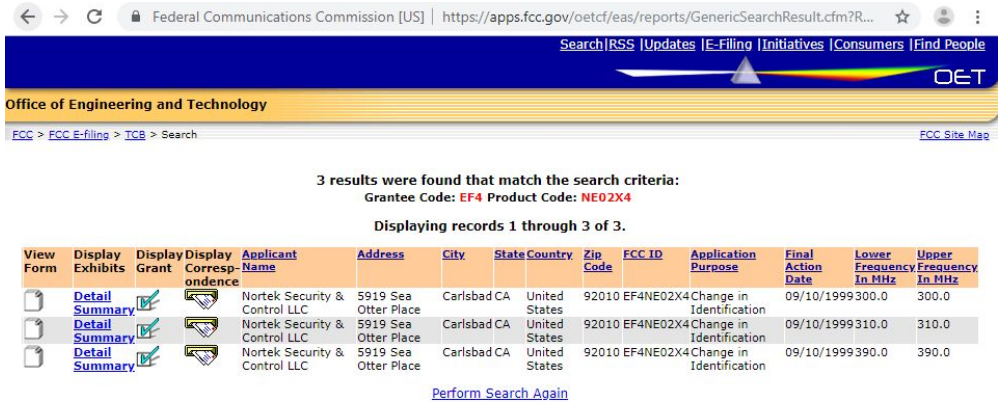
Hacking Wirelessly-Controlled Gates/Garages using Software Defined Radio

UCLA ECE209AS - Final Project

By: Won Ho Chung / Hailin Yu

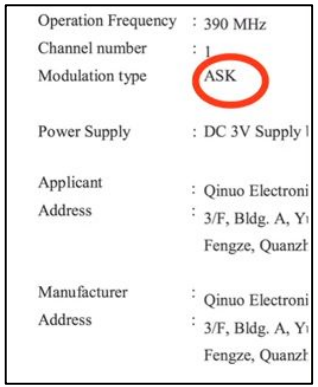
How Does Remote-Controlled Gates Work?



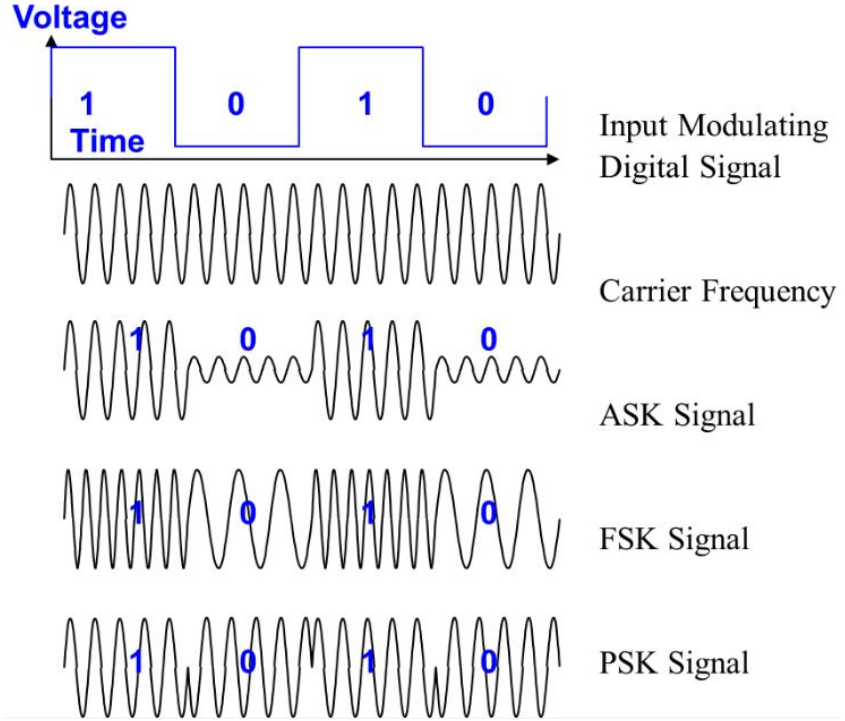
Modulation Scheme

- For digital signals, three main modulation techniques
  - Amplitude Shift Keying (ASK)
  - Frequency Shift Keying (FSK)
  - Phase Shift Keying (PSK)

