# Garage Door Hacking

Trevor Kems

# # whoami

- Trevor Kems
  - Penetration Tester at Waterleaf Internati
    - B.S. in Cyber Security Engineering from ISU
    - OSCP in Aug. 2022
  - Hardware hacking and reverse engineer
  - Collects and restores vintage computers

All opinions during this presentation are my own and not of my current or former employer(s).

# Disclaimer

- I am not a lawyer, and this is not legal advice. Transmitting on certain frequencies may be illegal or have restrictions. Check your local laws and regulations *before* transmitting. All transmissions conducted during the research and in this presentation occurred at low power, for short time periods, and followed FCC regulations.
- All information in this presentation is to be used for educational use only and not intended to be used in an unlawful manner.
- I am not associated with The Chamberlain Group and all Trademarks, Word marks, and images are property of their respective owners.

# Are Garage Door Openers Secure?

ANDY GREENBERG SECURITY JUN 4, 2015 7:00 AM

## This Hacked Kids' Toy Opens Garage Doors in Seconds

Security researcher Samy Kamkar can crack some garages' laughable safeguard codes in seconds, with little more than a hacked child's toy.


https://github.com/samyk/opensesame

ANDY GREENBERG SECURITY AUG 6, 2015 9:00 AM

## This Hacker's Tiny Device Unlocks Cars And Opens Garages

The $32 radio device, smaller than a cell phone, is designed to defeat the "rolling codes" security used in not only most modern cars and trucks' keyless entry systems, but also in their alarm systems and in modern garage door openers.

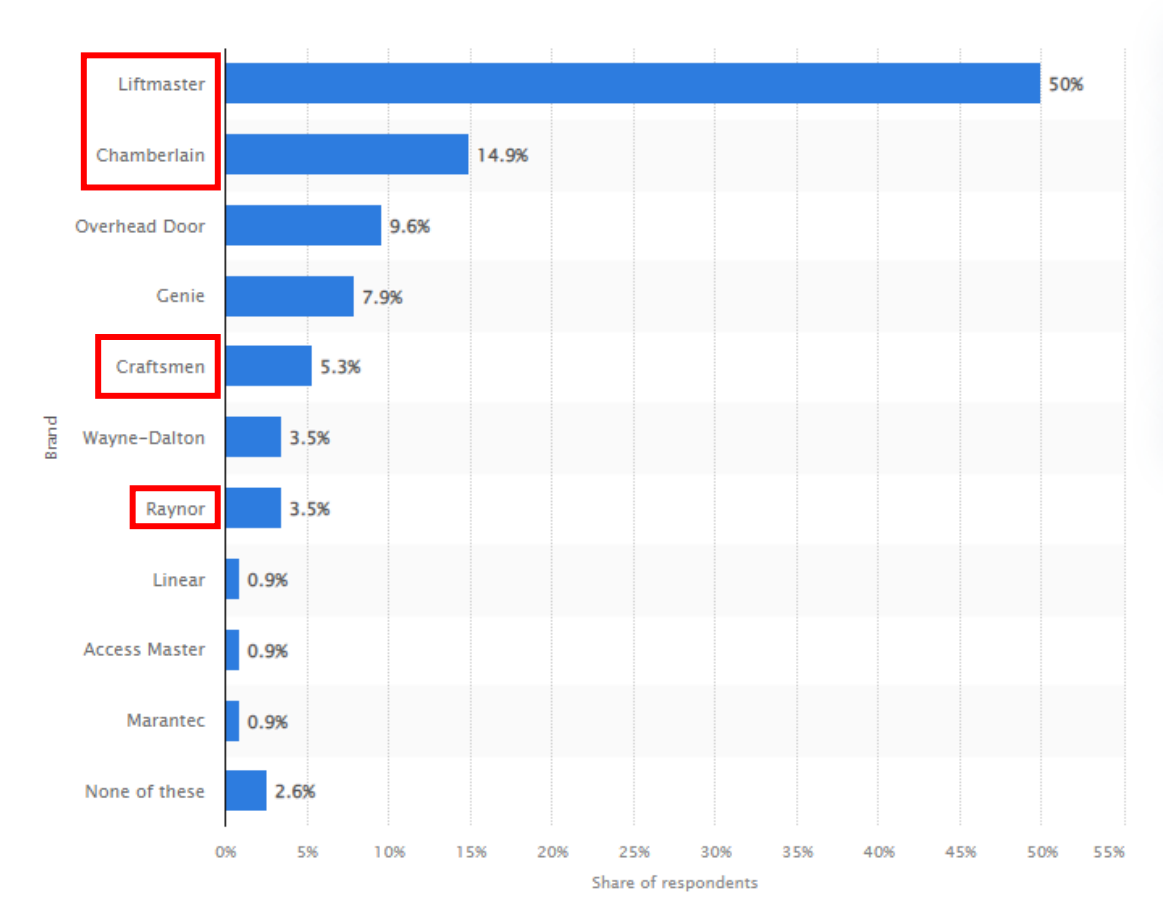
# The Chamberlain Group (CGI)

