The Internet of Attack Vectors

Exploration and Remediation of Vulnerabilities in Non-Computing Consumer Wireless Devices

By: Richard Givens, CPSC 59700, Section 4, Research in Computer Science

Lewis University, College of Arts and Sciences

Spring, 2017

Abstract

This paper discusses some of the vulnerabilities common to non-computing consumer wireless devices, such as smart refrigerators, wireless cooking appliances, and other household electronic devices collectively known as “The Internet of Things,” or IoT, how these vulnerabilities are effective avenues of attack or exploitation by malicious third parties, and discusses the importance of robust testing, particularly regarding security in the development and subsequent support of these devices.

To provide effective demonstration of these vulnerabilities, a commercially available IoT device is examined, the Black + Decker WiFi-Enabled 6-Quart Slow Cooker [20]. Through research and investigative methods, several previously undisclosed vulnerabilities are discovered and examples given how they affect consumers and businesses. By and large, the discovered vulnerabilities are common to many IoT devices. However, research uncovered a serious flaw in the slow cooker’s companion application software, which exposes Black + Decker to potential attack. Due to the nature of the discovered vulnerabilities, the author chose to formally disclose them to Black + Decker.

Finally, this paper discusses effective remediation which will address the vulnerabilities discovered, the variables requiring consideration, and immediate action Black + Decker should undertake to protect corporate interests.

This paper does not, however, provide specific methods used to exploit vulnerabilities. The testing, implementation and research conducted during the process used legally owned equipment and open source tools within the constraints of all applicable local, state, federal and international legal requirements. At no time did the author of this paper undertake any modification of proprietary source code or hardware. Furthermore, the use of or mention of any company, brand, product or organization is not a challenge to any patent, copywrite or trademark.

Introduction

The Internet of Things, or IoT, refers to modern consumer electronics which connect via wireless or physical means to the Internet or to a local network [1]. Initially limited to larger appliances, advances in computing and manufacturing have created smaller devices which accomplish their tasks with greater efficiency. The first device, launched in 2000 by LG and known as the Internet Digital DIOS Refrigerator, was a fully functional computer with a physical Internet connection, thirty-seven-inch LCD touchscreen, modem, hard drive, microphone, speakers, camera, and external DVD ports [16]. Though certainly a marvel of computer integration for its time, the $15000.00 cost did not endear it to customers. That same year, Russian computer security company Kaspersky exposed a mobile email virus targeting wireless phones, and warned that Internet connected devices would become the target for cybercriminals in the coming years [11].

Since then, the development of advance mobile communication technology, coupled with increasingly compact computing systems, has created an environment in which nearly any electronic device with which a consumer wishes to interact may receive or transmit signals between itself and the Internet [14]. Cellular telephones are now advanced minicomputers capable of providing a user with the information required to run a business, the desktop computing environment has largely given way to the mobile computing environment in which a tablet or laptop performs all the tasks a user requires. The new class of consumers, the prosumers, demand instantaneous feedback, information, resolution, service and support; they are willing to pay the costs necessary to purchase devices which cater to these demands, and manufacturers are willing to provide products which will meet them [9]. Similarly, the costs required to develop and construct highly complex, technological devices has decreased, creating a market in which these devices, once status symbols for the wealthy, have become easy to acquire conveniences for anyone, yet still confer the perception of status.

This rapid growth of technological information has created an environment where some goods are rushed to market without adequate testing. There is a perception that manufacturers of IoT devices little attention to details beyond the basic functionality, leaving multiple vulnerabilities in place as an avenue of exploit or attack by malicious third parties. Many IoT devices share common vulnerabilities not present in most wireless computing devices, which persist across product lines for no discernible reason. Given the relative availability and low price of most IoT devices, one assumes security is either an extremely low priority for most manufacturers, that they are either unaware or unconcerned about potential consequences. Regardless of motive or lack of clarity, these vulnerabilities exist, placing both consumers and businesses at risk.

In October of 2016, the Mirai botnet was responsible for crippling a portion of the Internet, striking the provider of Dyn DNS services [5] using Internet connected DVRs, routers, and other common IoT devices as part of its attack platform. On February 28, 2017, a massive Distributed Denial of Service Attack (DDoS) disrupted services at an unnamed college in the United States of America for fifty-four consecutive hours. Using a variant of the Mirai botnet, the attack originated from almost ten thousand unique IP addresses, and generated nearly 3 billion requests. Using known vulnerabilities, the attacker or attackers exploited CCTV cameras, routers, and DVRs, averaging thirty thousand requests per second [2].

These, and other events provide an effective backdrop for understanding the importance of IoT security, as well as the entire field of Information Security. The following sections will define key terms, and discuss each of these attacks in detail, describe the methodology of the attackers, and the specific disclosed vulnerabilities which allowed their exploitation. Next, this paper extrapolates the existence of one or more previously unreported vulnerabilities using a recently manufactured commercially available IoT device. Within this section, the specifications of the IoT device, the test equipment, and the general tools used in testing are also discussed.

In the section following testing, this paper will discuss the potential liability issues manufacturers and distributors face when knowingly selling potentially vulnerable devices, particularly regarding the device examined for this project. Also, recent legislation targeting unsecured IoT devices, and its application to the IoT industry, is discussed.

The final section discusses formal verification and testing methods, specifically the addressable variables responsible for the vulnerabilities. These methods are applicable to any potential future software upgrade or patching effort, but are also applicable to futured development of other products, when used properly in a formal testing environment.

Key Terms and Definitions

Within the industry of Information Security there are several terms which have unique meanings, or share a definition from within the parent industry of Computing. This section discusses those terms, and attempts to provide a definition easily understandable by a person of any background.

Access Point – An Access Point **(AP)**, commonly known as a **Wireless Access Point (WAP)** is a communication device used on wireless networks which send and receive wireless signals. They are commonly used in conjunction with a router to boost signals across a wide area, and are most often found broadcasting an open network notification in areas such as hotspots.

Botnet [18] – A botnet is an interconnected network of computing devices subverted by an attacker, which pools resources to infect other machines and launch massive attacks, or engage in other illegal activity. The concept behind a botnet is like that of parallel computing projects such as **SETI@Home**, in which internet connected computing devices pool processing power to complete a task. Many botnets, **Mirai [15]** for example, are platforms for **Distributed Denial of Service** attacks (explained below), or the distribution of spam or phishing emails, while others subvert the processing power of enslaved devices to decrypt sensitive data, or digitally "mine" cryptocurrency, such as Bitcoin.