Test Report



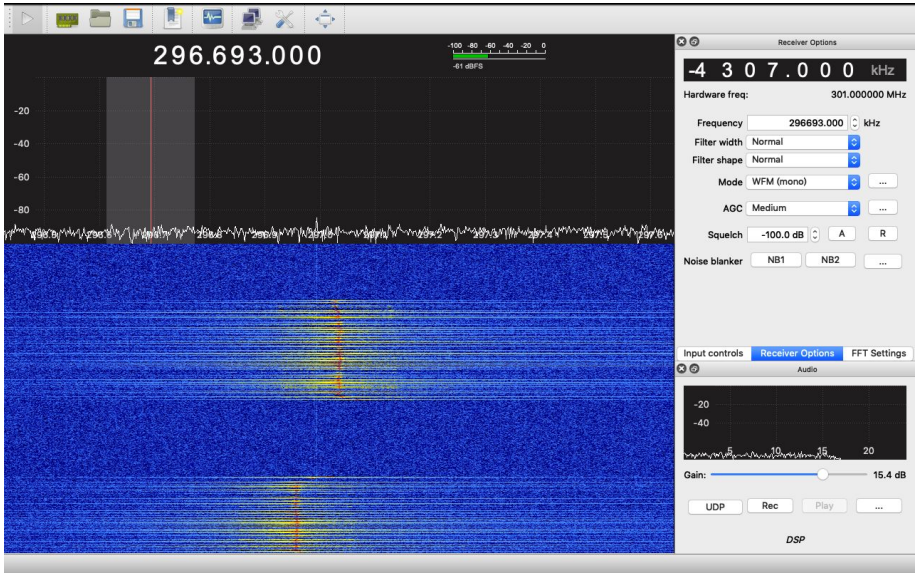
Operation Frequency	: 390 MHz
Channel number	: 1
Modulation type	: ASK
Power Supply	: DC 3V Supply
Applicant	: Qinuo Electroni
Address	: 3/F, Bldg. A, Y
	Fengze, Quanzh
Manufacturer	: Qinuo Electroni
Address	: 3/F, Bldg. A, Y
	Fengze, Quanzh



