Security and the Internet of Things

**An Examination of Common Vulnerabilities Present in Network Attached Consumer Devices and Guidelines to Protect the Consumer**

by: Richard Givens, CPSC 69700

Master’s Thesis for Master of Science in Computer Science

Instructor: Khaled Alzoubi, PhD

Lewis University, College of Arts and Sciences, Summer, 2019

Acknowledgements

Without the help of several persons within the Information Security Community, research into this topic would meet with very little success. The author thanks the following people (either by name, name and handle, or handle where name is unknown):

**Family** particularly the author’s wife and children for persevering throughout several years of false starts and study and for standing by the author during the challenges that life brings.

**Ben Actis (Ben-Ra)** for agreeing to examine the author’s project for any possible duplication of his previous work on an earlier generation Instant Pot Bluetooth device, and for sharing the resources, tools, and methods used in that project.

**Brenden Finnegan(LordBeer)** for his continuing assistance in this and various other security research projects as a friend and partner in learning.

**Dr. Khaled Alzoubi** for expert guidance and advice, creating an environment that allows the creative freedom to explore topics of scientific interest.

**Dr. Ray Klump** for providing continuing guidance, advice, and opportunities to all students, and to the author on more than one occasion.

**Johnny Xmas** for being the first security researcher and member of the security community to answer certain questions and provide a level of detail to the author, when few were willing to take the time.

**Lesley Carhart (Hacks4Pancakes)** for convincing the author to return to Information Security after an initial failure several years ago, and for ongoing advice and guidance to all who are new to field.

**Marcus Perry** who, in his position as a member of the Lewis University staff assisting Veterans, showed extreme patience with the author many times over.

**Mark Carney (LargeCardinal)** for sharing his Pentesting Hardware – A Practical Handbook, a work in progress which he is freely available for all to use on GitHub, and for answering specific questions regarding the use of hardware and techniques in the testing of hardware and firmware on electronic devices.

**Roman Ortega Jr.** who, in his position as a member of the Lewis University staff assisting Veterans, provided an example of character that the author strived to achieve.

**The Chicago Burbsec Community, particularly PhreakingGeek and HackrDefendr** friends who have at various times provided insight, direction, advice and assistance in many projects and efforts over the course of a few years.

There are many others within the security community who have provided insight, links, or other valuable resources and information freely when asked, often when seeing that the author directed a general question or request to a large audience via social media posts. Each one of these provided valuable insight, tools, and methods which may have proved difficult to achieve otherwise.

Table of Contents

**List of Figures**

**Chapter 1**

1.1 Introduction

1.2 Rise of the Machines

1.3 Recent Events

**Chapter 2**

2.1 Testing for Vulnerabilities in a Commercially Available Device

2.2 Review of Similar Work

2.3 Specifications

2.4 The Test Environment

2.5 Methodology

2.6 Testing and Experimentation

2.7 Results and Findings

**Chapter 3**

3.1 Understanding the Laws, Rules and Regulations Governing IoT

3.2 Recent Changes

3.3 Evaluating a Purchase

3.4 Securing the Home Environment

**Chapter 4**

4.1 Conclusions

**Bibliography**

Abstract

This paper is an examination of vulnerabilities present in network attached home devices or appliances, commonly known as the Internet of Things (IoT) [2]. Various methods of attack are examined, along with demonstrations of specific attacks and vulnerabilities present in one or more devices. The Instant Pot WiFi 6 Quart Pressure Cooker [6,7], a household appliance available for purchase both online and in brick and mortar stores throughout North America and the United Kingdom is examined in depth. Finally, this paper will provide guidelines to consumers acquiring these devices, forming the base for informed purchasing guidelines and personal data/privacy protection to a segment of the population which may be neglected or uninformed.

Though these devices contain vulnerabilities common to many IoT devices, there is a possibility of previously undisclosed or unpublished vulnerabilities affecting either the manufacturer, or consumers. The author will follow industry standard responsible disclosure guidelines.

