Security in Home Automation

Esmeralda Kadëna
Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary
kadena.esmeralda@phd.uni-obuda.hu

***Abstract* - Nowadays we live in the era where technology is smarter than ever. The newest devices and applications simplify tasks, make better use of resources and transform the way we live. As a consequence the world around us is rapidly changing. Smart home is a reality due to innovation in wireless connectivity and the protocols that allow devices to talk to each other. But with "The peace of mind" comes a critical point which is about security. Z-Wave protocol is the most widely used and the main reason is because of its security level. But is really this protocol secure enough? In this work are demonstrated the main security risks for a Home Automation system and how secure are the consumers while using these smart technologies.**

***Keywords*:** Home automation, security, Z-wave protocol .

1 INTRODUCTION

The Internet of Things, also called IoT is a system comprised of anything such as computing devices, machines, objects, humans, animals, etc., that have the ability to communicate with each other and transfer data over the network without human interaction. [1]. So it is what we get when we connect Things, which are not operated by humans, to the Internet [2].

Nowadays the technology is getting smarter and everything is expected to get smarter as well. Taking in consideration buildings, they are becoming more and more technology sophisticated, with smart features ranging from energy-management, self-sustainability, security control, entertainment and assisting disabled to the luxury of home automation. And when it comes to home residences, then the main idea of architecture and building structure becomes more about functional comfort of use, calmness and adaptivity, which are all suggesting ubiquitous human-building interaction [3].

The term "smart home" means improving the experience of home residents by using different sensors and actuators to observe the home and automatically control devices they want to [4]. The term "home automation" can be defined as the capability to automate and control multiple different systems [5]. A centralized control and monitoring function is provided for heating, ventilation and air conditioning (HVAC), lighting, physical security systems as well as home appliances and so on. The central control panel and various household devices are connected to each other to form a mesh network over wireless or wired communication links and act as a "smart home". Basically, there are three views that smart homes are perceived: functional, instrumental and sociotechnical [6]. The functional view intends to manage and automate in a better way the daily demands in a household. The instrumental view comprises efficient functions such as energy-management and security control. The socio-technical view seeks for digitalization of daily life and it is thought that opens the door for next generation of human - building interaction [3].

Smart adaptive homes began in early 1970s and first generation of home automation was X10 network technology that used existing power lines in the buildings as the communication medium, but as well as limited bandwidth, they were susceptible to signal loss and electrical interference [7]. Wireless home automation systems are better than power line systems and provide easier expansion and interconnectivity of different devices. Recent advancements has led to progress in building smart homes and their automation and making the consumers daily life easier and more convenient. It is estimated from Business Insider that by 2020 over 70% of all devices connected to the Internet will belong to the IoT [8] and according to Research and Markets, global home automation market it is estimated to reach $ 72.78 billion by 2020 [9].

So it is clearly that IoT and home automation is only expanding but on the other hand is always standing the most critical point, security. So as these devices get smarter, who is responsible for ensuring their security and protecting the customers? How secure are they? In this work are introduced some possible threats on home automation systems; technical and theoretical background about the security of the most widely used protocols with special emphasis on Z-wave.

2 SECURITY THREATS

In this part, the security threats related with home automation are presented. The main focus will be on the security risks of one of the most common used protocol in home automation systems, Z-Wave. This will offers insights to what people can do to take back control of such devices in order to protect themselves, homes and families. As home automation tends to directly connect our real life with the virtual world it has not a trivial impact on individual's everyday life and therefore has some associated threats. Security in this field is responsible to protect:

- Life and health
- Property
- Information
- Control of:
  - access to the home;
  - the connected devices.

To protect the above mentioned assets the local area and the web area must be considered [1]. Even such security services as key establishment, encryption, frame integrity protection and device authentication were included in the

specifications of open wireless protocols such as ZigBee although these security services are built on top of the recognized cryptographic algorithms such as Advanced Encryption Algorithm (AES), against them have occurred successful attacks that have been demonstrated that exploit the implementation vulnerabilities or insecure key management practices [2], [3].