Denial of Service – A Denial of Service **(DOS)** is a form of attack in which a malicious third party "attempts to prevent legitimate users from accessing information or services" [26]. Common forms of DOS attacks target network connections by sending multiple, simultaneous requests to servers. The servers, able to handle potentially tens of thousands of **requests per second (RPS)**, become overwhelmed with requests and then unable to fulfill any, creating a situation known as deadlock. A form of DOS attack, known as **Distributed Denial of Service**, or **DDOS**, attackers use multiple computers (some without the owners' knowledge or permission) which may or may not exist in proximity, to attack a target or targets with greater effect. DDoS attacks experience the greatest success because of the

exponential number of devices used in the attack, and difficulty in tracing its originating source. A subset of DoS Attacks is the **Denial of Convenience (DoC)**, in which a malicious party intentionally blocks user access to a device or device service, preventing its operation.

Domain Name Service – The Domain Name Service **(DNS)** translates human readable domain names, such as www.LewisU.edu, into a series of numbers separated by periods. This number series, known as an **Internet Protocol** or **IP address**, is used by computers and computing devices to communicate with one another across networks.

Evil Twin [22] – In an Evil Twin attack, malicious parties use various methods and techniques to create a duplicate of a legitimate AP, or create a new AP that appears genuine. When duplicating an AP, the Evil Twin AP mimics the exact **Service Set Identifier (SSID** or **Network Name)**, as well as the channel and the **Media Access Control (MAC) address**, a technique generally known as **spoofing** (spoofing is also interchangeable as a term in attacks which mimic phone numbers or other personal communication data). A general overview of methods used during and after an Evil Twin attack is discussed in a later section.

Firmware – Firmware is the operating system of most hardware devices. Generally closed, meaning inaccessible by Users, the firmware of any device is the programming which enables it to operate within its established criteria. Examples of firmware include the operating system of mobile devices, as well as the integral programming of most computer peripherals such as printers.

Hacker – The definitions of Hacker are as varied as the demographics and motives of those who claim affiliation with the term. A loose definition, suitable for the context of this paper, is any person who engages in the exploitation or modification of an electronic device, through its hardware, software, or firmware. Hackers generally utilize several mundane and highly technical methods, along with sociological and psychological methods (known as **social engineering**) to obtain desired results from an

electronic device (such as the execution of an unauthorized process), or from the users of the electronic device (such as a passphrase or physical access to the device itself). **Hacking** is the term given to the application of the methods. Other terms associated with Hacker(s) are **penetration testing (pentesting)**, which is the methodical testing of a device, group or organization with the express purpose of exposing and reporting vulnerabilities, usually as part of a business arrangement. A **pentester** is one engaged in this arrangement with a group or business. Such engagements are usually referred to as **Red Teaming** or **Red Team Engagements** where the pentesters and other information security professionals represent the "Red Team" and engage in both real and simulated attacks against the contracting party, while the term "Blue Team" generally refers to the group within the organization tasked with opposing the Red Team, and addressing any vulnerabilities or security shortcomings after the engagement.

Internet of Things [1] -The Internet of Things, or **IoT**, is the term given to the collection of consumer devices capable of receiving or transmitting a wireless signal, or any device connected to a **Local Area Network (LAN)**. Such devices range in size and function, creating a barrier to a comprehensive list. Examples of IoT devices are Smart TVs, Set Top Boxes and DVRs, Self-Programming NEST Thermostats, personal activity trackers, and wireless kitchen appliances. All IoT devices share the characteristic of sending and receiving network traffic.

Kali Linux [19] – Kali Linux, short form **Kali**, is an open source operating system built on the Debian Linux kernel. Kali is a free software distribution used as a robust computer security platform, including many of the tools used by hackers and security professionals to determine vulnerabilities, and in many cases, exploit them. Among the many benefits of Kali is its ability to operate as either a sole operating system on a computer or laptop, as a dual boot option, or carried on a USB Flash Drive usable on any computer with an available USB port. Kali Linux is customizable, making it visually indistinguishable from any version of Linux, using standard Linux tools for web browsing, productivity, or office applications.

Man-in-the-Middle [22] – The Man in the Middle Attack eavesdrops on the communication between a device or computer, and its access point. Using applications such as **Wireshark [21]**, a third-party intercepts network traffic in a technique known as **packet sniffing**, whereupon he or she may save it to a log for later examination and decryption. Some devices transmit **plaintext information**, also known as "**in the clear**," which consists of unencrypted data which is human readable. Both plaintext and decrypted data open attack avenues in the form of stolen network credentials, usernames, passwords, or intelligence gathering for possible social engineering attacks.

nmap [17] – nmap is an intelligence gathering application, usable from the command line or terminal of a Windows, Unix, or Linux computer which gathers information about an IP address or range of IP addresses. When initialized, nmap surveys the IP address or addresses in a technique known as **port scanning**, reporting information pertaining to the number of hosts, open ports (capable of receiving traffic outside of the local network, and hence, vulnerable), operating systems of the target, and other information of interest to hackers. Once an attacker knows the target's IP address and MAC address (also viewable as part of a port scan), he or she may connect to the device and access system files by means of entering default manufacturing information, such as the default administrative username and passwords of many network attached printers or routers. Such techniques are generally successful, given the relatively few number of users who change this default information.

Patch – In terms of computing, a patch is a modification to software files or source code, which occurs after development, to address some issue, shortfall, or problem not resolved during the development and testing phases. **Patching**, the act of applying a patch, generally occurs after a product or device is available for sale, though may occur immediately upon first use. The term refers to the hasty post development process to address shortcomings affecting a product that is currently for sale or in the hands of consumers, rather like patching a tire so that it stays inflated long enough to fix the leak.

Rise of the Botnet

The DDoS attack against the unnamed university in February of 2017 utilized a variant of the Mirai botnet malware, and resulted in an attack lasting approximately 54 hours. Rather than using infected computers, the hackers behind the attack created a massive botnet of nearly ten thousand IoT devices consisting of CCTV Cameras, their DVRs, and routers, effectively turning physical security devices into attack vectors. The combined processing power of this botnet created a DDoS attack which flooded the university's servers with HTTP traffic peaking at thirty-seven thousand requests per second.

While the Mirai variant used against the university resulted in the longest DDoS attack, the largest DDoS attack occurred the previous year, in October of 2016, and affected all computers, servers, and networking devices which relied upon Dyn's services. Three waves of attacks, utilizing "10s of millions of IP addresses" [5] belonging to Mirai infected IoT devices successfully overwhelmed Dyn's severs, and disrupted Internet access for millions of users, clients, and brands on the East Coast of the United States.

The motives for these attacks are unclear, however the common factor between them is the use of IoT devices. Both Mirai and its variant used against the university utilize infected computing devices to scour the Internet for unprotected devices. These devices, secured by manufacturer default usernames and passwords, are seized and infected by the botnet to become its agent, working concurrently with other infected agents.

