# Security Analysis of Electric Garage Doors

Calvin Chang [1], Erie Okada [2], Ernest Chu [3], and Wei (Williams) Lin [4]

*Electrical and Computer Engineering, University of British Columbia*

[1] dissent@shaw.ca, [2] e_okada@hotmail.com,

[3] ernechu@gmail.com, [4] leisurely12@yahoo.com.tw

*Abstract* – **This paper outlines a brute force attack on electric garage door openers that use dip switches to set the key. We decided to analyze and attack dip switch garages because the longevity of garage door openers means that a lot of people still own garages that use dip switches for security. An informal survey among friends also revealed that 50% of them still used dip switch garages. We successfully implemented a circuit that was able to crack two different garages. We also include a risk analysis and countermeasures for attacking garages.**

*Keywords* – **Rolling code, DIP switch, brute force attack, replay attack.**

## I. INTRODUCTION

Electric garage doors have become ubiquitous in our neighbourhoods. Almost every home has them and most apartment buildings use them as well to secure their parking areas. Many of these garages are attached directly to people's homes and are used to not only store cars, but other assets. This makes the security of garage doors very important as breaching that security would make a lot of assets vulnerable.

Our project investigates the feasibility of using brute force attacks on dip switch garage door openers. We decided to attack dip switch garages as it is beyond our scope and knowledge to be able to crack the encryption or the algorithms that rolling code garages use. We also decided to attack dip switch garages as an informal survey of our friends revealed that 6 out of 12, 50% of them, still used dip switch garage door openers. Out of the 6 who had dip switch garages, 1 of them included an apartment building, which in essence makes the assets of all the tenants vulnerable.

This report consists of five major parts. The first part will provide the background and evolution of garage door openers. The second part will explain the risk analysis of residential garages. The third and fourth parts will discuss the implementation and design of the electric garage door hacker we built. The countermeasures will be discussed in the last section.

## II. EVOLUTION OF GARAGE DOOR OPENERS

The first electric garage door opener was invented in 1926 by C.G. Johnson of Indiana. Early versions did not use a remote control, and it wasn't till after World War II that remotes were first introduced [1].

The first generation of remote controlled garage door openers were very simple and broadcast only on one frequency [2]. This worked well when the openers were not very widespread, but became a problem as they became more and more popular. Anybody with a remote control could open every garage that was equipped with a garage door opener and have access to all the contents within.

The second generation introduced dip switches, starting with 8 [2]. The 8 dip switches meant that there were 256 different codes that could be used to program a garage door opener, which made it difficult and time consuming to find the specific code to open a random garage.

The third generation introduced rolling code or added more dip switches with different manufacturers using different frequencies. Encryption of the signals and user verification was also introduced in addition to rolling code [2].

The only change for the fourth generation was that remotes would only communicate with receivers at 315 MHz to avoid interfering with the U.S. military's Land Mobile Radio System [3].

## III. RISK ANALYSIS

A risk analysis was done prior to the beginning of this project to determine whether this problem posed a significant risk to people and their assets. We found that the overall risk of having an insecure garage is extremely high, and will elaborate on why this is so in the following sections.

### *A. Assets at Risk*

Many home owners use their garages as storage areas because they view them as just another spare room. Homeowners tend to feel a sense of security in regards to their garages, which leads some people to store valuables in there. This may also lead some homeowners to not even bother locking their cars or locking the door that provides access to the main house. The list below just shows a few examples of the possible assets garage owners might store in their garages or assets considered at risk in our report:

- Frozen / canned food
- Furniture and appliances such as TVs, computers, microwaves, etc
- Sporting equipment such as snowboards, bicycles, hockey gear, etc
- Gardening tools such as lawn mowers, leaf blowers, chain saws, etc
- Machine tools such as drills, sanders, etc
- Motor vehicles and vessels such as boats, cars, motorcycles, etc
- Valuables stored inside the house
- Personal safety

### *B. Vulnerabilities*

With the assets at risk identified and the importance of security apparent, we were able to find some possible vulnerabilities that electric garage doors are faced with:

#### *1) Brute Force Attack:*

A brute force attack involves a system that attempts to gain access to the device under test by simply trying out all possible combinations to determine the correct key that accesses the device. Even though this type of attack can be considered the most primitive, it is very thorough and known to succeed every time. The disadvantages in using this attack is the fact that it is the most time-consuming attack, and it can only be done to dip switch garages.

