The Unspoken Vulnerability of Garage Doors and Gates

RIFAT RALFI SALHON

Tufts University

rifat.salhon@tufts.edu

December 12th, 2018

Abstract

Many short range devices such as garage door remotes use Industrial, Scientific and Medical (ISM) Bands. Usage of this band requires no license, and is therefore a popular choice among many manufacturers. When a key is pressed on a garage door remote, Amplitude Shift Keying (ASK) is executed. This consists of multiple bits being sent on a single frequency in a short range. The most popular choice for garage door remotes is using 12-bit switches inside of the remote that sends the correct bit pattern using ASK to unlock the door. For 12-bit switches, there are 2^12 = 4096 combinations. On the other hand, a 2 character web password which can consist of 52 unique lowercase/uppercase characters, 10 digits, and 10 special characters has 2^72 = 5184 combinations, already more secure than a 12-bit garage door remote. However, it's even simpler to unlock these doors. Most garage door receivers use shift registers, meaning that an incorrect bit combination just disregards the first bit rather than the entire 12 bits. Therefore, using a "deBruijn sequence," one can reduce the number of bits sent from 49152, to 4107, 8% of the original required amount. This paper will discuss how unlocking any 12-bit code garage door using this method takes less than 10 seconds, and what we can do to combat this vulnerability.

I. Introduction

A garage door opener is a motorized device that opens and closes a gate, controlled by switches on the wall or more commonly controlled by a remote control carried by the owner. When a key is pressed on a garage door remote, Amplitude Shift Keying (ASK) is executed. This consists of multiple bits being sent on a single frequency in a short range. These bits are typically set by 8 to 12 bit switches on the receiver and transmitter, allowing for up to 2^8 = 256 different codes for 8 bit switches and 2^12 = 4096 different codes for 12 bit switches. As long as neighbors use different codes, it is not possible to accidentally (or

intentionally) open another person's garage door. However, these systems were not designed with security in mind — the intent of having bit switches with no encryption or way to detect the actual owner was designed only to avoid interference with nearby garage doors. Therefore, they are very insecure.

II. To the Community

I chose to explore this topic because despite its popularity and everyday use, the vulnerabilities of such a common system are hugely overlooked. According to alarms.org, a home security services provider, "95% of all home invasions require some sort of forceful entry". Also, with the introduction of electrical cars (and the hackers who manage to unlock and take control of one in minutes), the need for security for our personal belongings is more than ever. However, we seem to have a misunderstood perception about the security of remote doors. Products like the *Garage Door Armor*[1] make promises only to protect against the physical tools that unlock garage doors, disregarding the simplicity of the electrical mechanism that promises to protect the entrance as well. It is important for us to know the various other malicious ways that could be used to break into properties, and how we have to change our current system to protect our homes from hackers.

III. Background on Subject

Many garage door remotes, like most short range devices, use Industrial, Scientific and Medical (ISM) Bands. Usage of this band requires no license, and is therefore a popular choice among many manufacturers. The frequency range of this band is 300-433 MHz, and with the press of a button on the garage door remote, it can be programmed to modulate a signal within the specified frequency. This is called Amplitude Shift Keying (ASK), seen in action on *Figure 1*. Every time a button is held down, multiple bits are sent on a single frequency. The shift on that frequency has to do with the time's that the data is on or off, indicated by sending a 1 or a 0. The remotes can be controlled by the bit switches inside of them. For example, on an

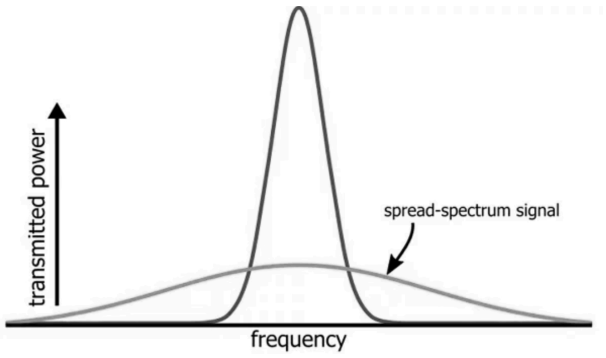

Figure 1: Spread-spectrum modulation

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

8 bit switch remote, the switches could be in formation “01100100” which would mean that is the data being sent on the frequency. There is no other special message formatting to make this unique from any other remote that would send the same data.

IV. Security of Garage Doors

Most garages use 8 or 12 bit switches to operate. Sending 8 bits of data takes around 32 ms, and therefore it would take around 32 ms * 2^8 = 8000 ms, or 8 seconds to test every possible variation. However, one would assume that sending codes back to back should be impossible, and that there is a safety mechanism preventing such an action. There is not. In fact, it’s even worse. Many garage door receivers use what is called a shift register, which means that in each string of bits, instead of considering one 8 bit string and then throwing it out if its wrong, it just throws out the first bit and considers the next 8 bits. And this has pretty profound security implications. Now, any gaps between the sent codes that cover all the combinations can be disregarded. Also, some of the combinations can be merged together by overlapping the codes. A sequence like this is called a “de Bruijn sequence,” illustrated for an alphabet size of 2 and substring length of 2 in *Figure 2*. This drastically reduces the number of combinations that need to be sent. Normally, all 8 bit combinations would require sending 256 * 8 = 2048 bits, but using a “de Bruijn sequence,” only 263 bits need to be sent to test every single variation. This is a reduction of almost 90% in the number of bits required to test every single combination, taking 1 second to crack an 8-bit code door and 10 seconds to crack a 12-bit code door (This would’ve taken around 4.5 minutes to test every sequence without using a de Bruijn sequence).

