Comp116: Introduction to Computer Security

Security Vulnerabilities in Z-Wave Home Automation Protocol

Katherine Hoskins

Tufts University Department of Computer Science

Fall 2016

I. Abstract

You have purchased a brand new home security device. The package promises that the device will give you full control of your home, allowing you to do everything from control the lights to see who's knocking at the door. It communicates through your home network using some sort of communication protocol, and perhaps even lets you set a password. Installation simply requires pairing the device to the central Internet of Things hub in your home, like pairing your phone to a Bluetooth speaker. All seems right in the world.

But what if the very device that you purchased to secure you home were a portal for attackers to gain access. What if there were open source tools on GitHub that anyone allowed anyone with a computer to intercept the messages being passed between you and your device. What if there were a search engine as simple as Google that specifically found IP addresses of devices such as yours, and allowed anyone to see the video content it captured with the click of a button. What if the personal computer security risks of the mid 1990's resurfaced, but on a larger, much riskier scale. What if your security device wasn't very secure at all?

II. Introduction

The Internet of Things, also called IoT is comprised of anything, from coffee pots to heart monitors, that can be assigned an IP address and transmit data over a network without any human interaction [1]. Home automation in particular is one of the forerunners driving development, with companies large and small releasing central hub technology to run the home, and peripheral devices to control door locks, light switches, thermostats and burglar alarms. To meet the growing demand for such products, manufacturers are pressured to release newer and better features at a faster rate than ever. However, oftentimes a "better" feature does not imply

"safer", as security and risk analysis become overshadowed by the drive to produce. A Hewlett-Packard study in 2015 found that of the top 10 home security systems, only one used two factor identification to prevent unauthorized users, none required very strong passwords and some used unencrypted methods to transmit updates, including FTP, a method that is widely known to be unsafe to secure data transfer [2].

These missteps open devices to a full range of attacks. On one hand of the spectrum, search engines such as Shodan allow anyone with a laptop to query for unprotected video devices and view their data. On the more extreme end, attackers can commandeer devices, causing door locks to open or surveillance to fail. Even devices from tech giants such as Google and Apple are not 100% secure. One user explained that someone was able to unlock a front door simply by yelling from the porch for Siri to please open the door [3]. This paper will delve into the architecture and security risks of one of the most ubiquitous protocols used in home automation systems, Z-Wave, as well as offer insights as to what consumers can do to take back control of their devices to protect themselves, their homes and their families.

III. To the Community

While IoT is largely a new technology, it has quickly become a juggernaut in the financial markets, and its popularity is only going to increase. Business Insider estimates that more than $5.5 billion was spent on home security in 2016, and that by 2020 over 70% of all devices connected to the Internet will belong to the Internet of Things [4]. In addition, revenues of IoT manufacturers are expected to exceed $470 billion in the next 4 years [5]. Clearly, IoT is only expanding, but as these devices get smarter, who is responsible for ensuring their security and protecting the customers that rely on them? Consumers may be tempted to believe that

manufacturers focus on security when designing devices. However, often businesses are motivated more by profits than device security. Even if innovation is what motivates production, the lack of security courses in higher education means that the engineers designing these products are more focused on implementing new features rather than testing their security. Businesses may then claim that it is the consumers' responsibility to create strong passwords and understand how to protect themselves from attacks, however consumers are often not even aware of the risks they face when purchasing IoT devices and simply do not know any better than to put their trust in the device [6].

This disconnect is where vulnerabilities lie and attacks can ensue. On October 21, 2016, an attacker was able to exploit IoT devices that were using default passwords to launch a massive distributed denial of service attack [7]. Consumers must therefore take control of their own security, and be aware of the technologies involved in the products they bring into their homes. Such self-education requires strong resources that break down complex technology into easy to understand concepts and provide action items for consumers. This paper serves as such a resource, with the goal of breaking down the Z-Wave protocol into its core technology, exposing some of its faults and offering more secure alternatives.

IV. Security Protocols – Z-Wave Devices

For any home automation system, the central hub and the devices that it coordinates may use a number of methods to communicate. The ZigBee and Z-Wave protocols are the most widely used, and according to the Z-Wave Alliance, over 80% of home security devices use Z-Wave [8]. Both protocols are favorable for their strong penetration into building walls, and work

using radio chips embedded in each device. In addition, Wi-Fi and Bluetooth also have the disadvantage of being "power hungry," and consume too much power to be reliably used in small devices [8].

