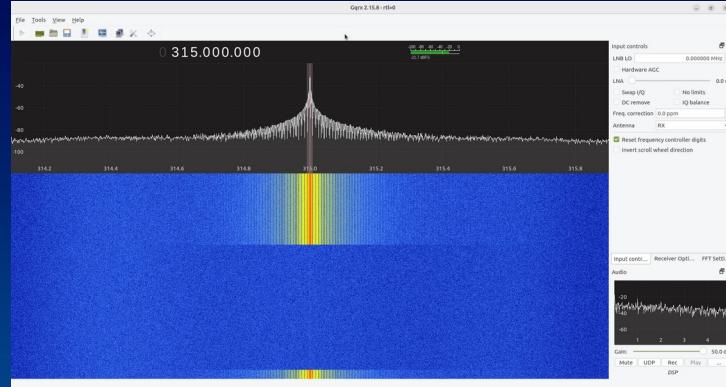


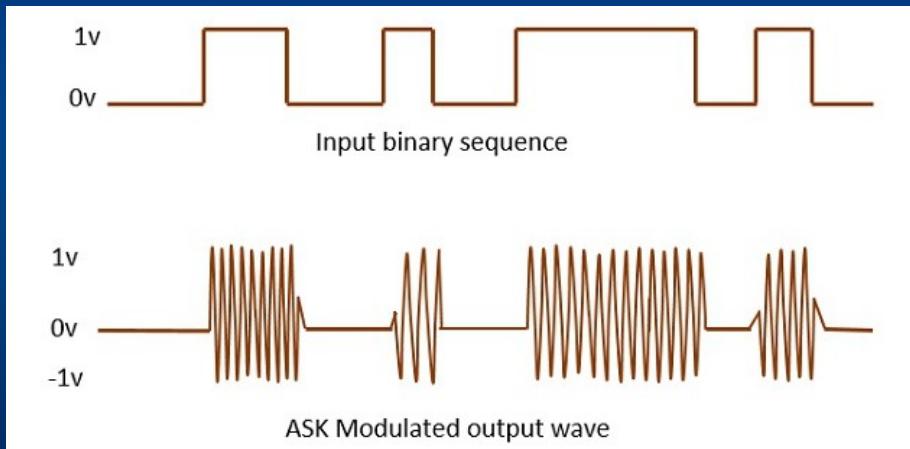
Car RF Signal Database



RF Signal Basics

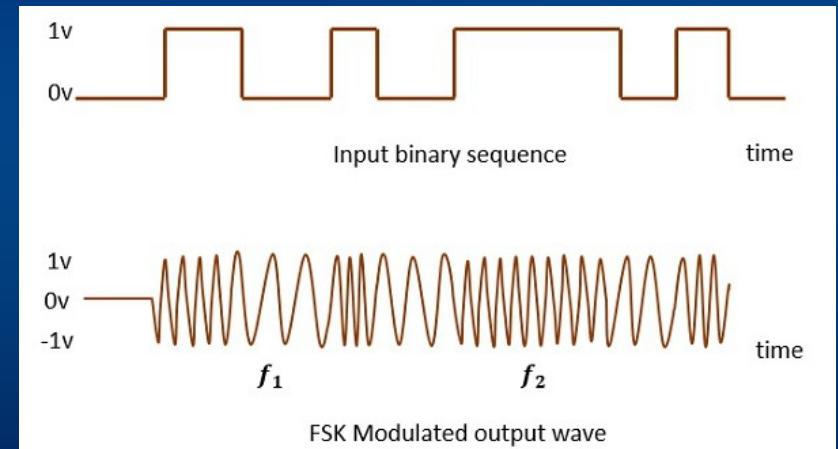
ASK: Amplitude Shift Keying

- Change in signal strength represents 1's & 0's
- AKA OOK: On Off Keying
- Similar to morse code



FSK: Frequency Shift Keying

- Change in frequency represents 1's & 0's

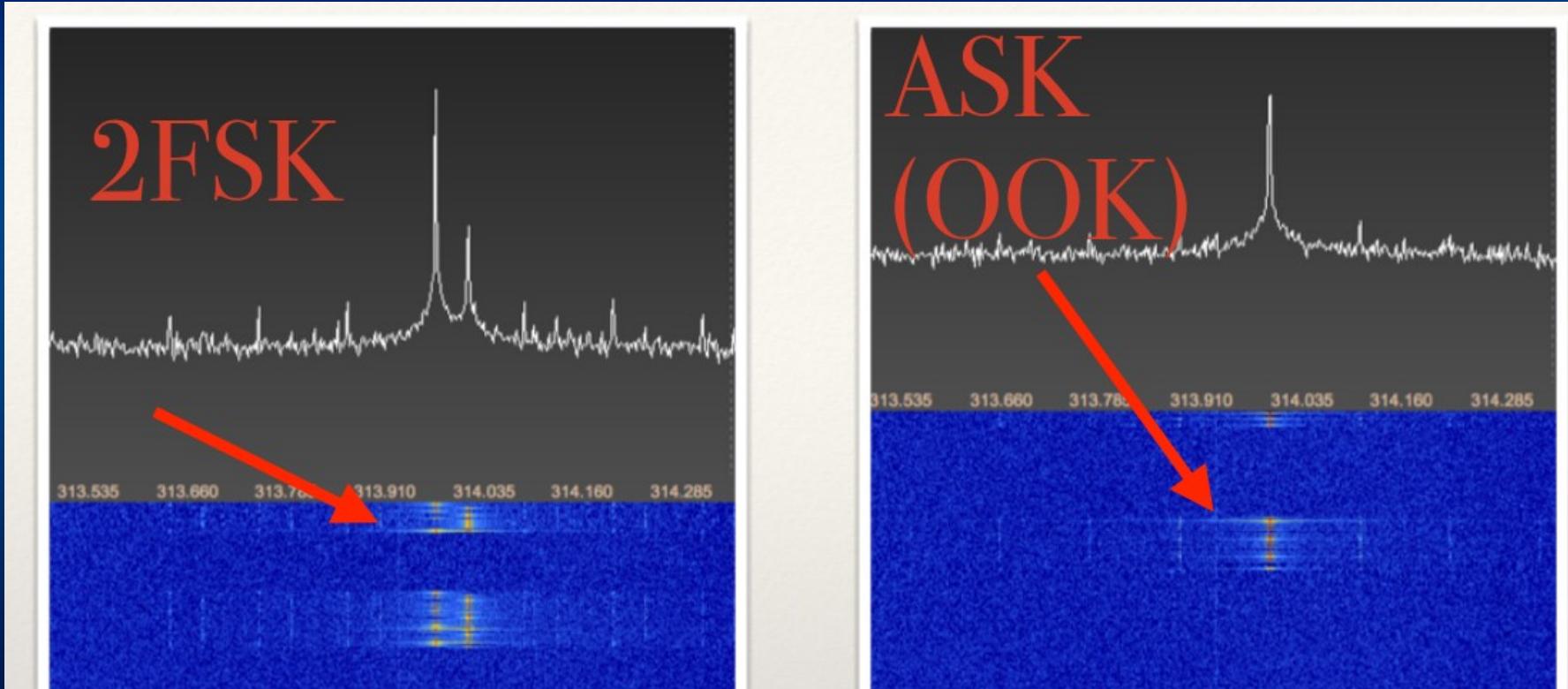


RF Signal Basics

FSK vs ASK in Spectrum Analyzer

FSK will have two peaks

ASK will be single peak, pulsing on and off

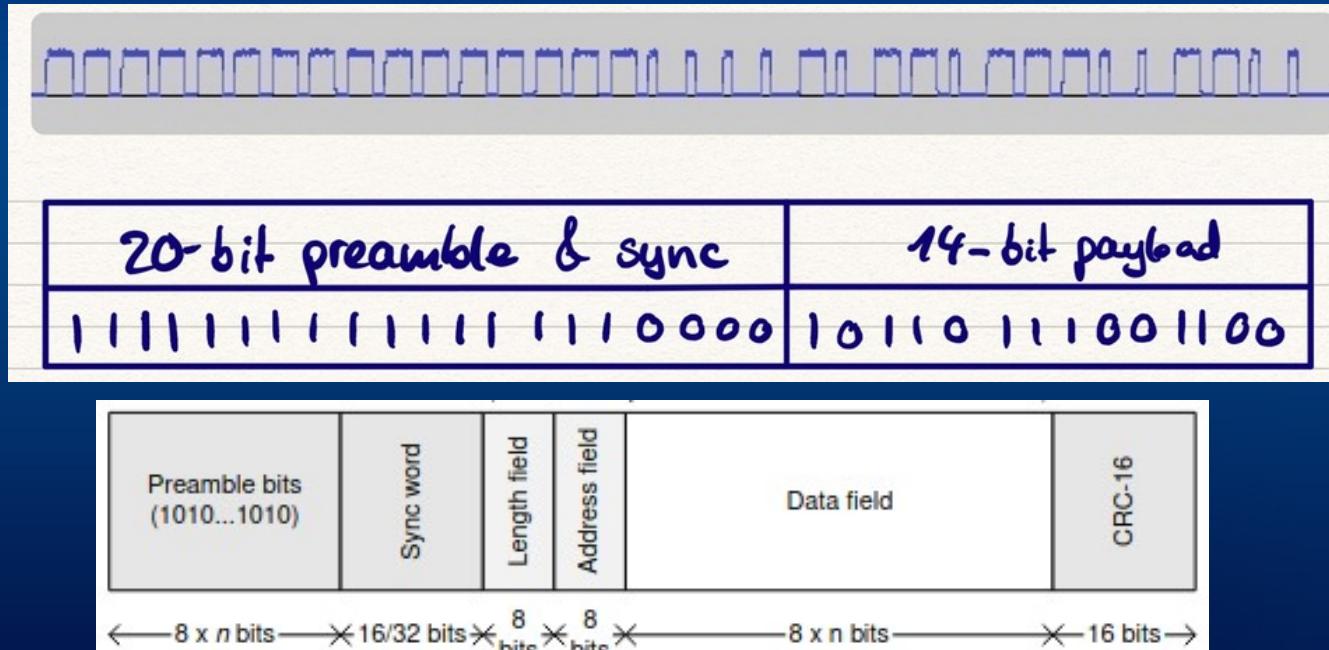


RF Signal Basics

Anatomy of signal

Preamble/Sync + Data + CRC (Checksum)

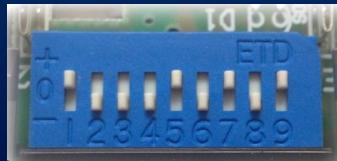
- Preamble & Sync wakes the receiver and syncs signal to receiver clock
- Data field will usually contain sub-fields, such as DeviceID, Command, Rolling Code
- CRC validates the packet data hasn't been corrupted during transfer



Fixed Code (Static)
VS
Rolling Code (Dynamic)
Remotes

Fixed Code Remotes

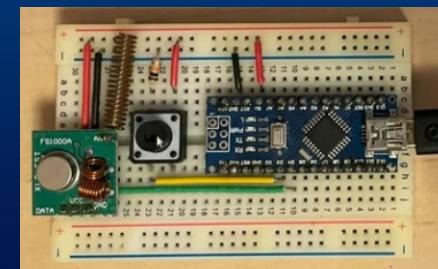
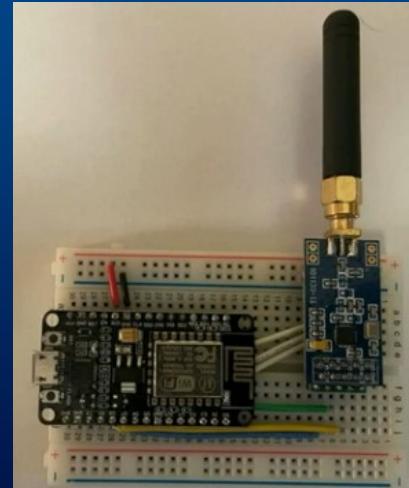
- Usually* older remotes from 20th Century
 - Older garage doors, gates, car alarms, generic remotes
 - Some remotes use DIP switch inside remote to set the code
- * Some current remotes still use fixed code (Linear garage doors, Hondas, household devices e.g. ceiling fans, light switches, etc.)