The use of default usernames and passwords is a common vulnerability affecting IoT devices, but not the only one. In 2014, the OWASP (Open Web Application Security Project) listed the top ten IoT Vulnerabilities [23]. Ranging from insecure web, cloud or mobile interfaces, to insufficient authentication processes, OWASP also defined multiple attack vectors. Among them are the use of plaintext usernames and passwords, as found in the Mirai attacks, the default level of trust between

devices or components, hardcoded administrative accounts or passwords, lack of firmware updates, administrative command line interfaces, and various others which open users of such devices to attacks by malicious third parties, or the use of these devices in concentrated attacks against substantially larger and lucrative targets.

Testing of a Commercially Available Device

Simply reporting facts as presented by other parties does little to further research in any given topic. Without original research, effort, and work presented, this paper only echoes the words of others. This section demonstrates the inherit risk of IoT devices by examining, exploring, and exposing flaws in a device with no previously disclosed vulnerabilities, which was purchased for the specific purpose of testing.

Testing is conducted on a Black + Decker WiFi-Enabled 6-Quart Slow Cooker, distributed exclusively through Walmart and retailing for approximately $50.00 USD. Researching FCC documents [7], [8], reveals that Black + Decker did not develop the slow cooker, but that it is manufactured by a third party, Midea Global with headquarters in Guangdong Province, People's Republic of China. Black + Decker's parent company, Spectrum Brands, applied for a new FCC ID on August 11,2016 with the permission of Guangdong MD Consumer Electronic Manufacturing Co., Ltd. In a later section, research will show that Midea Group is the original manufacturer of the slow cooker through port scanning and analysis of network traffic (Appendix E, Appendix F).

Interestingly, attempts to reach Midea's website from a location inside the United States resulted in failure, however circumventing U.S. servers and connecting directly to a server in Hong Kong via a Virtual Private Network (VPN) client, was successful.

The testing platforms consist of two computers: a custom Windows 10 PC equipped with an AMD Ryzen 7 1700X CPU and 32 Gigabytes of DDR4 RAM, and a Lenovo Yoga 710 laptop PC with an Intel Core i5 6th Generation Processor, and 16 Gigabytes of DDR3 Low Voltage RAM, with 64-bit Kali Linux as the operating system installed in Persistent USB mode on a 32 Gigabyte PNY USB 3.0 Flash drive. For those unfamiliar with using any Linux distribution with a removable drive, such as a USB Flash drive, Persistent USB Mode enables the flash drive to store long term data, such as saved files or operating

system upgrades, enabling the removable media to move from platform to platform, but continue from a saved stopping point. Logs, documents, and any saved data will transfer with the media and are available upon the next system boot, regardless if the platform hosting the media is the same or if the media is moved to a new host. The specific security testing applications used on the device were Wireshark, nmap, and airbase-ng, all tools which are available as part of the Kali Linux distribution or as separate downloads. For smartphone application testing, a Huawei Honor 6X operating on stock Android version 6.0 firmware was utilized.

Early Results

Verification of a vulnerability occurred within the first minutes of configuring the slow cooker. Users are directed to download the smartphone app from either the Apple App Store, or Google Play Store as appropriate as shown in Appendix A. Upon opening the smartphone app, users are prompted to register an account by entering an email address and creating a password consisting of at least six characters. The username field accepted arbitrary input resembling an email address in form, while the password field accepted any six characters except spaces. Test input consisting of username sss@ss.us was accepted, along with the password 111111, as well as sss@ss.is and the password -------- (six dashes in consecutive order). If a user enters a legitimate email address they receive a confirmation email thanking them for registering an account as shown in Appendix B, however there is no authentication requirement to filter fake users, multiple, or illegitimate accounts. Once a user registers an account they remain signed in (as is the case with most smartphone applications). However, users may log out of the account, and then register new accounts multiple times on the same device.

Simply going no further than account registration, the slow cooker displays two vulnerabilities for users, non-existent account verification/authentication, and weak security features in the form of arbitrary passwords. However, a significant vulnerability exists for Black + Decker as well. Exploiting the

non-existent verification, weak password security requirements, and the ability to create multiple accounts with the same device, a malicious third party is able attack Black + Decker through their user database. Such an attack could consist of a botnet, using automated programming scripts to create accounts, log off, and create new accounts utilizing every letter in the alphabet in random order, of random lengths, and random email domains. Another possible method is to use a “click farm”, a series of physically interconnected mobile phones, controlled by a host computer and user, which operate independently and concurrently to simulate user input. As click farms may consist of tens of thousands of devices under the control of a very limited number of users and computers, it may approach the effectiveness of a botnet. This attack is affects the victim, targeting both the username database and the mailserver for the business; the user database fills with junk input and runs out of space, while the mailserver constantly sends emails to nonexistent addresses, receives the bounceback notification, and attempts to resend the email over the course of several hours or days.

Further Testing

Though potentially substantial, these vulnerabilities are not alone. During the initial setup process, after creating an account for the smartphone app, users are prompted to enter the password for the network the slow cooker will connect to. After which, users power on the slow cooker, and enable its network connectivity by pressing two buttons at the same time. A flashing network icon appears, and the slow cooker broadcasts an SSID, “B+D_e8_” followed by four consecutive numbers (Appendix C). This SSID is consistent for all models as listed in the support documentation. Furthermore, all Black + Decker IoT slow cookers have the same password, 12345678 (Appendix A), which is hardcoded into the firmware of the device, preventing users from changing it or the SSID. This information, though possibly difficult to locate by the average consumer, is readily available within product documentation found both online and with the product manuals and quick-start guide.

Once the cooker's network is selected, and the password information entered, the smartphone app and the cooker sync together, whereupon the network credentials of the user's selected network are passed to the cooker. The slow cooker then ceases broadcasting its SSID, and the phone is re-connected to its host wireless network. The SSID is not broadcast again, however a user may enter their login information on any device with the Black + Decker app installed, and have the device configured to interact with the cooker, including virtual devices such as created with desktop Android emulators.

During testing, several key variables were observed. Any device may connect to the slow cooker using the broadcast SSID and default password as shown in Appendix C, there is an exchange of data between the devices as verified by using a packet sniffing program, such as Wireshark (Appendix E, Appendix F). With the proper decryption program, available as part of the Kali Linux program, the exchanged packets may be deciphered. Such a method may provide the means to access the filesystem, or gain root access, to the slow cooker and modify its source code or upload malware. Another observable interaction occurs between the slow cooker and the user's smartphone as it syncs via the app.

Utilizing a Man in the Middle technique, a malicious user may eavesdrop on the exchange of data, and capture the exchange of network credentials (Appendix E). Again, using a decryption program, it is possible to decipher the data. However, to Black + Decker's credit, the information exchanged between the smart device and the slow cooker is encrypted, with only the name of the phone and its type of operating system remaining in plaintext. However, there is no observable limit to the number of devices which may connect to the slow cooker, nor is there any authentication which occurs between the app and the device beyond the initial setup.