Several third parties have offered suggestions or mentioned casually how the device tested in this paper may be utilized as a physical weapon; these methods are not discussed out of an overabundance of caution, safety, and a moral obligation to prevent such knowledge from public discourse. The author strongly discourages such activity outside of a controlled environment with proper procedures, safeguards, and licensing, conducted only by professionals of appropriate authority and backgrounds.

Introduction

IoT refers to a collection of devices capable of communication via wireless or physical adapters, connecting them directly to the network of homes and businesses. This allows for near instantaneous communications between the device, command and control servers, users, administrators, mobile applications and web-based dashboards. Early IoT devices consisted of large appliances, such as refrigerators. In 2000, LG launched the Internet Digital DIOS Refrigerator for $15,000.00. The DIOS contained a modem, Ethernet port, LCD touchscreen, a camera, microphone, speakers, and external DVD ports and was as much of a computer as it was a kitchen appliance [12].

Since the launch of the LG DIOS, IoT has expanded to include many other devices in household and industrial applications. In the home baby monitors, televisions, digital picture frames, radios, light bulbs, coffee makers, air conditioners and thermostats comprise but a portion of the Internet connected devices consumers allow in their homes. Rather than following Moore’s Law of increased computing power and decreased cost [16] , these new computerized devices follow a new guideline: any device a consumer interacts with does now, or will in the future, contain network technology allowing it to send or receive signals via the Internet. This creates an environment of innovation as manufacturers scramble to meet consumer demand, creating new devices and new methods of interaction across the personal and household device landscape. Being able to control the temperature of one’s home, shop for necessities, and communicate with family from the comfort of a couch which provides charging for one’s smartphone is now the pinnacle of the consumer experience.

This scramble to bring goods to market first creates an environment in which the implications to privacy and data security become secondary or even tertiary concerns, resulting in negative impact to the personal data and privacy of consumers in an age where these issues are among the foremost in their minds.

The following section will define key terms and discuss several events involving IoT security which impact consumers. Next, this paper discusses the existence of one or more vulnerabilities, common or unreported, which exist in a commercially available IoT device, and exploited using commonly available or free tools. The device specifications, test equipment, methodology and software tools used in testing are also discussed.

In the final section, the paper develops security guidelines for consumers when purchasing an IoT device. These guidelines will borrow heavily from the best practices of businesses and recommendations by governing authorities, presenting them in a concise manner which assumes nothing regarding the technical expertise, training, experience or education of the reader. Following this information, a consumer should have the necessary facts, information, and guidelines enabling an evaluation of the need, risk, and benefit of purchasing IoT devices, thus allowing for an informed purchasing decision.

Relevant Terms and Definitions

Factors contributing, at least in part, to the frustration and confusion of consumers regarding IoT security, indeed all security concerning information systems, data, and privacy, are the numerous technical terms and abbreviations which makes sense to those familiar with computing but seldom used outside these specific cases. This section attempts to define common terms used within the practice of information security in a concise manner, easily understood by readers of all technical or non-technical backgrounds. These definitions are not exhaustive; however, these terms will appear in several places throughout this publication, thus defining them in the beginning is both necessary and valuable to the reader. Other unique terms will occur once, defined at that time.

**Access Point(AP):** Also known as a **Wireless Access Point (WAP)**; this is an electronic device physically connected to a network router, switch or hub and projects a WiFi signal to a designated area [23]. Examples of Access Points include devices found in many businesses which advertise free WiFi for customers.

**Botnet:** A botnet is a network of computers operating in parallel, pooling resources to achieve predetermined goals. The common definition for a botnet is a collection of Internet connected devices which have been compromised by a malicious third party and utilized to launch attacks, such as in the case of the Mirai Botnet [10]. Though botnets with mundane purposes exist, consumers will most likely encounter those exhibiting malicious behavior.

**Denial of Service (DOS):** “A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor,” [4,15 ]. Common methods involve flooding a target computer or server with connection requests or responses to fake connection requests, overwhelming the target machine until it is eventually unable to initiate or respond to any subsequent request. A form of DoS attack, the **Distributed Denial of Service Attacks (DDoS)**, involves multiple computers simultaneously initiating attacks against a single target or a small group of targets. DDoS attacks require a level of coordination which is present in botnets.

