

Breaking Learning Codes

How I discovered that I can unlock thousands of cars in my country

By Danilo Erazo

DEFCON 32 - 2024

Prepared for the Car Hacking Village

$Whoami: Danilo Erazo

Hobbie: Car/Hardware Hacking Researcher

Work: Penetration Tester (Web, Mobile, Infrastructure) at Fluid Attacks

First Steps in hacking: Hackem

Speaker: BSides Colombia, Ekoparty, Nerdearla

Malware Analyst/Forensics, Developer

Electronic & Systems Engineer

Ecuador

Certifications: OSWP, CEH, CBP, CCSP, CPAZ, CNSP, CAP, CPNA, CCNA, API Security for Connected Cars and Fleets, PJIT, others.



revers3everything@gmail.com

@revers3everything

@revers3everything

in/reverse-everything/

in/danilo-erazo/

DISCLAIMER



Hacking is illegal and should not be performed. This presentation does not condone or approve of hacking in any way. Automotive Security is an agreed form of audit between two parties and should be bound in writing defining the scope and nature of what is to be audited. This presentation is solely for academic and educational purposes only.



Agenda

1) Introduction
2) Radiofrequency Hacking
3) Hardware Hacking
4) Brute Force Learning Codes
5) Discovering/Setting Backdoor in KES
6) Identified Vulnerabilities
7) Exploiting Everything



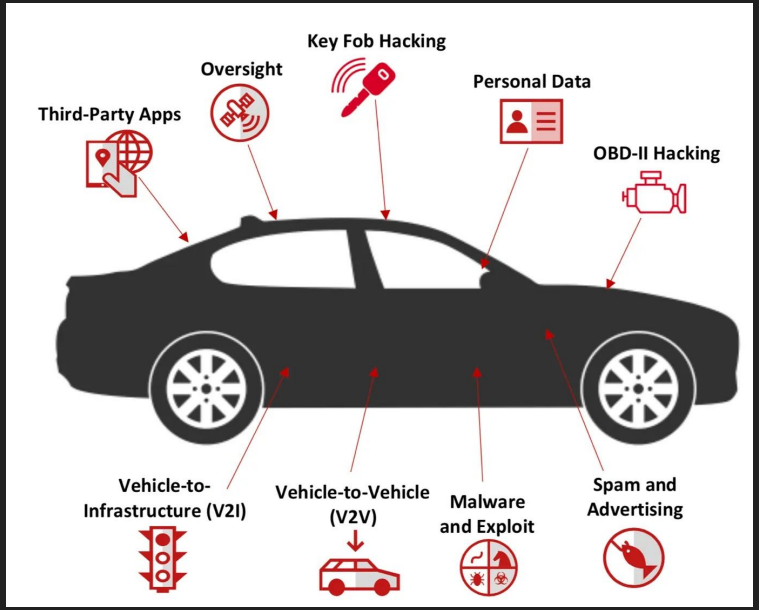
1
Introduction

I was trying to hack a 2023 car in every way possible

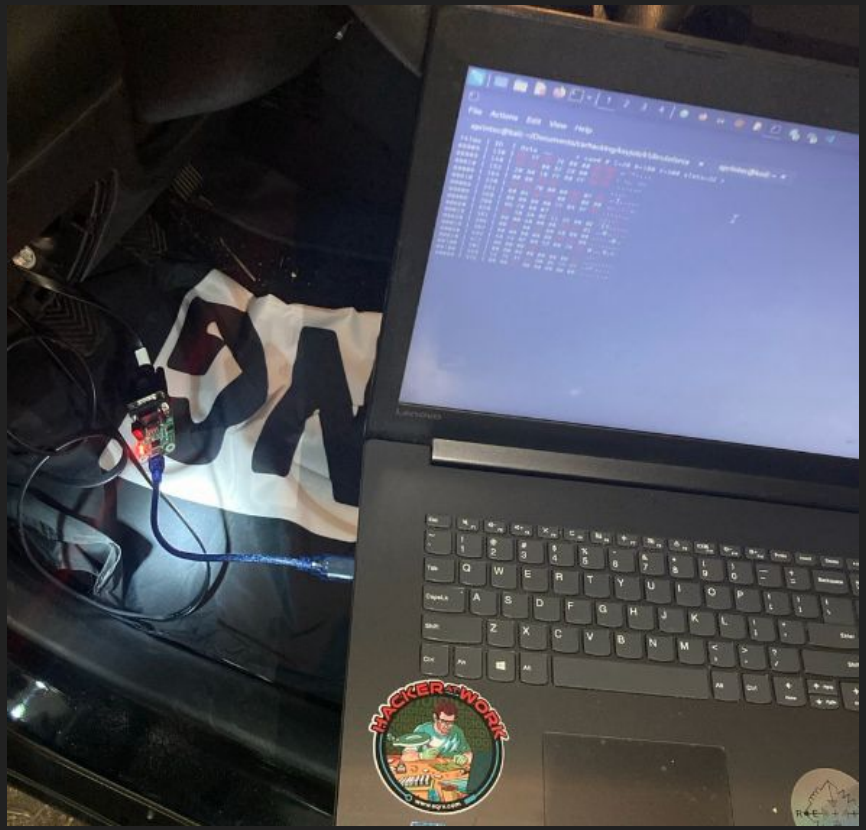
a) CAN injection research

b) Key Fob Hacking research - SUCCESSFUL

c) IVI Hacking research, and more



CAN Bus sniffing, UDS services discovered



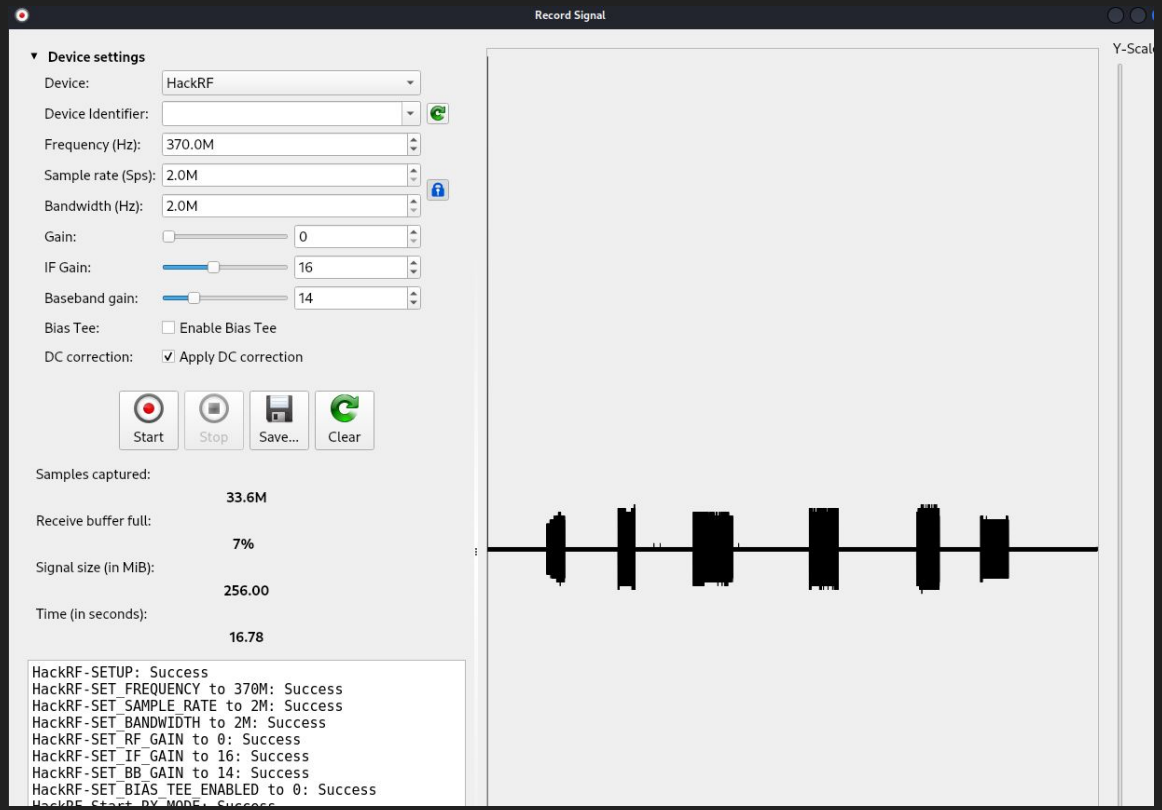
```
15|ms | ID   | data  ...      < can0 # l=20 h=100 t=500 slots=32 >
00009 | 130  | DC 7F 35 7E 00 00 01 3D  ..5~ ... =
00009 | 140  | 19 7E 00 60 20 00 01 20  .~.`  ..
00009 | 153  | 20 80 10 FF 00 FF A0 4E   .......N
00009 | 164  | 00 08 02 0A                ....
00009 | 220  | C5 23 7C 00 00 EE 0F 38  .#|....8
00009 | 251  | 00 04 25 D0 00 1F 08 80  ..%.....
00009 | 260  | 00 00 00 00 01 85 5F 3B  ......_;
00009 | 2B0  | E7 FD 00 07 D1             .....
00059 | 329  | 4F 5D 5A 0E 11 2E 00 0E  O]Z.....
00019 | 381  | 80 00 40 00 00 18 D9 01  ..@.....
00020 | 386  | 00 00 00 80 00 40 00 80  .....@..
00019 | 387  | 00 00 00 00 00 05 05 00  ........
00050 | 492  | 40 FE 0F 00 50 00 74 88  @... P.t.
00020 | 4F1  | 00 00 00 C0                ....
00100 | 50C  | 00 00 00 00 00 00 00 80  ........
00099 | 545  | 2A 1F 00 7A 00 00 00 00  *..z....
00099 | 549  | 08 7F 4B 10 D9 9D FF FF  ..K.....
00099 | 5CE  | 00 00 BD 00 00 00 80 00  ........
```