Another method of attack utilizes the Evil Twin method, in which a malicious user creates a digital clone of the slow cooker's access point. Utilizing standard tools within the Kali Linux distribution,

malicious parties can duplicate the exact MAC address, IP address, and SSID of any access point, and then boost the signal strength of the cloned device, intercepting any connection attempts and forcing users to connect to the digital clone. Once connected, the attacker may opt to present the with a sign in page offering them choices to use their social media profiles to login, thus creating the possibility of stealing the sensitive private information of any user. Advanced methods allow Internet access via a second network interface card, ethernet port, or peripherally connected network device. Fake landing pages may be customized, tricking victims into thinking they are visiting the setup page for the slow cooker, and then tracing them as they visit various other websites, allowing the hacker to collect all session information. It is also possible, though difficult, to seize control of the user's phone, or access sensitive files stored within. Appendix D demonstrates the ease of obtaining the necessary configuration information by connected directly to the slow cooker.

Testing Conclusions

The Black + Decker WiFi-Enabled 6-Quart Slow Cooker displays several vulnerabilities common to IoT devices, which place consumer information at risk, and one unsuspected vulnerability which places Black + Decker at risk. Using established methods and freely available tools, hackers can intercept and decrypt the network communication traffic between the slow cooker and any device with which it shares a connection. It is also possible for hackers to access any device connected to the slow cooker, or, because of the existence of a hardcoded password, seize control of the slow cooker or connected devices, modify system files, and upload malware such as Mirai. Using advanced methods, hackers using a botnet may create a unique form of a DDoS attack by using automated scripts to create multiple fake accounts, which trigger response emails from Black + Decker, and have the potential of overwhelming the user database. It is not a matter of if, but a matter of when an attacker finds these means convenient for their purposes. These vulnerabilities reinforce the common notion that IoT devices, in general, are not secure.

Disclosure of Results

Due to the unexpected vulnerability related to account creation, the author of this paper conferred with two established information security professionals who confirmed the plausibility of the findings (though they wish to remain anonymous). The entity responsible for distributing the Black + Decker slow cooker, Spectrum Brands was contacted via telephone on May 10, 2017, a representative of the company transferred the call to the executive responsible for the product, however the call was forwarded to voicemail. A second attempt to contact Spectrum occurred on May 13, 2017 via the company's support page. Unfortunately, there has been no further action and no contact from any representative of Spectrum Brands. The author will continue to follow ethical disclosure guidelines for all discovered vulnerabilities, set forth by industry standards [24], in the interest of providing reasonable safe information security assurance for consumers and for the affected business.

Remediation, Patching, and Verification

Account creation notwithstanding, the discovered vulnerabilities of the Black + Decker Wi-Fi slow cooker are expected. In fact, these vulnerabilities are among the Top IoT Vulnerabilities as defined by The Open Web Application Security Project (OWASP). While there is no insight regarding the development process for the device, nor the security mindset of either Black + Decker or Midea Group, it is plain to see that rigorous testing of privacy and security issues played no part.

The most concerning issue for Black + Decker/Spectrum Brands, is the possibility of disruption of its network operations through the insecure smartphone app. While the size of storage devices poses a barrier to crippling the user database, increasing numbers of fake accounts prompting email notifications creates a situation in which Spectrum Brands would be conducting a DDoS attack on itself. The steadily increasing stream of user account registration emails to fake accounts will create bounceback notifications and prompt the server to continue delivery attempts for a period defined by the mail application, potentially several days. The only way to immediately address this issue is to cease automatic emails for account registration. While this immediate action will prevent exploitation of the account registration vulnerability, further patching is required to prevent it or other vulnerabilities from affecting the company and users of the device.

For patching, multiple variables are at play which must be considered. Among them are the number of users allowed to create accounts from a single IP address or MAC address, as well as the amount of time separating accounts. An overhaul of the smartphone application is necessary, addressing the weak password creation policy, and restricting email address input to include only Top-Level Domains, such as addresses ending in .com, .us, .ca, .net and many others. However, a Top-Level Domain restriction will only decrease the number of possible fake account creations, so additional verification and authentication via an email notification link is necessary as well. These measures, a

strong password policy, restriction of email address input, and account verification will provide adequate security protection to consumers, as well as address issues affecting the companies in question.

Just as necessary will be an overhaul of the slow cooker's (or any similar device facing similar issues) firmware. This overhaul will address the hardcoded firmware password, as well as changing the visibility of the SSID from publicly viewable to hidden. Additional measures, such as adding some form of tamper resistance to the electronic components, may be necessary as well to prevent physical modification of a device.

The development of future IoT devices necessitates examination of the testing and verification process. As evidenced with the slow cooker, the company whose name is on the device is not necessarily the original developer; however, they should prioritize a robust testing method and require examination of all methods, tools, protocols and results before market release. Since the overhaul of both the smartphone app and the device constitute a new development process, it should expand to include security variables and then subjected to formal verification and physical testing to determine if the device meets security requirements. Additionally, random sampling of subsequent manufactured devices is necessary. This random sampling will provide quality and risk assurance, ensuring there is no modification to the manufacturing process or interference by a malicious third party.

Liabilities and Consequences

For manufacturers of IoT devices there are little to no consequences associated with security vulnerabilities. As evident with the Black + Decker slow cooker, the party distributing or selling the device may not be the original developer. Third party developers from nations other than target markets develop many of the consumer electronic (and many non-electronic) goods available globally, while the domestic companies engage in the practice of rebranding devices, essentially selling a product as its own when it was developed by a third party, with the permission of the developing company. Such as practice is common throughout the world, and as a result liability presents a difficult problem.

While the distributors and resellers of IoT devices face little liability, consumers and affected businesses face the risk. Exploits through common IoT vulnerabilities may steal private information, or allow access to a target network. While not the specific goal of a hacker, the IoT device may provide the means to reaching a goal, as it provides a stepping stone into the host network via an unprotected avenue of communication. This allows a hacker to work his or her way through a list of network devices, hopping from one to another until either the target device is located, or access credentials located which provide a means to accessing other devices. However other attacks do target the IoT device, effectively turning it into a slave of a distributed network of devices, which then search for and infect other devices. The goal of these attacks varies from launching DDoS attacks, spreading malware or email spam, to mining cryptocurrency such as Bitcoin. Users of these devices become unknowing accomplices, or themselves fall victim in the form of data overage charges from their Internet Service Providers. Thus, any IoT device introduced to a corporate network must meet rigorous testing and verification guidelines, to avoid potential exfiltration of company confidential information, while consumers should consider the inherit risk associated with an IoT device, and decide if it is worth the tradeoff for convenience. Without an effective means of holding developers and rebranding distributors liable for

releasing poorly secured devices to consumers, these risks will continue to rise; as well as the frequency, innovation, and scope of attacks.