Tools for Implementation

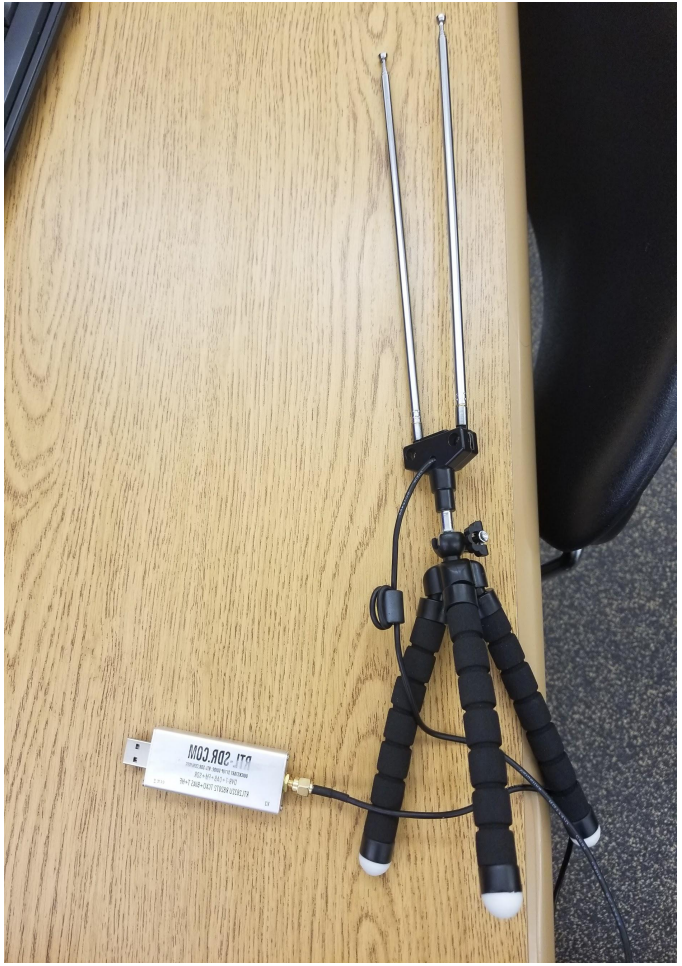
GQRX

- Open source software defined radio (SDR)
- Linux & OS X compatible
- Supported devices (e.g. rtl-sdr, HackRF, Airspy, Funcube Dongles, and many more)
- Features
  - FFT plot and waterfall view
  - record/playback audio to WAV file
  - Record I/Q raw data
  - demodulation

