the tragic death of Otto Lilienthal, a German innovator and an aviation pioneer who experimented with gliders. Lilienthal died in a glider crash, which the brothers noted may have been avoided had he remained calm when he began to lose control of his glider in a gust of wind. (Engel, Dixon, and Jackson, 22-25) Although the brothers certainly took their share of risks and failures, they remain to this day amongst the most remarkable inventors for their persistence, albeit their caution, in the development of modern aviation.

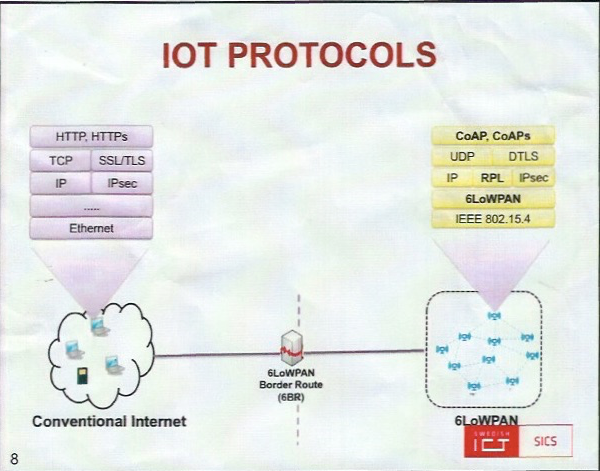
Like aviation, the takeoff of IoT calls for early adopters to take cautious steps even if their competitors are more hasty to move items on the consumer market. IoT development needs to take on the assumption that if something can be hacked, it will be. By preparing for failures developers will strengthen the security of their devices, and discover new ways of avoiding security vulnerabilities.

One factor to consider is the difference in IoT manufacturers. As time passes, the assumption that IoT companies will eventually create devices compatible with competitor manufacturers becomes more reasonable, but this is not yet the case. Different IoT developers are in production of a variety of products Many different security protocols have been developed for IoT. But quantity is not always a good thing. The orthodox solution would be to begin implementing firmware into things, gradually building an intricate network of computerized utilities, and then begin developing new security protocols as incidences occur. This solution will ultimately cost human lives as the eye-openers to vulnerabilities. Because of the differences in security protocols, difficulties arise when making different developers interoperate. However, some technologists have suggested that a better solution would be to unite the innovators developing the conflicting protocols to first create a single security protocol for IoT devices.

Figure 1, provided in an interview with security experts from Siemens, illustrates the disproportion in the amount of different security protocols created for IoT when compared to the amount created for the general internet.

IoT Protocols

*Figure1*. IoT Protocols (Garrabrandt, Brian, and Chibizov)

Security is not, and should not be, marketed with the same effort that products are marketed. Many black-hat hackers hack merely for the pleasure of inflicting harm on other people. By boasting of his system’s resistance to hackers, the owner challenges those same hackers to infiltrate his system. But IoT compatibility is a much easier feature to market. Because of this, companies are racing to release the newest, flashiest, most hyped up IoT linked machines. Security might be easy for developers to overlook when rushing to release new lines of products with IoT compatibility, and security like other features may also come to be seen as a necessary commodity. A company’s development of IoT features is put in a race against the development of its own security, a race that, if users are to keep the same level of security they are accustomed to, the security must win. None of this is to say that developers should not work on IoT. A multitude of low-risk applications that are ideal for developers and early adopters alike is on the table for innovators to develop, market, and test. Proposed *smart cement*, concrete filled with electronic sensors, for example, will enable structures to communicate their own status, faults, and damages to their owners. Because the technology is purely made for making observations about structural integrity the worst ways a hacker could misuse them would be to glean information about already existing problems with a structure, or manipulate the information being sent back to the owner. As another example, smart lightbulbs offer what appears to be a low-risk application. At worst, if these lightbulbs were used to illuminate a building with little external lighting, that building could be plunged into darknesses by a hacker. This is opposed to high-risk applications such as some IoT biomedical technologies. For example, IoT insulin pumps for diabetics and pacemakers with internet connections, and some industrial equipment, such as nuclear power plants that use IoT enabled PLCs threaten consumer and public safety.