For those vulnerable garages, the key has a maximum number of combination of 4096 (or $2^{12}$ for a 12-bit dip switch garage). This means that garages are extremely easy to crack open as the average number of tries to crack it is 2048. To put this in perspective, an eight character (alpha-numeric) password, one commonly used on the internet, has roughly 22 trillion ($62^8$) combinations.

#### *2) Replay/Repeat Attack:*

A replay attack is an attack where an intruder would intercept and record the key/password signal that is transmitted when someone uses their remotes to open or close their garage doors. The attackers would then use the recorded signal, simply replay the signal and the garage door would open, as the system does not have any sort of authentication or challenge protocols.

#### *3) Power Analysis Attack:*

Power analysis attacks are a form of side channel attack [4] that specifically targets garage doors with rolling/hopping code instead of dip switches. Attackers would study the power consumption of garage doors or remotes and extract the cryptographic keys and information from the doors or remote [5]. We determined that this was out of the scope of our project and decided to focus on other types of garages and their corresponding attacks.

### *C. Threat Agents*

Now that we know what is at risk and how the vulnerabilities can be exploited, the following is a list of potential threat agents that may take advantages of the vulnerabilities outlined above:

- Thieves
- Kidnappers
- Spies and stalkers
- Assassins and serial killers
- UBC EECE 412 students (mainly Group 8)

### *D. Violations of Secure System Guidelines*

Using the secure system guidelines, we have found that most manufacturers of electric garage door openers violated four of them

#### *1) Complete Mediation:*

Early models of garage door openers did not verify whether the signal that they received was

actually from an authorized user or remote. Any signal, as long as it was the right code, would be accepted.

*2) Open Design:*

Current models of rolling code openers violate the principle of open design as they use proprietary algorithms to implement the rolling code. Some of these proprietary algorithms include Intellicode and Keeloq.

*3) Defense in Depth:*

Garage door openers, especially early models had no defense in depth as they transmit their keys as plaintext and just having the right key would grant anyone access to the garage.

*4) Question Assumptions:*

The first generation of garage door openers violated this principle by assuming that only one key was needed for all garage doors, while the second generation assumed that increasing the number of keys would be enough to increase security. The third assumed that a proprietary algorithm for rolling code would be secure.

## IV. IMPLEMENTATION

After examining the many different technologies implemented by garage door openers, we decided to take a further look at how these manufacturers claimed to keep garage door secure, and whether we could find any vulnerabilities to the most popularly implemented designs. As we saw the average lifetime of garage doors were found to be around 10 to 15 years, [6] the average user is not very likely to replace or upgrade their garage doors unless there is a problem. The third generation implementation of garage door security made the most changes to security measures, but, we believe it is safe to assume that most users will not have this technology implemented on their doors unless their houses were constructed after 2003 or unless they have recently replaced their garage door systems with a newer model as the improved security was not implemented for until after the aforementioned year, and because the average lifetime of garage door openers are so long. We conducted a quick census with our friends who had garage doors on what type of technology or generation their garage door opener used or implemented. We found that out of 12 people with garage doors 6 of them had DIP switch garages. With this information, we decided our assumptions were valid and decided to see if we could develop a device to prove how easily we could bypass the security for the older generation of garages. In our device we implemented a brute force attack where we used the following implements and components to construct the following circuit.

## V. CIRCUIT DESIGN

The design of our circuit will be discussed in this section. Each component in the circuit will be discussed, such as 555 timer, ripple binary counter, and SPDT relay.

### *A. 555 Timer*

The 555 Timer (NE555) acts in the Astable Operation mode where the circuit is made to trigger itself so it does not require an external input to trigger the timer. The frequency of the pulses, as well as the duty cycle of the outputted pulses, depends on either the resistor values or the capacitors [7]. In our device, we determined that the capacitor values should be 1pF and 90uF while the resistor values needed to be 1kΩ with our second resistor being a 20kΩ potentiometer to easily adjust the timer frequency. The 555 timer is the starting point of the entire circuit, this is where the timing or frequency of the codes are triggered. The output is then sent to the 12-bit binary counter.