Fixed Code Remotes

Replay Attack

- Record the signal using off-the-shelf hardware. RTL-SDR, HackRF One, CC1101
Record with spectrum analyzer (GQRX, SDR#, URH) or command line rtl_sdr (linux)
- Replay the raw file (IQ format) with HackRF One, or reverse engineer (demodulate)
to binary signal and transmit with cheaper hardware
(CC1101, Yardstick One, fixed frequency 315/433 transmitter)

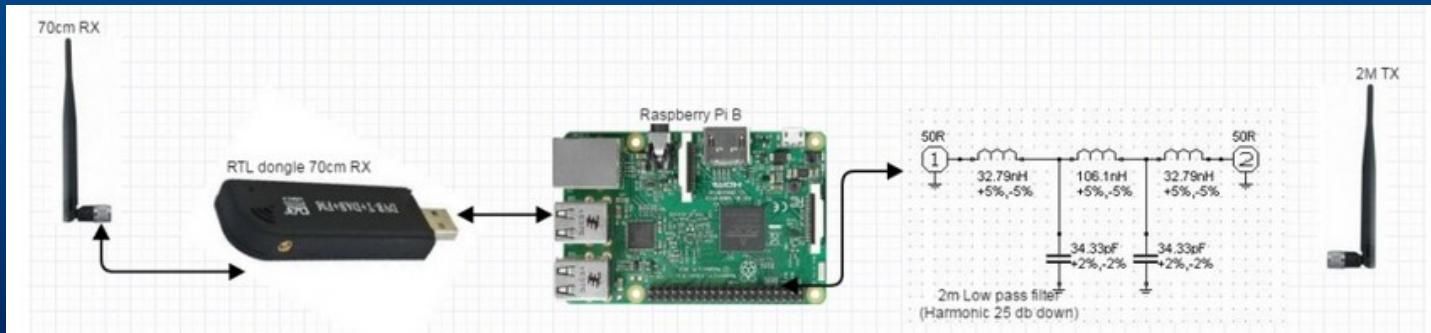


Fixed Code Remotes

Replay Attack (Cheap & easy way)

Don't have a transmitter? You can use a Raspberry Pi to transmit!

RpiTx: Attach a wire to GPIO pin 4 on the RasPi. The wire becomes an antenna
Ability to transmit frequencies from 5 KHz to 1500 MHz (low power)
Can replay IQ files, recorded with inexpensive (\$25) RTL-SDR dongle



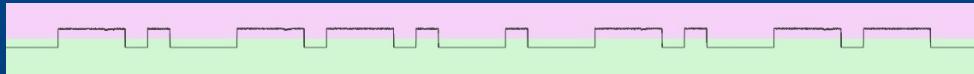
<https://github.com/F5OEO/rpitx>

Fixed Code Remotes

Brute Force Attack

- Purchase similar remote (Ebay, Walmart) e.g. Universal Garage Remote
- Reverse engineer format with Universal Radio Hacker (URH)
- Brute force all DIP switch combinations or Device ID

10 Position DIP = 2^{10} combinations = 1024 combinations to brute



Rolling Code Remotes

- Most 21st Century cars and garages use rolling code remotes
 - Transmitted code changes every time remote button is pressed
 - Receiver keeps track of codes that have been transmitted already
 - Can't replay attack using an old code
 - Receivers will have a button (or combination of button presses), or OBD/CANBUS code, or key turning combo to put receiver into learn mode to add a new remote
- Adds remote device ID, and sometimes crypto key, to list of acceptable remotes



Rolling Code Remotes

Rolling Window

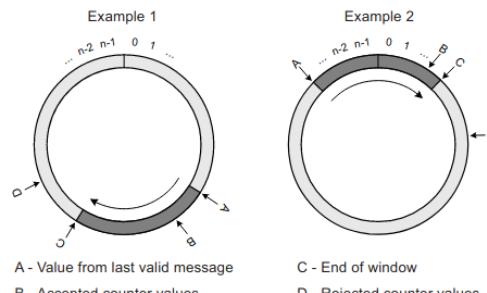
- Situations when users accidentally push remote button when away from receiver
 - Receiver has list of future, acceptable codes in case remote skips ahead a few codes
 - Not really a list (not memory efficient), but an increment counter
 - Some Rolling code algorithms are encoded/decoded using the counter and remote ID
 - Depending on what data type was used, the counter has to reset to prevent overflow
Eventually codes will repeat themselves (Rollback exploit)
- Byte = 255 max value. Unsigned Short = 65,535 values

2.1.1 Rolling Windows

The concept of simply ignoring messages having old sequential numbers leaves one problem: What if the counter value overflows and wraps back to 0? This section describes a solution.

Handling the sequential counter best described by two examples, given in [Figure 2-4](#). The first example shows a situation where the last received valid message had a counter value A. As there is always the possibility that the transmitter has been activated a number of times outside the receiver's range, the receiver must accept values up to some limit, labeled C in the figure. The simple approach of accepting all values larger than the last received value won't work, as is apparent in the second example where point A is close to the upper end of the counter value range. The dark segment from point A to C shows the window of acceptance for counter values. Point B is an example of a value that would be accepted while point D is a value that would be rejected. When a value is accepted, the window starting point moves to that point.

Figure 2-4. Rolling Window of Acceptance for Counter Values



Exploit Techniques

Relay Attack : Passive Keyless Entry systems

RollJam: narrowband jamming & sniffing

RollBack: resets receiver rolling window

Jamming: use signal that's stronger than remote

Relay Attack

Passive Keyless Entry Systems

- Usually on newer model cars, with push button starts
- Key has to be held close to door handle or igniton to unlock & start car
- Car sends low frequency (LF, ~135KHz) signals to keyfob, keyfob responds over UHF
- Challenge/response between car and keyfob uses crypto

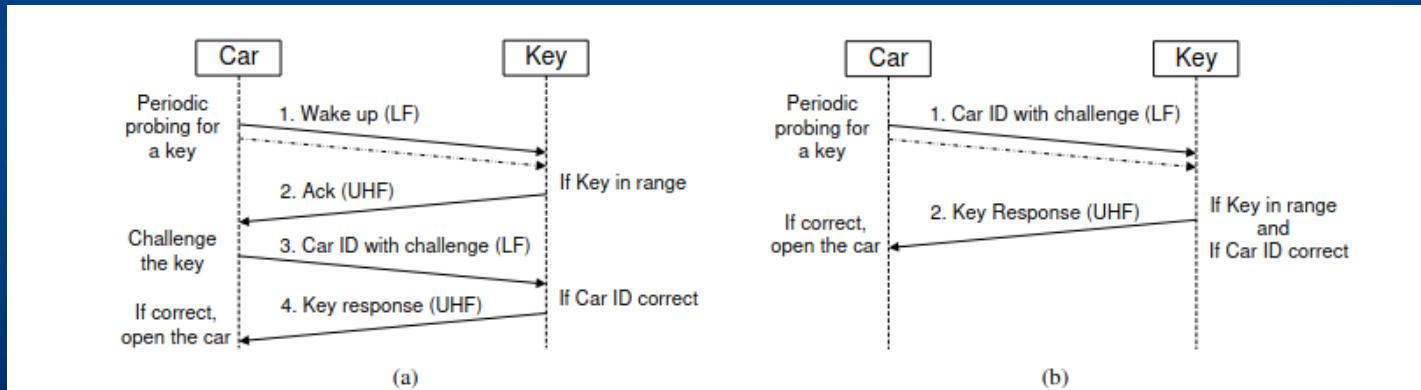
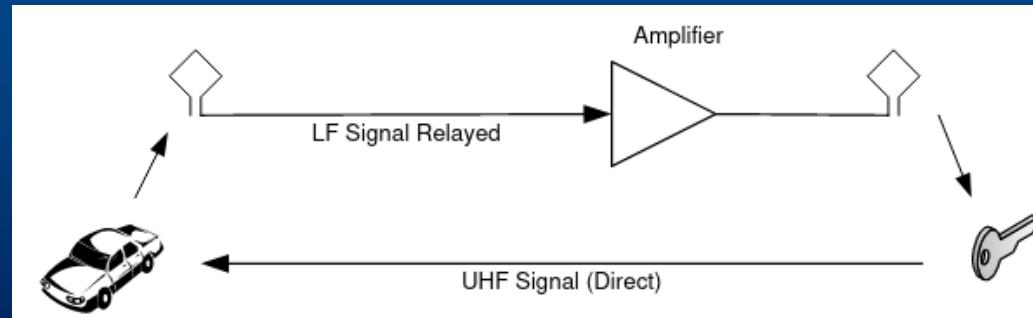


Figure 1. Examples of Passive Keyless Entry System protocol realizations. a) In a typical realization, the car periodically probes the channel for the presence of the key with short beacons. If the key is in range, a challenge-response protocol between the car and key follows to grant or deny access. This is energy efficient given that key detection relies on very short beacons. b) In a second realization, the car periodically probes the channel directly with larger challenge beacons that contain the car identifier. If the key is in range, it directly responds to the challenge.

Relay Attack

Passive Keyless Entry Systems

- Relay attack involves 2 people. One person stands next to car and sniffs LF signal and sends the recorded signal to 2nd person
- 2nd person is close to the keyfob (e.g. following the car owner on foot) and replays the LF signal to the keyfob
- Keyfob responds with UHF response. 2nd person records the UHF signal and sends back to first person at car
- 1st person replays UHF signal, and car unlocks/starts



Some researchers suggest this can be performed with Proxmark and CC1101, RasPi (e.g. Tesla exploit). However many cars expect small delays between challenge responses

<https://ioactive.com/nfc-relay-attack-on-tesla-model-y-2/>

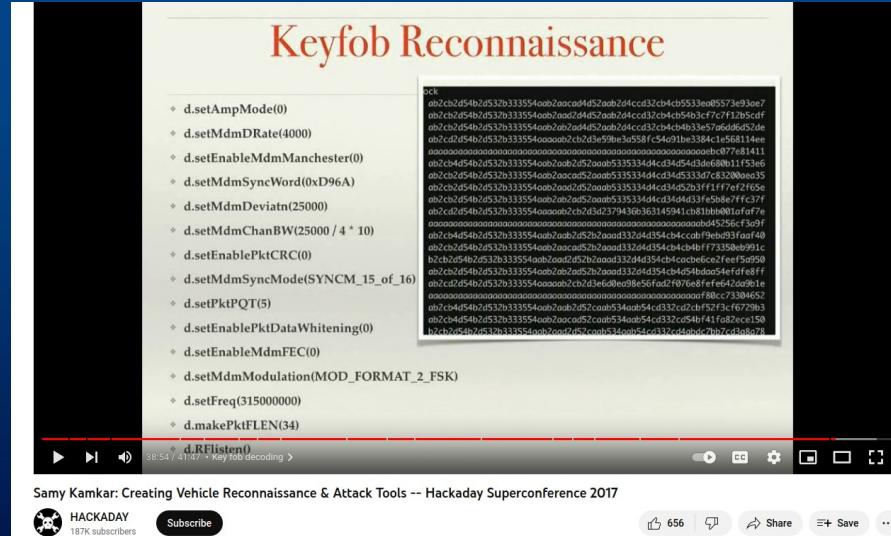
<https://blog.bi0s.in/2021/02/07/Hardware/ProxPi%20Relay%20Attack/>

<https://eprint.iacr.org/2010/332.pdf> (Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars)

Relay Attack

Passive Keyless Entry Keyfob Reconnaissance

- Samy Kamkar realized that the “wake up” LF signal is identical for same make/model car
- Create a database of make/models LF wake-up calls
- Play these signals these signals when persons of interest are in range, and keyfob(s) will respond with their keyfob ID
- Similar to wifi probe request sniffing



