Hacking the Neighbor's Home: How Secure are Proprietary Wireless Home Automation Protocols?
A Study of the Sub-GHz Spectrum

Jeroen Vollenbrock
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
j.h.j.vollenbrock@student.utwente.nl

ABSTRACT

The market for new home automation products has grown significantly over the past years and continues to introduce new smart home products into our daily lives. When the wrong people manage to take control of these devices, it could have far-reaching consequences. For example, door locks can no longer actually lock the doors and cease to properly execute their tasks. Therefore, home automation devices must use secure communication protocols. However, this may not always be the case when a product is designed for mass production and low manufacturing costs. This paper proposes a taxonomy, and presents radio frequency measurements and communication analysis in order to test 32 devices for possible vulnerabilities. The results are shocking; every analyzed device is vulnerable to at least one attack that compromises the device's communication security and makes the device vulnerable to misuse. Additionally, at least 12% of the analyzed devices that claim to use encrypted communication only use trivial obfuscation methods.

Keywords

Security, Radio Frequency, Smart Home, Home Automation, Proprietary Communication Protocols, Sub-GHz, Replay Attack, Jamming, 433Mhz, 868Mhz, 915Mhz

1. INTRODUCTION

In May 2013, the McKinsey Global Institute published a report on the most upcoming disruptive technologies [15]. A significant proportion of this report is dedicated to home automation and the Internet of Things. Home Automation involves the process of adding ambient intelligence to your home. This ultimately leads to smart homes, homes that are capable of assisting their residents in their daily routines. Smart Homes have been the subject of research for a number of years [9].

The creation of these smart homes is dependent on the rate at which devices become interconnected. Therefore, some smart-home controllers contain a variety of both older and newer wireless technologies in order to make the transition towards these smart homes easier [2, 12, 6]. These controllers connect the older close-range-controllable products, such as remote controllable power sockets, window blinds and doorbells, to the internet, in order to transform the devices into smart(er) devices. However, the older communication protocols are often not designed with security in mind, which may cause risks for everything that is interconnected in the smart home.

Proprietary sub-GHz radio frequency communication protocols use the unlicensed radio bands below 1GHz. The location of these bands can differ in each country, but the most common frequencies are 433MHz, 868MHz and 915Mhz. Recent research by Jansen[14] studies potential security vulnerabilities in the Zehnder CO2 ventilation system. In this research, a framework is proposed to efficiently measure proprietary sub-GHz communication protocols and determine their state of security.

Jansen's research, combined with other research in the sub-GHz home automation communication protocol area [4], suggests a lot of these devices may be insecure. In this work, an extended version of Jansen's framework is used on a variety of devices in order to determine the current state of security in the home automation market.

The main goal of this research is to answer the question: **"How secure are the proprietary sub-GHz communication protocols that are used in current home automation products?"**. In order to objectify the answer, this question is broken down into the following subquestions:

- RQ1: Into which product categories can products using the Sub-GHz bands be divided?
- RQ2: What kind of security vulnerabilities can occur in proprietary sub-GHz communication protocols?
- RQ3: What is the impact of a vulnerability in each of these product categories?
- RQ4: How are the most common devices in each of the product categories found in RQ1 impacted by the different vulnerabilities found in RQ2?
- RQ5: Can the discovered vulnerabilities and attacks be mitigated?

This paper is organized as follows: Section 2 discusses the ethics concerning this research. Section 3 discusses the pre-measurement findings, Section 4 discusses the methodology, Section 5 discusses the results and findings of this research and section 6 will conclude the research.

25th *Twente Student Conference on IT*, July 1, 2016

2. ETHICAL CONSIDERATIONS

The product names in this work are substituted by product indexes and a category suffix. Any other properties that can be used to identify or misuse the vulnerable products are excluded as well. These countermeasures make it harder for potential criminals to misuse the research and the research results. It also makes it harder for product owners and users to distinguish secure and insecure products, and for security researches to verify parts of the research. These are unintended side-effects, but the side-effect do not outweigh the legal consequences.