- Parent/Owner of:
  - LiftMaster, Chamberlain, Craftsman, Merlin, and more garage door opener brands.
  - Security+ and Security+ 2.0 Protocols
  - MyQ (Smart/IoT)
  - Access control systems/Gates

https://chamberlaingroup.com/our-brands/

Image of Chamberlain Group's headquarter in Illinois (CC 4.0, Original Image)
https://en.wikipedia.org/wiki/File:Chamberlain_Group_global_headquarters.jpg

# Garage door openers used the most by construction firms in the United States in 2018




https://www.statista.com/statistics/472288/most-used-garage-door-opener-brands-in-the-us/

# History of Garage Door RF Security

- Invented in 1931 by 2 different teams
- Popularized in the 1970’s
- 1984-1993: DIP switches
- 1993-1997: Billion Code
- 1997-Present: Security+
- 2011-Present: Security+ 2.0


https://spectrum.ieee.org/the-consumer-electronics-hall-of-fame-liftmaster-garage-door-opener
https://books.google.com/books?id=3ScDAAAAMBAJ&pg=PA32#v=onepage&q&f=false
https://en.wikipedia.org/wiki/Garage_door_opener

https://www.amazon.com/Allstar-1-Button-Control-Transmitter-190-109391/dp/B07ZRT61CQ

# Remotes






https://www.liftmaster.com/wireless-garage-door-keyless-entry-system/p/G877LMMC

https://www.liftmaster.com/893max-universal-gate-and-garage-door-opener-remote/p/G893MAXMC

Various product images are from: https://www.liftmaster.com/accessories/c/garage-door-opener-remotes#tab=products

# Security+ and Security+ 2.0

- “Encrypted” rolling code system introduced in 1997
- Not supported by newer openers but supported remotes are still sold
- Phased out after Security+ 2.0 roll out in 2011

**Prevention:** If you are using a gate or garage which uses "fixed codes", to prevent this type of attack, ensure you upgrade to a system which clearly states that it's using **rolling codes, hopping codes, Security+ or Intellicode**. These are **not** foolproof from attack, but do prevent the OpenSesame attack along with traditional brute forcing attacks. Suggested vendors: current products from LiftMaster and Genie.