**Evil Twin:** An Evil Twin is an Access Point created by a malicious third party which mimics a legitimate Access Point in general appearance, network name, channel, and electronic address, also known as the **Media Access Control (MAC) address**.An Evil Twin is designed to lure unsuspecting users to connect to it, thinking it is a legitimate AP, and then either harvest credentials such as usernames and passwords, or as platform from which the attacker launches other attacks. Some Evil Twins may present an account sign on page, requesting social media account credentials. It is possible that a user will never detect this attack, as the Evil Twin AP could pass legitimate traffic to the Internet once it has completed its task (while still monitoring traffic from the user and collecting as much as possible); in other cases, the Evil Twin will drop all traffic from the user and seemingly disconnect after completing its initial task. [24].

**Firmware:** Firmware is the operating system of an electronic device, permanently programmed into Read Only Memory (ROM). In most cases, the only access of firmware allowed to users is the ability to update it by a means called flashing. Examples of firmware include the operating systems of most mobile devices, printers, routers, and integrated electronic components of computers and computer peripherals.

**Man in the Middle (MITM):** Man in the middle attacks involve a third party inserting custom traffic in, or eavesdropping on network traffic between one or more devices, such as computer and a router or access point [22]. MITM attacks may be either active or passive. In an active MITM attack, the malicious third party engages in sending or altering traffic, while in the passive attack, the malicious third party observes and records traffic. The traffic observed is either encrypted, meaning that it is not readable by an outside party, or “in the clear”, which is plaintext characters easily decipherable.

**Patch:** A patch is a software or firmware modification which occurs post production to remediate an issue which was undetected or unresolved during the development and testing phases of the product or service, or to provide enhanced reliability, performance, or compatibility in the wake of a technological improvement or innovation. At times, a patch may include several modifications which both provide remediation and enhancement. **Patching** is the term associated with applying a patch and may occur at any time post production. Though the purpose of a patch is to improve a product, or remediate some unaddressed issue, it may at times introduce other flaws, particularly if the patch is developed hastily.

Rise of the Machines

In 1966, German Computer Scientist Karl Steinbuch is reported as saying “In a few decades time, computers will be interwoven into almost every industrial product,” [18]. This prediction has indeed come true, as computers or computing devices form the backbone of nearly every modern convenience, product, or service. The pace of innovation in computing is such that computers and computing devices have moved from the realm of enterprise business and government research to mainstream use by home users, small businesses, and classes in only 73 years. The ENIAC computer came into service in 1946 [5], after the end of World War Two; though an ever-decreasing number, there are still Veterans alive who fought in the battles of World War Two, and civilians who lived through those times. The entire existence of modern computers, from vacuum tubes to Quantum Computing is measured in less than a human lifetime. This rapid pace of development and deployment creates a unique set of problems in which the products sold to consumers are released before society and the legal system has time to catch up. While government regulation has largely kept pace with industrial standards since at least the turn of the 20th Century, regulators generally possess a great deal of uncertainty about the newest innovations in computing, creating a loop of inaction which stifles further creativity and adoption [5].

Of interest is the Internet of Things (IoT) and so called “smart homes” in which numerous Internet connected devices, many of them mundane household appliances, occupy space in the home’s network connected infrastructure, exchange

data, and communicate both within the local network and over areas of geographical distance via web and mobile applications. Many of these devices are “always on”, or constantly providing updates and communicating with various end points, whether a server or the homeowner’s phone. As stated by the National Institutes of Health through the National Center for Biotechnology Information: “Application of the IoT model to smart homes, by connecting objects to the Internet, poses new security and privacy challenges in terms of the confidentiality, authenticity, and integrity of the data sensed, collected, and exchanged by the IoT objects. These challenges make smart homes extremely vulnerable to different types of security attacks, resulting in IoT-based smart homes being insecure. Therefore, it is necessary to identify the possible security risks to develop a complete picture of the security status of smart homes,”[1].