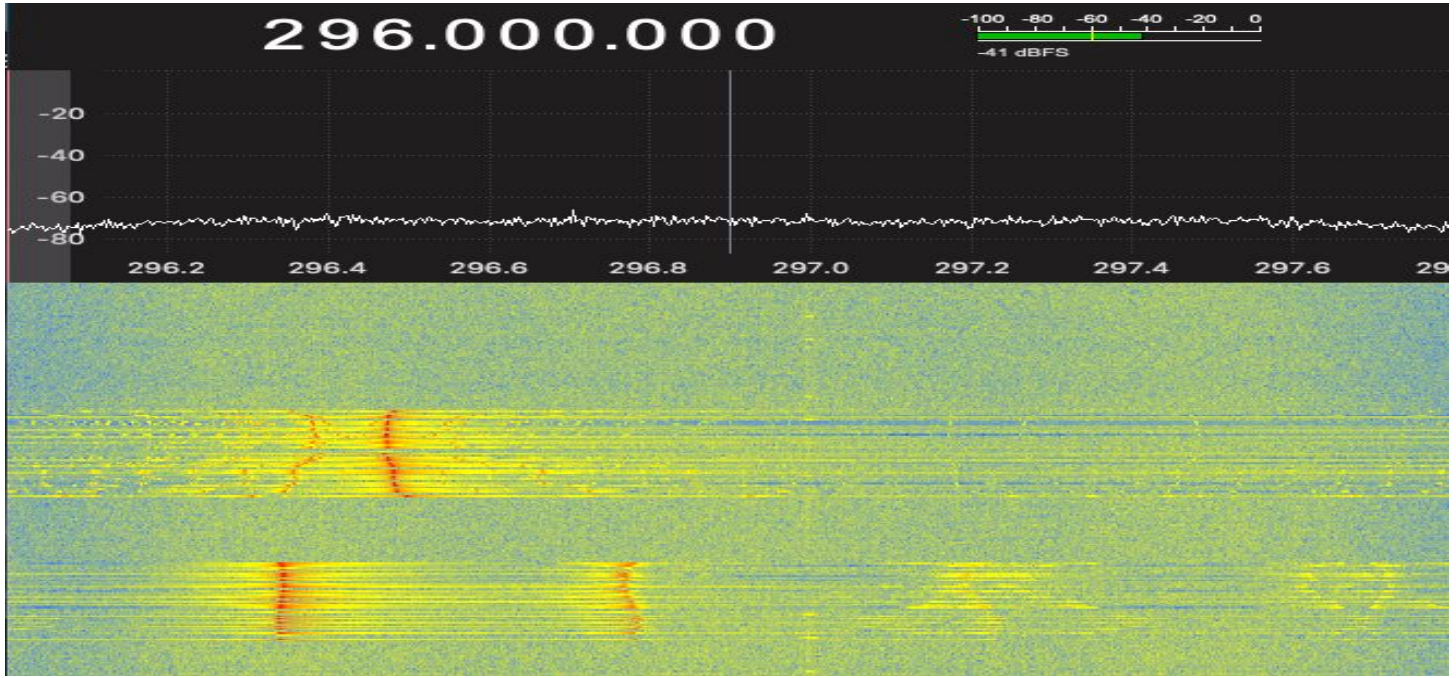


RTL-SDR

- Can only receive signal
- 24 - 1766 MHz
- Cheap (about $20)
- Raw I/Q samples



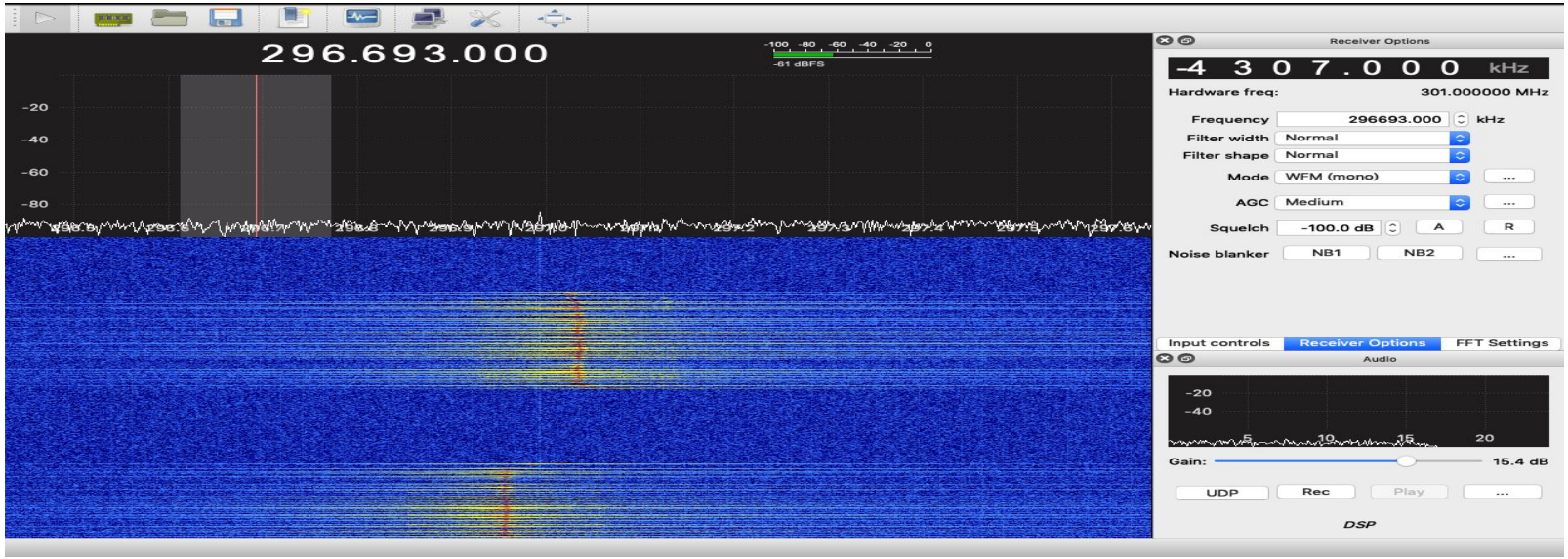
RTL-SDR on GQRX



HackRF One

- Can both receive/transmit signal
- 1MHz - 6GHz
- Expensive(about $300)
- Raw I/Q samples
- Open source software

HackRF One on GQRX



Identifying Code

- 10 bits
- The total possible combination
  - 2^10 = 1024
- Right key: xxxxxxxxxx
- Left key: yyyyyyyyyy

(actual key combination has been removed for security reasons)