Necessary steps included enforcement by government bodies of rigorous testing methods, certifications, and notifications to consumers. New Jersey State Law S-2582, signed by Governor Chris Christie on May 12, 2017 requires all Internet connected baby monitors sold in the state to include security features to prevent malicious hacking, and warnings to consumers of risks associated from using an unsecured device [25]. Companies selling baby monitors which do not meet these requirements will incur penalties up to $10000.00 for a first offense, and up to $20000.00 for subsequent offenses. This law represents the first step in government regulation of IoT security. By leveraging fines and other legal or civil penalties against companies selling or developing devices with security flaws, particularly common security flaws, governments or regulating bodies will force developers to comply with the same standards as other technologies, bringing a common level of assurance across the spectrum of electronic and computerized devices. While this will most likely create an increase in price, it will also result in an increase in peace of mind, and in the quality of goods purchased.

Conclusion

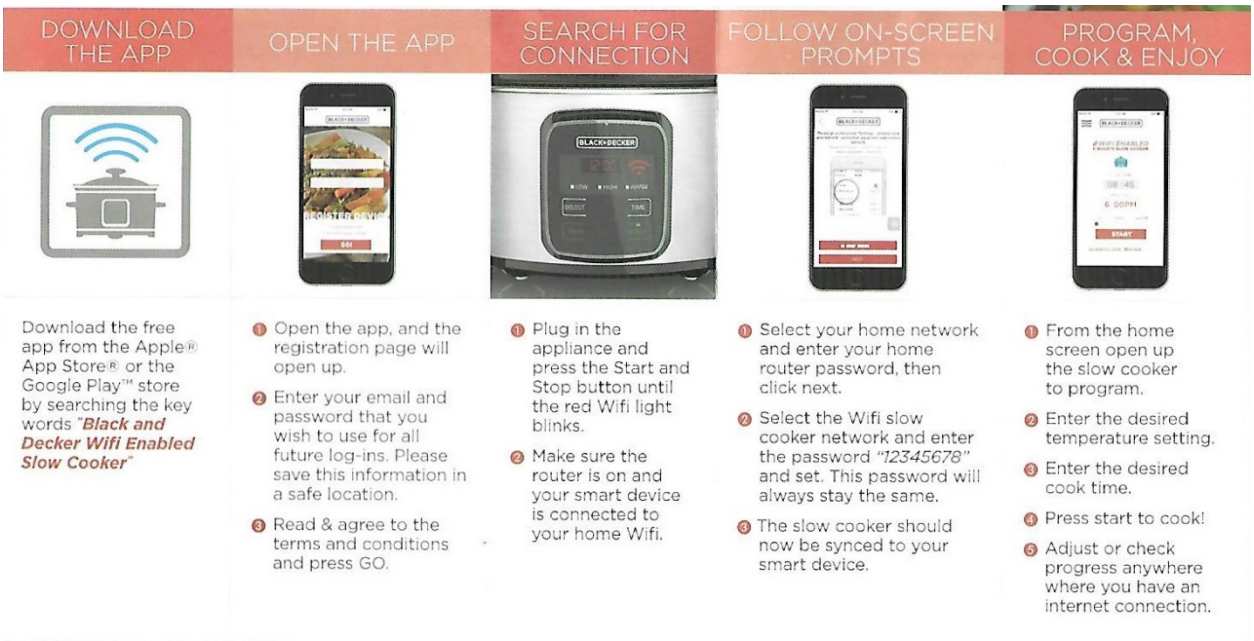
IoT devices are ubiquitous, and poised for increasing market growth [9], [14]. Society's fascination with technology, the perceived status associated with IoT devices, the conveniences offered, as well as decreased development costs and innovation in computerized technologies, all combine to create a perfect storm for market demand. However, this increased demand and the ease of which devices may be incorporated into the Internet creates issues with security.

This project has demonstrated through practical testing of a commercially available product, that any IoT device may possess one or more common security flaws, and may possess other flaws with far-reaching implication. Because of the lack of regulations, enforcement, and the immaturity of the development process for the Internet of Things, it is reasonable to assume that any device is vulnerable to exploitation by a malicious third party. It has demonstrated, through examination of previous Internet attacks using IoT as a platform, the potential risk to consumers, businesses, and to any person on the Internet regardless of ownership of any IoT device. These risks range from loss of private information, loss of financial information, loss of company confidential information, denial of service or convenience, monetary losses associated with high data use, or from any liabilities incurred which resulted from an IoT attack.

This project has contributed to the information security industry's body of knowledge by discovering previously undisclosed vulnerabilities present in the tested device. Through ethical disclosure methods, consumers now have adequate information required for informed purchases and personal data security, while the responsible company is provided adequate time to respond to, address, remediate, or patch security vulnerabilities. However, this one device represents a small portion of the total number of devices, each with inherit risks, available on the open market.

Appendix

A. Scanned Image of Black + Decker Quick Setup Guide.



DOWNLOAD THE APP	OPEN THE APP	SEARCH FOR CONNECTION	FOLLOW ON-SCREEN PROMPTS	PROGRAM, COOK & ENJOY
Download the free app from the Apple® App Store® or the Google Play™ store by searching the key words ***"Black and Decker Wifi Enabled Slow Cooker"***	❶ Open the app, and the registration page will open up. ❷ Enter your email and password that you wish to use for all future log-ins. Please save this information in a safe location. ❸ Read & agree to the terms and conditions and press GO.	❶ Plug in the appliance and press the Start and Stop button until the red Wifi light blinks. ❷ Make sure the router is on and your smart device is connected to your home Wifi.	❶ Select your home network and enter your home router password, then click next. ❷ Select the Wifi slow cooker network and enter the password *"12345678"* and set. This password will always stay the same. ❸ The slow cooker should now be synced to your smart device.	❶ From the home screen open up the slow cooker to program. ❷ Enter the desired temperature setting. ❸ Enter the desired cook time. ❹ Press start to cook! ❺ Adjust or check progress anywhere where you have an internet connection.

B. Verification of account creation email.

LEWIS UNIVERSITY

givens, richard <richardpgivens@lewisu.edu>

Wifi Enabled Slow Cooker Registration
1 message

support@spbcustomersupport.com <support@spbcustomersupport.com> Sat, Apr 22, 2017 at 5:24 PM
To: richardpgivens@lewisu.edu