Recent Events

Though a relatively young technology, IoT attacks continue to increase at an alarming rate. One contributing factor is the increase of adoption by consumers; the number of installed IoT devices is expected to increase five hundred percent from 2015 levels, reaching an estimated seventy-five billion devices [8]. Recent advances in communication technology, namely 5G wireless networks, may alter this prediction, resulting in an increase above forecasts. The rate and number of attacks affecting IoT devices will rise in direct proportion to the rate of adoption and deployment of these devices. All attacks follow the path of least resistance; a malicious third party will stop searching for a method to obtain their goal once they have identified the first available means matching their criteria.

In 2007, doctors treating former Vice President Dick Cheney disabled the WiFi connectivity of his implanted pacemaker amid fears that a malicious third party could access and gain control of the device, causing it to administer shocks or shutdown completely [ ]. Though there were several other implantable medical device vulnerabilities disclosed in the preceding and following years, in 2017 nearly half a million pacemakers manufactured by Abbott were the subject of a recall by the FDA amid demonstration that an attacker could use commercially available equipment to intercept wireless signals from pacemakers, and issue malicious commands causing serious injury or death [20 ].

In 2017 Burger King released a commercial that, as a marketing stunt, utilized keywords which activated Google Home devices in the homes of consumers, prompting the device to describe one of Burger King’s menu items [14]. Google responded by altering the Google Home devices in some manner, which prevented them from responding to the commercials. While not explicitly malicious, this action by Burger King is viewed by many as an unethical violation of privacy.

In 2018, a software update to the Tesla line of automobiles caused some models to experience performance issues and loss of power [11]. This software was delivered wireless to the Tesla automobiles, as part of an update to the Linux operating system powering all Tesla models [21]. As Linux is an open source operating system, one may expect to see other vulnerabilities surface, such as the March 2019 exploit which caused a Tesla vehicle on autopilot to switch lanes into oncoming traffic [9].

In 2016, security researchers found a flaw in the Android app controlling IoT devices manufactured by Belkin, which allowed anyone on the same network as the device gain access to the user’s cellphone to copy files and track the phone’s location [17 ]. Additional research revealed a flaw enabling control of the IoT devices by a third party. Belkin has since patched these flaws, but until their discovery, they affected a wide range of devices, all managed under the same Android app.

It is unclear if these vulnerabilities ever reached the point of exploitation by malicious third parties. However, other vulnerabilities in commercial, medical, and industrial IoT devices exist while remaining unidentified. Both the pace of innovation and feasible scope of security research make it impossible to disclose all, if many, of the risks associated with these devices. Further research and a concerted effort of cooperation between the manufacturers of these devices and the researchers examining them, in tandem with robust product development and testing procedures can address some of the concerns, however.

Testing Vulnerabilities in a Commercially Available Device

Review of Similar Work

The Test Environment

Methodology

Testing and Experimentation

Results and Findings

Understanding the Laws, Rules, and Regulations Governing IoT

Recent Changes

Evaluating a Purchase

Securing the Home Environment

Conclusions

Bibliography

[1] Ali, Bako, and Ali Ismail Awad. “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes.” US National Laboratory of Medicine and National Institutes of Health, MDPI, 8 Mar. 2018, www.ncbi.nlm.nih.gov/pubmed/29518023. Accessed May 19, 2019.

[2] “English Oxford Living Dictionaries.” English Oxford Living Dictionaries, en.oxforddictionaries.com/definition/Internet\_of\_things. Accessed 4 Jun. 2019.

[3] Franceschi-Bicchierai, Lorenzo. “How Hackers Could Steal Your Cellphone Pictures From Your IoT Crock-Pot.” Vice, VICE, 2 Nov. 2016, www.vice.com/en\_us/article/wnx7n9/how-hackers-could-steal-your-cellphone-pictures-from-your-iot-crock-pot. Accessed 4 Jun. 2019.

[4] Fruhlinger, Josh. “The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet.” CSO Online, CSO, 9 Mar. 2018, www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html. Accessed 4 Jun. 2019.

[5] History of Computers, The University of Rhode Island Department of Computer Science and Statistics, homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.htm. Accessed May 19, 2019.