Additionally, an attempt is made to inform the product manufacturers of all vulnerabilities concerning their products. Coordinated disclosure policies are the preferred way to accomplish this, as it allows those manufacturers to resolve vulnerabilities before anything is published. Unfortunately, none of the product manufacturers of the selected devices have published these policies on their website and none of these manufacturers are listed on disclosure mediation services such as HackerOne [8].

The measured devices are supplied by a third party, in return for which unprocessed measurement results are shared. The ethics concerning this have been analyzed, and the chances of any impact on research objectivity and data misuse are considered negligible [28].

3. TAXONOMY

This section discusses the different product categories and types of security vulnerabilities targeted by the measurements. A risk assessment using the vulnerabilities and product categories is also included in order to visualize different impacts.

3.1 Product Categories

Using a variety of webshops [13, 11, 24, 1], home automation books [9] and other resources [27, 18], six product categories can be isolated requiring further security research:

- Door & Gate Locks (LCK)
- Alarm Systems & Alarm Sensors (ARM)
- Heating & Climate Control (CLM)
- Lighting & Sockets (PWR)
- Rollers & Blinds (SUN)
- Communication & Notification Systems (COM)

3.2 Security Vulnerabilities

In order to determine to what kind of attacks the products are vulnerable, the attacks are also categorized. Existing research [20, 23, 25, 17, 3] and surveys [29, 30, 22, 16] mention the following attack categories:

Presence Detection (PrD) - Is it possible to determine human presence in a home? A potential attacker could use this information to determine when to break-in. A product is vulnerable to these attacks when a transmission can always be directly contributed to actions performed by humans, and can be resolved by transmitting on occasions that are not bound by manual actions.

Payload Decryption (PaD) - Is it possible to read the contents of the transmission? A potential attacker could use this information to accurately determine the precise location of human presence. A product is vulnerable to this attack when the data is unencrypted or decryptable, and this attack results in a loss of confidentiality.

Signal Jamming (SiJ) - Is it possible to cause a Denial of Service by blocking the signals? This attack could be used to completely disable some systems. For instance, a jamming attack on a lock or alarm system may prevent actual locking or arming. The presence of this attack can be determined by transmitting a long-duration signal without embedding any useful data. The device is vulnerable if it does not actively respond to this. For instance, an alarm system is not vulnerable if it goes off within a very short period of time after this attack is started. Signal Jamming is the only vulnerability that does not rely on the actual communication. Therefore, it can easily be executed with very cheap and accessible hardware.

Signal Replay (SiR) - Can a signal be recorded and replayed to cause the same action? For instance, if the device is vulnerable, a recording of an "unlock" or "disarm" command can be replayed to disable home security by unlocking a lock or disarming an alarm system. This attack results in a loss of message authenticity.

Payload Construction (PaC) - Is it possible to broadcast a custom command without recording it? An attacker could use this attack, for instance, to unlock a door by only recording a command to lock the door and modify it to unlock the door. This adds more flexibility and decreases the execution complexity of the attack. This attack also results in a loss of message authenticity.

3.3 Risk Assessment

Some vulnerabilities are more important than others, therefore a system is required in order to compare these different vulnerabilities. For each kind of vulnerability and each kind of product group, a CVSS vector has been constructed [5, 10]. A CVSS vector consists of metric values describing the Attack Vector, Attack Complexity, Required Privileges, User Interaction, Scope, Confidentiality, Integrity and Availability. These metric values are weighted using the CVSSv3 score calculator as described in the CVSSv3 specification [5]. Each score represents the severity of the attack on a scale of zero to ten, where ten is the most severe. This makes it possible to identify the product categories with increased severity requiring additional security.

Table 1 shows the CVSS scores. Attack scores above the attack average are highlighted in bold.