Hello,

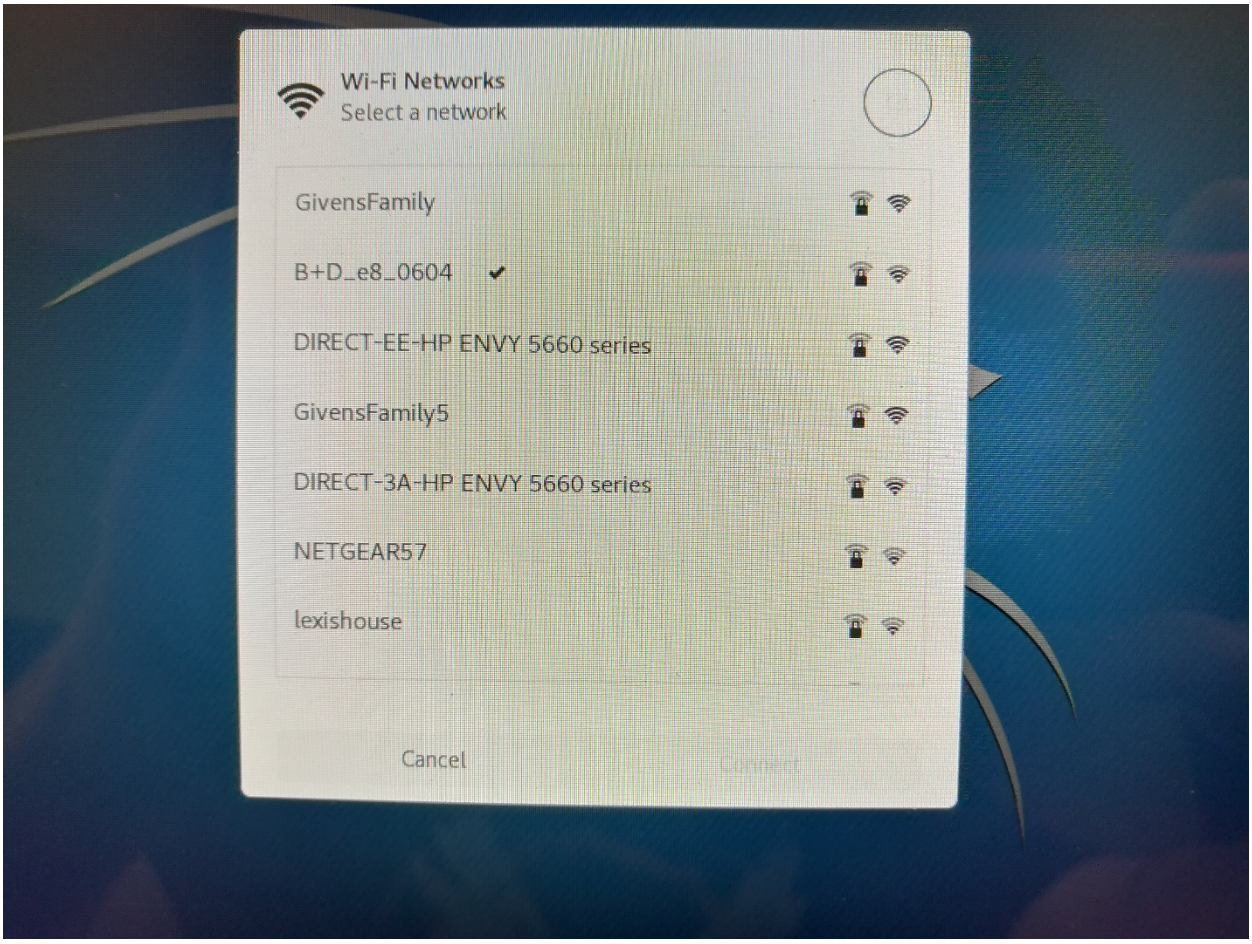
Congratulations on your Black+Decker Wi-Fi Slow Cooker purchase! You recently used this email account to register for a Black+Decker Wi-Fi Slow Cooker account.

This a system generated email, please do not reply. If you did not use this account to register or if you have any additional comments, questions or concerns, please contact Black+Decker customer support at the following:

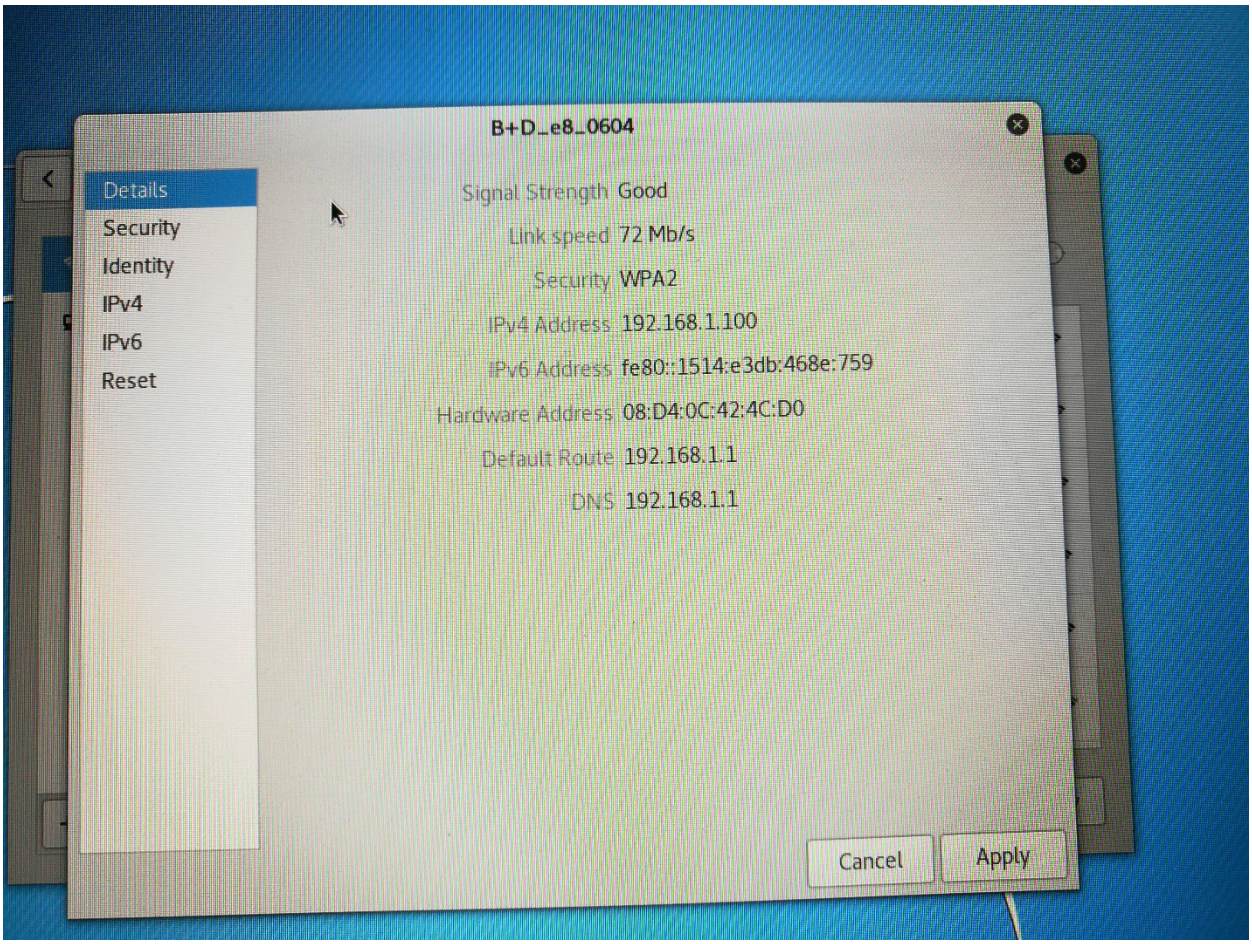
Phone: (800) 231-9785 (Monday-Friday, 8:30 a.m.- 7:00 p.m.)