CAN ID and data to unlock/lock the car

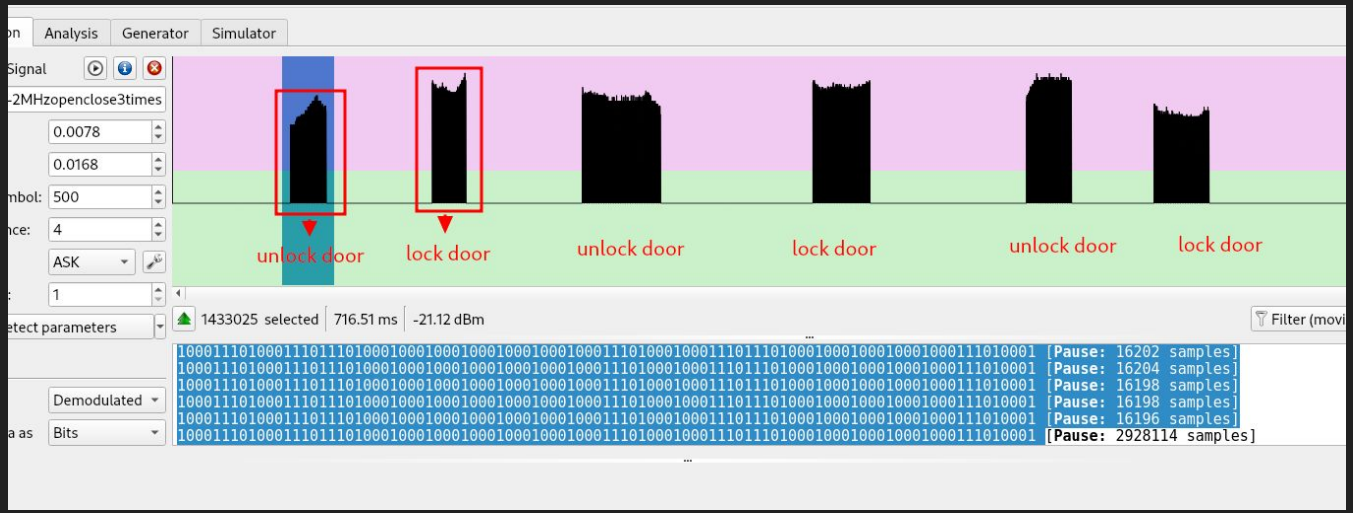
2
Radiofrequency Hacking

Detecting the signal

Tool URH

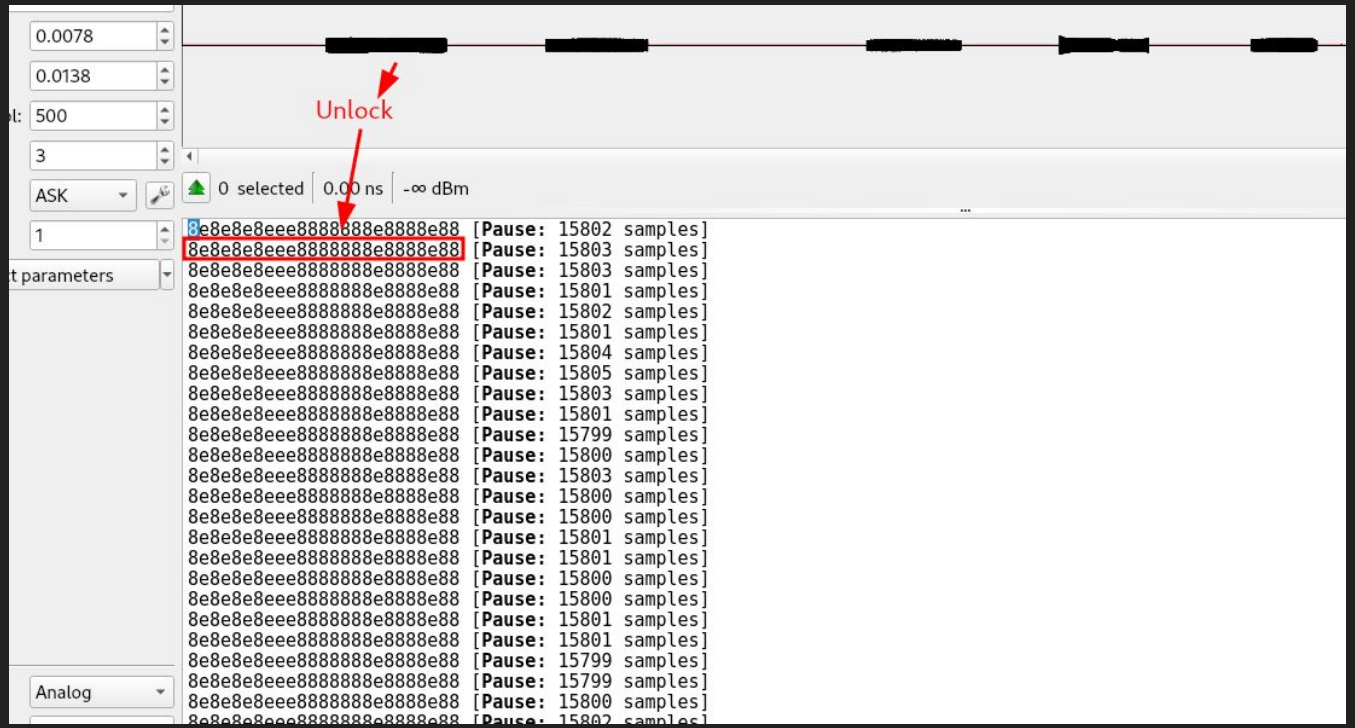


Demodulated signal



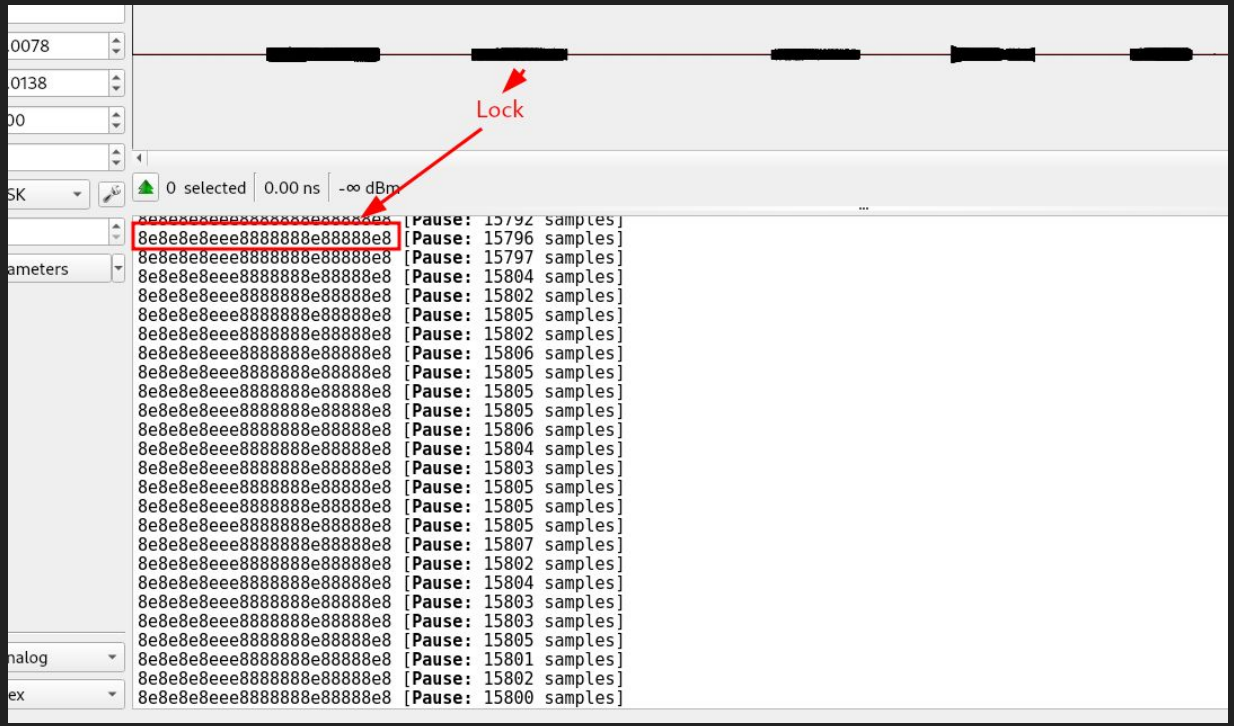
Unlock signal

Code: 8e8e8e8eee8888888e8888e88



Lock signal

Code: 8e8e8e8eee8888888e88888e8



Replay Attack works (I verify that the code doesn't change)

Play video here.



3
Hardware Hacking

Opening the key fob

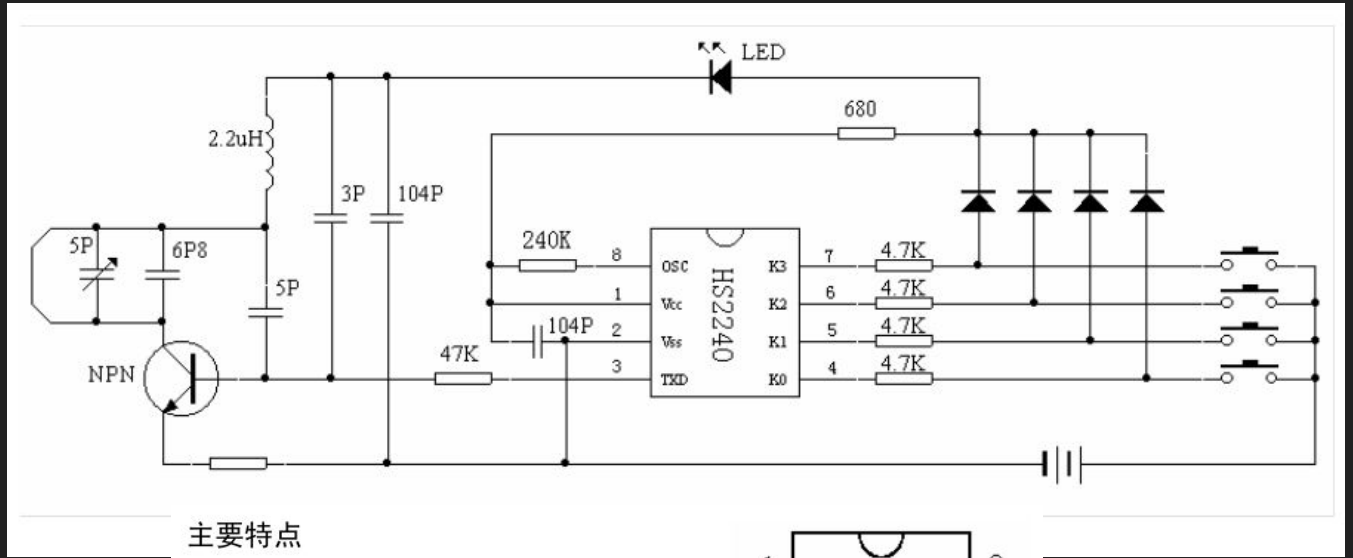
- Learning Code Chip HS2240
- Oscillator: LR370T2
- 2 Batteries: 6.38 V
- LED RF tx
- ASK circuit: Capacitors, Transistors and Resistors





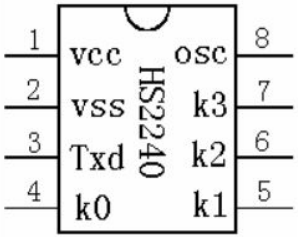