	PrD	PaD	SiJ	SiR	PaC	AVG
LCK	**5.7**	**6.6**	**8.5**	**8.8**	**9.6**	7.8
ARM	**4.3**	**7.1**	**8.1**	**8.5**	**9.6**	7.5
CLM	**4.3**	**6.5**	6.5	7.1	8.8	6.6
PWR	3.5	5.7	6.5	7.6	**9.6**	6.6
SUN	3.5	5.7	6.5	7.6	8.3	6.3
COM	3.0	4.3	6.5	7.3	8.3	5.9
AVG	4.0	6.0	7.1	7.8	9.0	6.8

Table 1. CVSSv3 Score Matrix

All vulnerabilities except payload decryption are more severe when they exist in a lock compared to an alarm system. This is probably due to the nature of these systems. An alarm system's main function is to warn its owner of an attack, while a lock attempts to prevent an attack. Payload decryption (PaD) of communication with an alarm system can be used by an attacker to access information that was previously inaccessible without triggering the alarm system itself, thus modifying the "scope" of the alarm system, while PaD of communication with a lock does not necessarily accomplish this.

4. MEASUREMENTS

The results from Section 3 provide a context and scope for actual measurements. Capturing Radio Frequency (RF) traffic involves the construction of a setup that is able to identify the properties of a transmitted signal, such as the precise frequency and modulation type, and extract data from the signal. Ideally, the system should also be able to transmit data during further research. Finally, the measurement setup has to be independent on the communication that is going to be analyzed.

4.1 Tools

This resulted in the use of two measurement tools. Initially, a Software Defined Radio (SDR) is used to determine signal properties [21]. Then, a Texas Instruments CC1101 is used for the data extraction [26]. In order to capture the actual data, a Logic Analyzer is connected to a computer running analytic software and is connected to both the RX and carrier detection pins of the CC1101 Development Kit [19]. Additionally, a Digital Pattern Generator could be connected to the computer and the TX pin of the CC1101 in order to generate actual transmissions.

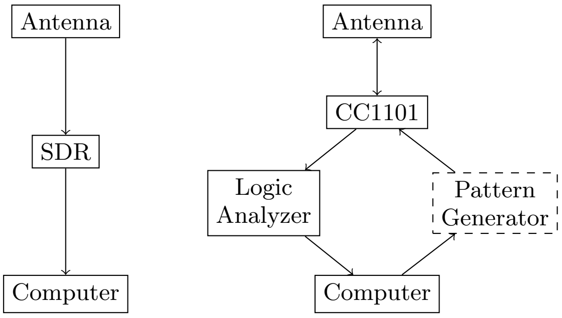


Figure 1. Measurement setup

4.2 Devices

Next to these tools, actual home automation devices are required as well, before any tests and measurements can be conducted. The same resources from Section 3.1 are used to compile a list of top listed home automation devices using sub-GHz communication protocols on e-commerce sites. Based on this list, 32 devices are analyzed. The devices are obtained through a partnership with Athom[1], the creator of Homey, a smart home hub and digital assistant [2]. The devices are measured, and a copy of the raw measurement data is supplied back to Athom. This enables Athom to integrate these devices with Homey.

Each device is set-up next to both measurement tools. The device communication is then triggered multiple times, and the communication is recorded. These recordings are used to determine if these payloads are protected at all, and if they are theoretically vulnerable to any of the attacks described in Section 3.2.

4.3 Objectives

In order to minimize the required time per measurement, the following objectives have been identified:

Preparation phase:

- Use the SDR to determine RF properties
- Configure the CC1101 with proper parameters
- Confirm if the setup records data

Recording phase:

- Collect five recordings of each supported command

Presence detection (PrD):

- Verify if user interaction causes a distinguishable transmission

Signal Jamming (SiJ):

- Transmit a carrier and attempt to use the device

Payload analysis:

- Compare the signal repetitions within each recording
- Compare the five recordings for each command (SiR)
- Identify changes and reconstruct data format (PaD)
- Predict every field in data format (PaC)