Subscribe

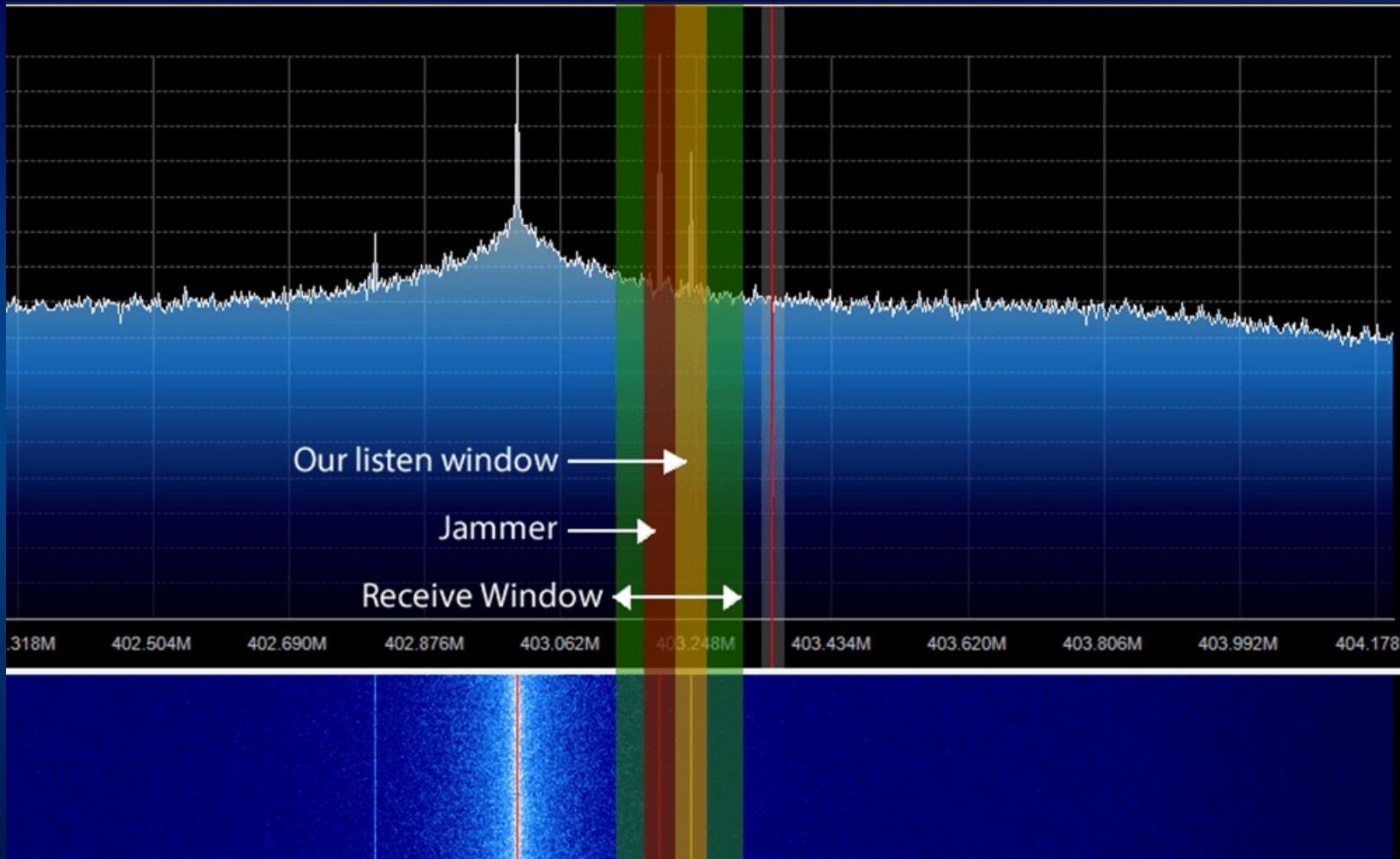
656



RollJam Attack

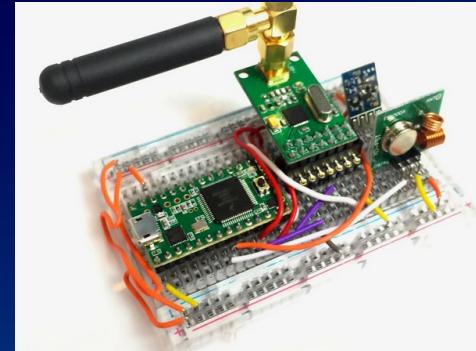
- Conceived by Samy Kamkar
- Cars have a wide receiving bandwidth and are easy to jam
- Involves knowing the EXACT frequency of the remote (usually offset several hertz from the documented value)
- Jam the car with a narrowband signal that is within receivers bandwidth, but different from remotes exact frequency
- Sniff the remote signal with a narrowband receiver, listening for The keyfob but ignoring the jammer signal
- Victim tries to unlock the car, and attacker sniffs first rolling code while the jammer prevents the car from actually unlocking
- Victim tries to unlock the car again, pressing the remote button a second time. Attacker sniffs/records a second rolling code
- Once two rolling codes have been recorded, the jammer automatically stops and transmits the first rolling code
- The car unlocks, the victim thinks the remote was just being finicky, and the attacker is in possession of a valid, unused rolling code (the second code sniffed during the jam session)

RollJam Attack



RollJam Attack

Disadvantages



Targeted attack. Requires research & recon of the signal before deploying

If victim presses their remote again, the captured rolling code becomes invalid

Most remotes have multiple buttons/commands. Capturing a “lock” signal won’t unlock the car. The attackers captured “unlock” signal will become invalid when the victim locks the car again. Possible to change the command if there’s no CRC

More relevant with one button remotes (garage doors, gates)

Jammer antenna can’t be too close to sniffing antenna (anecdotal. Evil Crow chats)

I’ve never seen a successful, fully automated, video demo of this exploit

RollBack Attack

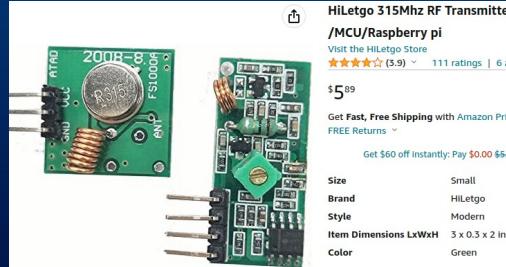
- Technique to reset some car's rolling window
- If the car hears enough (2-5) old codes, in a row (sequential), it thinks that the keyfob button was accidentally pushed many times while away from the car, and the keyfob looped/reset its rolling window (e.g. you let a baby play with your keys, it pressed the button 255+ times)
- The receiver rolling window counter resets so it can “resync” with the keyfobs counter
- Old rolling codes become new again, and can be replayed to unlock car
- Requires capturing and replaying 2-5 (different for make/model) sequential signals to reset
- Targeted attack that requires following the car to capture these 2-5 signals (e.g. follow a car during its lunch break or running errands)
- A lot of Hondas and Mazdas are susceptible. Can capture/replay with usual replay hardware (Flipper Zero, CC1101, HackRF, RTLSDR & RPiTx)

Rollback Attack

Car Make	Model	Model date	Mfg. date	RKE manufacturer	RollBack (variant)
Honda	Fit (hybrid)	2016-2018	2016	NXP F2951X	RollBack ^{Strict(5)}
	Fit	2018	2018	NXP 61X0915	RollBack ^{Strict(5)}
	City	2017	2017	NXP F2951X	RollBack ^{Strict(5)}
	Vezel	2016-2022	2017	NXP F2951X	RollBack ^{Strict(5)}
Hyundai	Elantra	2013-2015	2015	Omron MD-015	RollBack ^{Loose(2)}
	Elantra	2012	2012	NXP 32182C ^[15]	NO
	Avante	2018-2020	2020	NXP F7936 ^[16]	NO
Kia	Cerato/Forte K3	2016-2018	2017	Omron MD-011	RollBack ^{Loose(2)}
	Cerato/Forte K3	2012-2018	2015	Omron MD-011	RollBack ^{Loose(2)}
Mazda	3	2018	2018	NXP A2V25	RollBack ^{Strict(3)}
	2 Sedan	2018	2018	NXP F7953	RollBack ^{Strict(3)}
	2 HB (facelift)	2020	2020	NXP A2V25	RollBack ^{Strict(3)}
	Cx-3	2019	2019	NXP A2V25	RollBack ^{Strict(3)}
	Cx-5	2018	2018	NXP F7953	RollBack ^{Strict(3)}
Nissan	Teana	2014	2014	NXP 063168C	NO
	Latio	2007-2012	2009	Microchip	RollBack ₅ ^{Strict(2)}
	Sylphy	2012-2019		NXP F7952	RollBack ₈ ^{Strict(2)}
Toyota	Wish	2009-2017			NO
	Corolla Axio	2015-2017		TI 37143ADN	NO
	Altis	2005		TI 37200A	NO
	Prius (hybrid)	2020	2020	TI	NO

Jamming

- Uses a stronger or closer signal (tone) than the car's keyfob
- Same transmitters for replay attacks can also jam (CC1101, HackRF, Flipper)
- Some US cars and many European/Asian cars use 433.92 MHz
- 433.92MHz can be jammed with off-shelf low-cost HAM radios (Baofeng)
- Some keyfob use dual/alternating channels; makes jamming more difficult (e.g. FCC ID HYQ12BDM)



HiLetgo 315Mhz RF Transmitter /MCU/Raspberry pi
Visit the [HiLetgo Store](#)
 111 ratings | 6 an
\$5.69
Get Fast, Free Shipping with Amazon Prime
FREE Returns
Get \$60 off Instantly: Pay \$0.00 \$5.69
Size Small
Brand HiLetgo
Style Modern
Item Dimensions LxWxH 3 x 0.5 x 2 inch
Color Green

Your email address [Subscribe](#)

BUSINESSTECH

≡ BANKING BUSINESS FINANCE MOTORING INDUSTRY NEWS PROPERTY TRAVEL

Remote jamming on the rise in South Africa

Staff Writer 13 June 2021



A photograph showing a person's hand holding a black remote keyfob, pointing it towards the rear of a white car parked in a parking lot. The background is slightly blurred, showing other cars and a building.

MOTHERBOARD
TECH BY VICE

Watch Dozens of Cars Go Haywire, Apparently Due to Signal Jammers

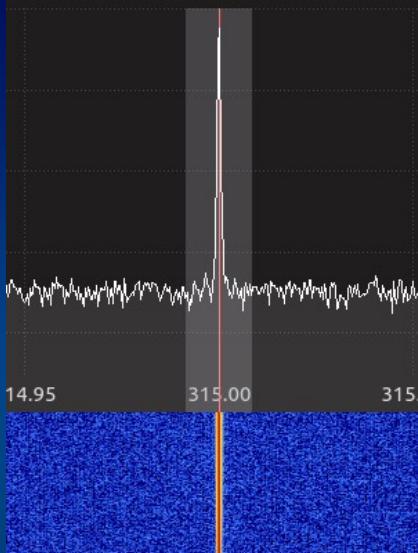
Cars honked relentlessly, and their bewildered owners stood around the full parking lot, unable to enter their vehicles.