Reversing the circuit - DataSheet HS2240

- Modes: k0,k1,k2,k3
- Source: Vcc
- GND: Vss
- Code signal: Txd
- Oscillator: osc
- ASK modulation



主要特点

1. 低静态电流<1ua；
2. 宽工作电压 3.0-12.0V；
3. 4 按键组合输入，可有 15 个组合按键；
4. 单端振荡电路，只需一个外围电阻。
5. 小体积 8 脚 SOP 封装



How the learning code is formed

- Preamble: Indicates the start of the code (how many bits?)
- 20 bits code: Learning code, 2^20=1048576 possible codes
- Mode: Unlock, lock, etc. (4 bits)



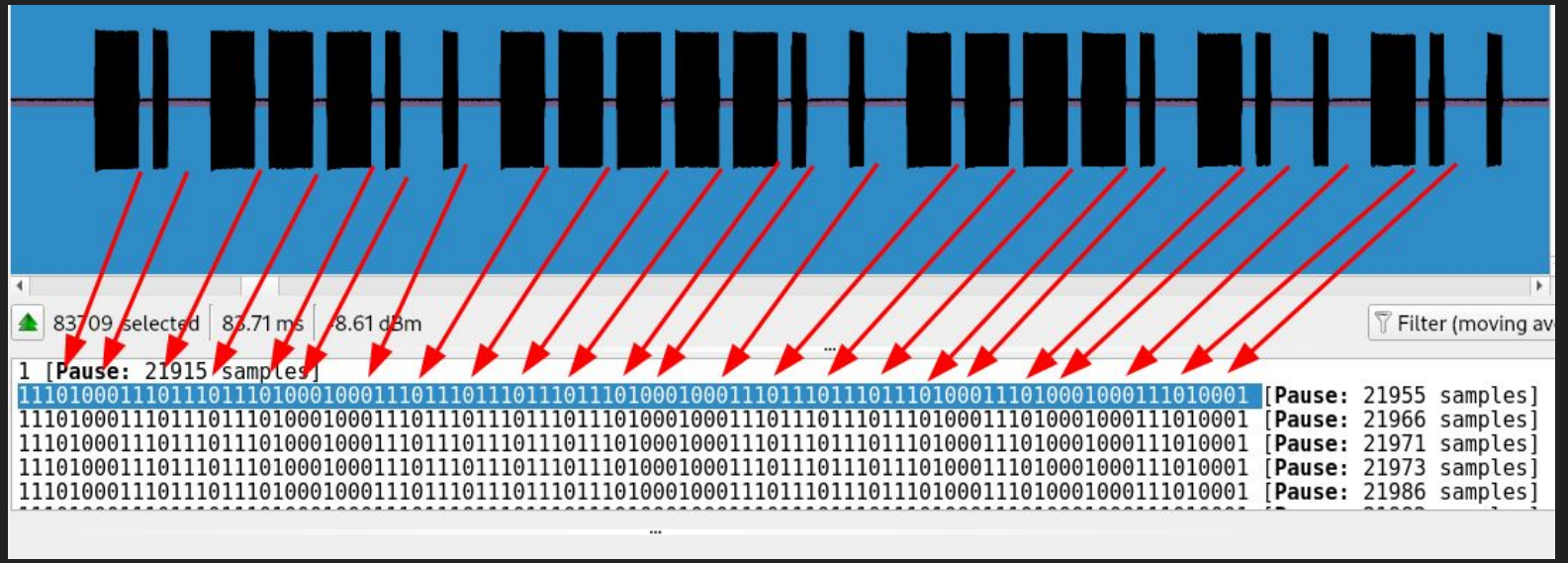
K0~K3 按键组合表（HS2240）

MODES

K3	K2	K1	K0	D3	D2	D1	D0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	1	1	0	0
0	1	0	1	1	1	0	1
0	1	1	0	1	1	1	1
0	1	1	1	1	1	1	0
1	X	X	X	1	1	1	1