5. RESULTS

	PrD	PaD	SiJ	SiR	PaC	CVSS	€
LCK1	V	V	V	V[3]	V[4]	9.3	500
LCK2	V		V			7.1	460
LCK3	V	V	V	V	V	9.6	450
LCK4	V	V[1]	V	V[3]	V	9.6	360
LCK5	V	V	V	V[3]	V[4]	9.3	300
LCK6	V	V	V	V[3]	V[4]	9.3	150
ARM1			V[2,6]			8.1	400
ARM2	V		V[2,6]			8.1	150
ARM3	V	V	V	V	V	9.6	150
ARM4	V	V	V	V	V	9.6	120
ARM5	V	V	V	V	V	9.6	35
ARM6	V	V	V	V	V	9.6	30
ARM7		V	V	V	V	9.6	10
CLM1	V	V	V[2]	V[3]	V[5]	8.3	500
CLM2	V	V	V	V	V	8.8	40
CLM3	V	V	V	V	V	8.8	15
PWR1	V		V			6.5	80
PWR2	V	V[1]	V	V[3]	V	9.6	30
PWR3	V	V	V	V	V	9.6	25
PWR4	V	V	V	V	V	9.6	20
PWR5	V	V	V	V	V	9.6	20
PWR6	V	V	V	V	V	9.6	20
PWR7	V	V	V	V	V	9.6	15
PWR8	V	V	V	V	V	9.6	15
SUN1			V			6.5	500
SUN2		V[1]	V	V[3]	V	8.3	450
SUN3		V	V	V	V	8.3	100
SUN4		V	V	V	V	8.3	30
COM1	V	V	V	V	V	8.3	45
COM2	V	V	V	V	V	8.3	25
COM3	V	V	V	V	V	8.3	20
COM4	V	V	V	V	V	8.3	15
COUNT	26	27	32	27	27		

Table 2. Vulnerability analysis

[1] https://www.athom.com

[1] Payload is obfuscated
[2] Device detects loss of signal
[3] Only when target is shielded from original signal
[4] Uses KeeLoq encryption, broken in 2008
[5] Uses an 8-bit “hopping” code, requires bruteforce
[6] Alarm does sound after a certain interval

Table 2 shows the measurement results. Each “V” implies the device is vulnerable to an attack of the given category. In the CVSS column, the CVSS score of the most severe encountered vulnerability is shown, and the last column contains the average price[2] of the products. In some cases the tested product is modular, in those cases, the price of the remote-control module is used.

100% of the measured devices are vulnerable to at least one attack, 94% of the devices are vulnerable to at least two attacks, and 84% is vulnerable to three or more attacks. The vulnerability in the most secure device has a CVSS score of 6.5, and the vulnerabilities in the least secure device have a maximal CVSS score of 9.6.

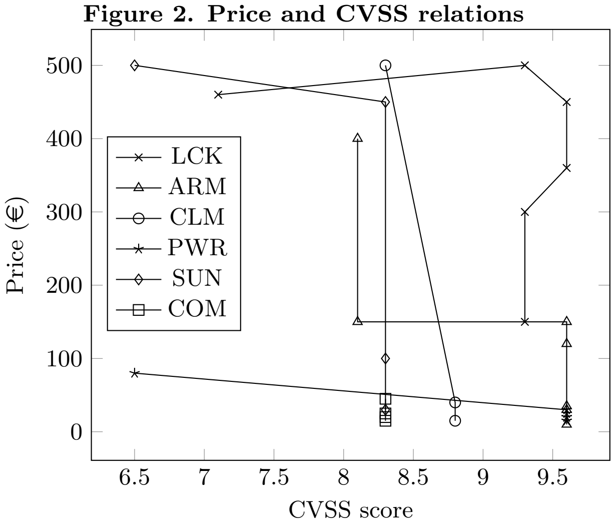
5.1 Discussion

The results show severe problems with almost every device. At least 12% of the devices that claim to use encryption, actually use trivial obfuscation methods, such as communicating the XOR value of each succeeding byte. Some of the devices even mention properties such as “securely coded signal” on their package, while being vulnerable to every category of attack.