By Joseph Cox

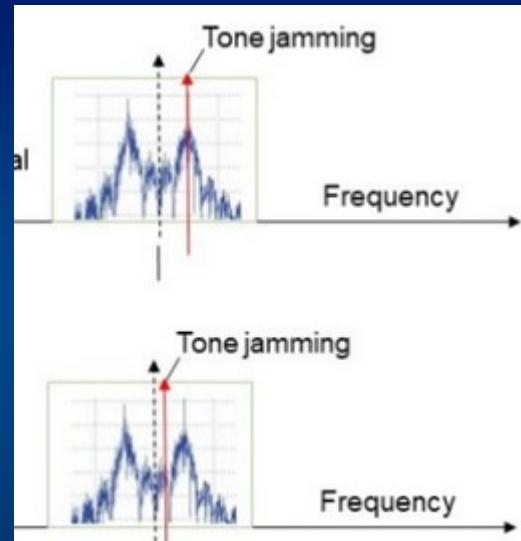
May 21, 2015, 9:17am [Share](#) [Twitter](#) [Snap](#)

Jamming

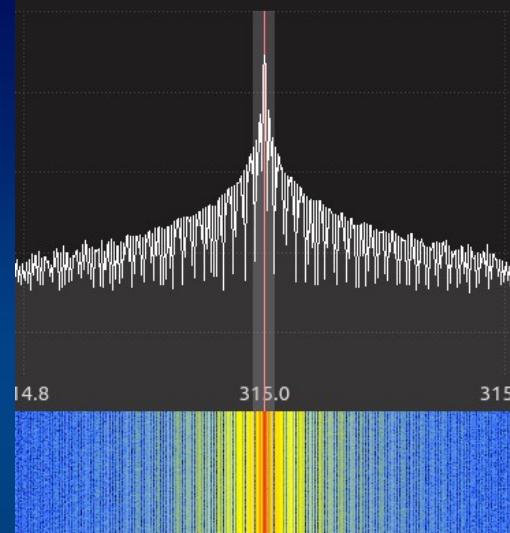
Narrowband jammer



When narrow jamming FSK, try to jam mark or space freq., not center



“Wideband” jammer



Lots of Phase Noise,
Generated with square wave
Arduino tone() function

Capure Effect: Receiver will only listen to the strongest signal during FSK.
You can jam with binary signal instead of tone (known noise)

<https://www.emsopedia.org/entries/tones-jamming-against-radio-communications/>

<https://www.ndss-symposium.org/wp-content/uploads/2023/02/vehiclesec2023-23037-paper.pdf> (Enhanced Vehicular Roll-Jam Attack using a Known Noise Source)

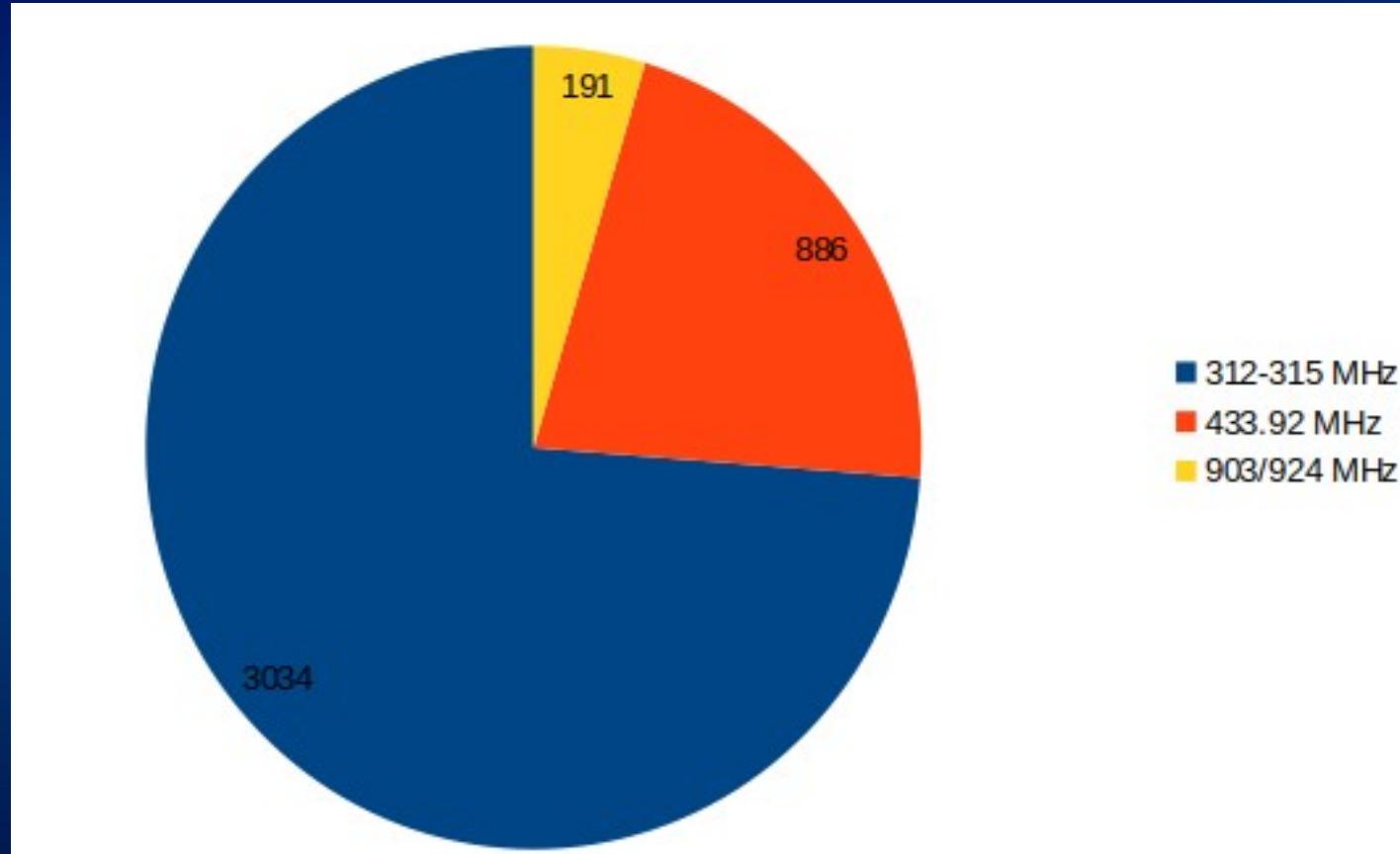
Garage Door Frequencies (MHz)

Liftmaster, Do-It, Master Mechanic, Raynor, True Value and Sears are compatible with Chamberlain

	Brand	Type/Color of Smart/Learn	Year		Brand	Description	Year
318	Linear®	Mega-Code	'97-Current	390	Chamberlain®*	9 Position	'90-'92
390	Chamberlain®*	Orange/Red	'97-'03		Chamberlain®*	9 Position	'83-'89
315	Chamberlain®*	Purple	'05-Current		Canada		
390	Chamberlain®*	Green	'93-'96		Genie®	12 Position	'85
315	Genie® Overhead Door®	Intellicode	'95-Current	300	Linear Multicode®	10 Position	'76
390	Genie®** Overhead Door®	Intellicode	'93-Current	390	Chamberlain®	8 Position	'83-'89
310	Stanley®	Secure Code	'98	310	Stanley/ Multicode®	10 Position	'76
390	Chamberlain®*	Yellow	'11-Current		Genie®	9 Position	'85
372.5	Wayne Dalton®	Rolling Code	'99	310	Linear® Moore-O-Matic®	8 Position	'76
390	Chamberlain®	9 Position	'90-'92	390	Chamberlain®	7 Position	'83-'89

Common Car Frequencies

Approx 4000 makes/models/years. Most US cars use 315 MHz



Published Exploits

Chamberlain Garage Doors

Security+ and Security+2.0 rolling code has been reverse engineered
Decoder and encoder available

<https://github.com/argilo/secplus>

RTL_433 also has decoder
https://github.com/merbanan/rtl_433



https://github.com/argilo/secplus

README.md

Usage

Receiving:

```
$ ./secplus_rx.py

Security+: rolling=2320616982 fixed=876029923 (id1=2 id0=0 switch=1 remote_id=32445552 button=lef
Security+: rolling=3869428094 fixed=876029922 (id1=2 id0=0 switch=0 remote_id=32445552 button=mid
Security+: rolling=2731817112 fixed=876029924 (id1=2 id0=0 switch=2 remote_id=32445552 button=rig
Security+: rolling=2731817116 fixed=876029924 (id1=2 id0=0 switch=2 remote_id=32445552 button=rig
Security++: rolling=2615434900 fixed=72906373 (id1=0 id0=0 switch=1 pad_id=1478 pin=1234)
Security++: rolling=2615434904 fixed=595608121 (id1=0 id0=0 switch=1 pad_id=1478 pin=enter)
Security++ 2.0: rolling=240124680 fixed=70678577664 (button=16 remote_id=1959100928)
Security++ 2.0: rolling=240124681 fixed=70678577664 (button=16 remote_id=1959100928)
Security++ 2.0: rolling=240124682 fixed=62088643072 (button=14 remote_id=1959100928)
Security++ 2.0: rolling=240124683 fixed=66383610368 (button=15 remote_id=1959100928)
Security++ 2.0: rolling=240124684 fixed=74973544960 (button=17 remote_id=1959100928)
```

Transmitting Security+:

```
$ ./secplus_tx.py --freq 315150000 --rolling 2731817118 --fixed 876029924
```

The rolling code should be at least 2 higher than the previously transmitted rolling code.

Transmitting Security+ 2.0:

With rolling and fixed codes only:

```
$ ./secplus_v2_tx.py --freq 315000000 --rolling 0xe50030d --fixed 0x1074c58200
```

With optional supplemental data (e.g. PIN):

```
$ ./secplus_v2_tx.py --freq 315000000 --rolling 0xe50030d --fixed 0x1074c58200 --data 0xd204b000
```

The rolling code should be at least 1 higher than the previously transmitted rolling code.

Published Exploits

Linear Garage Door Mega-Code

Discovered there is no rolling code. Susceptible to replay attack

Decoder available on Github and RTL_433
<https://github.com/aaronsp777/megadecoder>



<https://github.com/aaronsp777/megadecoder/blob/main/Protocol.md>

Decoding the bits

The first bit (the start bit) is always a binary 1, followed by a 4-bit Facility Code, a unique 16-bit Unique Remote Code, and a 3-bit Button Code.

24 bit frames: A diagram showing a 24-bit frame structure. It consists of four colored segments: a blue "start" segment, a yellow "Facility code (4)" segment, an orange "Unique code (16)" segment, and a blue "Button code (3)" segment. The segments are separated by thin vertical lines.

Facility Codes, Remote Codes, and Button Codes

Facility Codes

Remotes are programmed with a 4-bit facility code that ranges from 1 to 15. I've never seen 0 used on a transmitter, though often 0 is used on receivers to mean match any facility code number.

Unique Remote Code

Remotes that are sold individually typically have a 16-bit unique code printed in decimal on a sticky label. The label is important in that many receivers require the number for programming from a touch-tone keypad.

With 16 bits, in theory this yields values in theory from 1 to 65535. Values less than 10000 will have a leading 0. I've never seen a value less than 1000.

Bulk packages of transmitters are often sold in blocks of 100 and have a start range and end range of codes. Each remote has a number one higher than the previous in the pack. They typically also share the same Facility code. This allows convenient *Block Programming* on the receiver.

I've heard of resellers breaking these packs up and selling them individually though typically they don't have the sticker on the back of each remote with the code necessary for programming most systems that require the number. However they can work with Linear Garage Door Openers that have a *Learn Button* even if you don't know the code.

For the record, I mainly made this project so I could figure out what the code was when presented with a remote without a label.

RTL-SDR.com blog

Great resource for finding RF security news & exploits

The screenshot shows a web browser window with the URL [https://www.rtl-sdr.com/category/security-2/](https://www rtl-sdr com/category/security-2/). The page title is "RTL-SDR.COM". Below it, a sub-headline reads "RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRplay and more.". A navigation bar includes links for HOME, ABOUT RTL-SDR, QUICK START GUIDE, FEATURED ARTICLES, SOFTWARE, SIGNAL ID WIKI, FORUM, RTL-SDR STORE (which is highlighted in orange), and GUIDE BOOK.

Category: **Security**

FEBRUARY 28, 2025

RTL-SDR JAMMING DETECTOR SOFTWARE

Over on GitHub, Alejandro Martín has recently released his [open-source 'rtl-sdr-analyzer' software](#), which is an RTL-SDR-based signal analyzer and automatic jamming detector. The software is based on Python and connects to the RTL-SDR via an `rtl_tcp` connection.