Email: homeappliancesupport@spectrumbrands.com

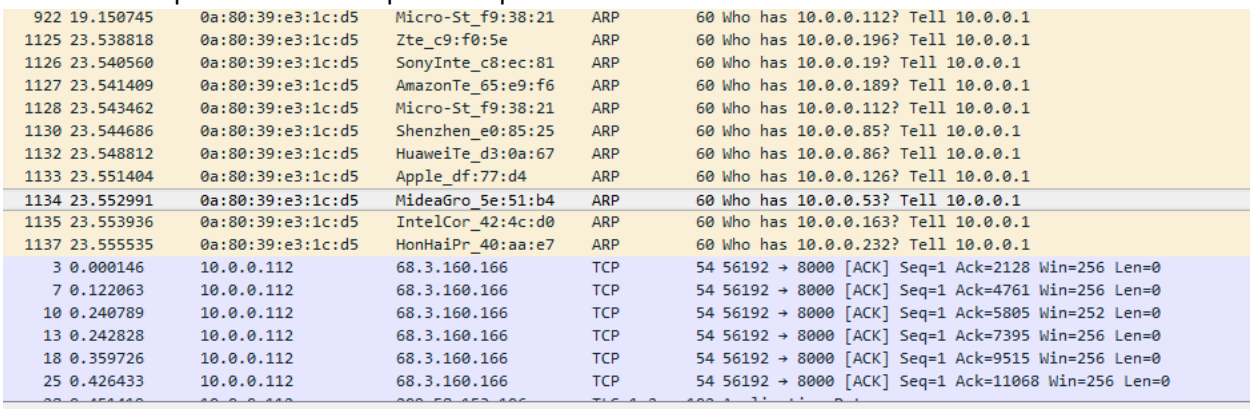
C. Desktop screenshot of Kali testing platform connected to the Black + Decker WiFi-Enabled 6-Quart Slow Cooker.



D. Desktop screenshot of the Kali showing the network details of the Black + Decker WiFi-Enabled 6-Quart Slow Cooker.

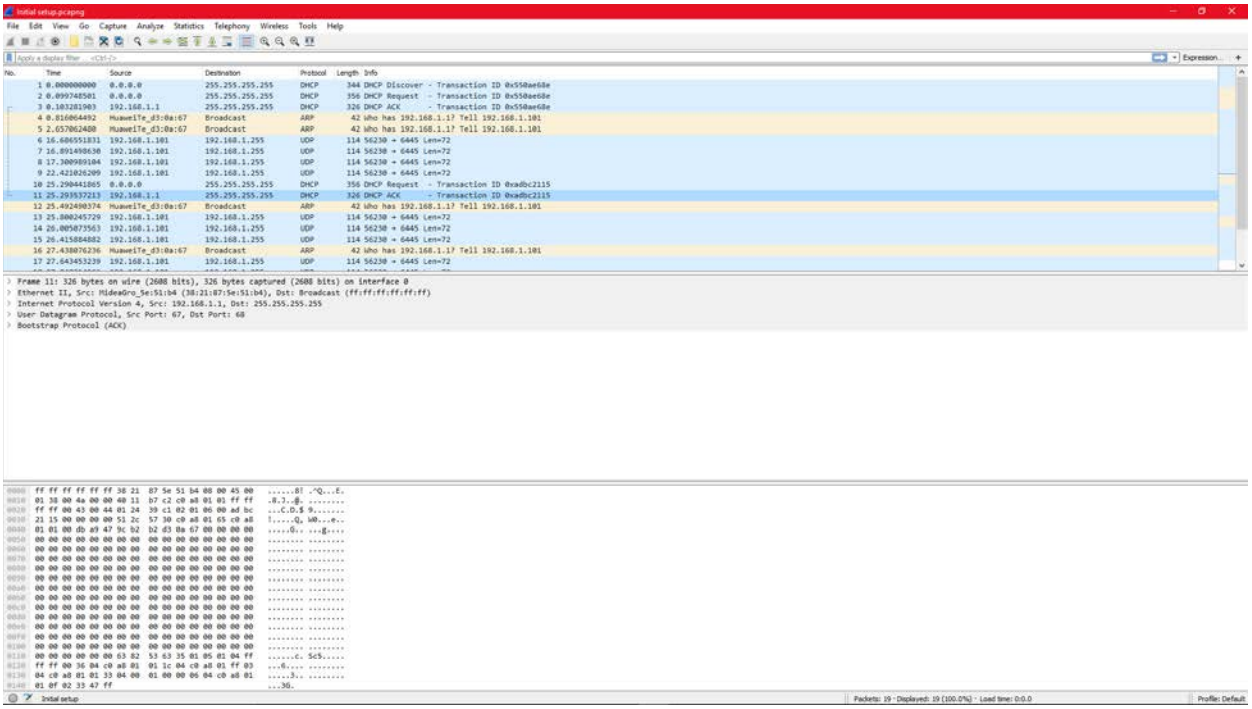


E. Screenshot of partial Wireshark packet capture on a Windows PC



922	19.150745	0a:80:39:e3:1c:d5	Micro-St_f9:38:21	ARP	60	Who has 10.0.0.112? Tell 10.0.0.1
1125	23.538818	0a:80:39:e3:1c:d5	Zte_c9:f0:5e	ARP	60	Who has 10.0.0.196? Tell 10.0.0.1
1126	23.540560	0a:80:39:e3:1c:d5	SonyInte_c8:ec:81	ARP	60	Who has 10.0.0.19? Tell 10.0.0.1
1127	23.541409	0a:80:39:e3:1c:d5	AmazonTe_65:e9:f6	ARP	60	Who has 10.0.0.189? Tell 10.0.0.1
1128	23.543462	0a:80:39:e3:1c:d5	Micro-St_f9:38:21	ARP	60	Who has 10.0.0.112? Tell 10.0.0.1
1130	23.544686	0a:80:39:e3:1c:d5	Shenzhen_e0:85:25	ARP	60	Who has 10.0.0.85? Tell 10.0.0.1
1132	23.548812	0a:80:39:e3:1c:d5	HuaweiTe_d3:0a:67	ARP	60	Who has 10.0.0.86? Tell 10.0.0.1
1133	23.551404	0a:80:39:e3:1c:d5	Apple_df:77:d4	ARP	60	Who has 10.0.0.126? Tell 10.0.0.1
1134	23.552991	0a:80:39:e3:1c:d5	MideaGro_5e:51:b4	ARP	60	Who has 10.0.0.53? Tell 10.0.0.1
1135	23.553936	0a:80:39:e3:1c:d5	IntelCor_42:4c:d0	ARP	60	Who has 10.0.0.163? Tell 10.0.0.1
1137	23.555535	0a:80:39:e3:1c:d5	HonHaiPr_40:aa:e7	ARP	60	Who has 10.0.0.232? Tell 10.0.0.1
3	0.000146	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=2128 Win=256 Len=0
7	0.122063	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=4761 Win=256 Len=0
10	0.240789	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=5805 Win=252 Len=0
13	0.242828	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=7395 Win=256 Len=0
18	0.359726	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=9515 Win=256 Len=0
25	0.426433	10.0.0.112	68.3.160.166	TCP	54	56192 → 8000 [ACK] Seq=1 Ack=11068 Win=256 Len=0