*Recommendations to the United States*

As the homeland for many information technology companies, the United States ought to set a precedent for its respect of its citizens’ technological rights. Governments need to adjust laws and evaluate constitutions to maintain the freedom and the privacy of their citizens. In the United States, a company’s ownership of personal information could lead to an infringement of users’ Constitutional rights. Aside from this possibility, personal information may someday be so freely waived to technology developing companies that an American’s Constitutional right to privacy will be totally given up in user-manufacture agreements.

*Recommendations to Consumers*

Consumer awareness will make IoT a safer place. By using IoT, consumers add a multitude of hackable devices to the internet. These devices could be used later as entry ways for hackers to corrupt a system. Often times hackers will infect computers with viruses not set to take effect on a consumer until a certain amount of time has expired. Consumers must understand the risks they put on themselves and others by using IoT devices. As such, consumers should work as users of the internet to be responsible in the usage of their devices. Further, showing prudence in one’s choices of IoT products will decrease the pressure on developers to create more hackable features and increase the pressure to boost security. However, all IoT applications present a common threat to the owner. Hackers can use devices to spread viruses. Such a virus could be placed on a low-risk IoT application which in turn could contaminate other devices. For example, suppose a company sees the efficiency of upgrading a building’s lighting with IoT enabled florescent lights. A hacker, hoping to steal an important document from a computer could instead target the lighting system. The lighting system, in contact with the company’s computer mainframe, is designed to save data on the company’s computer network. Thus, a hacker could gain access to a high-risk application by attacking a low-risk application.

*Recommendations to the General Public*

IoT will affect all aspects of modern life. Whether using IoT or abstaining, people will be helped and harmed by the existence of IoT. As technology is developed, IoT and the dangers it presents will become more commonplace. Not owning IoT devices does not exclude a person from the dangers IoT security vulnerabilities present. The general public needs to be aware of the danger.

**Conclusion**

As with all great innovations, IoT will provide mankind with new and useful tools that will be better synchronized with each other and better suited to assist their human masters in their activities. However, IoT, like many great innovations of the past, adds many dangers to the security, privacy, and safety of its users which must not be ignored. IoT developers must address these issues by lowering the rate at which high-risk IoT applications are produced to build the appropriate security protocols and experiment with low risk applications.

Works Cited

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes.” Wired.com

21 November 2014. Web. 18 February 2015.

---. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com

26 November 2014. Web. 28 March 2016.

Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet*

*Security Second Edition.* AT&T and Lumeta Corporation, 2003. Print.

Clark, Richard A. *Cyber War: The Next Threat to National Security and What To Do About It.* Tantor Media, 2010. CD.

Clarke, Zuley, James Clawson, and Maria Cordell, Maria. *A Brief History of Hacking.* Historical Approaches to Digital Media.steel.ICCgatech.edu. November 2003. Web. 9 February 2016.

Cook, Tim. “A Message to Our Customers.” apple. *apple.com.* 16 February 2016. Web. 29 February 2016.

Corman, Joshua. “Swimming with Sharks- Security in the Internet of Things.” TEDx. Naperville, IL. 20 December 2013. Lecture.

Daya, Bhavya. “Network Security: History, Importance, and Future.” University of Florida Electrical and Computer Engineering, *Dissertation*. (May 2009):1-13. PDF file. Web. 24 March 2016

Dhanjani, Nitesh. *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*. Sebastepol, CA: O’Reilly Media, 2015. Kindle.

Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail.*

20 October 2015. Toronto: Telecom Media. Web. 28 February 2016

Engel, Dixon, and Mike Jackson. *The Wright Brothers: First in Flight.* Sterling: New York, 2007. Print.

Fields, James. “Internet of Things Will Ease Lives.” *The Tennessean.* 31 October 2014: 2. Nashville. Web. 28 March 2016.

Finley, Kint. “Get Email Notifications on Your TV With Comcast and IFTTT.” *Klint Finley Buisness*. 12 April 2015. Web. 29 February 2016.

---. “Tech Tycoon Bets Business Is the Internet of Things’ Future.” *Kint Finley Business,* 25 February 2016. Web. 29 February 2016.

Forester Consulting. “The Internet of Things Has the Potential to Connect and Transform Businesses But Most Early Adopters Have Focused on Efficiency Plays.” Forester. August 2015. Web. 29 February 2015.

Garrabrandt, Frank. and Harry Brian. and Sergey Chibizov. Personal interview. 8 January 2015.

General Electric. “GE Digital’s OT Cyber Security Division to Refocus Industrial Internet Discussion at Arc Industry Forum.” G*E*. San Ramon, CA:(NYSE:GE), 3 February 2016 Web. 8 February 2016.