Alejandro's software is advertised as having the following features:

“ • **Real-time Visualization:** Advanced spectrum analysis with waterfall display
• **Smart Detection:** Automatic signal anomaly and jamming detection
• **Dynamic Analysis:** Adaptive baseline calculation and threshold adjustment
• **Flexible Configuration:** Fully customizable detection parameters
• **Network Support:** Built-in RTL-TCP compatibility for remote operation **”**

The software works by continuously monitoring a frequency range, and creating a log whenever a signal is detected that exceeds a certain power value and duration. It can also monitor 'z-score', which determines if the current signal mean has deviated significantly from the baseline, which could indicate a jamming or interference event.

DISCOVER

Affordably Receiv
- L-band Weather
- Hydrogen Line R
- Inmarsat STD-C

FOLLOW US

WEEKLY NEWSLETTER UPDATES

Enter your email address:

Subscribe

Published Exploits

Cars: Replay attacks and weak rolling codes

The screenshot shows the RTL-SDR.com homepage with a navigation bar at the top. Below the navigation, a news article is displayed with a timestamp, title, and a summary paragraph.

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDR

HOME ABOUT RTL-SDR QUICK START GUIDE FEATURED ARTICLES SOFTWARE SIGNAL ID WIKI FORUM RSS

OCTOBER 27, 2017

USING AN RTL-SDR AND RPITX TO DEFEAT THE ROLLING CODE SCHEME USED ON SOME SUBARU CARS

Over on GitHub Tom Wimmenhove has been [experimenting with the car keyfob on his Subaru car, and has discovered that the rolling code scheme used is very weak](#) and so can be easily exploited.

Some early model (2005-2010) Subarus; FCC ID NHVWB1U711
Rolling code only increments by 1

<https://www rtl-sdr com/using-an-rtl-sdr-and-rpitx-to-defeat-the-rolling-code-scheme-used-on-some-subaru-cars/>

<https://github.com/tomwimmenhove/subarufobrob>

Published Exploits

Cars: Replay attacks and weak rolling codes

Replay attack. 2006 Toyota Camry; FCC ID GQ43VT14T

The screenshot shows the RTL-SDR.COM homepage with a navigation bar at the top. Below the navigation, a specific blog post is displayed. The post's title is "USING AN RTL-SDR AND RPITX TO UNLOCK A CAR WITH A REPLAY ATTACK". The date of the post is December 17, 2018. The main content of the post discusses how a YouTube user named "ModernHam" used a Raspberry Pi running RPiTX and an RTL-SDR to perform a replay attack on a 2006 Toyota Camry. It explains that a replay attack involves recording an RF signal and then replaying it with a transmit capable radio. RPiTX is described as a program that turns a Raspberry Pi into a general purpose RF transmitter. The post also mentions the process of recording a raw IQ file with the RTL-SDR and using RPiTX's "sendiq" command to transmit the recorded signal.

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRplay a

HOME ABOUT RTL-SDR QUICK START GUIDE FEATURED ARTICLES SOFTWARE SIGNAL ID WIKI FORUM RTL-SDR

DECEMBER 17, 2018

USING AN RTL-SDR AND RPITX TO UNLOCK A CAR WITH A REPLAY ATTACK

Over on YouTube user [ModernHam](#) has uploaded a video showing how to perform a replay attack on a car key fob using a Raspberry Pi running RPiTX and an RTL-SDR. A replay attack consists of recording an RF signal, and then simply replaying it again with a transmit capable radio. RPiTX is a program that can turn a Raspberry Pi into a general purpose RF transmitter without the need for any additional hardware.

The process is to record a raw IQ file with the RTL-SDR, and then use RPiTX V2's "sendiq" command to transmit the exact same signal again whenever you want. With this set up he's able to unlock his 2006 Toyota Camry at will with RPiTX.

<https://www rtl-sdr com/using-an-rtl-sdr-and-rpitx-to-unlock-a-car-with-a-replay-attack/>

https://youtu be/M2JY1_Xmokg

Published Exploits

Cars: Replay attacks and weak rolling codes

Replay attack: 2006 Jeep Patriot; FCC ID OHT692427AA / OHT692713AA

The screenshot shows the RTL-SDR.COM homepage with a search bar containing the word "jeep". Below the search bar, the date "MAY 4, 2016" is visible. A large, bold title "USING A HACKRF TO PERFORM A REPLAY ATTACK AGAINST A JEEP PATRIOT" is displayed prominently. The URL of the article is visible at the bottom of the page.

RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRpla

HOME ABOUT RTL-SDR QUICK START GUIDE FEATURED ARTICLES SOFTWARE SIGNAL ID WIKI FORUM RTL-S

Search results for: jeep

MAY 4, 2016

USING A HACKRF TO PERFORM A REPLAY ATTACK AGAINST A JEEP PATRIOT

<https://www rtl-sdr com/using-a-hackrf-to-perform-a-replay-attack-against-a-jeep-patriot/>

Published Exploits

Cars: Replay attacks and weak rolling codes

Replay and Rollback: Honda; many models. FCC ID KR5V1X / KR5V2X

JULY 14, 2022

ROLLING-PWN: WIRELESS ROLLING CODE SECURITY COMPLETELY DEFEATED ON ALL HONDA VEHICLES SINCE 2012

Back in May [we posted](#) about CVE-2022-27254 where university student researchers discovered that the wireless locking system on several Honda vehicles was vulnerable to simple RF replay attacks. A replay attack is when a wireless signal such as a door unlock signal is recorded, and then played back at a later time with a device like a HackRF SDR. This vulnerability only affected 2016-2020 Honda Civic vehicles which came without rolling code security.

MAY 5, 2022

OPENING AND STARTING HONDA CIVIC VEHICLES WITH A HACKRF REPLAY ATTACK

A few months ago University student [Ayyappan Rajesh](#) and [HackingIntoYourHeart](#) reported [cybersecurity vulnerability CVE-2022-27254](#). This vulnerability demonstrates how unsecure the remote keyless locking system on various Honda vehicles is, and how it is easily subject to very simple wireless replay attacks. A replay attack is when a wireless signal such as a door unlock signal is recorded, and then played back at a later time with a device like a HackRF SDR.

<https://www rtl-sdr com/opening-and-starting-honda-civic-vehicles-with-a-hackrf-replay-attack/>

<https://www rtl-sdr com/rollingpwn-wireless-rolling-code-security-completely-defeated-on-all-honda-vehicles-since-2012/>

Published Exploits

RollBack Table w/ FCC IDs

Car Make	Car Model	Car Model year	Car Built year	Vulnerable to RollBack?	# SIGNALS	SEQUENCE	TIMEFRAME	FCC ID
BMW	1 series (e87)	2004-2007	2005	NO				KR55WK49121
Hyundai	Avante		2020					OSLOKA-420T
Hyundai	Elantra	2013-2015		2015 YES				RKE-4F07
Hyundai	Elantra		2012	2012 NO				SVI-MDFEV03
Kia	Cerato/Forte K3	2016-2018		2017 YES				OSLOKA-870T
Kia	Cerato/Forte K3	2012-2018		2015 YES				OSLOKA-870T
Kia	Cerato/Forte K3	2012-2018		2015 YES				OSLOKA-870T
Mazda	3 skyactive	N/A, 2018		2018 YES				SKE13E-02
Mazda	2 sedan skyactive		2018	2018 YES				SKE13E-01
Mazda	2 Hatch-back		2020	2020 YES				SKE13E-02
Mazda	CX-5		2018	2018 YES				SKE13E-01
Mazda	CX-3		2019	2019 YES				SKE13E-02
Nissan	Teana		2014	2014 NO				N/A
Nissan	Latio	2007-2012		2009 YES			Within 5 seconds	N/A
Nissan	Sylphy	2012-2019	N/A	YES			Within 8 seconds	CWTWB1U815
Toyota	Wish	2009-2017	N/A	NO				N/A
Toyota	Corolla Axio	2015-2017	N/A	NO				N/A
Toyota	Altis		2005	N/A				BA4EQ
Toyota	Prius (hybrid)	2020-		2020 NO				HYQ14FBC
Opel	Crossland		2018	2018 NO				N/A
Honda	Fit (hybrid)	2016-2018	N/A	YES			No restiction	KR5V1X
Honda	Fit		2018	N/A			No restiction	MLBHLIK6-1T
Honda	City		2017	2017 YES			No restiction	KR5V1X
Honda	Vezel	2016-2022		2017 YES			No restiction	KR5V1X
VW	Touareg		2007	2008 NO				KR55WK45032
BMW	X3		2011	2011 NO				KR55WK49863
Opel	Vivaro		2012	2011 NO				N/A
Mazda	Mazda 2 Sedan		2017	2017 YES			No restiction	SKE13E-01
Toyota	Toyota Rush	N/A		2017 YES			No restiction	N/A
Toyota	Toyota Hilux Conquest	N/A		2020 NO				BM1EW

Keyfob Database

- If we know the FCC ID of a vulnerable car/keyfob, we can find other vulnerable makes/models that share the same keyfob ID
- Amazon will usually list other cars that use the same FCC ID
- Time consuming to search & scrape Amazon

The screenshot shows an Amazon search results page for the query "kr5v2x". The search bar at the top has "All" selected and contains "kr5v2x". Below the search bar is a navigation menu with categories like Best Sellers, Amazon Basics, New Releases, Prime, Today's Deals, Music, Books, Registry, Fashion, Amazon Home, Gift Cards, Pharmacy, One Medical, and Toys & Games. A secondary navigation menu below it includes Best Sellers, Parts, Accessories, Tools & Equipment, Car Care, Motorcycle & Powersports, Truck, RV, Tires & Wheels, and Vehicle Showroom. A promotional banner in the center says "Get prepared for your next summer adventure" with a link to shop car care, accessories & more. The main search results area displays a product listing for a "Key Fob Remote Replacement Fits for Honda Civic 2016 2017 2018 2019 2020 2021 KR5V2X Smart Proximity Keyless Entry Remote Control Uncut 5 Buttons 433Mhz (72147-TBA-A11)". The product is from the brand MechanMagic, has a 4.4 rating from 26 reviews, and is priced at \$37.95. It includes a "FREE Returns" link and a note about getting \$60 off with an Amazon Store Card. Below the main listing are detailed product specifications: Brand: MechanMagic, Vehicle Service Type: Car, Number of Buttons: 5, and Product Dimensions: 2.36" L x 1.38" W. To the right of the main listing, there is a sidebar for Prime members with a "Deliver to" button and a large "37" price indicator.

All kr5v2x

Best Sellers Amazon Basics New Releases Prime Today's Deals Music Books Registry Fashion Amazon Home Gift Cards Pharmacy One Medical Toys & Games

Best Sellers Parts Accessories Tools & Equipment Car Care Motorcycle & Powersports Truck RV Tires & Wheels Vehicle Showroom

Get prepared for your next summer adventure
Shop car care, accessories & more

Key Fob Remote Replacement Fits for Honda Civic 2016 2017 2018 2019 2020 2021 KR5V2X Smart Proximity Keyless Entry Remote Control Uncut 5 Buttons 433Mhz (72147-TBA-A11)

Brand: MechanMagic 4.4 ★★★★☆ 26 ratings

\$37⁹⁵

FREE Returns

Get \$60 off instantly: Pay \$0.00 \$37.95 upon approval for the Amazon Store Card. No annual fee.

Brand: MechanMagic
Vehicle Service Type: Car
Number of Buttons: 5
Product Dimensions: 2.36" L x 1.38" W

About this item

Keyfob Database

OEMcarKeyMall.com has FCC IDs for keyfobs in description. Easy to scrape

Acura, Buick, Cadillac, Chevrolet, Chrylser, Dodge, Ford, GMC, Honda, Hyundai, Infiniti, Jaguar, Jeep, Kia, LandRover, Lexus, Lincoln, Mazda, Mitsubishi, Nissan, Saturn, Scion, Subaru, Toyota

The screenshot shows a grid of eight car keyfobs for sale on the OEMcarKeyMall.com website. Each keyfob is shown with its model name, FCC ID, price, and an 'Add to Cart' button.