Preamble? Let’s go to check

I get 97 bits, so 97 - 20 bits - 4 bits = 73 bits preamble???? No dude



Reversing with Logic Analyzer

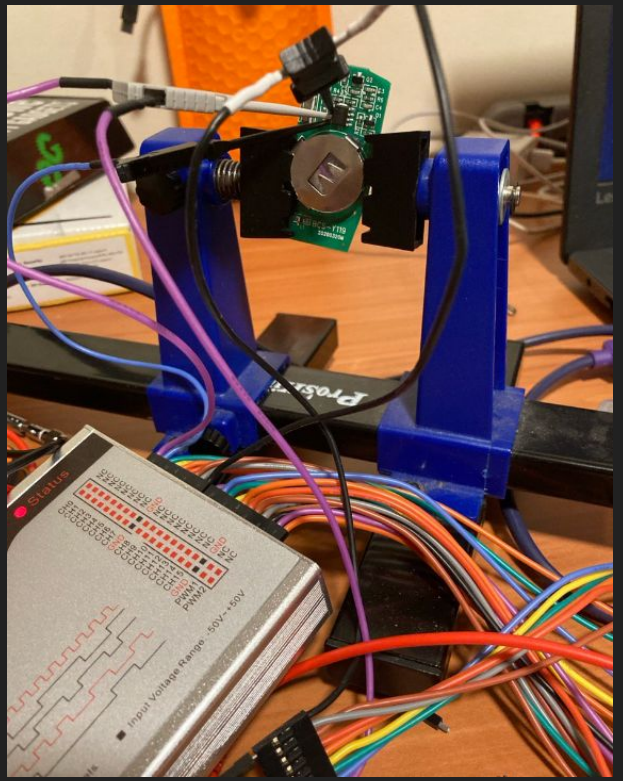
Frequency 370MHZ

- CH0 -> Txd
- GND -> Vss
- CH1 -> K0/k1/k2/k3

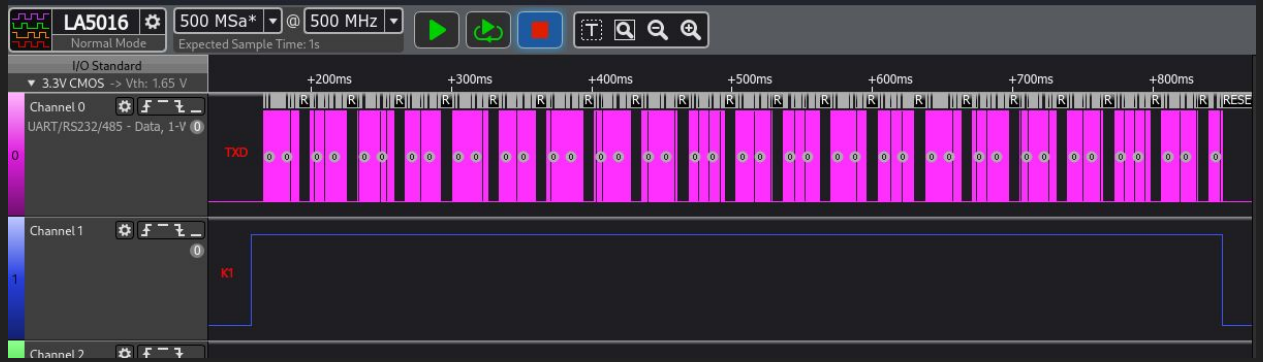


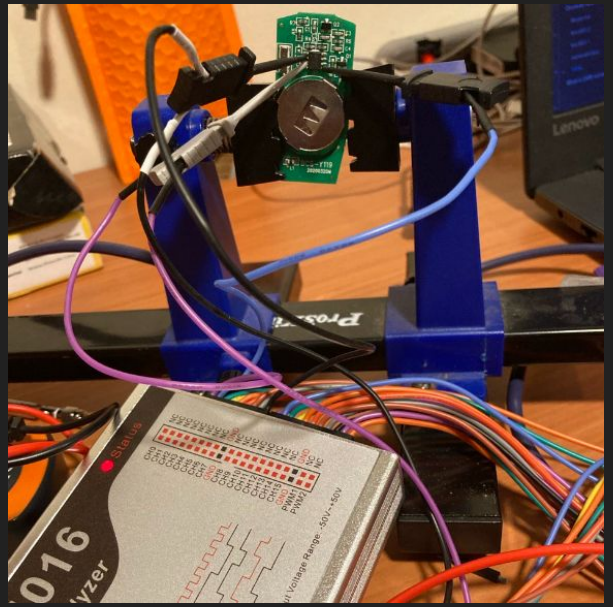
K0 Disabled - Mode 1000



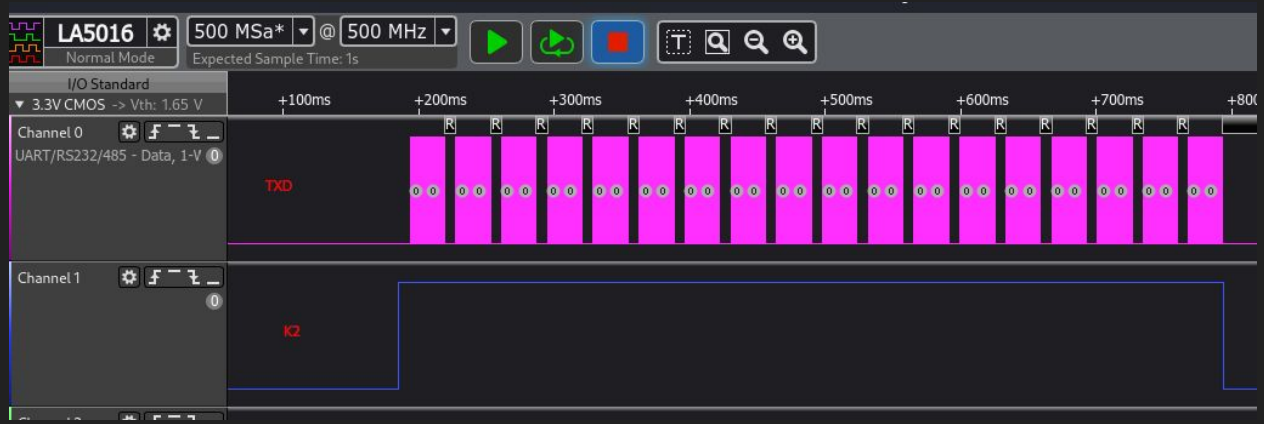


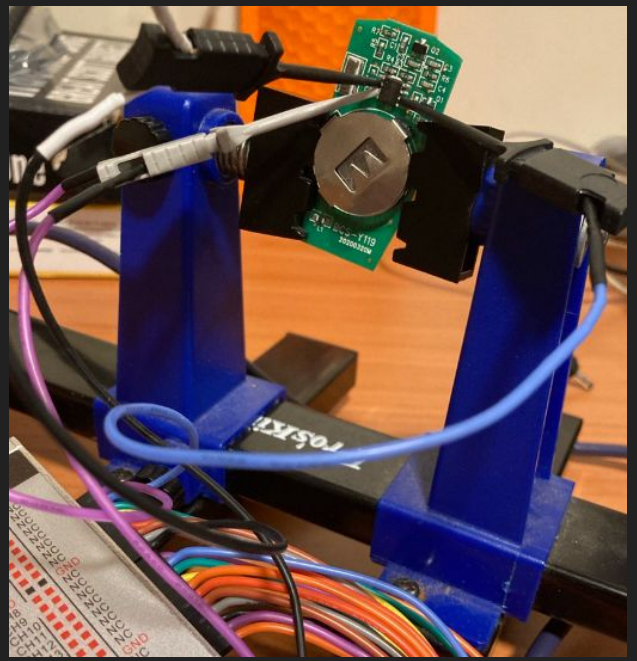
K1 Disabled - Mode 0100



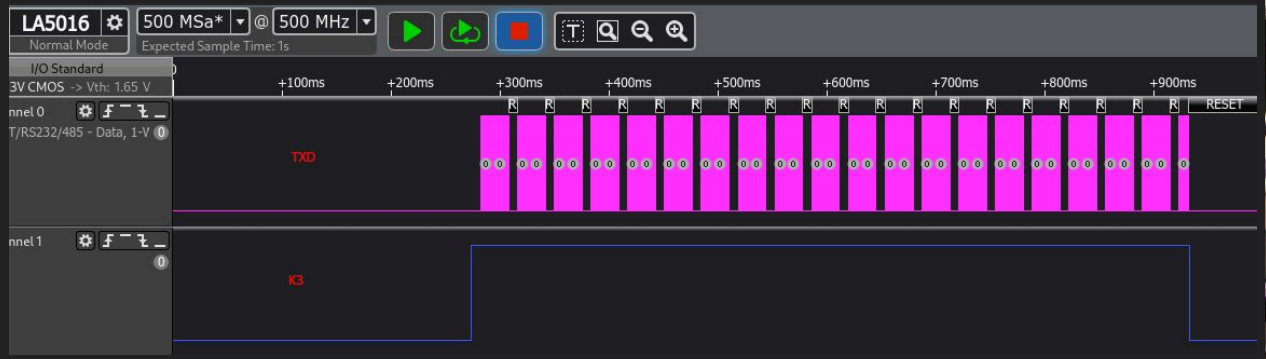


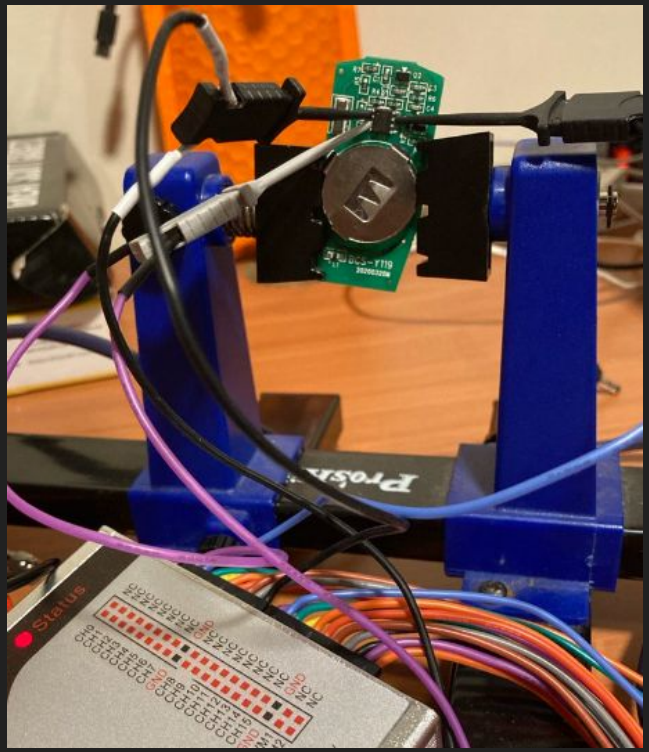
K2 Unlock - Mode 0010



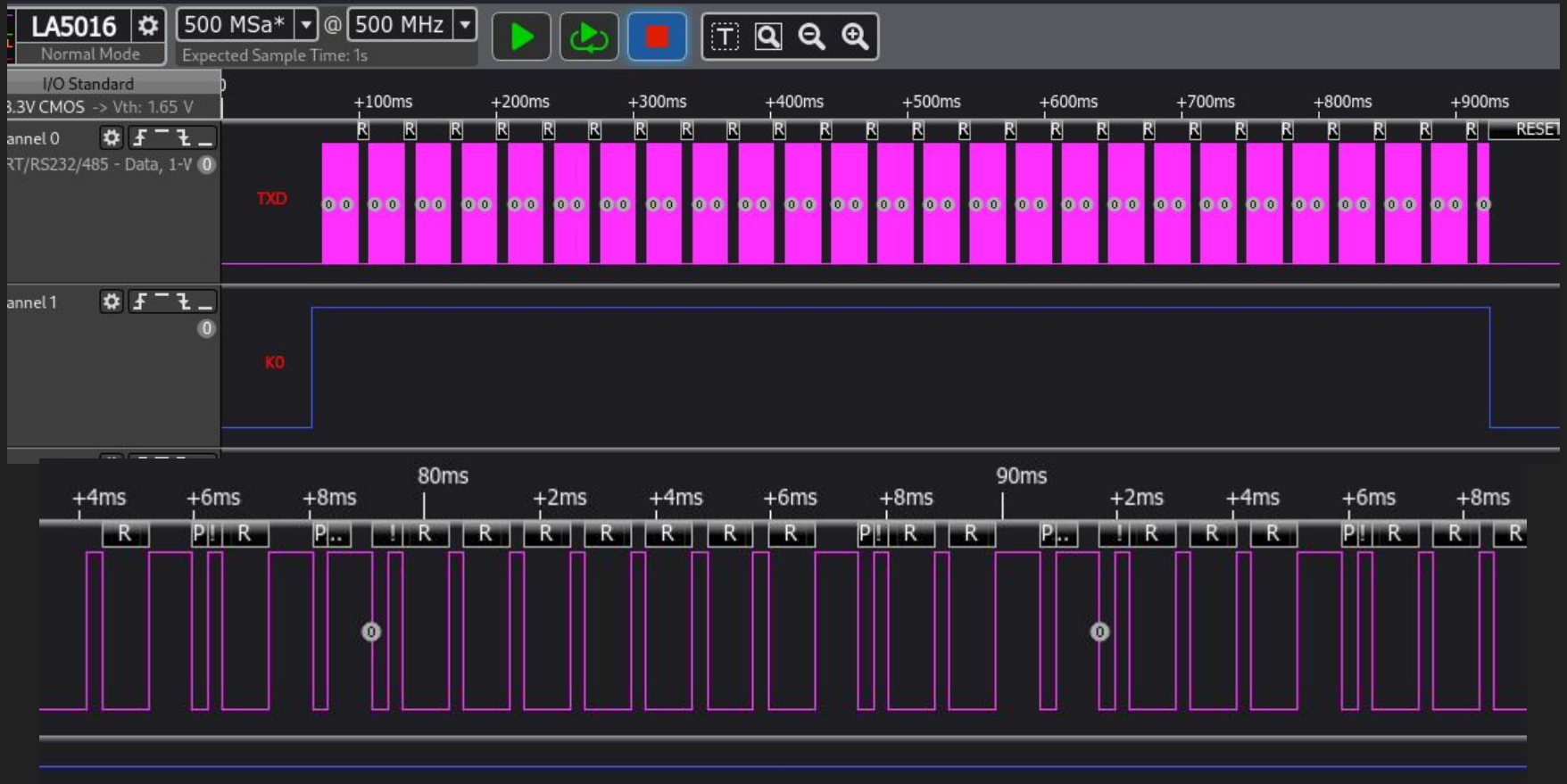


K3 Lock - Mode 0001