Decoding Signal

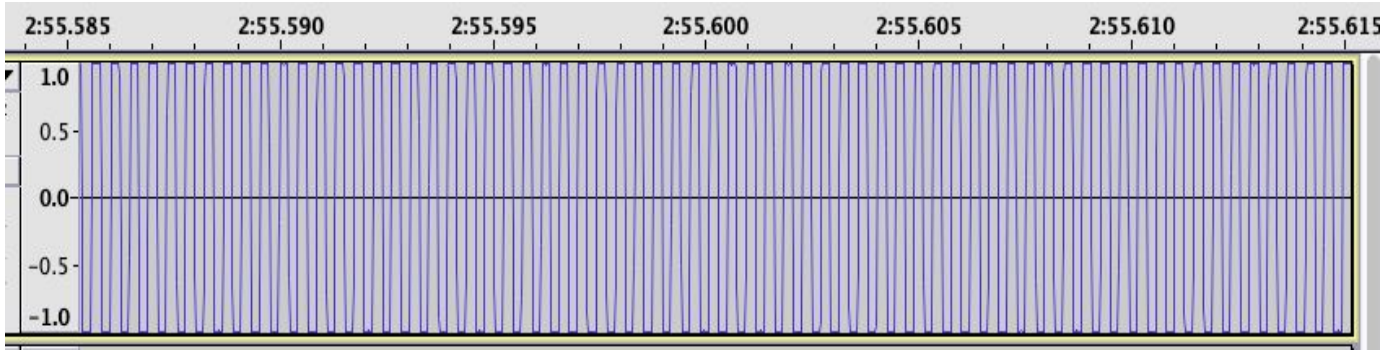
Left key:zzzzzzzzzz

(actual screenshot of signal wave files has been removed for security reasons)

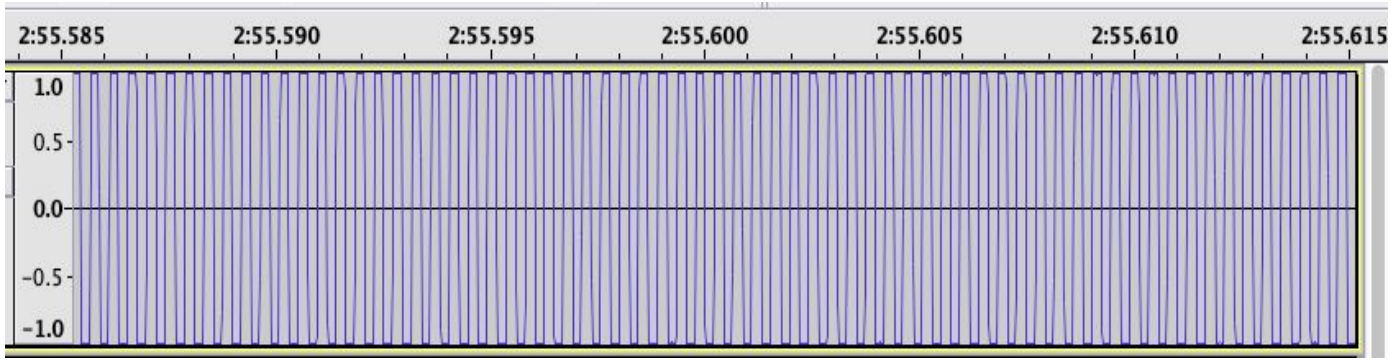
Right key:xxxxxxxxxx

Expand

Short(0)



Long (1)



Implementation Results

HackRF information

```
hailindeMacBook-Air:~ yhltc$ hackrf_info
hackrf_info version: unknown
libhackrf version: unknown (0.5)
Found HackRF
Index: 0
Serial number: 0000000000000000087c867dc2a8b685f
Board ID Number: 2 (HackRF One)
Firmware Version: 2018.01.1 (API:1.02)
Part ID Number: 0xa000cb3c 0x00574f64
```

