ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

https://zenodo.org/records/14506377

Concerns Regarding the Security of the Z-Wave Home Automation Protocol

Madipalli Sumalatha[1], Assistant Professor[1], Department of ECE, Siddhartha Institute of Technology & Sciences, Telangana, India

Nomula Madhavi[2], Assistant Professor[2], Department of CSE, Siddhartha Institute of Technology & Sciences, Telangana, India.

Abstract

You have purchased a brand new home security device. The package promises that thedevice will give you full control of your home, allowing you to do everything from control thelights to see who's knocking at the door. It communicates through your home network usingsome sort of communication protocol, and perhaps even lets you set a password. Installationsimply requires pairing the device to the central Internet of Things hub in your home, like pairingyour 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 forattackers to gain access. What if there were open source tools on GitHub that anyone allowedanyone 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 ofdevices such as yours, and allowed anyone to see the video content it captured with the click of abutton. What if the personal computer security risks of the mid 1990's resurfaced, but on alarger, much riskier scale. What if your security device wasn't very secure at all?

Introduction

The Internet of Things, also called IoT is comprised of anything, from coffee pots toheart monitors, that can be assigned an IP address and transmit data over a network without anyhuman interaction [1]. Home automation in particular is one of the forerunners drivingdevelopment, 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. Tomeet the growing demand for such products, manufacturers are pressured to release newer andbetter features at a faster rate than ever. However, oftentimes a "better" feature does not imply "safer", as security andrisk 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 factoridentification to prevent unauthorized users, none required very strong passwords and some usedunencrypted methods to transmit updates, including FTP, a method that is widely known to beunsafe 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 videodevices and view their data. On the more extreme end, attackers can commandeer devices,causing door locks to openor surveillance to fail. Even devices from tech giants such as Googleand Apple are not 100% secure. One user explained that someone was able to unlock a front doorsimply by yelling from the porch for Siri to please open the door [3]. This paper will delve intothe architecture and security risks of one of the most ubiquitous protocols used in homeautomation systems, Z-Wave, as well as offer insights as to what consumers can do to take backcontrol of their devices to protect themselves, their homes and their families

To the Community

While IoT is largely a new technology, it has quickly become a juggernaut in thefinancial markets, and its popularity is only going to increase. Business Insider estimates thatmore than $5.5 billion was spent on home security in 2016, and that by 2020 over 70% of alldevices connected to the Internet will belong to the Internet of Things [4]. In addition, revenuesof IoT manufacturers are expected to exceed $470 billion in the next 4 years [5]. Clearly, IoT isonly expanding, butas these devices get smarter, who is responsible for ensuring their securityand protecting the customers that rely on them? Consumers may be tempted to believe that manufacturers focus on security when designing devices. However, often businesses aremotivated 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 theseproducts 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 andunderstand how to protect themselves from attacks, however consumers are often not even awareof the risks they face when purchasing IoT devices and simply do not know any better than to puttheir 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 massivedistributed denial of service attack [7]. Consumers must therefore take control of their ownsecurity, and be aware ofthe technologies involved in the products they bring into their homes.Such self-education requires strong resources that break down complex technology into easy tounderstand concepts and provide action items for consumers. This paper serves as such aresource, with the goal of breaking down the Z-Wave protocol into its core technology, exposingsome of its faults and offering more secure alternatives

Security Protocols – Z-Wave Devices

For any home automation system, the central hub and the devices that it coordinates mayuse a number of methods to communicate. The ZigBee and Z-Wave protocols are the mostwidely used, and according to the Z-Wave Alliance, over 80% of home security devices use ZWave[8]. Both protocols are favorable for their strong penetration into building walls, and work using radio chips embeddedin each device. In addition, Wi-Fi and Bluetooth also have thedisadvantage of being "power hungry," and consume too much power to be reliably used insmall devices [8].