https://samy.pl/opensesame/

## Rolling Code Technology and how it works

Rolling code technology

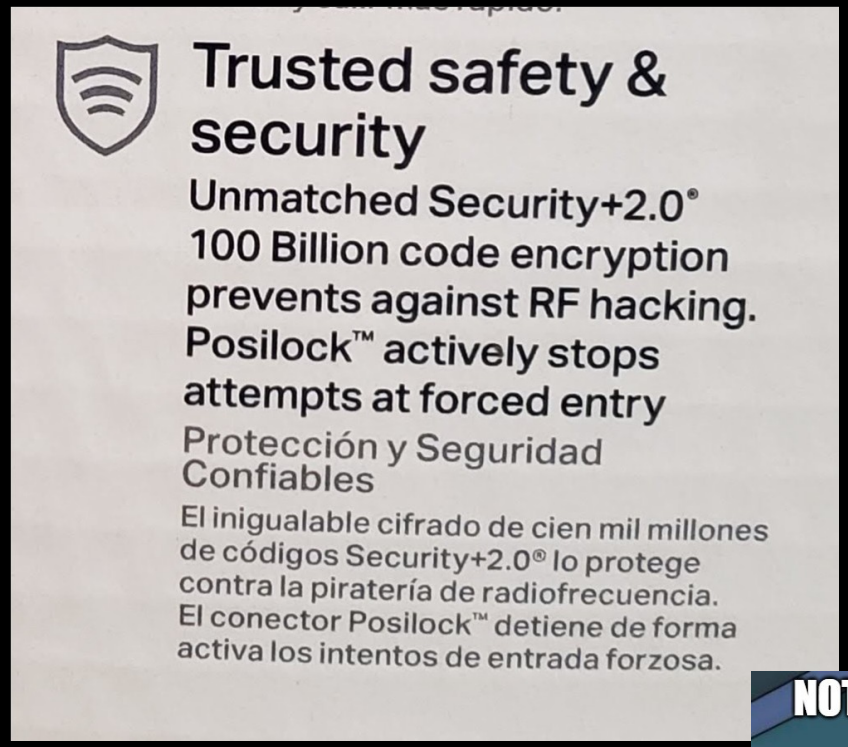
Chamberlain strives to continually raise industry standards in security, safety and convenience. As technology advances, we continue to improve our products and increase security measures.

One advancement is rolling code technology. Rolling code protects against intruders by generating a new security code every time the remote control is used on your garage door opener.

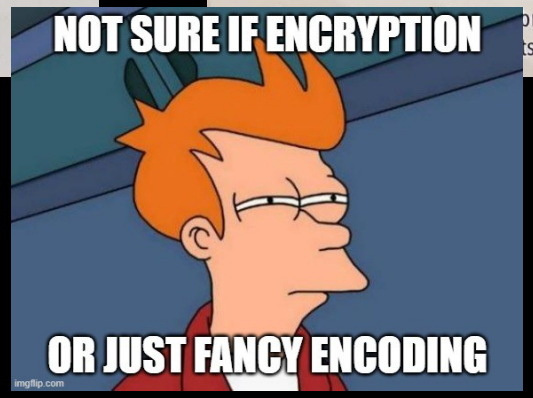
When the remote control activates the garage door opener, a unique algorithm "rolls" the remote control's code to one of more than 100 billion possible codes. The previously used code will be discarded, and the opener will only to respond to the new code the next time the remote control is used. The same code will never be used more than once. Stolen codes are useless to intruders.

https://support.chamberlaingroup.com/s/article/What-is-rolling-code-technology-and-how-does-it-work-1484145611618

# “Encryption”


Trusted safety & security
Unmatched Security+2.0®
100 Billion code encryption prevents against RF hacking.
Posilock™ actively stops attempts at forced entry
Protección y Seguridad Confiables
El inigualable cifrado de cien mil millones de códigos Security+2.0® lo protege contra la piratería de radiofrecuencia.
El conector Posilock™ detiene de forma activa los intentos de entrada forzosa.


Control 1 Garage Door or Gate
Control 1 puerta o garaje de la puerta
BILLION CODE ENCRYPTION
Keeps your remote codes secure from hacking and your family safe.
CIFRADO CON MIL MILLONES DE CÓDIGOS
Mantiene los códigos de control remoto seguros de ataques y a su familia a salvo.
WALK IN OR LOCK UP WITHOUT A KEY
Entre a pie o cierre sin usar una llave
Look for our Wireless Keypad
Buscar nuestro teclado numérico inalámbrico
Compatible with all Chamberlain®, LiftMaster® and most Craftsman® garage door openers manufactured after 1993 with safety sensors.
pre-puertas de garaje Chamberlain®, LiftMaster® y la mayoría de los
tsman® fabricados a partir de 1993 con sensores de seguridad.


NOT SURE IF ENCRYPTION
OR JUST FANCY ENCODING
imgflip.com

# SecPlus (GitHub)

- Created by Clayton Smith after reverse engineering the Security+ and Security+ 2.0 protocols. Uses GNU Radio with support for HackRF One.