### *B. 12-bit Ripple Carry Binary Counter*

The input of the 12-bit binary counter comes from the 555 timer. The 12-bit binary counter then uses this input as a trigger so that the state of the counter advances one count on the negative transition of each input pulse [8]. The values are incremented so that the output goes from the 0 to $2^{12}$. In other words, it goes through all the possible combinations to determine the actual garage door key, hence a brute force attack. This is only possible because the key is static and would not change unless the owners themselves change it. The output is then sent to both the LED array and the single pole double throw relays.

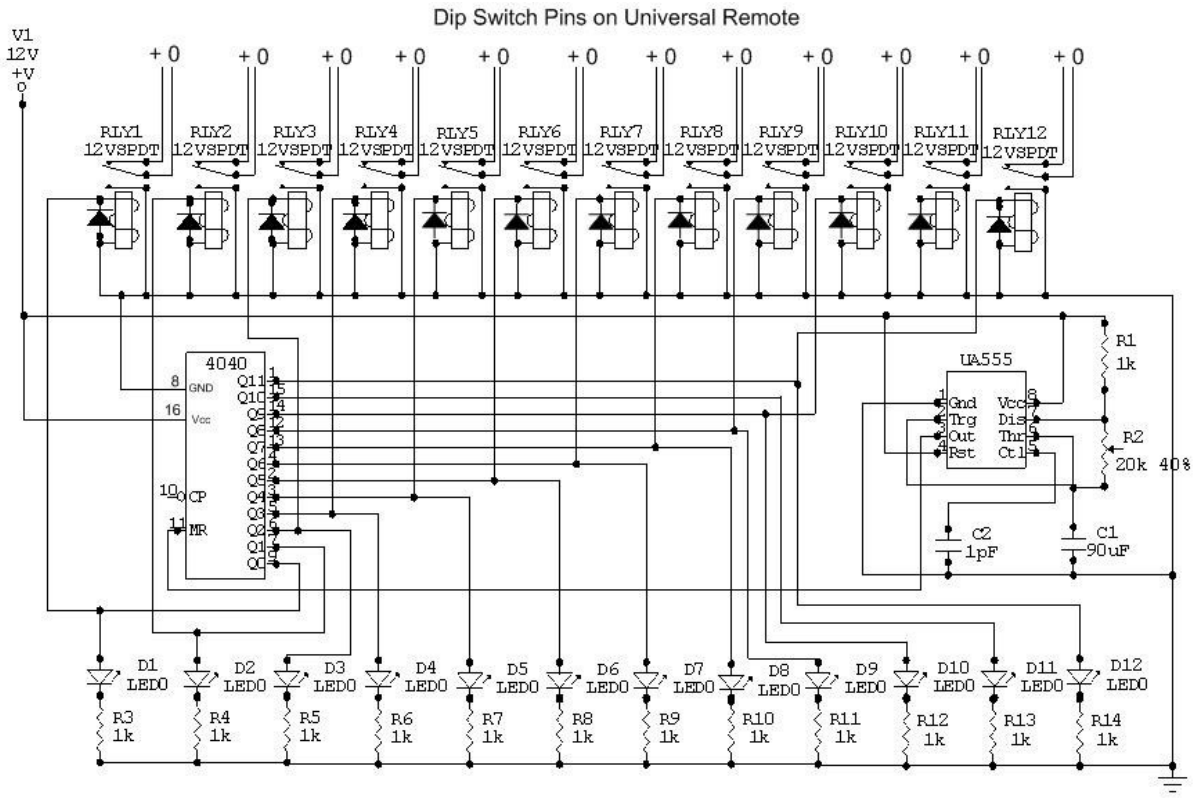


Figure 1. Schematic of our circuit.

### *C. LED Display Array*

This LED array is used more for our convenience to ensure that the output of the binary counter can be easily displayed so we can determine if the values are being incremented sequentially and at what pace, or even the fact that the binary counter is incrementing the values at all. The LED display also lets us know what code opens the garage.

### *D. Single Pole Double Throw (SPDT) Relay*

This is used as a switching mechanism for each bit of the key or combo that is being toggled either to a high or low. The relay acts similar to the LED array, as it is connected directly to the output of the binary counter so that the relays also switch corresponding to the value that displayed on the LED array. The binary counter will send the appropriate output through the SPDT relay to the universal remote.