Keyfob Model	Product Description	Price	Status
2018 Mitsubishi Outlander Smart Remote Key Fob 3B	(FCC: OUC644M-KEY-N, P/N: 8637A316)	\$95.00	Add to Cart
2018 Toyota Camry Remote Flip Key Fob 4B w/ Trunk	(FCC: HYQ12BFH, H Chip, P/N: 89070-06790)	\$45.00	Add to Cart
2017 Dodge Durango Smart Remote Key Fob 5B w/ Hatch, Remote Start	(FCC: M3N-40821302, P/N: 68150061)	\$75.00	Add to Cart
2019 Kia Forte Remote Flip Key Fob 4B w/ Trunk	(FCC: CQOTD00660, P/N: 95430-M6000)	\$69.00	Add to Cart
2012 Nissan Altima Smart Remote Key Fob 4B w/ Trunk	(FCC: KR55WK48903, P/N: 285E3-JA05A)	\$50.00	Add to Cart
2018 Lexus NX300 Smart Remote Key Fob 4B w/ Hatch	(FCC: HYQ14FBA, AG Board 2110, P/N: 89904-78470)	\$115.00	Add to Cart
2017 Jeep Renegade Smart Remote Key Fob 3B	(FCC: M3N-40821302, P/N: 6MP33DX9)	\$55.00	Sold Out
2018 Ford Mustang Smart Remote Key Fob 5B w/ Trunk, Remote Start	(FCC: A2C931426, P/N: 164-R8162)	\$75.00	Add to Cart

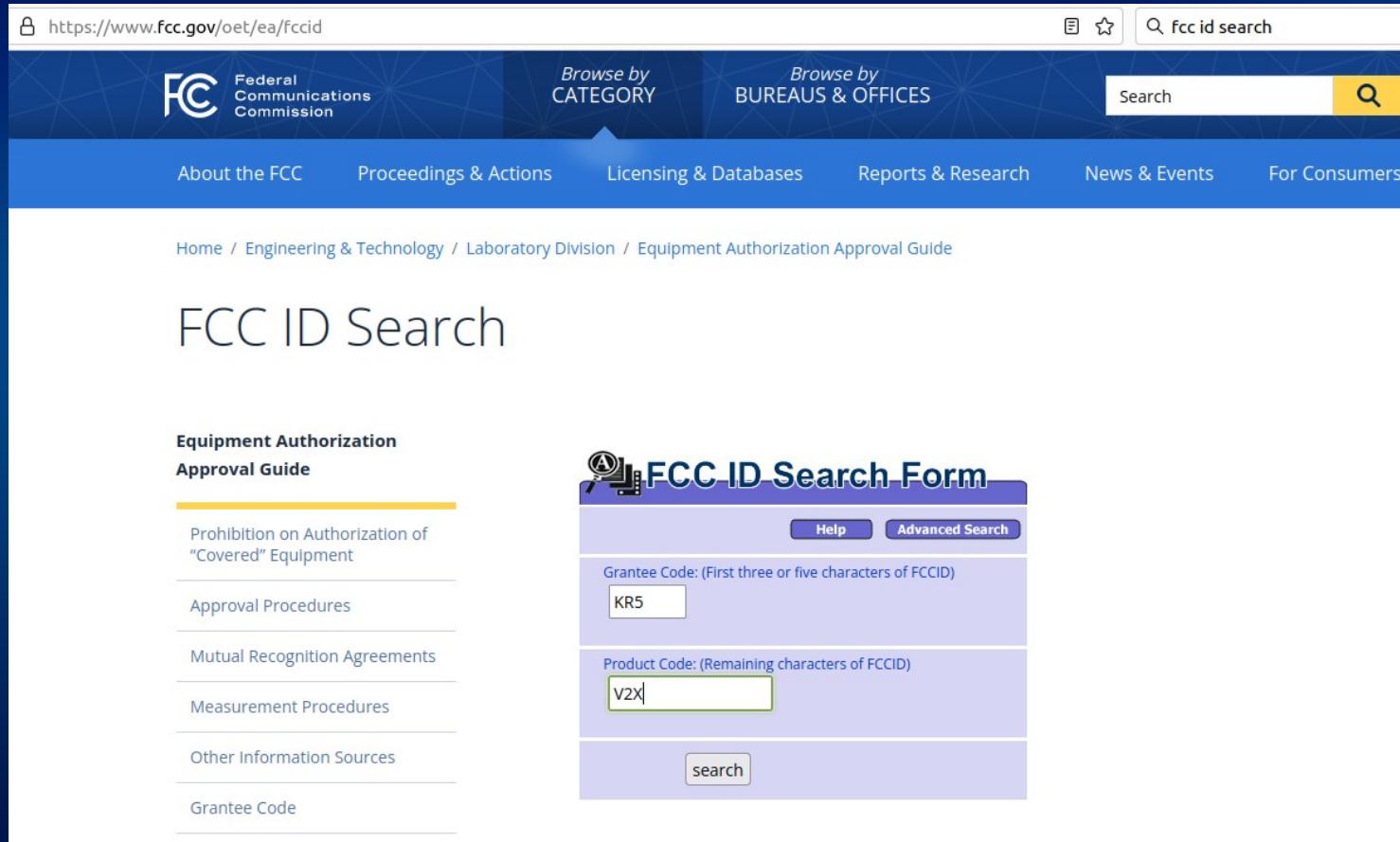
Keyfob Database

Approx 250 FCC ID's shared across ~5000 vehicles

1	Num of models that use FCC ID	FCC ID	Frequency	Modulation
2	380	OUC60270 / OUC60221	315	ASK
3	223	CWTWB1U793	315	ASK
4	175	HYQ14FBA	312.1/314.35	FSK
5	170	M3N-40821302	433.92	ASK
6	162	CWTWB1U331	314.5/315.5	ASK
7	160	IYZ-C01C	433.92	ASK/FSK
8	124	GQ43VT20T	315	ASK
9	114	HYQ14AAB	314.35	ASK
10	107	OHT692713AA	315	ASK
11	100	OUCD6000022	315	ASK
12	84	HYQ14ACX	314.35	FSK
13	79	HYQ4EA	433.92	ASK/FSK
14	79	OHT01060512	315	ASK
15	78	M3N5WY8609	315	ASK/FSK
16	77	M3N-32337100	314.9	ASK
17	75	SY5HMFNA04	315	FSK
18	74	KR5S180144014	433.92	FSK
19	73	KR5V1X	313.55/314.15	FSK
20	69	M3N-A2C93142300	314.95	FSK
21	68	HYQ12BBX	314.35	ASK
22	67	CWTWB1U821	315	ASK
23	65	N5F-A08TAA	314.95	ASK
24	63	HYQ4AA	314.9	ASK/FSK
25	62	OHT692427AA	315	ASK
26	59	M3N-A2C93142600	902.375/903.425	FSK
27	57	KBRASTU15	315	ASK
28	56	BGBX1T478SKE125-01	315	FSK
29	55	KR55WK49622	315	FSK
30	53	GQ4-29T	315	ASK
31	52	KOBGT04A	315	ASK
32	51	GQ43VT14T	315	???
33	46	KR580399900	924/924.6	FSK
34	45	CWTWB1U766	433.92	ASK
35	44	M3N-A2C931426	902.375/903.425	FSK
36	44	WAZSKE13D02	315	FSK
37	42	GQ4-54T	433.92	ASK
38	42	HYQ12BBY	314.35	ASK

Keyfob Database

- Had to manually search 250 FCC IDs for frequency & modulation
- FCC site is not easy to scrape, uses PDFs



The screenshot shows the FCC ID Search page. At the top, there's a navigation bar with links for About the FCC, Proceedings & Actions, Licensing & Databases, Reports & Research, News & Events, and For Consumers. Below the navigation bar, a breadcrumb trail shows Home / Engineering & Technology / Laboratory Division / Equipment Authorization Approval Guide. The main title is "FCC ID Search". On the left, there's a sidebar with a link to the "Equipment Authorization Approval Guide". The main content area features a form titled "FCC ID Search Form" with fields for "Grantee Code" (containing "KR5") and "Product Code" (containing "V2X"). A "search" button is at the bottom of the form.

https://www.fcc.gov/oet/ea/fccid

Federal Communications Commission

Browse by CATEGORY

Browse by BUREAUS & OFFICES

Search

About the FCC Proceedings & Actions Licensing & Databases Reports & Research News & Events For Consumers

Home / Engineering & Technology / Laboratory Division / Equipment Authorization Approval Guide

FCC ID Search

Equipment Authorization Approval Guide

Prohibition on Authorization of "Covered" Equipment

Approval Procedures

Mutual Recognition Agreements

Measurement Procedures

Other Information Sources

Grantee Code

FCC ID Search Form

Help Advanced Search

Grantee Code: (First three or five characters of FCCID)
KR5

Product Code: (Remaining characters of FCCID)
V2X

search

Keyfob Database

FCC ID Searching for Frequency & Modulation

The screenshot shows a search result for the FCC ID KR5V2X. The result is displayed in a table with the following columns:

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State/Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
				Continental Automotive Technologies GmbH	Siemensstrasse 12	Regensburg	N/A	Germany 93055	KR5V2X	Original Equipment	04/15/2013	433.66	434.18

Two red arrows point to the "Detail Summary" link in the first row of the table and the "Upper Frequency In MHz" value of 434.18 in the last column.

“Detail” link will provide more information

Frequency

Keyfob Database

FCC ID Test Report usually contains modulation info

itReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&ap... 

OET Exhibits List

10 Matches found for FCC ID KR5V2X

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
declaration of authorization	Cover Letter(s)	04/12/2013	pdf	04/15/2013
long term confidentiality	Cover Letter(s)	04/12/2013	pdf	04/15/2013
external photo	External Photos	04/12/2013	pdf	04/15/2013
ID label/Location info	ID Label/Location Info	04/12/2013	pdf	04/15/2013
internal photo	Internal Photos	04/12/2013	pdf	04/15/2013
test report	Test Report	04/12/2013	pdf	04/15/2013
test report(Occupied Bandwidth Plot)	Test Report	04/12/2013	pdf	04/15/2013
test report(Periodic Operation Characteristics)	Test Report	04/12/2013	pdf	04/15/2013
test setup photo	Test Setup Photos	04/12/2013	pdf	04/15/2013
user manual	Users Manual	04/12/2013	pdf	04/15/2013



https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=1937653 

Date of order : 2013-03-15
References : Mrs. Dagmar Kolar

5. Product and product documentation

Samples of the following apparatus were submitted for testing:

Manufacturer	: Continental Automotive GmbH
Trademark	: Continental
Type designation	: V2x
Hardware versions	: ---
Variants	: V4x
Serial number	: ---
Software release	: ---
Type of equipment	: Transmitter
Power used	: 3.0 V DC
Frequency band used	: 433.660 MHz to 434.180 MHz
Generated or used frequencies	: Channel 1: 433.660 MHz (carrier) / 13.08 MHz (crystal) Channel 2: 434.180 MHz (carrier) / 13.08 MHz (crystal)
ITU emission class	: Channel 1: 58K6 F1D / Channel 2: 63K7 F1D
FCC ID	: KR5V2X



Emission Designator "F" means FSK

Keyfob Database

What if we don't know the make/model of a target vehicle?
If you know the license plate, several websites will provide
vehicle VIN, year, make, model, etc.