Record and transmit by HackRF

#record hack_transfer -r test.bin -f 297000000 -b 10000000

#transmit hack_transfer -t test.bin -f 297000000 -b 10000000

```
[hailindeMacBook-Air:~ yhltc$ hackrf_transfer -r right.bin -f 297000000 -b 100000
00 -g 62
call hackrf_set_sample_rate(10000000 Hz/10.000 MHz)
call hackrf_baseband_filter_bandwidth_set(10000000 Hz/10.000 MHz)
call hackrf_set_freq(297000000 Hz/297.000 MHz)
Stop with Ctrl-C
19.9 MiB / 1.001 sec = 19.9 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
20.2 MiB / 1.004 sec = 20.1 MiB/second
19.9 MiB / 1.004 sec = 19.8 MiB/second
^CCaught signal 2
 5.2 MiB / 0.254 sec = 20.6 MiB/second
```

Garage 1 Configuration

- RX antenna exposed

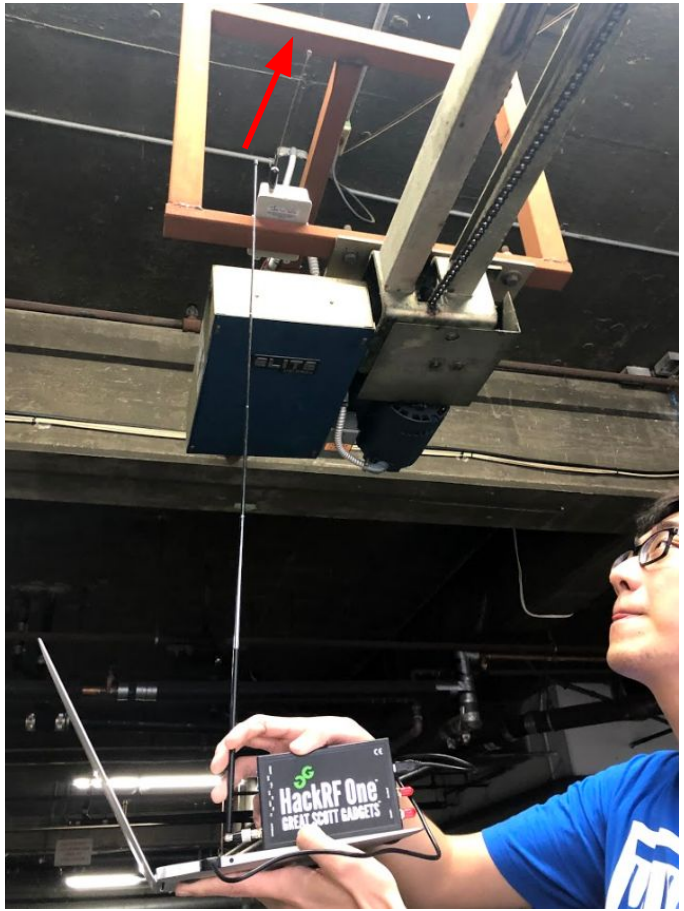
- Vertical opening structure

Testing Result (Garage 1)

- Opening the garage 1 successed! BUT...
- Transmitting antenna (HackRF) must be very close with the garage door's receiving antenna
- About **~ 10 cm** (as shown on the figure)

VS

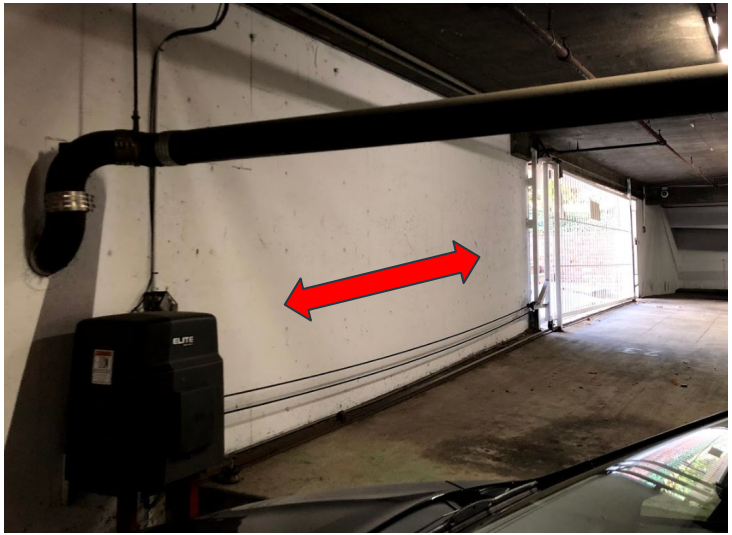
- About **500 cm** (with original remote control)