When the product price is compared to the CVSS score of each product (Figure 2), the most secure products happen to be the most expensive products, and the most vulnerable products align with the cheapest products. This however, does not imply every expensive product is secure. The cheaper products are all insecure, but a significant amount of the expensive products are also insecure. Therefore, simply buying expensive products will not guarantee safe products. However, buying the cheapest available products does result in the worst secured product for each measured device category. This is the case for every product, except LCK2. This may be due to the fact that LCK2 is much newer than LCK1, which is a less-secure, more-expensive remote control module for older electric garage doors.

Only two of the measured devices have the possibility to install software updates. However, even if the vulnerabilities can be resolved with a software update, the devices would become inoperable with devices that have not been updated due to changes in the communication protocol. While we can only speculate, it seem unlikely the problems are going to be resolved at all because of this.

Figure 2. Price and CVSS relations



6. CONCLUSION

The proprietary sub-GHz communication protocols that are being used by current hardware are not secure. Obfuscation is often mistaken for encryption, message authenticity and confidentiality cannot be guaranteed, and Denial-of-Service attacks can be executed with easily accessible and cheap hardware.

Using market research, a taxonomy was constructed and used to categorize the different devices and vulnerabilities. These categories have been used to successfully analyze the impacts of possible attacks using CVSS scores. This shows increased impacts for locks and alarm systems.

The 32 supplied devices have been tested against a variety of attacks and 100% of these devices are vulnerable to one or more of these attacks. This research shows a serious lack of disregard for security by manufacturers of home automation products. It also illustrates a strong need for secure, standardized communication protocols such as the ZWave protocol [7]. This will not only contribute to security, but also to interoperability of smart home devices.

An attempt has been made to inform product manufacturers of the encountered issues. This process could have been much more trivial to counter if the product manufacturers published a coordinated-disclosure policy on their website. This shows a more general problem: Manufacturers of single-purpose hardware seem to be very unfamiliar with procedures that are very common in the software industry, and sometimes even made it impossible to fix a vulnerability in the software that is embedded in their devices. This calls for more awareness, but it may already be too late for current vulnerable devices.

7. FUTURE WORK

Even though most discovered vulnerabilities cannot be resolved in the current hardware revisions, it may still be possible to design a device that is capable of detecting intrusions by using signal strengths to multilaterate signals and estimate the origin of the signal. Instead of warning their owner, these devices may even be capable of actively mitigating the attack by using jamming techniques. Further research is required to determine the feasibility of and demand for such a device. This can also be extended by more research with regards to possible attack ranges and signal amplification.

8. ACKNOWLEDGMENTS

I would like to thank Athom for providing all the required hardware for this research. I would also like to thank Roland van Rijswijk and Anna Sperotto for their guidance, support and feedback during this research.

9. REFERENCES

[1] Athom B.V. Athom App Store. https://apps.athom.com/ (accessed at 2016-05-11), 2016.

[2] Athom B.V. Homey, the living room. http://www.athom.com/ (accessed at 2016-05-11), 2016.

[3] E. Çayırcı and C. Rong. *Security in Wireless Ad Hoc and Sensor Networks*. John Wiley & Sons, Ltd, Chichester, UK, 1 2009.

[4] M. Chernyshev. Verification of primitive Sub-Ghz RF replay attack techniques based on visual signal analysis. In *Proceedings of the 11th Australian Digital Forensics Conference, ADF 2013*, pages 26–35. Edith Cowan University, 2014.

[2] As observed on e-commerce sites

[5] D. Czagan. Common Vulnerability Scoring System. *IEEE Security and Privacy*, 2015(February 20):1–2, 2013.

[6] Domoticz. Domoticz - Control at your fingertips. https://domoticz.com/ (accessed at 2016-05-11), 2016.