Attacks and vulnerabilities are being more and more in the headlines of news and those related with smart home are not less important. The trend of hacking smart environments is likely to grow because of the recent adoption of the new technologies in smart homes. During the last years some successful attacks were executed and in the following list, we can see a review of them:

In July 2013, Kashmir Hill a report was published in Forbes Magazine, "When 'Smart Homes' Get Hacked: I Hunted a Complete Stranger's House via the Internet". Kashmir Hill declared in this report how she was able to hack into Thomas Hatley's home remotely by turning on and off the lights in the master bedroom of Hatley's Oregon home. That was possible because the smart home lack password protection by default [4] [5].

According to Sarah Griffiths report in August 2013, "Computer hackers can now hijack toilets: 'Smart Toilet' users in Japan could become victim to Bluetooth bidet attacks and stealthy seat closing". This famous "Smart Toilets" in Japan called Satis is known to let people raise and lower the toilet set as well as triggers a bidet function and flush by using a mobile app. It was hacked or attacked remotely because of the Bluetooth security vulnerability found in the implementation of this toilet [6].

In August 2013, Heather Kelly, a reporter for CNN, published a report titled "Smart Homes' are vulnerable, say hackers". Karotz, a cute bunny toy could be controlled from an app in smartphone and is outfitted with a video camera, microphone, RFID (Radio Frequency Identification) chip, and speakers. She reported how a Software engineer Jennifer Savage was able to take control of it from a computer and remotely watch live video, turning it into a malicious surveillance camera for attackers. Furthermore it was reported how Daniel Crowley demonstrated live at a Black Hat session, how it is possible for a third party to hack into a front-door lock and open it from a computer. Finally, the report was also about how Fouladi and Ghanoun demonstrated a hack that opened a smart lock that used the ZWave protocol [7].

Some other reports were published in August 2013 on ABC news. One of them was about the issue of the growing concerns that computerized homes make it easier for thieves to get personal information [17]. Another one raised the issue of the growing concerns of security experts about homes wired so everything can be controlled remotely. [18]

It was reported in December 2015 how a security researcher at Fortinet accomplished a hack into a video stream without any coding skills [20]. The researcher simply visited a webpage Shodan.io, which is a website where varieties of internet connected devices were found, and was able to hack into the video stream just by entering the word "admin" for the camera's username and password. The author also emphasized on the need to urgently address the security of these devices, because billions of sensors will soon be designed into various appliances, security systems, health and other equipment in the future [8].

In May, 2016, Nicole Casal published "Hacking into homes: 'Smart home' security flaws found in popular system". In this article was shown how the researchers at the University of Michigan were able to hack into smart home and get the PIN code to a home's front door [9]. They could perform four successful proof-of-concept attacks and demonstrated how a SmartApp can eavesdrop on someone setting up a new PIN code for a door lock, and subsequently send by text message the PIN to a possible hacker. Through the second attack they showed how could be remotely exploited an existing Smart app to virtually make a spare door key by programming an additional PIN codes into the electronic locks. Furthermore they presented how "Vacation mode" could turn off through the Smart app while you are away and how fire alarm could not be activated by injecting false message via Smart app. [9].

3 SECURITY PROTOCOLS

Smart home can be built on a wide variety of protocols. Each of them has its own language which speaks to different connected devices and gives them instructions to perform a function. All protocols have an API[1] and most of them are not open. There are several technologies competing to become the standard of choice. .Here can be mentioned many of them such as: X10-Wireles technology, Blootouth Mesh, KNX, Thread, Zig Bee, Z-Wave, etc. But the most widely used are ZigBee and Z-Wave protocols. According to the Z-Wave Alliance, over 80% of home security devices use Z-Wave [19].

There are some reasons about the range of its use, for instance, Wi-Fi consumes a lot of power, and Bluetooth is limited in signal range and number of devices. Comparing with Thread and Zig Bee, Z-Wave has the longest operating rate, at 300 feet (outdoor) and 80+ feet (indoor). ZigBee has the largest number of maximum device capability [20]. Considering data transmission, Thread has the fastest rate at 250 kbps. The interoperability of Z-Wave is better than ZigBee, but ZigBee has a faster data transmission rate. Thread operate on the busy Wi-Fi standard frequency of 2.4 GHz, while Z-Wave operates at 908 MHz in the USA and this has contributed in noise reduction and a greater coverage area. ZigBee operates on both 915 MHz and 2.4 GHz frequencies. All three are mesh networks[2]. You can see the following table for more details on their comparison [21].