- https://github.com/argilo/secplus

# Security+ “Encryption”

- Rolling codes used to prevent simple relay attacks
- Transmitted in 2 packets with 20 payload bits each for 40 total payload bits
- Trinary system with symbols 0,1,2 with 3 being invalid.
- Fixed data: Remote ID, button, pin. Max 3^20
- Rolling data: Max 2^32 and increases by 2 each button press

# Security+ 2.0 “Encryption”

- Manchester encoding and bit operations
- 2 packets with 40 payload bits each
- Rolling: 2^28 max. Increases by 1 each press
- Fixed: 2^40 max
- Bits are interleaved

# Attacks

## DoS

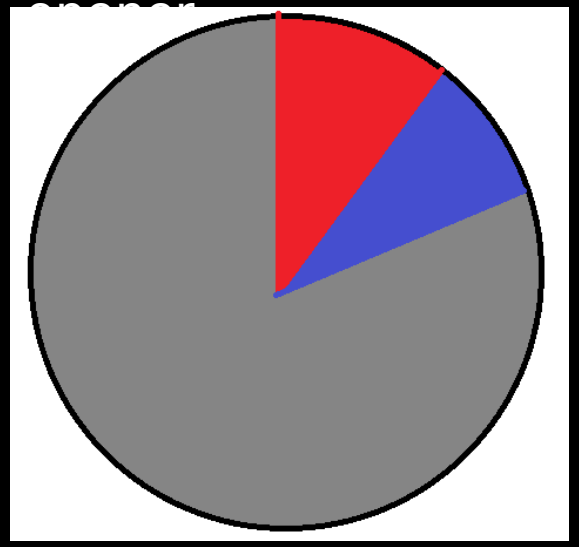
- Transmit code 1024 ahead of current value
- Remote can’t be used until paired again or button clicked ~512/1024 times

## Persistent Replay

- Once any code is captured, the remote cannot be reset
- Remote becomes ‘useless’ and must be forgotten to secure an opener

## Rolling Bruteforce

- If the fixed code (i.e. serial number) is known, the rolling code can be brute forced
- Fairly impractical due to key space (3^20 or 2^28) but possible



Red: Valid
Blue: Resync
Gray: Invalid

# Mitigations

- Lock button, camera, MyQ, monitoring…
- Stop using remotes that may be captured
- Vote with your wallet! Look for encrypted systems
- Lock the door between your house and garage
- Look into monitoring RF for ‘rouge’ remote transmissions

# Tools

## Flipper Zero

- ~$200
- Capture Security+/2.0 but can’t make custom remotes from known codes without custom firmware


https://shop.flipperzero.one/

## HackRF One

- ~$300-$400
- Huge frequency range and bandwidth for the money
- Lots of support
- Portapack


https://greatscottgadgets.com/hackrf/one/

## DIY

- ~$20-25
- Off-the-shelf parts, no soldering
- Limited frequency range (sub-GHz)
- Requires some knowledge to setup

# DIY Hardware

- ESP32 (~$10)
  - Cheap Wi-Fi dev board
  - Widely supported

- CC1101 Radio Module (~$5-10)
  - Popular Texas Instruments (TI) chip
  - Breakout board with antenna
- Dupont Jumper Kit

https://www.amazon.com/HiLetgo-ESP-WROOM-32-Development-Microcontroller-Integrated/dp/B0718T232Z

https://www.amazon.com/CC1101-Wireless-Transceiver-915MHZ-Antenna/dp/B01DS1WUEQ

# RFQuack – The software

- Build an “SDR” without the SDR!
- Abstracts the radio module while still allowing low level register access
- iPython shell over serial or MQTT

- https://github.com/rfquack/RFQuack

# Flash and Configure

- Follow the steps to flash your ESP32 with RFQuack
- Connect the CC1101 board to your ESP32
  - Take care to examine the pinout of each to make sure everything is correct
- Set the radio module settings once connected to the Python CLI
  - Set the freq, modulation, and bitrate
  - Set the packet length
  - Enable Manchester hardware decoding
  - Receive!