[6] “Instant Pot Smart WiFi 6 Quart Multi-Use Electric Pressure, Slow, Rice Cooker, Yogurt, Cake Maker, Sauté, Steamer and Warmer, Silver.” Amazon, Amazon, www.amazon.com/Instant-Pot-Smart-Electric-Pressure/dp/B0777XQ4S8?ref\_=bl\_dp\_s\_web\_3031632011. Accessed May 19, 2019.

[7] “Instant Pot Smart Wifi.” Instant Pot, instantpot.com/portfolio-item/instant-pot-smart-wifi/. Accessed May 19, 2019.

[8] “IoT: Number of Connected Devices Worldwide 2012-2025.” Statista, www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 4 Jun. 2019.

[9] Jr., Tom Huddleston. “These Chinese Hackers Tricked Tesla's Autopilot into Suddenly Switching Lanes.” CNBC, CNBC, 3 Apr. 2019, www.cnbc.com/2019/04/03/chinese-hackers-tricked-teslas-autopilot-into-switching-lanes.html. Accessed 4 Jun. 2019.

[10] Korolov, Maria. “What Is a Botnet? And Why They Aren't Going Away Anytime Soon.” CSO Online, CSO, 27 Feb. 2019, www.csoonline.com/article/3240364/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html. Accessed 4 Jun. 2019.

[11] Kumar, Kalyan. “Tesla Model S Update Causes Performance Bug, Struggles With Limited Power.” International Business Times, 9 May 2019, www.ibtimes.com/tesla-model-s-update-causes-performance-bug-struggles-limited-power-2790824. Accessed 4 Jun. 2019.

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

[13] Mariani, Joe. “Guiding the IoT to Safety.” Deloitte Insights, www2.deloitte.com/insights/us/en/focus/internet-of-things/regulating-iot-technology-role-of-government.html. Accessed May 19, 2019.

[14] Maheshwari, Sapna. “Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google.” The New York Times, The New York Times, 12 Apr. 2017, www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html. Accessed 4 Jun. 2019.

[15] NCCIC. “Security Tip (ST04-015).” US CERT Security Tip (ST-015)O, United States Department of Homeland Security, 4 Nov. 2009, www.us-cert.gov/ncas/tips/ST04-015. Last Revision June 28, 2018. Accessed 4 Jun. 2019.

[16] “Over 50 Years of Moore's Law.” Intel, www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html. Accessed 10 Jun. 2019.

[17] Raposo, Kevin. “Hackers Have Found a Way to Hack Your IoT Crock-Pot.” KnowTechie, 2 Nov. 2016, knowtechie.com/connected-crock-pot-hotbed-hackers/. Accessed 4 Jun. 2019.

[18] Ruß-Mohl, Stephan. Die Informierte Gesellschaft Und Ihre Feinde Warum Die Digitalisierung Unsere Demokratie gefährdet. Herbert Von Halem Verlag, 2017. Accessed May 19, 2019.

[19] “Smart WiFi 60 Pairing.” Instant Pot, instantpot.com/smart-wifi-60-pairing/#tab-id-2. Accessed May 19, 2019.

[20] Vaas, Lisa. “Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking.” Naked Security, 22 Oct. 2013, nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/. Accessed 4 Jun. 2019.

[21] Vaughan-Nichols, Steven J. “Tesla Starts to Release Its Cars' Open-Source Linux Software Code.” ZDNet, ZDNet, 18 Jan. 2019, www.zdnet.com/article/tesla-starts-to-release-its-cars-open-source-linux-software-code/. Accessed 4 Jun. 2019.

[22] “What Is a Man-in-the-Middle Attack?” Official Site, us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html. Accessed 4 Jun. 2019.

[23] “What Is an Access Point and How Is It Different from a Range Extender?” Linksys, www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/. Accessed 4 Jun. 2019.

[24] “Wi-Fi Alert: The Evil Twins of Access Points.” Panda Security Mediacenter, 8 Jan. 2019, www.pandasecurity.com/mediacenter/security/wifi-evil-twins-access-points/. Accessed 4 Jun. 2019.