[1] Application programming interface (API): a set of subroutine definitions, protocols, and tools for building application software. It is a code that allows two software programs to communicate with each other [33].

[2] Mesh Network: a local network topology where the nodes such as bridges, switches and other infrastructure devices are connected directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another in order to provide efficiently route data from/to clients [34].

	Z-Wave	Zig Bee	Thread	Bloot outh Mash
Operating range	100 feet	35 feet	100 feet (theoritical)	330 feet
Max no. devices	232	65,000	250-300	32,000
Data rate	9.6-100 kbps	40-250 kbps	250 kbps	1 Mbps
Frequency	908/916 MHz (U.S.)	915 MHz/2.4 GHz	2.4 GHz	2.4 GHz
Network type	Mesh	Mesh	Mesh	Mesh
Needs hub?	Yes	Yes	Yes	Yes

Table 1: Comparison of Security Protocols

	Z-Wave	Zig Bee	Thread	Bluetooth Mash
Operating range	100 feet	35 feet	100 feet (theoretical)	330 feet
Max no. devices	232	65,000	250-300	32,000
Data rate	9.6-100 kbps	40-250 kbps	250 kbps	1 Mbps
Frequency	908/916 MHz (U.S.)	915 MHz/2.4 GHz	2.4 GHz	2.4 GHz
Network type	Mesh	Mesh	Mesh	Mesh
Needs hub?	Yes	Yes	Yes	Yes

3.1 Z-Wave - technical background – security

The construction of Z-Wave as every protocol consists on a series of layers, each with different functionality, that together compose the protocol stack. In the figure below is shown the Z-wave protocol stack [10]:

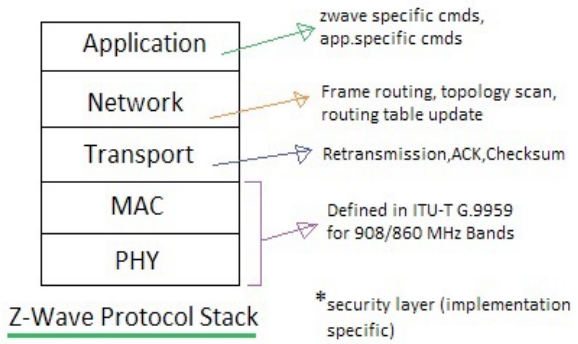

Figure 1: Z-Wave protocol stack

Physical layer: here the actual data is transmitted. The data is transferred in bit representation, using either Manchester or Non Return Zero encodings [23], [19]. 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 [24]. 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 [19]. 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.

MAC layer: it is responsible for HomeID and NodeID, controls the medium between nodes based on collision avoidance algorithm and backoff algorithm.

Transport layer: where error detection and retransmission acknowledgement occurs

Network layer: its focus is on frame routing, topology scan and routing table updates. 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.

Application layer: contains command and parameters specific to the device and manufacturer. It takes care of control of payloads in the frames received or to be transmitted.

Z-Wave protocol is developed by ZenSys, part of Sigma Designs, Inc. It is a radio based communication protocol managed and improved by the Z-Wave Alliance [25]. The frequency area it uses is between 868.4 MHz and 926.3 MHz with data rates of 9.6 kb/s, 40 kb/s (most common) or 100 kb/s. Since the Z-Wave 400 Series also 2,4 GHz, 200 kb/s and an 128-Bit AES encryption are provided. The specification of the protocol isn't publicly available. It is just provided for vendors after they sign a nondisclosure agreement. Z-Wave offers some different security mechanisms [23] in order to prevent the threats - starting with the 400 series chips. Actually older chips do

not have any security features. Requirement Mechanism Confidentiality AES-128 OFB-Mode Authenticity & Integrity CBC-MAC Freshness 64 Bit Nonce. Nut there is a problem in the way encryption keys are transferred to new devices. When a new device joins a Z-Wave network, a hardware based pseudo random generator generates a symmetric key. After that, this key is encrypted with a temporal default key consists of 16 bytes with the value 0, which is hardcoded in the Z-Wave chip. If this is known there is the risk that an attacker could sniff the initial device pairing and steal the encrypted key to decrypt it with a default key. Another publicly known problem is an implementation fault of a Z-Wave door lock [23], rather than a general protocol vulnerability. An attacker could pretend to be a Z-Wave controller (central node that coordinates all client nodes) and start the initial key exchange mechanism with the door lock. The door lock automatically accepts this and establishes a connection with the attacker's controller, even if it is already connected to a real controller. Afterwards, the attacker is e.g. able to open the door lock. This is a typical case of missing mutual authentication. It is mandatory to bear in mind that all the mentioned security mechanisms are optional and are just provided by Z-Wave chips starting with series 400. Older generations of the protocol are completely unprotected.