Like any protocol, Z-Wave is constructed with a series of layers, each with different functionality, that together compose the protocol stack. The Z-Wave stack begins with the application layer, which contains commands and parameters specific to the device and manufacturer. Next is the security layer, where the MAC address is stored and encryption occurs, if enabled. The network layer contains a 32-bit unique ID for the home controller and 8-bit node ID for each accessory, which is assigned when a new device is paired with the system. The fourth layer is the transport layer, where error detection and retransmission acknowledgement occurs, followed by the physical layer, where actual data is transmitted. In the United States, this transmission has frequency 908.42 MHz. The data is transferred in bit representation, using either Manchester or Non Return Zero encodings [8]. Manchester encoding uses the transitions between transmitted 1s and 0s to indicate logical bit values (a shift from 1 to 0 indicates a logical 1 for example) [9], while the Non Return to Zero method (NRZ) relies on frequency differences of + or – 20 KHz from some baseline to indicate logical bits [10].

For this transmission to occur between a device and the central controller of the home, both must share a network key that allows for communication. When a new device is paired via Z-Wave, a specific syncing protocol is executed in order to share this network key with the device. First, a "preamble" packet is sent between the receiver and transmitter, containing a specific series of bits, the home ID and node ID of the device to pair [8]. It is in this period when the protocol becomes susceptible to attack, as unencrypted identifying information is being transmitted. Though the exact specifications of the Z-Wave transmission are not documented,

researchers and attackers have been able to reverse engineer and exploit the system by examining these packets and impersonating the controller from the outside.

V. First Attacks and Responses

The syncing protocol to pair a new device via Z-Wave relies on the derivation of a network key through several calculations, which Z-Wave designers assumed would be too complex for attackers to derive without any open documentation [8]. However, as Behrang Fouladi and Sahand Ghanoun explained in their presentation at Black Hat 2013, entitled *Honey, I'm Home!! – Hacking Z-Wave Home Automation Systems*, they were able to intercept the unencrypted packets being sent between devices and the controller, and easily retrieve the home and node IDs. Using a GUI they developed themselves, they could easily dissect packets for timestamps, home IDs, sources and targets, as none of this information is encrypted. Using this information, the team was able to spoof the controller, sending raw packets to devices that appeared to come from the real controller [8]. With information from a single packet, an attacker could easily construct a network map of all the devices and then send instructions to disarm or unlock security devices throughout the home.

This attack relies greatly on the lack of encryption in the first generation of Z-Wave. Therefore, in the later generations, Z-Wave radio chips support encryption to increase security. The new chips use two different encryption methods, AES-OFB and AES-CBCMAC, and a 64-bit nonce value, a random value that can only be used once, as well as a 128-bit random number key to encrypt transmission of the network key. Using a custom key establishment protocol, network keys could now be securely transmitted from controller to device during pairing[8]. Or so the designers hoped.

"The word 'custom' in cryptography rings off alarms", says Fouladi in the same Black Hat presentation. After further investigation, even without documentation and despite the new encryption, the team was able to crack the key establishment protocol and even carry out attacks. The protocol begins with the controller sending an initialization packet to the device, perhaps a door lock, which responds with a ready packet. The controller responds with a nonce value and the lock returns it to confirm that communication has successfully been initialized. Now the controller generates a random network key and temporary encryption key, which are sent along with the actual network key to the device. The device then constructs a secure packet using this information to prove that it has properly decrypted the securely transferred network key [8]. Now, both controller and device have the same network key and can use it for further communication when the homeowner wants to lock or unlock their front door.

Once the protocol was derived, several attacks could be carried out. The first simple attack would be to intercept the temporary key as it is being transferred. However, this would only be possible during the 5 or 6 second window when that key is being transmitted. During this time the controller also enters low power transmission mode, so an attacker would have to be in extremely close physical range at the exact proper time to intercept the key [8]. The team also describes a "Key Reset Attack" which takes advantage of the fact that the pairing protocol can be run multiple times for a single device. Using the home ID of the controller, which is still easily retrieved from any intercepted packet, the team, or an attacker, could pretend to be the controller and run the key establishment protocol with the door lock again. Once the protocol is complete, the fake controller will be able to control the door lock without the door lock or homeowner ever knowing that malicious commands are being sent. All this can be done with about $75 worth of equipment [8].

Clearly, encryption is not always the answer to security vulnerabilities. The problem could be rectified by ensuring the key establishment protocol can be run only once for a device rather than multiple times, or by using public key cryptography to have the controller and device authenticate one another during pairing. However, even if Z-Wave were to implement these additional precautions, it would be up to the manufacturers to use them in new products and release patches for existing embedded systems, a nontrivial task that in many cases would require company and user action.