The screenshot shows two consecutive pages from the FAXVIN website:

Page 1: License Plate Lookup

URL: <https://www.faxvin.com/license-plate-lookup>

The page features a navigation bar with links to Home, VIN Check, VIN Decoder, Sample Reports, Help, Contact Us, and Account Login. Below the navigation is a logo for "FAXVIN™" with a green circular icon. A horizontal progress bar indicates the user is at the "Type a Plate" step. The main content area is titled "License Plate Lookup" and includes the sub-instruction "Search and Check License Plate and get Vehicle History Report". There is a search form with input fields for the license plate number "36014", a dropdown for the state "Nebraska (NE)", and a green "Check Plate" button. An example plate number "6SRM917 CA" is shown below the input fields.

Page 2: Result Page for License Plate 36014

URL: <https://www.faxvin.com/license-plate-lookup/result?plate=36014&state=NE>

The page title is "2020 Ford Explorer". The top navigation bar and FAXVIN logo are identical to the previous page. The progress bar now highlights the "Decoder" step. The main content area displays a blue header "Successfully Decoded" followed by the vehicle information: "2020 Ford Explorer" and the VIN "1FMSK8AB2LGA41722". To the right is a small image of the license plate "36014". Below this, a table provides detailed decoded information:

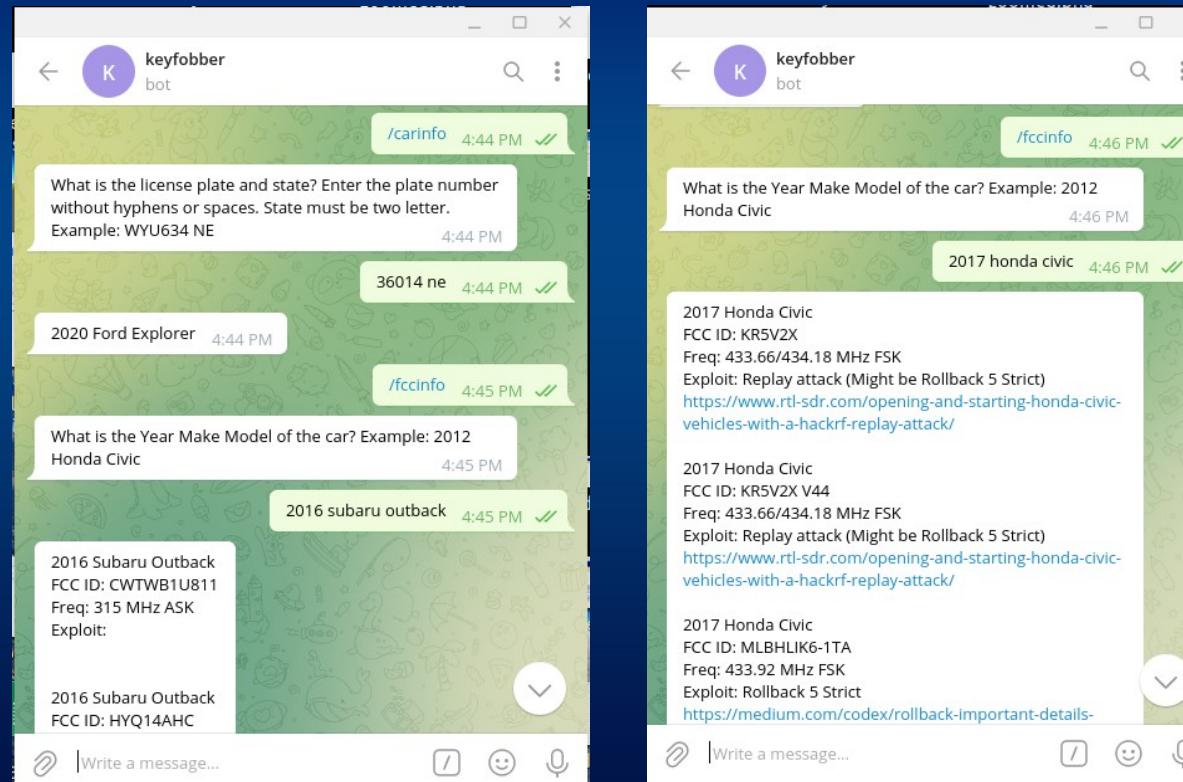
VIN	Make	Model	Year	Trim
1FMSK8AB2LGA41722	Ford	Explorer	2020	Police 4WD
Style/Body	Engine	Manufactured in	Age	
SPORT UTILITY 4-DR	3.3L V6 DOHC 24V	UNITED STATES	3 years	

At the bottom are two buttons: "Check Next Plate" and a green "Continue" button with a right-pointing arrow.

Keyfob Database

Telegram Bot

Automated database and license plate lookup, accessible over Telegram app (smartphone)
Provides year/make/model of vehicle, keyfob frequency, modulation, FCC ID,
and known exploits github.com/gusgorman402/keyfobDB



Database is just a CSV file that bot greps

keyfobDB / car_fcc_info_DB.csv								Top		
	Preview	Code	Blame	4207 lines (4207 loc) · 232 KB				Raw	CSV	JSON
67	2000	Ford	Ranger	CWTWB1U331	314.5/315.5	ASK				
68	2000	Ford	Taurus	CWTWB1U331	314.5/315.5	ASK				
69	2000	Ford	Windstar	CWTWB1U331	314.5/315.5	ASK				
70	2000	Nissan	Altima	KOBUTA3T	315	???				
71	2000	Nissan	Frontier	KOBUTA3T	315	???				
72	2000	Nissan	Quest	KOBUTA3T	315	???				
73	2000	Nissan	Xterra	KOBUTA3T	315	???				
74	2000	Subaru	Forester	NHVWB1U711	433.92	ASK	Rolling code increments by 1		https://www rtl sdr com using an rtl sdr and rpi tx to defeat the rolling code scheme used on some subaru cars	
75	2000	Toyota	4Runner	HYQ12BBX	314.35	ASK				
76	2000	Toyota	Avalon	HYQ12BAN	314.35	ASK				
77	2000	Toyota	Camry	GQ43VT14T	315	???	Replay attack		https://www rtl sdr com using an rtl sdr and rpi tx to unlock a car with a replay attack	
78	2000	Toyota	Celica	GQ43VT14T	315	???	Replay attack		https://www rtl sdr com using an rtl sdr and rpi tx to unlock a car with a replay attack	
79	2000	Toyota	Celica	HYQ12BAN	314.35	ASK				
80	2000	Toyota	Celica	HYQ12BBX	314.35	ASK				
81	2000	Toyota	Echo	HYQ12BBX	314.35	ASK				
82	2000	Toyota	Sienna	GQ43VT14T	315	???	Replay attack		https://www rtl sdr com using an rtl sdr and rpi tx to unlock a car with a replay attack	
83	2000	Toyota	Solara	GQ43VT14T	315	???	Replay attack		https://www rtl sdr com using an rtl sdr and rpi tx to unlock a car with a replay attack	
84	2000	Toyota	Solara	HYQ12BAN	314.35	ASK				
85	2000	Toyota	Tacoma	ELVATDD	433.92	ASK				
86	2000	Toyota	Tacoma	HYQ12BBX	314.35	ASK				

Future Plans

- Make the database relational (SQL) to reduce space
(e.g. one FCC ID may be linked to 200 cars)
- Add info if a RTL_433 decoder is available

```
waffles@junco:~/rtl_433/src/devices$ ls -1 | grep remote
dish_remote_6_3.c
fordremote.c
generic_remote.c
hondaremote.c
```

- Add more data. Focus more on forensics & surveillance
(e.g. Kismet)

Kismet can use RTL_433

- Kismet monitors & logs wifi, bluetooth, and radio (RTL-SDR)
- RTL_433: linux cmd line decoder for sensors and keyfobs. Users can submit new decoders

The screenshot shows the Kismet web interface running on DragonOS_10_Public [Running]. The main page displays a table of detected devices, with columns including Name, Type, Phy, Crypto, Signal, Channel, Last Seen, Data, Packets, Clients, BSSID, and QBSS Chan Usage. Below the table, a message log shows various ADSB detections:

Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID	QBSS Chan Usage
ADS8 afe24e	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:08	0 B	0	0	n/a
ADS8 afebcfa	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:15	0 B	0	0	n/a
ADS8 a446b6	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:09	0 B	0	0	n/a
ADS8 aafed1	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:09	0 B	0	0	n/a
ADS8 aaf251	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:12	0 B	0	0	n/a
Airbus A319-111 AAY7001 Allegiant Air	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:14	0 B	0	0	n/a
Airbus A319-114 DAL1900 Delta Air Lines	Airplane	RTLADSB	n/a	n/a	1.090 GHz	Mar 22 2020 18:41:09	0 B	0	0	n/a

Below the table, a "Messages" section shows log entries:

```
Mar 22 2020 18:41:05 Detected new ADSB device ICAO a6b137 type 'pa31' operator 'Private owner'
Mar 22 2020 18:41:06 Detected new ADSB device ICAO afe24e type 'c172'
Mar 22 2020 18:40:54 Detected new ADSB device ICAO a385da type 'a319' operator 'Allegiant Air'
Mar 22 2020 18:40:46 Detected new ADSB device ICAO abed21 type 'b738' operator 'Southwest Airlines'
Mar 22 2020 18:40:46 Detected new ADSB device ICAO a65119 type 'a320' operator 'JetBlue Airways'
Mar 22 2020 18:40:46 Detected new ADSB device ICAO a14e8 type 'a319' operator 'Delta Air Lines'
Mar 22 2020 18:40:45 Detected new ADSB device ICAO ac533c type 'crj2' operator Delta Connection
```

At the bottom, a footer notes: "Powered by many OSS components, see the [credit page](#)".

Sensor - SDR rtl_433

Kismet can leverage the cheap [rtl-sdr](#) software defined radio and the amazing [rtl_433](#) tool to collect information about RF sensors, weather stations, tire pressure monitors, switches, humidity, power meters, gas meters, water meters, lightning detectors, and more.

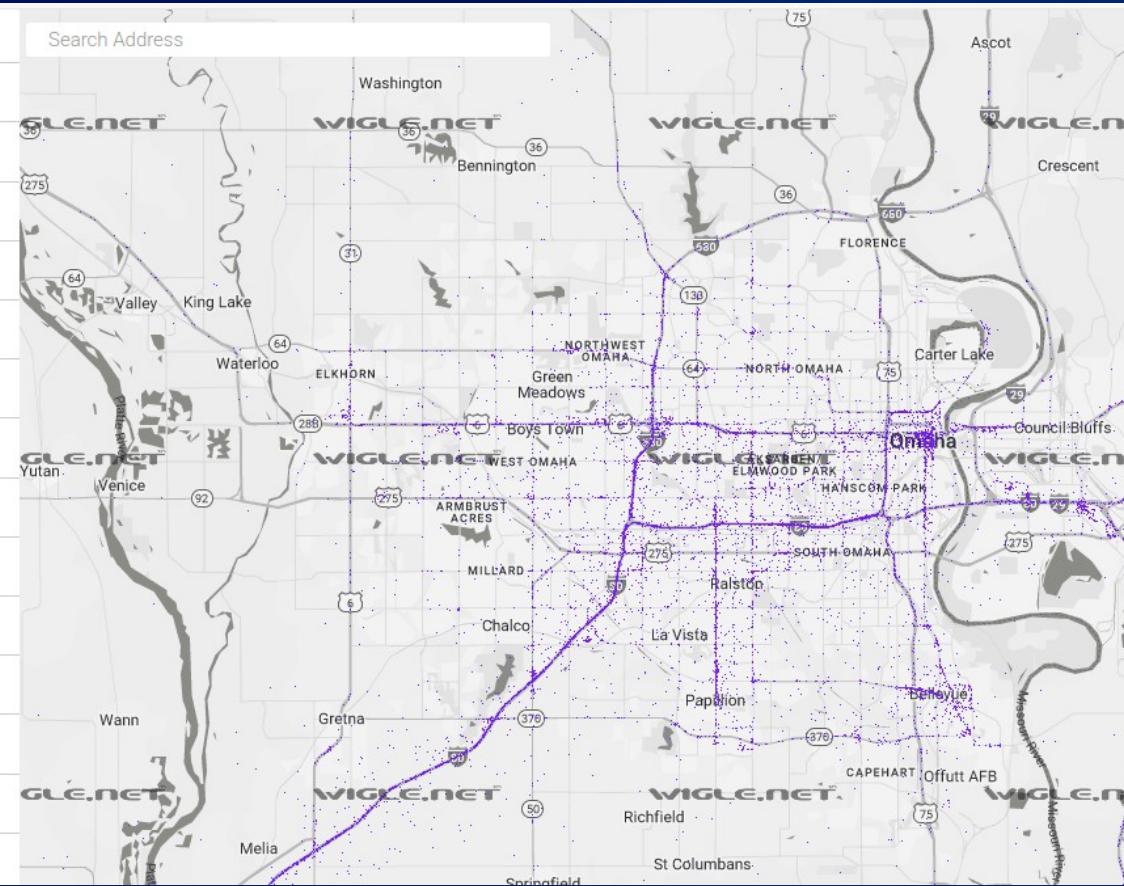
The SDR RTL_433 source can autodetect rtl-sdr devices automatically, and can be manually specified with `type=rtl433` :

```
source=rtl433-0:type=rtl433
```