This disconnect is where exist vulnerabilities followed by attacks. In 2016, an attacker was able to exploit IoT devices that were using default passwords to launch a massive distributed denial of service attack [26].

But stronger standards on security of devices were announced by the Z-Wave Alliance, on November 2016. The certification was received on April 2017. It is called Security 2 (S2) and provides more advanced security for devices, gateways and hubs in smart homes [27], [28]. It supports encryption standards for transmissions between nodes, and warrants new pairing procedures for each device, so now each device is paired with unique PIN or QR codes. The intention of this extra layer of security is to prevent hackers to take control on devices with lack or poor security [29], [30]. According to the Z-Wave Alliance, the new security standard is the most advanced security available on the market for smart home devices and controllers, gateways and hubs [31].

3.2 More challenges

Encryption is not always the answer to security. The newest security layer S2 where each device is paired with a unique PIN or QR codes is similar to the approach Apple takes with HomeKit-compatible smart gadgets, each of which comes with a unique pairing code printed on the device.

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. The security of the Z-Wave ecosystem as a whole relies not only on the Z-Wave Alliance and the protocol itself, but also on the manufacturer of the device.

Another challenge are the consumers, if they take control of their own security and are or not aware of the technologies of the products they have into homes. Another characteristic of Z-Wave is that old security systems can be automate with Z-Wave. Let's suppose that "old systems" can work with Z-wave automation solutions as the company really promotes this on official website. First of all it will cost more than just starting over. Another important thing is that the users would be missing out the new security features and functions. Or they must update manually the devices. Is it convenient? Are the consumers aware about that? This could be an important resource for hackers to gain access.

Such self-education requires strong resources that break down complex technology into easy to understand concepts and provide action items for consumers.

4 CONCLUSIONS

In this work was presented an overview on security challenges of smart home systems. As the number of consumers adopting the concept of the smart home is growing every single day and the number of devices is rapidly increasing, more and more challenges are posed. These smart devices live in a constant and never ending cycle where new features are released. On the other hand are followed by attacks and then new features are realised in order to prevent the attacks.

Z-Wave protocol was taken in consider because of widely usage, convenience that offers at consumers and security layers. Some technical background was included in order to understand how the previous attacks were performed and to find the problems which were supposed to be fixed with the newest security layer S2, which provides more advanced security for gateways, devices and hubs in smart homes. Even it supports encryption standards for transmission and warrant new pairing procedures for each device, the attacks can be performed. So encryption is not always the answer. Humans are the weakest link in the internet. We can protect ourselves through education, learning and researching more. We have to be aware of the technologies and products that choose to install in our homes.

In future work deep analyses on technical part and human behaviour can be considered to provide (a) solution(s) for better security in home automation systems.

5 REFERENCES

[1] D. Schwarz, „The Current State of Security in Smart Homes Systems," SEC Consult Vulnerability Lab, Vienna, 2016.

[2] D. Kennedy és S. Dave, „Pentesting Social-Engineering over Power lines," Defcon, 2011.

[3] W. J, „KillerBee: Practical ZigBee Exploitation," 2009.

[4] ABC News, „'Smart Homes' Convenient But Are They Safe?," ABC News.go.com, 2013.

[5] K. Hill , „When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet," Forbes, 2013.

[6] S. Griffiths, „Computer hackers can now hijack TOILETS: 'Smart toilet' users in Japan could become victim to Bluetooth bidet attacks and stealthy seat closing," Dailymail, 2013.

[7] H. Kelly, „'Smart homes' are vulnerable, say hackers," CNN, 2013.

[8] L. Hautala, „Internet-connected homes open the door to hackers," cnet, 2015.

[9] N. C. Moore, „Hacking into homes: 'Smart home' security flaws found in popular system," University of Michigan News, 2016.