Gilchrist, Alasdair. *A Concise Guide to the Internet of Things for Executives.* RG Consultants, 2015. Kindle.

Greenberg, Andy, and Kim Zetter. “How the Internet of Things Got Hacked.” *Wired.com*. 28 December 2015. Web. 29 February 2016.

Hardy, Quentin. “Beyond the Internet of Things.” *New York Times.* 2 January 2016. Web.

7 February 2016.

Holben, Dave. Personal interview. 3 March 2015.

*The Holy Bible: English Standard Version,* Crossway: Wheaton, Illinois. 2010. Print.

Horwitz, Julia, Marc Rotenburg, and Jeramie Scott. *Privacy in the Modern Age: The Search For Solutions.* New York: The New Press, 2015. Print.

Kontron. “Adding IoT to Water Works Wonders For Malaysian Rice Growers.” (Kontron). PDF file. 2015 Web. 16 February 2016.

Lee, Dave. “Gilbc: Mega Bug May Hit Thousands of Devices.” *BBC.com BBC: Technology*. 17 February 2016.Web. 29 February 2016.

Marr, Bernard. “17 ‘Internet of Things’ Facts Everyone Should Read.“ Forbes. 27 October 2015. Web. 25 January 2016.

Matyszczyk, Chris. “Samsung’s Warning: Our Smart Tvs Record Your Living Room Chatter.” Cnet. 8 February 2015 Web. 29 February 2016.

New, Charlotte. *Hacking at the Royal Institution. Rgib.* 11 July 2016. Web. 9 February 2016.

Newton, Harry, and Steve Schoen. *Newton’s Telecom Dictionary.* Ironmark, New York: Ironmark 2016. Print.

Patrick, Mathew. “Game Theory: Death by Hacking.” *Youtube* 10 October 2014. Web. 1 March 2016. Video.

---. “Game Theory: Watch Dogs Warning! You’re Not Safe!” *Youtube* 2 July 2014. Web. 1 March 2016. Video.

Raymond, Stephen. “How to Become A Hacker.” *Catb*. Thyrsus Enterprises, (revision 1.50).

19 July 2015. Web. 9 February 2016.

"Researchers Submit Patent Application, 'Enhanced DNS-Based Service Discovery in an Internet of Things (IoT) Environment', for Approval (USPTO 20150341446)." *Computers, Networks & Communications* 17 Dec. 2015: 1995. *Computer Database*. Web. 18 Dec. 2015.

Samsung. “Products” samsung. Web. 4 Feb 2016

Santosh, Aala. “Reaping the Benefits of the Internet of Things.” *Cognizant Reports.* (Nasdaq). May 2014. Web. 29 February 2016. PDF File.

Scantlebury, Mark.”Design Solutions for the Internet of Things.” *Embedded Innovator*. Web. 29 February 2016.

Sterling, Bruce. “The Epic Struggle of the Internet of Things.” Strealka Press, 2014. Kindle.

Styles, Kirsty. “Passive ‘Wi-Fi’ Uses 10,000 Times Less Power Than Normal to Save Your Phone Battery.” T*henextweb.* 24 February 2016. Web. 29 February 2016.

Tarapore, Shahrukh. “‘Internet of Things’ Raises Big Ethical Questions for Banks.” *American Banker*. Bank Think, 29 January 2016. Web. 29 February 2016.

*The* *Washington Post.* “A History of Internet Security.”*Washington Post Reporting*. 30 May 2015 Web. 16 February 2016.

Thomas, Rolland. “Invest, Make Money & Retire Early From The Internet Of Things Revolution.” Rolland Thomas. 2015. Kindle.

United States Congress. *Computer Fraud & Abuse Act.* Washington: GPO, 1986. Print.

Van der Meulen, Rob and Janessa Rivera. “Gartner Says Smart Cities Will Use 1.1 Billion Connected Things in 2015. *Gartner*. Egham, UK: Gartner Research, 18 March 2015. Web. 29 February 2016.

Waangaurd, Karan. “Building Cities of the Future.” *Business Today.* 17 Jan. 2016.

Wind River. “Security in the Internet of Things.” *Wind river* Web. 9 February 2016. PDF file.

Zetter, Kim. “How to Hack the Power Grid Through Home Air Conditioners.” Wired.

9 February 2016. Web. 9 February 2016.