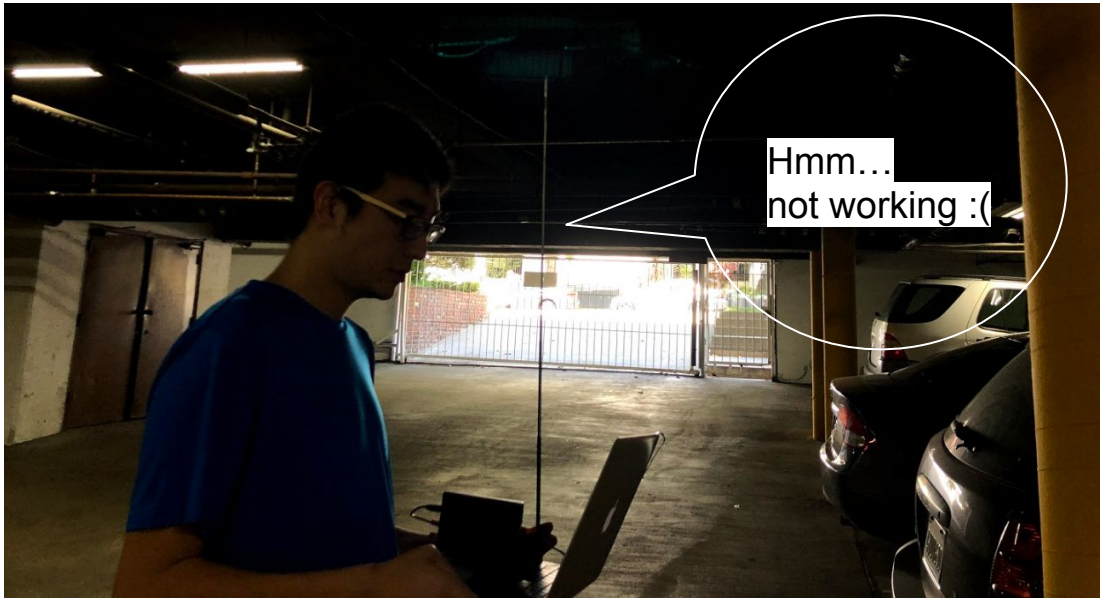
Garage 2 Configuration

- RX antenna hidden

- Horizontal opening structure



Testing Result (Garage 2)