[10] RF Wireless World, „z-wave protocol stack | z-wave protocol layer basics," RF Wireless World, [Online]. Available: http://www.rfwireless-world.com/Tutorials/z-wave-protocol-stack.html. [Hozzáférés dátuma: October 2017].

[11] M. Rouse, „Internet of Things (IoT),” IoT Agenda, Tech Target, 2015.

[12] P. Waher, Learning Internet of Things, Birmingham: Packt Publishing Ltd., 2015.

[13] H. S. Alavi, D. Lalanne, J. Nembrini, E. Churchill, D. Kirk és W. Moncur, „Future of Human-Building Interaction,” in *CHI EA '16 Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, San-Jose, California, 2016.

[14] N. Boers, D. Chodos, J. Huang, P. Gburzyski, I. Nikolaidis és E. Stroulia, „The Smart Condo: Visualizing independent living environments in a virtual world,” in *Pervasive Computing Technologies for Healthcare*, 2009.

[15] B. A. Brush, R. Mahajan, B. Lee, S. Agarwal, S. Saroiu és C. Dixon, „Home automation in the wild: challenges and opportunities,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Vancouver, BC, 2011.

[16] C. Wilsom, T. Hargreaves és R. Hauxwell-Baldwin, „Smart homes and their users: a systematic analysis and key challenges,” *Personal and Ubiquitous Computing,* %1. kötet19, %1. szám2, pp. 463-476, 2015.

[17] D. Rye, „My life at X10,” X10 (USA) Inc., USA.

[18] J. Greenough, „How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond,” Business Insider, 2016.

[19] Research and Markets, „Global $78 Bn Home Automation Market Size, Demand Forecasts, Industry Trends and Updates 2016-2022,” CISION PR Newswire, Dublin, 2017.

[20] B. Fouladi és S. Ghanoun, „Black Hat 2013 - Honey, I'm Home!! - Hacking Z-Wave Home Automation Systems-You Tube,” HackersOnBoard, 19 November 2013. [Online]. Available: https://www.youtube.com/watch?v=KYaEQhvodc8. [Hozzáférés dátuma: 30 October 2017].

[21] B. Lewis, „Z-Wave opens up as smart home connectivity battle closes in,” Embedded Computing Design, 2016.

[22] K. Parrish, „ZigBee, Z-Wave, Thread and WeMo: What's the Difference?,” Tom's Guide, 2017.

[23] B. Fouladi és S. Ghanoun, „Security Evaluation of the Z-Wave Wireless Protocol,” *Black Hat USA,* 2013.

[24] Electronics Research Group, „Manchester Encoding,” Electronics Research Group, March 2007. [Online]. Available: http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/man.html. [Hozzáférés dátuma: October 2017].

[25] Z-Wave Alliance, „About Z-Wave Technology - Z-Wave Alliance,” [Online]. Available: https://z-wavealliance.org/about_z-wave_technology/. [Hozzáférés dátuma: October 2017].

[26] M. Campbell, „Mirai-based DDoS attack highlights benefits of Apple's secure HomeKit platform,” Apple Insider, 21 October 2016. [Online]. Available: http://appleinsider.com/articles/16/10/22/mirai-ddos-attack-highlights-benefits-of-apples-secure-homekit-platform. [Hozzáférés dátuma: October 2017].

[27] L. Hamilton, „Z-Wave Alliance Announces Board Member and New Security Mandate,” CED Magazine, 2016.

[28] W. Wong, „Q&A: S2’s Impact on Z-Wave and IoT Security,” Electronic Design, 2017.

[29] R. Crist, „Z-Wave smart-home gadgets announce new IoT security standards,” CNET, 2016.

[30] R. Crist, „Your Z-Wave smart home gadgets just got more secure,” CNET, 2017.

[31] K. Briodagh, „Mandatory Security Implementation for Z-Wave IoT Devices Takes Effect,” IoT Evolution, 2017.

[32] T. Jorgensen, „Z-Wave as Home Control RF Platform,” HomeToys, 2005.

[33] P. Christensson, „API Definition,” Tech terms, 20 June 2016. [Online]. Available: https://techterms.com/definition/api. [Hozzáférés dátuma: October 2017].

[34] M. Rouse, „Definition: Mesh Network Topology (mesh network),” December 2015. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network. [Hozzáférés dátuma: October 2017].