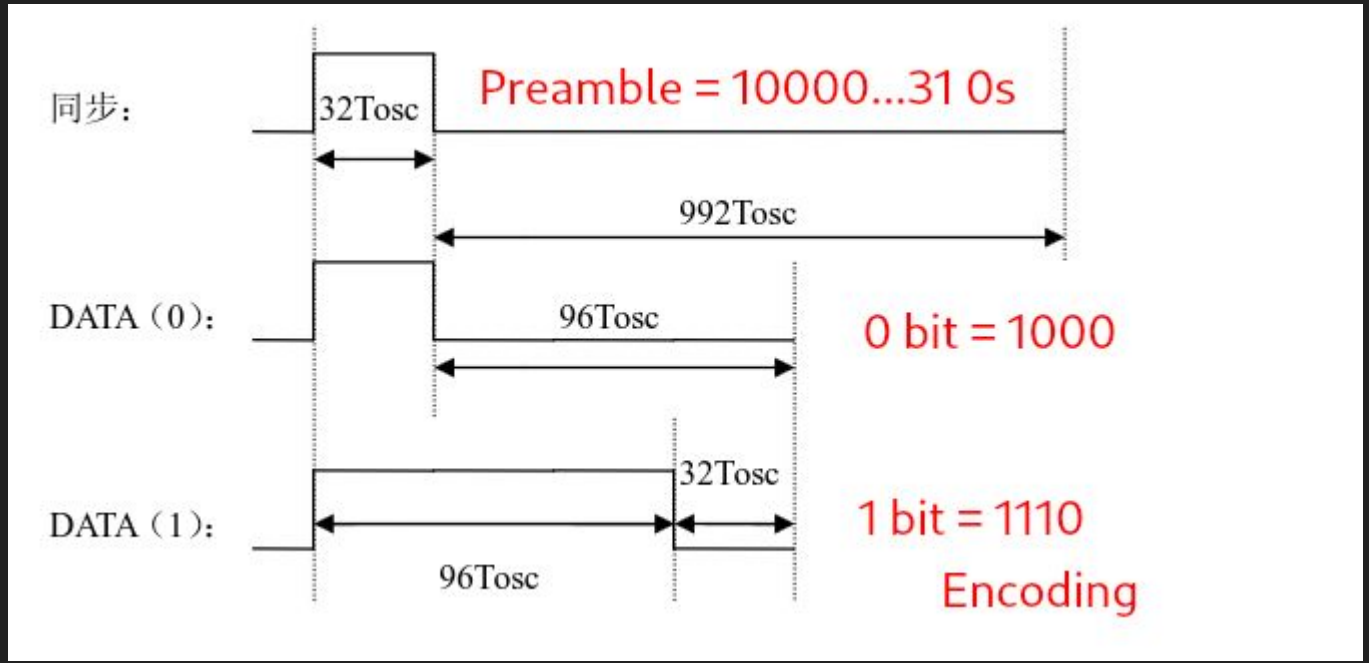


It doesn't match what I get when I demodule? Are you sure



Solved

I find that there is an encoding to the code



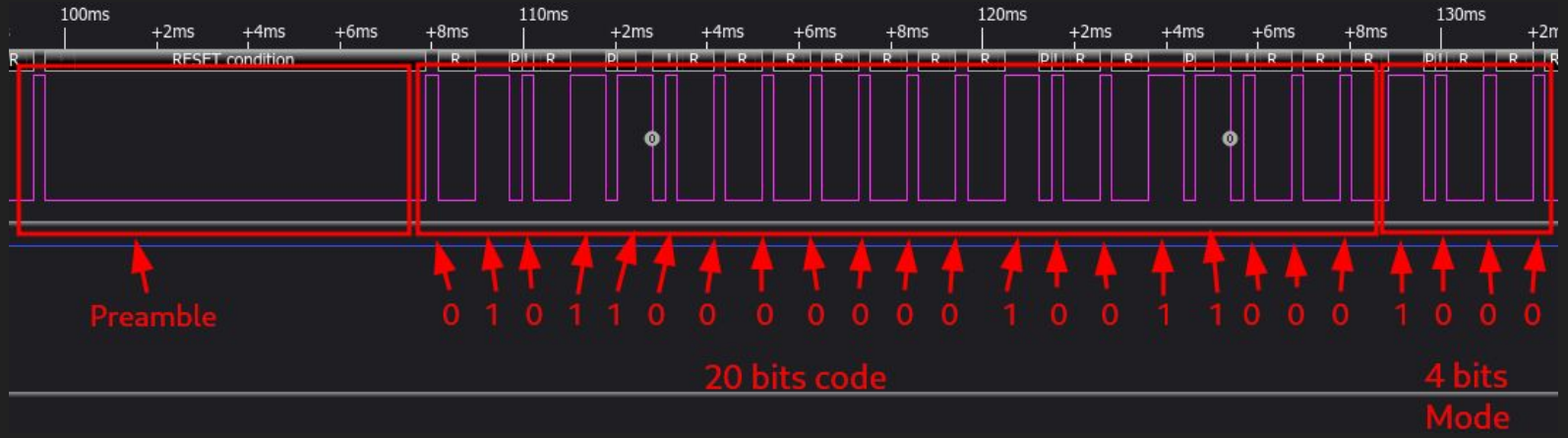
Decoded signal: I get the learned code with a logic analyzer!!!



Mix Frequency Hacking with Hardware Hacking

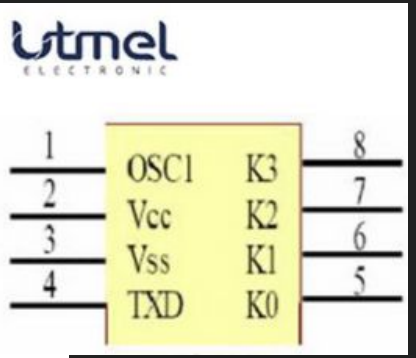
We have all the information to encode/decode any signal





Another vulnerables RF Chips





Product Specification

Usage/Application	Electronics
Mounting Type	SMD
Package	SOP8
Voltage	3V to 12V DC
Number Of Pins	8
IC Pin	8
I Deal In	New Only
Minimum Order Quantity	1 Piece

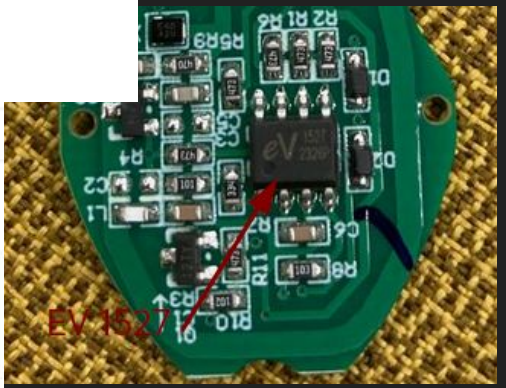
EV1527 Features: (Compatible:EV1527,RT1527,FP1527)

CMOS Technology
Low stand by Current:1.0uA
Wide range of Operating Voltage:Vcc＝3.0～12V
Up to 4 data pins
Total 1048576 address codes
Single Resistor Oscillator
Available in DIP and SOP Package

Product Description

Are you sure??

The EV1527 RF Encoder is OTP Encoder utilizing CMOS technology process. It has a maximum of 20 Bits providing upto 1 million codes. And So, it can reduce any code collision and unauthorized code scanning possibilities. Its a learning type since the receiver needs to first store its code and than only it can detect the future packets, therefore provides better security.