### *E. Universal Garage Remote*

The universal garage remote is a store bought proprietary device, it is used as an RF device to transmit the key under test to the garage door receiver. We determined first how the pins on the device worked so the corresponding input could be detected by the device as the correct predetermined key. Once that was determined, the device was connected to our constructed circuit (see Figure 1.) so that the input can be generated and relayed through the universal garage remote.

Using this device, and testing on two garage doors, we were able to crack them at an average of 12 minutes for one door and 30 minutes for the other when transmitting a different key every two seconds.

## VI. COUNTERMEASURES

We propose a number of countermeasures to increase the safety of residential garages against the risk analysis we summarized in the earlier section. Homeowners should be informed on the security garage doors provide, as garages are not as well protected and safe as they may be lead to believe.

Higher levels of security for electric garage door openers can be achieved by purchasing models with the latest security technology, extending the alarm and security systems to cover the garage, and mounting motion detecting lights on the garage. In addition, a remote lockout feature would provide the ability to turn off the radio receivers on the openers

when homeowners leave their houses for work or vacation. Furthermore, a biometric system can be introduced to the garage door openers. Instead of entering and leaving the garages with remote controls, fingerprint sensor technology provides the ability to distinguish strangers from homeowners and ensures a more secure garage.

Countermeasures against garages being broken into are easy to implement and should follow defense in depth in the secure system guidelines. Homeowners should avoid storing valuables in the garage. In other words, they should use the garage to only house their vehicles.

Homeowners can increase the safety level of the vehicles parked in their garage by installing alarm and immobilizer systems, and always setting those systems. Moreover, they should consider the security of doors in the garage that are linked to the house as important as the front doors, or any doors that serve as outside entrances. The garage doors linked to the houses should be built more securely with more robust locks. Most importantly, the garage doors linked to the houses should always be locked.

## VII. DISCUSSIONS AND CONCLUSIONS

Improvements to our circuit can be made to improve on the speed of our brute force attack. We could have programmed our circuit using a PIC (Programmable Interface Controller) or FPGA (Field- Programmable Gate Array) and transmitting that signal with a simple transmitter instead of building a circuit physically and using a universal remote as our transmitter. This would remove a lot of circuitry bugs and errors that we encountered during the construction of our circuit. It would also allow us to speed up the process of counting through all the possible combinations and therefore decrease the time needed to crack open the garage door.

Despite the fact that the functionality of our circuit design can still be improved, our circuit is capable of breaking most garages with dip switches. Homeowners need to be aware of the vulnerabilities of their garages and take necessary precaution against the potential threats.

## REFERENCES


[1] Maitam, Martial. (2005, June 16). History of Garage Door Openers. *Searchwarp.com*. Retrieved on Dec. 3, 2009 from the World Wide Web: http://searchwarp.com/swa9610.htm

[2] Brain, Marshall. (2001, Aug. 15). How Remote Entry Works. *HowStuffWorks, Inc*. Retrieved on Dec. 4, 2009 from the World Wide Web: http://auto.howstuffworks.com/remote-entry.htm

[3] Francis, Paul L. (2005, Dec. 1). Potential Spectrum Interference with Military Land Mobile Radios. *The U.S. Government Accountability Office*. Retrieved on Dec. 4, 2009 from the World Wide Web: http://gao.gov/products/GAO-06-172R

[4] Wikipedia, the Free Encyclopedia. (2009, May 20). Power Analysis. *Wikipedia, the Free Encyclopedia*. Retrieved on Dec. 2, 2009 from the World Wide Web: http://en.wikipedia.org/wiki/Power_analysis

[5] Eisenbarth, Thomas. Et al. (2008 Feb. 2). Physical Cryptanalysis of Keeloq Code Hopping Applications. *p.7-9*.

[6] Jackson, Jackie. Et al. (2007, Feb.). Study of Life Expectancy of Home Components. *National Association of Home Builders / Bank of America Home Equity. p.4*.

[7] Texas Instruments. (2008, Mar.). NE555 Precision Timers. *Texas Instruments Incorporated. p.1, 10-11*.

[8] Philips Semiconductors. (2005, Sept. 14). 74HC4040 12-Stage Binary Ripple Counter Product Data Sheet. *Koninklijke Philips Electronics. p.1, 4, 6*.