Like any protocol, Z-Wave is constructed with a series of layers, each with differentfunctionality, that together compose the protocol stack. The Z-Wave stack begins with theapplication layer, which contains commands and parameters specific to the device andmanufacturer. 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 nodeID for each accessory, which is assigned when a new device is paired with the system. Thefourth layer is the transport layer, where error detection and retransmission acknowledgementoccurs, followed by the physical layer, where actual data is transmitted. In the United States, thistransmission has frequency 908.42 MHz. The data is transferred in bit representation, usingeither Manchester or Non Return Zero encodings [8]. Manchester encoding uses the transitionsbetween transmitted 1s and 0s to indicate logical bit values (a shift from 1 to 0 indicates a logical1 for example) [9], while the Non Return to Zero method (NRZ) relies on frequency differencesof + 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 viaZ-Wave, a specific syncing protocol is executed in order to share this network key with thedevice. First, a "preamble" packet is sent between the receiver and transmitter, containing aspecific series of bits, the home ID and node ID of the device to pair [8]. It is in this period whenthe protocol becomes susceptible to attack, as unencrypted identifying information is beingtransmitted. Though the exact specifications of the Z-Wave transmission are not documented researchers and attackershave been able to reverse engineer and exploit the system by examiningthese packets and impersonating the controller from the outside.

First Attacks and Responses

The syncing protocol to pair a new device via Z-Wave relies on the derivation of anetwork key through several calculations, which Z-Wave designers assumed would be toocomplex for attackers to derive without any open documentation [8]. However, as BehrangFouladi and SahandGhanoun explained in their presentation at Black Hat 2013, entitled *Honey,I'm Home!! – Hacking Z-Wave Home Automation Systems*, they were able to intercept theunencrypted packets being sent between devices and the controller, and easily retrieve the homeand node IDs. Using a GUI they developed themselves, they could easily dissect packets fortimestamps, home IDs, sources and targets, as none of this information is encrypted. Using thisinformation, the team was able to spoof the controller, sending raw packets to devices thatappeared to come from the real controller [8]. With information from a single packet, an attackercould easily construct a network map of all the devices and then send instructions to disarm orunlock 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 numberkey 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]. Orso the designers hoped.

The word 'custom' in cryptography rings off alarms", says Fouladi in the same BlackHat presentation. After further investigation, even without documentation and despite the newencryption, 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 adoor lock, which responds with a ready packet. The controller responds with a nonce value andthe lock returns it to confirm that communication has successfully been initialized. Now thecontroller generates a random network key and temporary encryption key, which are sent alongwith the actual network key to the device. The device then constructs a secure packet using thisinformation 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 furthercommunication when the homeowner wants to lock or unlock their front door.

Once the protocol was derived, several attacks could be carried out. The first simpleattack would be to intercept the temporary key as it is being transferred. However, this wouldonly be possible during the 5 or 6 second window when that key is being transmitted. During thistime the controller also enters low power transmission mode, so an attacker would have to be inextremely close physical range at the exact proper time to intercept the key [8]. The team alsodescribes a "Key Reset Attack" which takes advantage of the fact that the pairing protocol can berun multiple times for a single device. Using the home ID of the controller, which is still easilyretrieved from any intercepted packet, the team, or an attacker, could pretend to be the controllerand 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 everknowing that malicious commands are being sent. All this can be done with about $75 worth ofequipment [8].

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

Recent Attacks – EZ-Wave Tool

Since 2013, additional researchers have taken up the task of exploiting the Z-Waveprotocol, including Joseph Hall and Ben Ramsey, who developed an open source reconnaissancetool, called EZ-Wave, which they presented at ShmooCon 2016. Under 200 lines of python codeand built on top of Scapy-radio, the tool is made up of three parts. Ezstumbler can be used to findout what Z-Wave devices are in the system. Ezrecon allows for device reconnaissance, exposingthe device name, manufacturer, software, current state and available commands. Finally,fingerprint 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 todirectly attack the devices it examines. However, other malicious tools could use the informationfrom EZ-Wave to take control. For example, in their presentation, Hall and Ramsey showed thatthey could turn fluorescent lights on and off at such a rapid rate that the lights broke, andexplained how someone could lower a thermostat so that pipes freeze and burst.

Z-Wave designers quickly responded to the presentation and announced earlier this yearthat they are implementing a new key exchange strategy using

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

https://zenodo.org/records/14506377

the Elliptic Curve Diffie Hellman protocol. Accordingto Michell Klein, Executive Director of the Z-Wave Alliance, “Z-Wavetakes IoT security very seriously, and we believe with the combination of existing and newsecurity 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 beplaying catch-up with the attackers of the world, who will always be able to find a loophole orbackdoor into a system. Furthermore, even if protocols become more secure, like Z-Wave has bysupporting encryption, the manufacturers must adopt the new technology by opting in. Somemanufacturers 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].