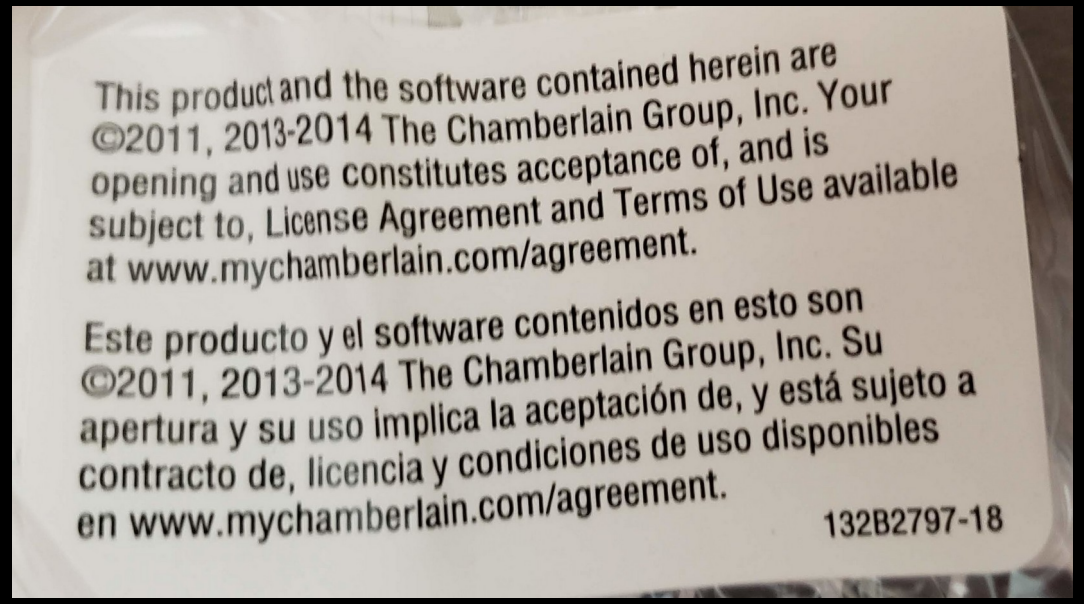
```
Set modem config

q.radioA.set_modem_config(modulation="OOK",
                    ...: carrierFreq=315.00,
                    ...: bitRate=4.0,
                    ...: useCRC=False,
                    ...: syncWords=b"")


Set packet length

q.radioA.set_packet_len(isFixedPacketLen=True,
                    ...: packetLen=50)

Get register

q.radioA.get_register(int("0x12",16))


Set register

q.radioA.set_register(address=int("0x12",16), value=int("0bXXXX1XX",2))


Set RX

q.radioA.rx()
```

# Decode Data

Manually decode the packet data with the help of secplus and a short Python script (https://github.com/TKems/Garage-Door-Hacking)

- Use secplus or GNU Radio to generate the next code and transmit to open the garage door (Using HackRF to transmit)