Increasing the Distance

#record

```
hack_transfer -r test.bin -f 297000000 -b 2000000 -g 62
```

#transmit

```
hack_transfer -t test.bin -f 297000000 -b 2000000 -x 47
```

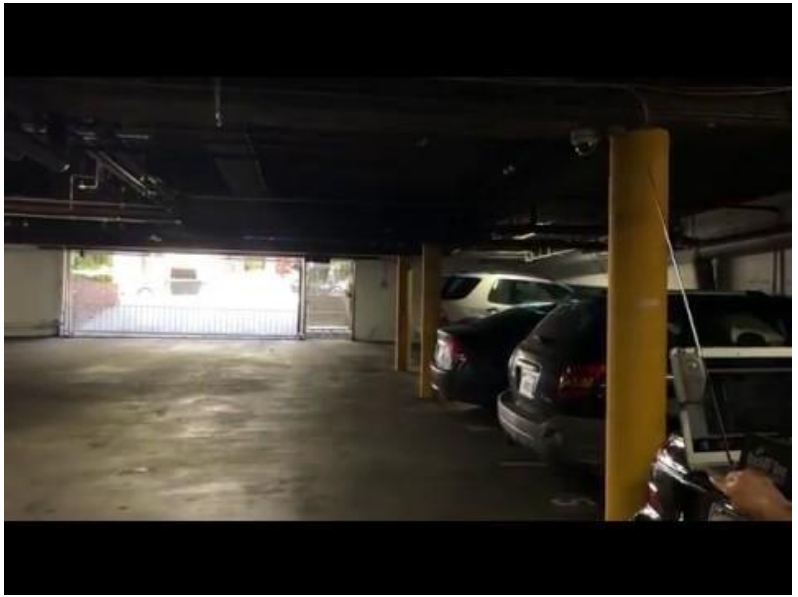
Improved Performance

Garage 1

Garage 2

Testing Outside of Garage 1

Testing Inside of Garage 2



Concluding Remarks

Future Work/Improvements

- Main drawback
  - Need to wait nearby and record all the time until some people presses the key
  - The average waiting time should be 10-15 minutes during daytime
  - You need a 10G recording file!

What If We Brute Force Attack?

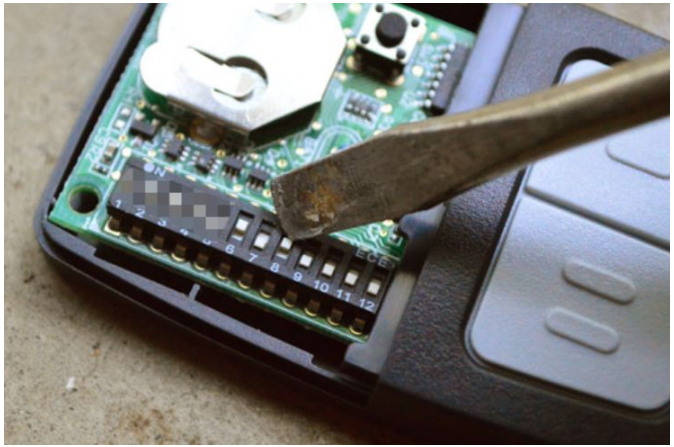
How long does it take?

- 10 bit code
- ~2ms per bit + ~2ms delay
- 5 signals per transmission

((2 ** 10)*10) = **10240bits**

10240 bits * (2ms signal + 2ms delay) * 5 transmissions = 204800ms = 204 secs = **3.3minutes**

Throw away delay and repeat: **20s**



Lessons

- Don't use a small key space
- Require a preamble word for beginning of each key
- Use more complex encoding methods
- Have deadlock device installed when leaving the home for a while

Acknowledgement

ECE 209AS - Security and Privacy for Cyber-Physical Systems, IoT (Spring ‘19)

- Professor: Mani Srivastava

References

[1]https://www.youtube.com/watch?v=1RipwqJG50c

[2]https://www.youtube.com/watch?v=BnwBdeQB7vQ

[3]http://samy.pl/dingdong/

[4]https://www.youtube.com/watch?v=iSSRaIU9_Vc

[5]http://samy.pl/opensesame/

[6]https://www.itstactical.com/intellicom/physical-security/how-to-hack-a-garage-door-in-under-10-seconds-and-what-you-can-do-about-it/

References

[7]https://www.youtube.com/watch?v=CyYteFilozM&feature=youtu.be

[8]https://cafe.naver.com/hackrf/6

[9]https://www.jeffreythompson.org/blog/2015/10/11/sdrhackrf-one-mac-setup-and-basics/

[10]https://k1fm.us/2014/08/i-finally-got-my-hackrf-and-i-have-a-mac-now-what/

[11]https://wiki.gnuradio.org/index.php/MacInstall

[12]https://wiki.gnuradio.org/index.php/GNURadioCompanion

Thank you