Other Options – Apple HomeKit

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

To work with HomeKit, manufacturers must send their device plans to Apple, whoinvestigates the plan for any security flaws. If the plans meet Apple’s stringent requirements, thedevice is granted the certification and will work with HomeKit. The entire process from proposalto certification is long, which caused a significant delay between when HomeKit was announced and the firstcompatible products were released [14]. Only a select set of devices will thereforework with HomeKit, a tradeoff consumers pay for the heightened security measuresIn addition, HomeKit claims “perfect forward secrecy”, meaning that everycommunication session between the controller and a device gets a brand new session key that isthrown away afterwards [12]. Communications are also fully encrypted, so that even Applecannot 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 areextremely 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 byhijacking IoT devices that still had default passwords set. Had HomeKit style security protocolsbeen implemented on the devices, such a massive takedown would not have been possible [7].

Action Items

Devices in the Internet of Things promise to make lives easier by automating mundanehabits and providing home security. They are not, however, excuses for laziness, and consumerslooking to purchase home automation IoT devices must fully research products on the marketbefore making a choice. Different companies have different product security policies and willrequire different action items on the part of the consumer. For instance, a device that requires astrong, original password is going to be much more secure than one that allows you to perform afull installation with the defaultpassword and never asks for a new one. All manufacturers willonly provide security to a point, and sometimes thatpoint 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’sNest [16]. At the end of the day, it is the consumers’ responsibility to take control of their owndevices and ensure that the products they buy meet their own security standards. Look fordevices that use encryption to transmit data, have more than one way of authenticating that a useris actually you andnot an attacker, and require a strong original password. The devices exist, youjust have to be willing to find themOn the manufacturer side, device and protocol designers need to realize that “security byobscurity fails” and should moveto an open source approach, or at least release more transparentdocumentation. The Black Hat presenters were ableto derive the Z-Wave protocols even thoughdesigners purposely did not release documentation on the systems.Clearly, a lack oftransparency is not an effective security measure. By making home automation code open sourceand

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 4, 2024

https://zenodo.org/records/14506377

increasing transparency, researchers would be able to detect and rectify vulnerabilities ratherthan discoveringthem after they are already embedded in millions of homes

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 endingcycle of new feature release, followed by new attacks and new features meant to prevent thoseattacks. Even popular protocols like Z-Wave that are used in the majority of devices on themarket are not always safe or uniformly implemented across different devices. While avoidinghome automation altogether may seem like the only viable option, the consumer does have theadvantage in this case, because in the IoT market the consumer has choices. Consumers canprotect themselves by formulating their own security standards for devices and only purchasing devices that meetthose standards, instead of blindly choosing a product. It's your home, yourdata, and your responsibility to take control of your own security

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-PackardDevelopment 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-sirisecurity/#46e1cbdc6e8a

[4] Greenough, John. "How the 'Internet of Things' Will Impact Consumers, Businesses, andGovernments in 2016and beyond." Business Insider. Business Insider, 18 July 2016.Web. 1 Nov. 2016. URL: http://www.businessinsider.com/how-the-internet-of-thingsmarket-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-thingsforecasts-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 SecureHomeKit Platform." AppleInsider. AppleInsider, 2016. Web. 12 Dec. 2016. URL:http://appleinsider.com/articles/16/10/22/mirai-ddos-attack-highlights-benefits-of-applessecure-homekit-platform

[8] HackersOnBoard. "Black Hat 2013 – Honey, I'm Home!! – Hacking Z-Wave HomeAutomation 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. ElectronicResearch 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, AbusingZ-Wave Devices." Network World. Network World, 2016. Web. 1 Dec. 2016. URL:http://www.networkworld.com/article/3024217/security/ez-wave-z-wave-hacking-toolcapable-of-breaking-bulbs-and-abusing-z-wave-devices.html

[12] "What's New in HomeKit." What's New in HomeKit - WWDC 2016 - Videos – AppleDeveloper. 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 HomeAutomation 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-withcompeting-home-automation-platforms/

[14] Ritchie, Rene. "HomeKit FAQ: Everything You Need to Know." IMore. IMore, 2 June2015. 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-homehomekit-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-homegadge/