VI. Recent Attacks – EZ-Wave Tool

Since 2013, additional researchers have taken up the task of exploiting the Z-Wave protocol, including Joseph Hall and Ben Ramsey, who developed an open source reconnaissance tool, called EZ-Wave, which they presented at ShmooCon 2016. Under 200 lines of python code and built on top of Scapy-radio, the tool is made up of three parts. Ezstumbler can be used to find out what Z-Wave devices are in the system. Ezrecon allows for device reconnaissance, exposing the device name, manufacturer, software, current state and available commands. Finally, Ezfingerprint gives information about the specific Z-Wave protocol being used in the device [11]. Note that EZ-Wave is purely a reconnaissance tool and does not have the capability to directly attack the devices it examines. However, other malicious tools could use the information from EZ-Wave to take control. For example, in their presentation, Hall and Ramsey showed that they could turn fluorescent lights on and off at such a rapid rate that the lights broke, and explained how someone could lower a thermostat so that pipes freeze and burst.

Z-Wave designers quickly responded to the presentation and announced earlier this year that they are implementing a new key exchange strategy using the Elliptic Curve Diffie Hellman

protocol. According to Michell Klein, Executive Director of the Z-Wave Alliance, "Z-Wave takes IoT security very seriously, and we believe with the combination of existing and new security features, our devices will be the most secure in the smart home market." [11]

Despite this statement, Z-Wave and other protocols like Zigbee constantly seem to be playing catch-up with the attackers of the world, who will always be able to find a loophole or backdoor into a system. Furthermore, even if protocols become more secure, like Z-Wave has by supporting encryption, the manufacturers must adopt the new technology by opting in. Some manufacturers even require the consumer to manually opt in to extra security measures, something that the average consumer will most likely not do unless made aware [11].

VII. Other Options – Apple HomeKit

Originally introduced at the World Wide Developers Conference in 2014, Apple's home automation service, HomeKit, has been gaining more traction this year. HomeKit runs on an Apple TV or iPad and serves as the controller for the home. Security is a major concern in the architecture design of HomeKit, and the system uses a completely different approach to device communication [12]. Devices that do not control the home but rather share data, can be bridged via hardware with the controller, while devices that allow physical access into the home, such as door locks, cannot be bridged, but instead must go through Apple's rigorous MFi certification process [13].

To work with HomeKit, manufacturers must send their device plans to Apple, who investigates the plan for any security flaws. If the plans meet Apple's stringent requirements, the device is granted the certification and will work with HomeKit. The entire process from proposal to certification is long, which caused a significant delay between when HomeKit was announced

and the first compatible products were released [14]. Only a select set of devices will therefore work with HomeKit, a tradeoff consumers pay for the heightened security measures.

In addition, HomeKit claims “perfect forward secrecy”, meaning that every communication session between the controller and a device gets a brand new session key that is thrown away afterwards [12]. Communications are also fully encrypted, so that even Apple cannot read the messages being sent [15].

Though the additional security measures mean that the speed of feature release is slower, something that demanding consumers may see as a detriment, the additional precautions are extremely beneficial. On October 21, 2016, an attacker was able to wage a massive DDoS (Distributed Denial of Service) attack that crashed popular sites like GitHub and Netflix by hijacking IoT devices that still had default passwords set. Had HomeKit style security protocols been implemented on the devices, such a massive takedown would not have been possible [7].

VIII. Action Items

Devices in the Internet of Things promise to make lives easier by automating mundane habits and providing home security. They are not, however, excuses for laziness, and consumers looking to purchase home automation IoT devices must fully research products on the market before making a choice. Different companies have different product security policies and will require different action items on the part of the consumer. For instance, a device that requires a strong, original password is going to be much more secure than one that allows you to perform a full installation with the default password and never asks for a new one. All manufacturers will only provide security to a point, and sometimes that point is not what the consumer expects. Even placing full trust in big-ticket names without full research can be dangerous. Amazon’s

Alexa, for instance, does not have as strict security standards as Apple's HomeKit or Google's Nest [16]. At the end of the day, it is the consumers' responsibility to take control of their own devices and ensure that the products they buy meet their own security standards. Look for devices that use encryption to transmit data, have more than one way of authenticating that a user is actually you and not an attacker, and require a strong original password. The devices exist, you just have to be willing to find them.

On the manufacturer side, device and protocol designers need to realize that "security by obscurity fails" and should move to an open source approach, or at least release more transparent documentation. The Black Hat presenters were able to derive the Z-Wave protocols even though designers purposely did not release documentation on the systems. Clearly, a lack of transparency is not an effective security measure. By making home automation code open source and increasing transparency, researchers would be able to detect and rectify vulnerabilities rather than discovering them after they are already embedded in millions of homes.