And more…they use the same or very similar coding method

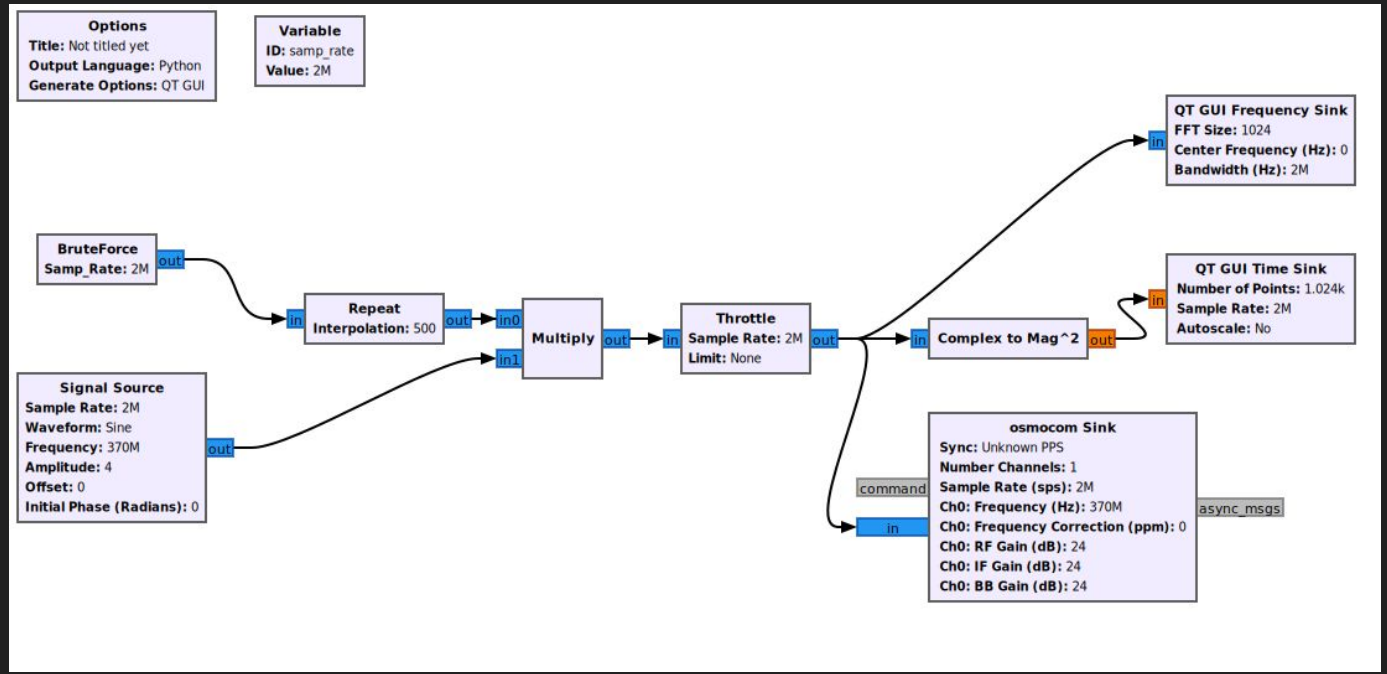
Fixed Code: SC2260; SC2262, HS2260, HS2262; PT2264, 5326 all manufacturers

Learning Code: HS1527, HS2240, HT6P20B, HT6P20D all manufacturers

4
Brute Force Learning Codes

GNU Radio with custom Python Block to brute force attack

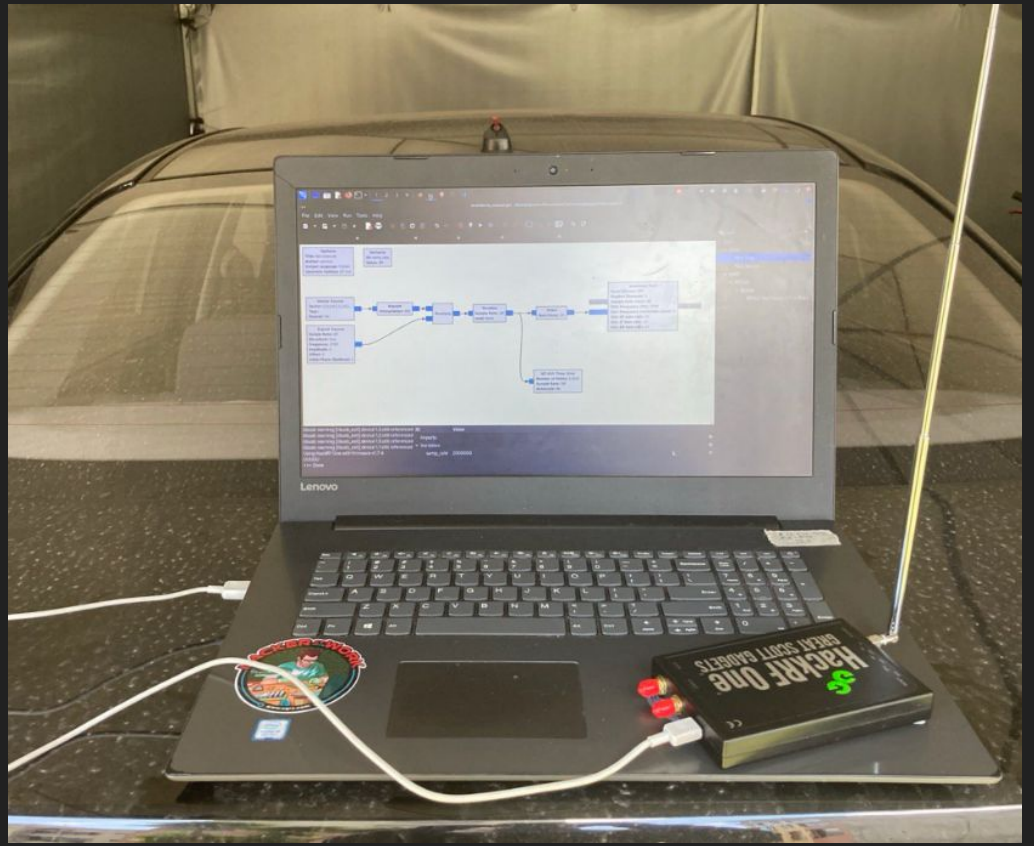
- Samp rate: 2MHz
- Frequency: 370 MHz
- Interpolation: 500



Video demo

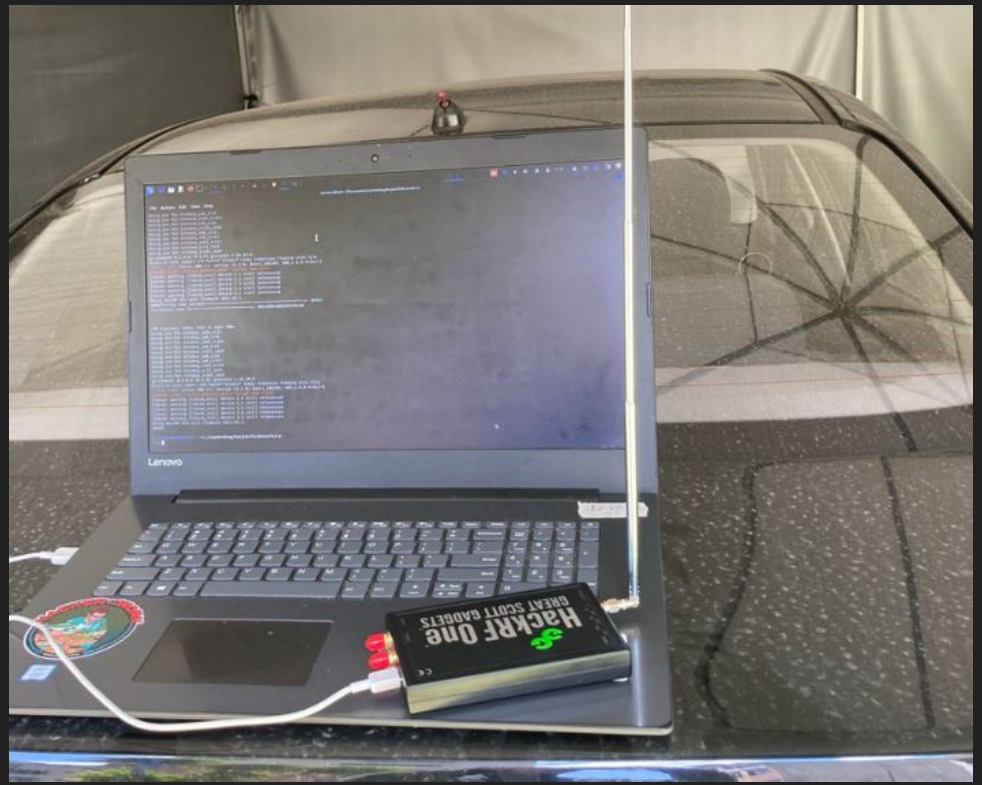
Lets go to unlock a car!