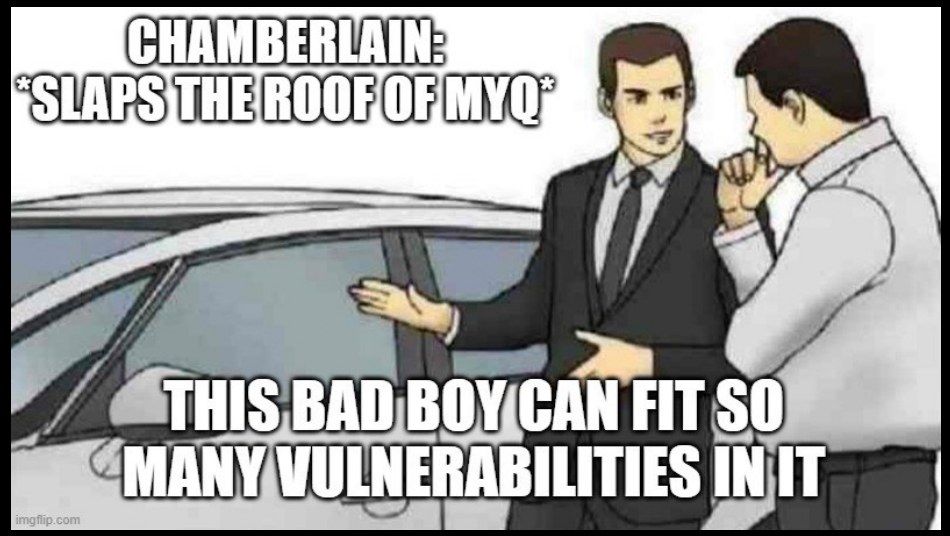
# MyQ



This product and the software contained herein are ©2011, 2013-2014 The Chamberlain Group, Inc. Your opening and use constitutes acceptance of, and is subject to, License Agreement and Terms of Use available at www.mychamberlain.com/agreement.

Este producto y el software contenidos en esto son ©2011, 2013-2014 The Chamberlain Group, Inc. Su apertura y su uso implica la aceptación de, y está sujeto a contracto de, licencia y condiciones de uso disponibles en www.mychamberlain.com/agreement.

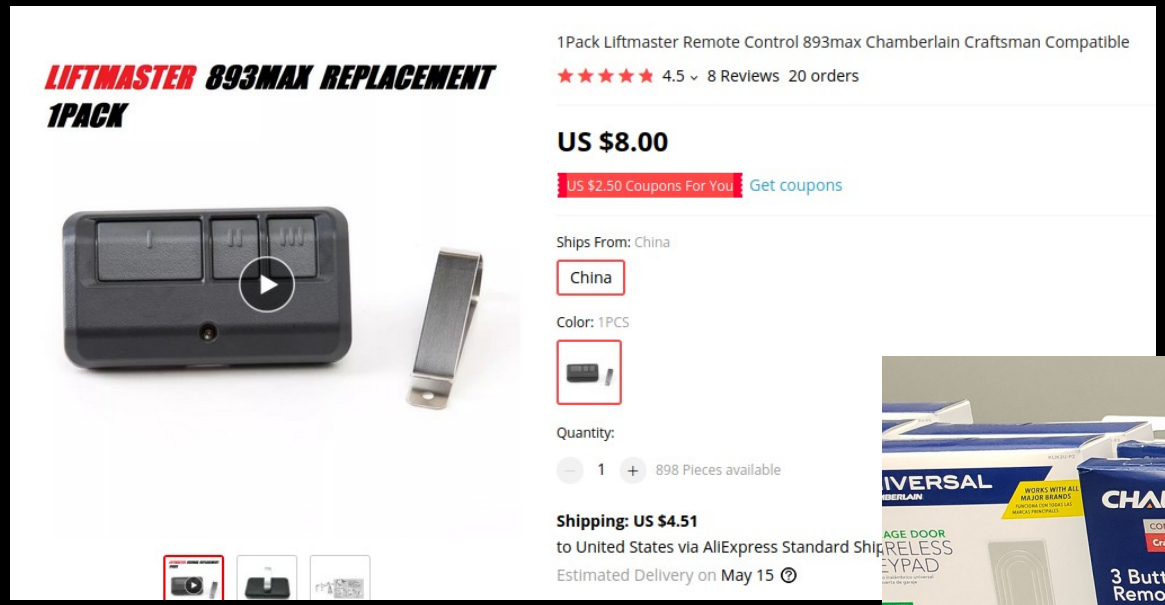
132B2797-18




Part VIII, Section 3,

F. You agree to not reverse engineer, perform penetration testing, or otherwise attempt to identify vulnerabilities in the MyQ System without our prior written approval. Please contact us at technicalsupport@chamberlain.com to arrange a discussion of your desire to perform any such testing. Your email should provide your contact information and the purposes for such testing. If we do not respond, we will be deemed to have rejected your request.

# Remote Pricing





# Future Work

- Implement auto decode within RFQuack with a custom module
- Implement transmitting Security+/2.0 packets using RFQuack
- Investigate even cheaper ways to RX/TX
- Would this work with rpitx? (https://github.com/F5OEO/rpitx)

# Other Articles and Links

- MyQ RF Door Sensor Security Issues
  - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/we-be-jammin-bypassing-chamberlain-myq-garage-doors/

# Questions?