[7] B. Fouladi and S. Ghanoun. Security Evaluation of the Z-Wave Wireless Protocol. *Black hat*, page 6, 2013.

[8] HackerOne. HackerOne. https://hackerone.com/ (accessed at 2016-06-15), 2016.

[9] R. Harper. *Inside the Smart Home*, volume 5. Springer, 2003.

[10] H. Holm and K. Khan. An expert-based investigation of the Common Vulnerability Scoring System. *Computers & Security*, 53:18–30, 9 2015.

[11] Home Depot. Home Depot Webshop. http://www.homedepot.com/ (accessed at 2016-05-11), 2016.

[12] Home Wizard. Home Automation System. http://www.homewizard.co.uk/ (accessed at 2016-05-11), 2016.

[13] Intellihome. Intellihome Web Store. https://www.intellihome.be/en/ (accessed at 2016-05-11), 2016.

[14] J. Jansen. Exploring Possible Vulnerabilities of 868MHz Communication Systems: A Step-By-Step Framework. In *23rd Twente Student Conference on IT*, volume 23, pages 1–6. University of Twente, 2015.

[15] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and Marrs. *Disruptive technologies: Advances that will transform life, business, and the global economy*. Number May. McKinsey Global Institute, 2013.

[16] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys and Tutorials*, 11(4):42–56, 2009.

[17] A. S. K. Pathan, H.-W. Lee, and C. S. Hong. Security in wireless sensor networks: issues and challenges. In *The 8th International Conference on Advanced Communication Technology, {ICACT} 2006*, volume 2, pages 1043–1048, 2006.

[18] PiLight. Pilight supported protocols. https://wiki.pilight.org/doku.php/protocols (accessed at 2016-05-11), 2016.

[19] Saleae. Saleae Logic Analyzers Website. https://www.saleae.com/ (accessed at 2015-05-12).

[20] I. Sanchez, R. Satta, I. N. Fovino, G. Baldini, G. Steri, D. Shaw, and A. Ciardulli. Privacy leakages in Smart Home wireless technologies. In *2014 International Carnahan Conference on Security Technology (ICCST)*, number October, pages 1–6. IEEE, 10 2014.

[21] A. F. B. Selva, A. L. G. Reis, K. G. Lenzi, L. G. P. Meloni, and S. E. Barbin. Introduction to the software-defined radio approach. *IEEE Latin America Transactions*, 10(1):1156–1161, 1 2012.

[22] J. Sen. A Survey on Wireless Sensor Network Security. *Computer Networks*, 1(2):55–, 2009.

[23] R. A. Shaikh, H. Jameel, B. J. D'Auriol, H. Lee, S. Lee, and Y.-J. Song. Achieving network level privacy in Wireless Sensor Networks. *Sensors (Basel, CH)*, 10(3):1447–72, 1 2010.

[24] Smarthome. Home Automation Superstore. https://www.smarthome.com/ (accessed at 2016-05-11), 2012.

[25] X. Tang, P. Ren, Y. Wang, Q. Du, and L. Sun. Securing Wireless Transmission against Reactive Jamming: A Stackelberg Game Framework. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 12 2014.

[26] Texas Instruments. CC1101/CC2430/CC2510 Development Kit User Manual. *SWRU039B*, pages 1–28, 2005.

[27] R. Torbensen, K. M. Hansen, and T. S. Hjorth. My home is my bazaar - A taxonomy and classification of current wireless home network protocols. In *Proceedings - 2011 2nd Eastern European Regional Conference on the Engineering of Computer Based Systems, ECBS-EERC 2011*, pages 35–43. IEEE, 9 2011.

[28] J. Vollenbrock. Hacking the neighbor's home: Reflection Report. Technical report, University of Twente, Enschede, 2016.

[29] Y. Wang and G. Attebury. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 8(2):2–23, 2006.

[30] Yun Zhou, Yuguang Fang, and Yanchao Zhang. Securing wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*, 10(3):6–28, 2008.