IX. Conclusion

For every engineer that designs a new IoT device, protocol, or feature, there will always be someone looking for a loophole to exploit. Our devices live in a constant and never ending cycle of new feature release, followed by new attacks and new features meant to prevent those attacks. Even popular protocols like Z-Wave that are used in the majority of devices on the market are not always safe or uniformly implemented across different devices. While avoiding home automation altogether may seem like the only viable option, the consumer does have the advantage in this case, because in the IoT market the consumer has choices. Consumers can protect themselves by formulating their own security standards for devices and only purchasing

devices that meet those standards, instead of blindly choosing a product. It's your home, your data, and your responsibility to take control of your own security.

X. References

[1] Rouse, Margaret. "Internet of Things (IoT)." *IoT Agenda*. Tech Target, n.d. Web. 12 Dec. 2016. URL: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[2] "How safe are home security systems: An HP study on IoT security." Hewlett-Packard Development Company, Hewlett-Packard Development Company, 2015. Web. 1 Nov. 2016. URL: https://go.saas.hpe.com/l/28912/2015-07-21/32bhy5/28912/69170/IoT_Home_Security_Systems.pdf

[3] Tilley, Aaron. "How A Few Words to Apple's Siri Unlocked a Man's Front Door." *Forbes*. Forbes Magazine, 21 Sept. 2016. Web. 1 Nov. 2016. URL: http://www.forbes.com/sites/aarontilley/2016/09/21/apple-homekit-siri-security/#46e1cbdc6e8a

[4] Greenough, John. "How the 'Internet of Things' Will Impact Consumers, Businesses, and Governments in 2016 and beyond." *Business Insider*. Business Insider, 18 July 2016. Web. 1 Nov. 2016. URL: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[5] Columbus, Louis. "Roundup Of Internet Of Things Forecasts And Market Estimates, 2016." *Forbes*. Forbes Magazine, 27 Nov. 2016. Web. 09 Dec. 2016. URL: http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#121993024ba5

[6] Jensen, Bjorn. "How to Protect Clients from Home Automation Hacker Bots." *CEPro*. CEPro, 22 Apr. 2013. Web. 1 Nov. 2016. URL: http://www.cepro.com/article/how_to_protect_clients_from_home_automation_hacker_bots/

[7] Campbell, Mikey. "Mirai-based DDoS Attack Highlights Benefits of Apple's Secure HomeKit Platform." *AppleInsider*. AppleInsider, 2016. Web. 12 Dec. 2016. URL: http://appleinsider.com/articles/16/10/22/mirai-ddos-attack-highlights-benefits-of-apples-secure-homekit-platform

[8] HackersOnBoard. “Black Hat 2013 – Honey, I’m Home!! – Hacking Z-Wave Home Automation Systems.” Online video clip. YouTube. YouTube, 19 Nov 2013. Web 1 Nov. 2016. URL: https://www.youtube.com/watch?v=KYaEQhvodc8

[9] Fairhurst, Gorry. "Manchester Encoding." *Electronics Research Group*. Electronics Research Group, 1 Mar. 2007. Web. 10 Nov. 2016. URL: http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/man.html

[10] Fairhurst, Gorry. "Non-Return to Zero (NRZ) Encoding." *Electronics Research Group*. Electronics Research Group, 1 Oct. 2001. Web. 10 Nov. 2016. URL: http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/man.html

[11] Smith, Ms. "EZ-Wave: A Z-Wave Hacking Tool Capable of Breaking Bulbs, Abusing Z-Wave Devices." *Network World*. Network World, 2016. Web. 1 Dec. 2016. URL: http://www.networkworld.com/article/3024217/security/ez-wave-z-wave-hacking-tool-capable-of-breaking-bulbs-and-abusing-z-wave-devices.html

[12] "What's New in HomeKit." *What's New in HomeKit - WWDC 2016 - Videos - Apple Developer*. Apple Inc., 2016. Web. 12 Dec. 2016. URL: https://developer.apple.com/videos/play/wwdc2016/710/

[13] Kahn, Jordan. "Apple Details HomeKit Compatibility with Competing Home Automation Platforms, Rules out Rival Wi-Fi Gear." *9to5Mac*. N.p., 2015. Web. 1 Nov. 2016. URL: https://9to5mac.com/2015/01/22/apple-details-homekit-compatibility-with-competing-home-automation-platforms/

[14] Ritchie, Rene. "HomeKit FAQ: Everything You Need to Know." *IMore*. IMore, 2 June 2015. Web. 12 Dec. 2016. URL: http://www.imore.com/homekit-faq

[15] Pullen, John Patrick. "Apple's New Smart Home Platform Has One Major Flaw." *Time*. Time, 8 Sept. 2016. Web. 1 Nov. 2016. URL: http://time.com/4480681/apple-home-homekit-notifications/

[16] Crist, Ry. "How Secure Is Your Home Automation?" *CNET*. CNET, 27 Oct. 2016. Web. 1 Nov. 2016. URL: https://www.cnet.com/news/how-hackable-are-your-smart-home-gadgets/