Play video here



Python script CLI to brute force attack

- 1 code/0.06ms to avoid errors
- 1000 codes/1 min
- Redundancy: 2, to avoid interference
- Play video here (I can unlock any car with learning codes)



5
Discovering/Setting Backdoor in KES

KES with learning codes

- KES programmed using learning codes generally accept up to 4 codes.
- When car dealerships give you a car, the car comes programmed with two controls, one main and another in case the main one is lost (only 2 codes).
- How do you know that there is not a 3rd programmed remote control that can open your car, or a 4th remote control?



How a malicious actor backdoors your KES?

1. When installing the alarm and programming it, the malicious actor preprograms one or more backdoor codes for a control that he hides. The relationship is (1 remote control - unlock N cars). The installation of KES is done by car dealerships, but what security control is there?
2. A malicious actor who has access to the car can access the Key Fob receiver and program a backdoor code.

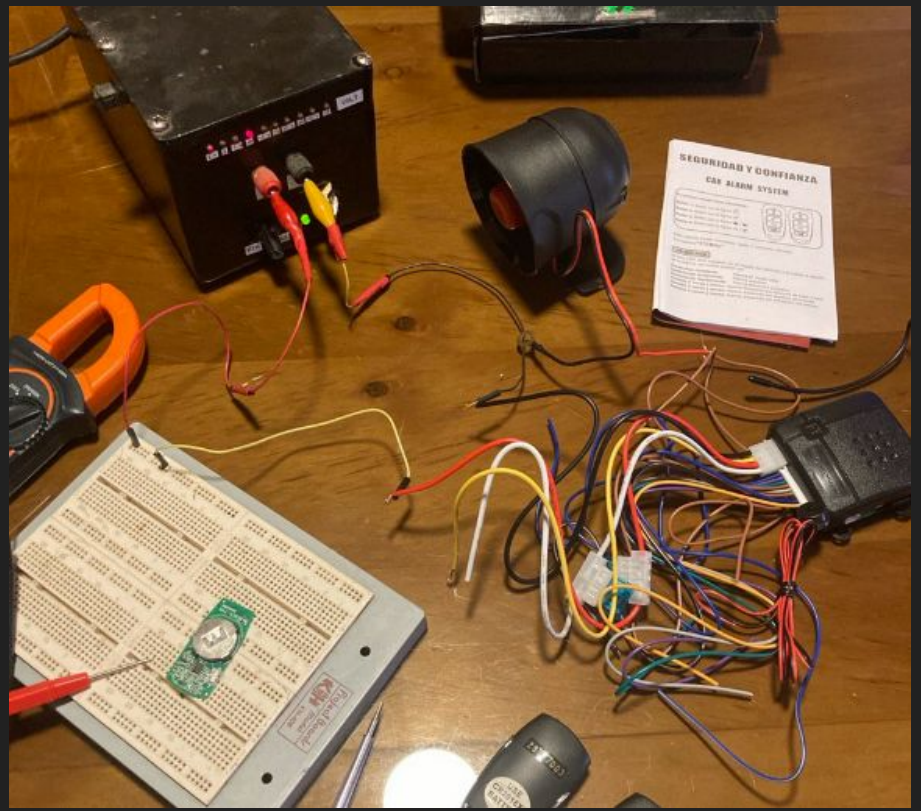


Programming a backdoor code on a KES with learning code

Play video here.

I set up a test lab with the vulnerable KES:

- 12 Volt Voltage Source.
- Receiver.
- Horn.
- 3 Key Fobs.
- Multimeter



6
Identified Vulnerabilities

List of vulnerabilities

A) Lack of protection against brute force attacks: The tested receiver is not damaged after a 16-hour brute force attack. The attack is not detected, the attack is not stopped

B) The system is backdoorizable: A malicious actor can set backdoor code at any time in the production chain or after.

C) Collision attack: Most IC learning code chips use 2^20 bits (only 1048576 combinations), therefore, increasing the possibility that a Key Fob will unlock another car that does not necessarily emit the signal with the same chip. In my country alone there are thousands of cars that are programmed with learning codes. If we unite all the cars programmed with learning codes in the world, there is a high probability that a remote control will open more than one car. There will come a time where the 1048576 codes will be filled all over the world and there will be a collision and no one will find out. Or maybe this figure has already been reached?.

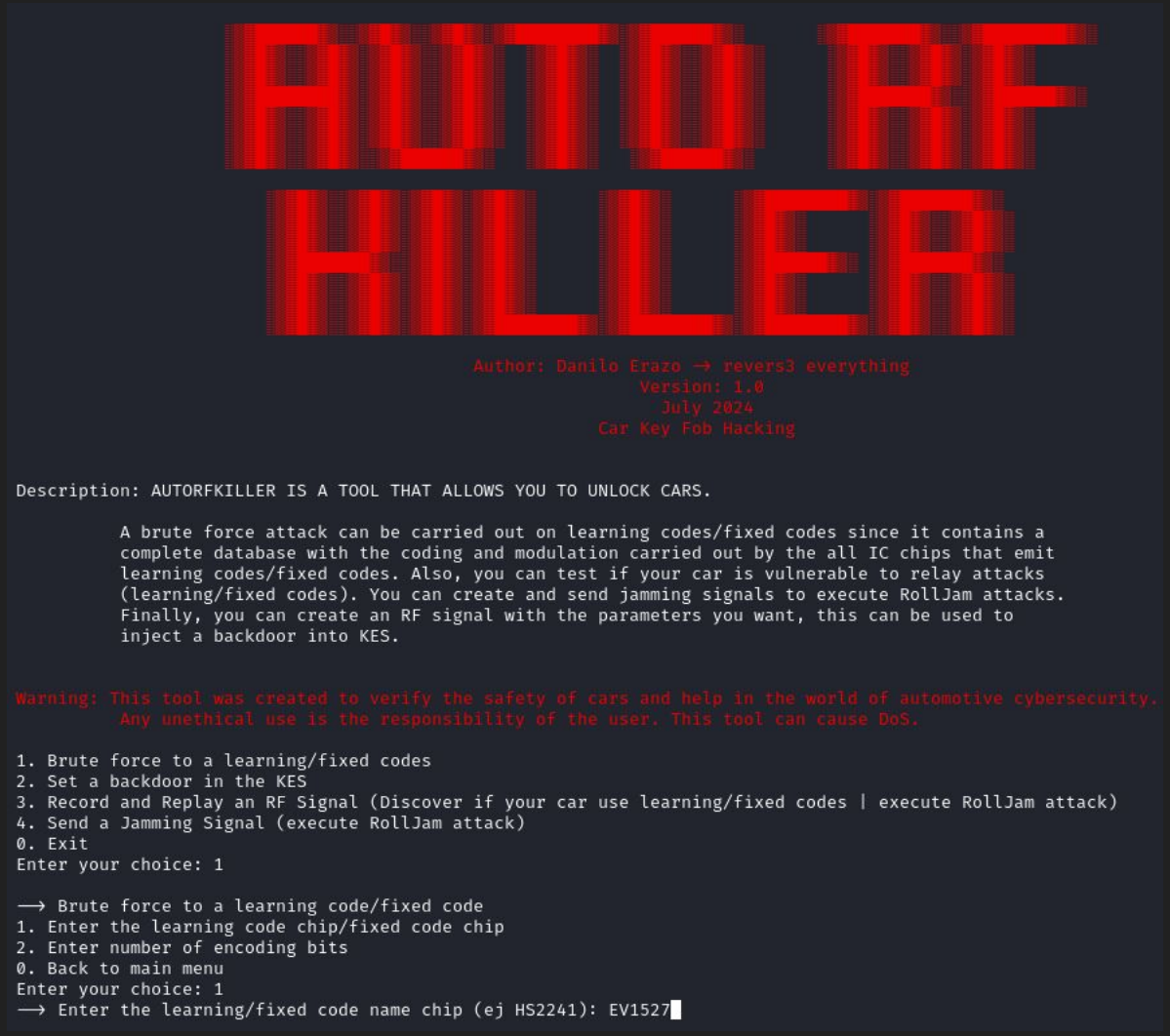
My message:

STOP IMPLEMENTING LEARNING CODES IN CARS

7
Exploit Everything

Developed Hacking Tool

Play video demo here



Thank you very much and
Reverse Everything!!