F. Screenshot of full Wireshark interface during device setup



Works Cited

[1] “English Oxford Living Dictionaries.” English Oxford Living Dictionaries, en.oxforddictionaries.com/definition/Internet_of_things. Accessed 7 Apr. 2017.

[2] Bekermin, Dima. “New Mirai Variant Launches 54 Hour DDoS Attack against US College.” Incapsula.com, Imperva Incapsula, 30 Mar. 2017, www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html. Accessed 9 Apr. 2017.

[3] Regel, Jens. “Full Disclosure: [CVE-2017-7240] Miele Professional PG 8528 - Web Server Directory Traversal.” Full Disclosure: [CVE-2017- 7240] Miele Professional PG 8528 - Web Server Directory Traversal, 24 Mar. 2017, www.seclists.org/fulldisclosure/2017/Mar/63. Accessed 9 Apr. 2017.

[4] “PG 8528.” PG 8528 Washer-Disinfector - Large Capacity Washer- Disinfectors, www.miele.co.uk/professional/large-capacity-washer-disinfectors-560.htm?mat=10339600&name=PG_8528#item-2-2. Accessed 9 Apr. 2017.

[5] York, Kyle. “Dyn Statement on 10/21/2016 DDoS Attack | Dyn Blog.” Dyn Statement on 10212016 DDoS Attack Comments, 22 Oct. 2016, dyn.com/blog/dyn-statement-on-10212016-ddos-attack/. Accessed 9Apr. 2017.

[6] Crook, Jordan. “Samsung's LCD Fridge With Apps Is A Fridge That Has An LCD And Apps.” TechCrunch, TechCrunch, 21 June 2011, techcrunch.com/2011/06/21/samsungs-lcd-fridge-with-apps-is-a-fridge- that-has-an-lcd-and-apps/. Accessed 9 Apr. 2017.

[7] “FCC Documentation.” *FCC Documentation*, apps.fcc.gov/eas/GetApplicationAttachment.html?id=3115790.

[8] “FCC ID TAPMD-TC6006W Slow Cooker by Guangdong MD Consumer Electric Manufacturing Co., Ltd.” *FCCID.io*, fccid.io/TAPMD-TC6006W. Accessed 13 May 2017.

[9] “Global Internet of Things Market Size 2009-2019 | Statistic.” *Statista*, www.statista.com/statistics/485136/global-internet-of-things-market-size/. Accessed 13 May 2017.

[10] Hanlon, Mike. “LG Internet Refrigerator.” *New Atlas - New Technology & Science News*, New Atlas, 4 June 2004, newatlas.com/go/1132/. Accessed 13 May 2017.

[11] Harrison, Linda. “Fridges to Be Hit by Net Viruses.” *The Register*, 21 June 2000, www.theregister.co.uk/2000/06/21/fridges_to_be_hit_by/. Accessed 13 May 2017.

[12] Harvey, Brian. “What Is a Hacker.” *What Is a Hacker?*, University of Berkeley, California, people.eecs.berkeley.edu/~bh/hacker.html. Accessed 13 May 2017.

[13] “Internet of Things (IoT) History.” *History of IoT | Background Information and Timeline of the Trending Topic*, www.postscapes.com/internet-of-things-history/. Accessed 13 May 2017.

[14] “IoT Devices Installed Base Worldwide 2015-2025 | Statistic.” *Statista*, www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 13 May 2017.

[15] “Krebs on Security.” *Brian Krebs*, krebsonsecurity.com/tag/mirai-botnet/. Accessed 13 May 2017.

[16] “LG Electronics Introduces Digital Refrigerator.” *Appliance Design Magazine RSS*, www.appliancedesign.com/articles/89516-lg-electronics-introduces-digital-refrigerator. Accessed 13 May 2017.

[17] “Nmap.” *Nmap: the Network Mapper - Free Security Scanner*, nmap.org/. Accessed 13 May 2017.

[18] “Norton - Antivirus Software and Spyware Removal.” *Norton - Antivirus Software and Spyware Removal*, us.norton.com/botnet/. Accessed 13 May 2017.

[19] “Our Most Advanced Penetration Testing Distribution, Ever.” *Kali Linux*, Offensive Security, www.kali.org/. Accessed 13 May 2017.

[20] “WiFi-Enabled 6-Quart Slow Cooker.” *WiFi-Enabled 6-Quart Slow Cooker | BLACK + DECKER*, Black + Decker, www.blackanddeckerappliances.com/products/cooking-appliances/slow-cookers/SCW3000S-Wifi-Enabled-6-Quart-Slow-Cooker-Silver.aspx. Accessed 13 May 2017.

[21] “Wireshark · Go Deep.” *Wireshark · Go Deep.*, www.wireshark.org/. Accessed 13 May 2017.

[22] Dieterle, Daniel W. *Basic Security Testing with Kali Linux 2: Test Your Computer System Security by Using the Same Tactics That an Attacker Would Use*. Place of Publication Not Identified, CreateSpace Independent Publishing Platform, 2016.

[23] “OWASP Internet of Things Project.” *OWASP Internet of Things Project - OWASP*, www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas . Accessed 14 May 2017.

[24] Trull, Jonathan. “Responsible Disclosure: Cyber Security Ethics.” CSO Online, 26 Feb. 2015, www.csoonline.com/article/2889357/security0/responsible-disclosure-cyber-security-ethics.html. Accessed 14 May 2017.

[25] Lowe, Claire. “New State Law Requires Safeguards against Hacking for Baby Monitors.” Press of Atlantic City, 12 May 2017, www.pressofatlanticcity.com/business/new-state-law-requires-safeguards-against-hacking-for-baby-monitors/article_7067ab70-c9dc-5e87-9db3-499cf1f93b79.html. Accessed 14 May 2017.

[26] “Security Tip (ST04-015).” *Understanding Denial-of-Service Attacks | US-CERT*, www.us-cert.gov/ncas/tips/ST04-015. Accessed 14 May 2017.