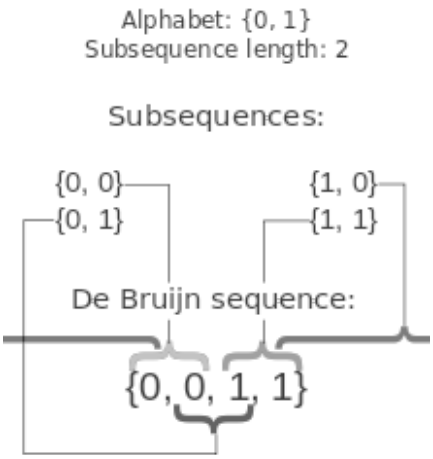

Figure 2: de Bruijn sequence example

V. Using the *IM-me* to Brute Force Fixed Codes

The *IM-me* is a toy from *Mattel* that is no longer in production. During its production cycle, it was discovered by hackers that the *IM-me* could be used to brute force its way into any fixed code garage or gate. This is possible because of a chip inside, called the *CC1110*. This chip consists of a micro-controller with a transceiver. The transceiver is very interesting, because it transmits and receives from 200 MHz to 950 MHz, a very wide range.

Using the *IM-me*, it is possible to talk to a lot of things like garages, cars, power meters, and even alarm systems. There is also some context underneath the battery in the back, which allows the board to be flashed, erased, and even installed with new software. Using these methods, the *IM-me* can be programmed to execute the de Bruijn sequence in the specified frequency to test all 8-bit and 12-bit codes, therefore unlocking all nearby fixed-code garages in a matter of seconds.

VI. Caveat: Rolling Codes

Although the majority of the garage door market is flooded with fixed code combinations, some companies have taken the extra mile to integrate software security in their mechanisms. “Rolling Code” combinations mean that both the remote control and the remote receiver have an algorithm that uses a seed (a number) to generate a pseudo random number, and that is the code that they use to communicate. It’s okay if the algorithm gets known, because the thing that is secret between the transmitter and the receiver is the seed that is used to generate the next pseudo number in the sequence[2]. It will be useless if an attacker plants a device outside and stores the code being transmitted, because the code just got used up and the receiver can be programmed to never respect that code again. However, the problem is not really solved. Because the issue of not knowing who the sender of the code is exists, a trick can be used to gain control of a valid code to unlock the garage. As explained by Samy Kamkar, an American privacy and security researcher: A hacker could listen for a signal directed towards a garage, and then interfere that signal, but keep note of the secret code being sent to unlock the gate. Then, the user would inevitably have to press the remote button again to open the gate. This signal could also be jammed, gaining access to the next secret generated code. Now, the first code could be transmitted by the hacker to unlock the garage, giving the impression that a bug prevented the door opening the first time. Now, the hacker has a secret code that can be used to open the garage door once. These receivers have no sense of time as they are just looking for a sequence, making them very vulnerable to attacks.

VII. Defenses

Protection against remote door security has been scarce over the years. In fact, “[Vulnerable] garages have been known to be easily opened or cracked for over 30 years,

[2] A free example can be found from https://leventozturk.com/engineering/random/

yet vendors continue to manufacture and irresponsibly sell them to consumers without any warning of their inherent weaknesses" (Kamkar). Black markets for criminals buying and selling code grabbers have also been around for years, which can easily exploit garage door vulnerabilities in the ways mentioned above. To know if you are vulnerable, open up your garage door remote and see if it contains any bit switches. If it does, you may be vulnerable. Replace your garage door remote and receiver with brands advertising as "Security +", as these brands at the very least utilize rolling codes that makes a very mundane hacking task somewhat complicated.

VIII. Conclusion

For customers: While it is easy to choose price and functionality over security, it is important to remember the implications that bad programming practices bring with them. Although the average person in your neighborhood cannot hack a garage door open in 10 seconds, this paper has proven that those who are experienced and with malicious intentions easily can. As a consumer, spreading awareness of these profound security implications is important, because it renders vulnerabilities like such to be less viable.

For vendors: Implementing security features into any device that a customer depends on is critical. Although the basic nature of bit-switches and data transmission over ISM bands allows for a working product to be produced very easily, it does not outweigh the cons of being extremely vulnerable. Doing the right thing and spreading awareness takes extra effort, but is a step that must be taken. Make sure the product that you are selling is secure.

References

- Kamkar, Samy. “DEFCON 23 Speech by Samy Kamkar on Garage Door Hacking” , https://youtu.be/K2ZJDZVeheU
- Veritasium. “This Toy Can Open Any Garage”, https://youtu.be/CNodxp9Jy4A
- Kamkar, Samy. “OpenSesame - hacking garages in seconds using a Mattel toy”, https://youtu.be/iSSRaIU9_Vc
- AdamDIY. “How to open a garage door with a phone”, https://youtu.be/4wCyo0wAr_w
- All About Circuits. “Low-Power RF Devices and the ISM Bands”, https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/electromagnetic-spectrum/low-power-rf-devices-and-the-ism-bands/
- Wikipedia. “De Bruijn sequence”, https://en.wikipedia.org/wiki/De_Bruijn_sequence
- Alarms. “Burglary crime statistics and facts”, https://www.alarms.org/burglary-statistics/