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, but in particular 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

Abstract

This paper is an examination of vulnerabilities present in network attached home devices or appliances, commonly known as the Internet of Things (IoT). 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, 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 these devices 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.

Since the launch of the 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, 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.

In the following section, this paper will define key terms and discuss several events involving IoT security which impact consumers, as well as discussing the specific vulnerabilities and methodologies preceding these events. 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.

Literature Review

Project Experimentation

Guidelines for Consumers

Conclusions and Summary

Bibliography