Easy to associate wifi SSID & MAC to car make, not so easy to determine model or year

MAC starts with
00:92:A5

 myChevrolet3226 QoS: 0 type: infra 00:92:A5:65:A7:86 ch: 44 2024-11-04 - 2024-11-04
 myChevrolet3226 QoS: 2 type: infra 00:92:A5:65:A7:87 ch: 1 2024-03-17 - 2024-11-04
 myChevrolet5469 QoS: 2 type: infra 00:92:A5:65:AC:0E ch: 44 2024-05-29 - 2024-06-26
 myChevrolet5438 QoS: 2 type: infra 00:92:A5:65:AC:0F ch: 6 2001-01-01 - 2024-06-26
 myChevrolet6960 QoS: 0 type: infra 00:92:A5:65:AE:1E ch: 44 2024-10-05 - 2024-10-04
 myChevrolet6960 QoS: 0 type: infra 00:92:A5:65:AE:1F ch: 1 2024-10-05 - 2024-10-04
 myChevrolet2999 QoS: 0 type: infra 00:92:A5:65:AE:EB ch: 1 2024-12-02 - 2024-12-02
 myChevrolet8705 QoS: 0 type: infra 00:92:A5:95:C3:DA ch: 44 2023-12-05 - 2023-12-05
 myChevrolet8705 QoS: 0 type: infra 00:92:A5:95:C3:DB ch: 1 2023-12-05 - 2023-12-05
 myChevrolet5968 QoS: 0 type: infra 00:92:A5:95:C4:E2 ch: 44 2024-02-14 - 2024-02-20
 myChevrolet8532 QoS: 0 type: infra 00:92:A5:95:D2:07 ch: 1 2024-08-20 - 2024-12-22
 myChevrolet8674 QoS: 0 type: infra 00:92:A5:95:D4:6D ch: 1 2023-12-22 - 2024-02-20
 myChevrolet5724 QoS: 0 type: infra 00:92:A5:95:DE:7B ch: 1 2024-02-02 - 2024-02-02
 myChevrolet0828 QoS: 0 type: infra 00:92:A5:95:E5:22 ch: 44 2024-05-20 - 2024-05-20
 myChevrolet9926 QoS: 0 type: infra 00:92:A5:95:EB:3D ch: 6 2024-03-03 - 2024-12-26



(Wigle warbiking has given me more info than google)

Sometimes the car model is in the AP name (Toyota bluetooth)

search for networks

WiFi Cell BT

Lat: 40.9688 to: 41.4539

Lon: -96.4081 to: -95.7489

Last Updated: 20010925174546

BSSID/MAC: 0A:2C:EF:3D:25:1B or 0A:2C:E

Network Name (wildcards¹: % and _:)

TOYOTA%

Only Nets I Was the First to See

Query

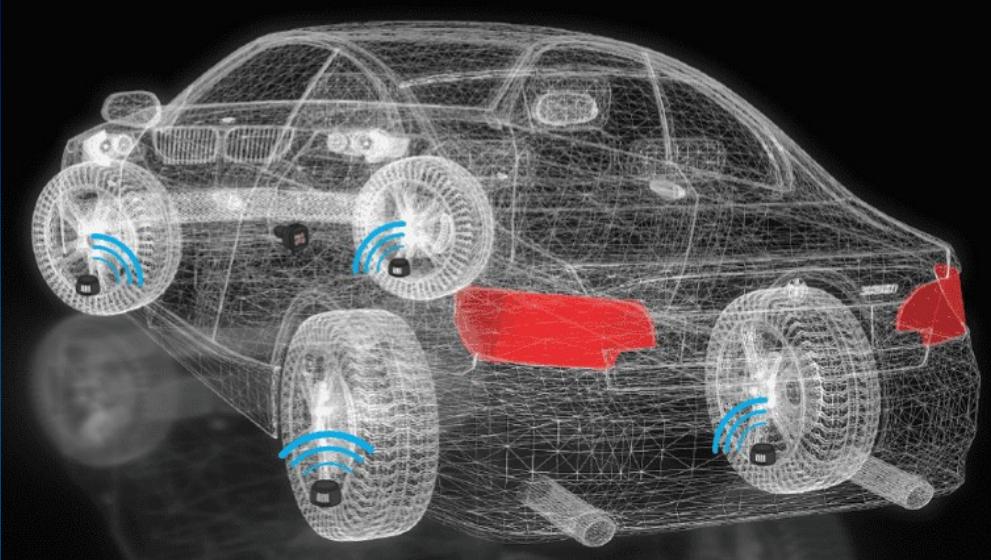
¹ '%': 0-or-more characters, '_': a single character.

- Bluetooth TOYOTA RAV4 QoS: 0 type: BT
30:df:17:5e:14:02 ? 2025-03-03 - 2025-03-03
- Bluetooth TOYOTA RAV4 QoS: 0 type: BT
30:df:17:5f:ec:25 ? 2024-10-15 - 2024-10-15
- Bluetooth TOYOTA RAV4 QoS: 0 type: BLE
30:df:17:62:9d:24 ? 2024-06-30 - 2024-06-29
- Bluetooth TOYOTA Corolla QoS: 0 type: BT
30:df:17:c1:e2:4a ? 2023-06-22 - 2023-06-22
- Bluetooth TOYOTA Highlander QoS: 0 type: BT
44:eb:2e:29:39:42 ? 2022-07-01 - 2022-07-01
- Bluetooth TOYOTA Camry QoS: 0 type: BT
74:d7:ca:53:4c:38 ? 2024-08-16 - 2024-08-18
- Bluetooth Toyota Venza QoS: 0 type: BT
74:d7:ca:6a:b3:31 ? 2024-03-15 - 2024-03-21
- Bluetooth TOYOTA 4Runner QoS: 0 type: BT
74:d7:ca:94:51:64 ? 2024-03-26 - 2024-03-29
- Bluetooth TOYOTA Camry QoS: 2 type: BT
74:d7:ca:a6:6b:72 ? 2020-11-19 - 2024-12-27
- Bluetooth TOYOTA RAV4 QoS: 0 type: BLE
84:70:51:51:a7:89 ? 2024-10-15 - 2024-10-15
- Bluetooth TOYOTA RAV4 QoS: 0 type: BLE
84:70:51:52:b0:55 ? 2024-04-05 - 2024-04-04
- Bluetooth TOYOTA Corolla QoS: 0 type: BT
84:70:51:55:ab:a8 ? 2025-03-25 - 2025-03-26
- Bluetooth TOYOTA RAV4 QoS: 0 type: BLE
84:70:51:85:1a:16 ? 2024-10-09 - 2024-10-09
- Bluetooth TOYOTA Tacoma QoS: 0 type: BT
84:70:51:87:19:98 ? 2024-08-10 - 2024-08-10



Tire Pressure Monitoring System

(usually same frequency as the keyfob)



- Usually transmits every few minutes
- Some cars only transmit while driving
- You can make TPMS transmit with TPMS “reset tool”
 - 125 kHz pulse that activates sensor
 - Cheap tools online ~\$10

TPMS

- RTL_433 has decoders for several car makes
- Can link decoders to more makes by TPMS brand

```
waffles@juncos:~/rtl_433/src/devices$ ls -1 | grep tpms
tpms_abarth124.c
tpms_ave.c
tpms_citroen.c
tpms_eezrv.c
tpms_elantra2012.c
tpms_ford.c
tpms_hyundai_vdo.c
tpms_jansite.c
tpms_jansite_solar.c
tpms_kia.c
tpms_nissan.c
tpms_pmv107j.c
tpms_porsche.c
tpms_renault_0435r.c
tpms_renault.c
tpms_toyota.c
tpms_truck.c
tpms_tyreguard400.c
```

ITM Application Chart




Make	Model	Start Year	End Year	Frequency	OEM Sensor Part#	OEM
CHRYSLER	300	2017	2019	433MHZ	68241067AB	SCHRADER
CHRYSLER	300C	2014	2015	433MHZ	56029400AE/ 56029398AB	SCHRADER
CHRYSLER	300M	2002	2004	433MHZ	52088990AC	SCHRADER
CHRYSLER	300 MEDIUM SPECIAL SERIES	2018	2018	433MHZ	56029400AE	SCHRADER
CHRYSLER	300 SRT8	2010	2014	433MHZ	56029400AE	SCHRADER
CHRYSLER	ASPEN	2007	2009	315MHZ	68001696AB	SIEMENS
CHRYSLER	CONCORDE	2002	2004	433MHZ	52088990AC	SCHRADER
CHRYSLER	CROSSFIRE	2004	2005	433MHZ	52088990AC	SCHRADER
CHRYSLER	CROSSFIRE	2005	2005	315MHZ	68001696AB	SIEMENS
CHRYSLER	CROSSFIRE	2006	2008	433MHZ	52088990AC	SCHRADER
CHRYSLER	CROSSFIRE	2006	2008	315MHZ	68001696AB	SIEMENS
CHRYSLER	INTREPID	2002	2004	433MHZ	52088990AC	SCHRADER
CHRYSLER	PACIFICA	2004	2004	433MHZ	52088990AC	SCHRADER
CHRYSLER	PACIFICA	2004	2005	315MHZ	04727392AB	SIEMENS
CHRYSLER	PACIFICA	2006	2008	315MHZ	68001696AB	SIEMENS
CHRYSLER	PACIFICA	2017	2019	433MHZ	68313387AB	CONTINENTAL
CHRYSLER	PROWLER	2002	2002	433MHZ	52088990AC	SCHRADER
CHRYSLER	PT CRUISER	2008	2010	315MHZ	68001696AB	SIEMENS
CHRYSLER	SEBRING	2008	2009	433MHZ	68001696AB	SIEMENS
CHRYSLER	SEBRING	2007	2011	315MHZ	68001696AB	SIEMENS
CHRYSLER	TOWN&COUNTRY	2002	2003	433MHZ	52088990AC	SCHRADER
CHRYSLER	TOWN&COUNTRY	2004	2005	315MHZ	04727392AB	SIEMENS
CHRYSLER	TOWN&COUNTRY	2006	2006	315MHZ	68001696AB/ 68053030AB/ 68001696AB	SIEMENS
CHRYSLER	TOWN&COUNTRY	2007	2008	315MHZ	68053030AB/ 68001696AB	SIEMENS
CHRYSLER	TOWN&COUNTRY	2008	2010	433MHZ	68001698AB	SIEMENS
CHRYSLER	TOWN&COUNTRY	2011	2018	433MHZ	56029398AA	SCHRADER
CHRYSLER	VOYAGER	2002	2003	433MHZ	52088990AC	SCHRADER
DODGE	AVENGER	2008	2014	315MHZ	56053030AB	SIEMENS
DODGE	CALIBER	2007	2012	315MHZ	56053030AB	SIEMENS
DODGE	CARAVAN	2002	2003	433MHZ	52088990AC	SCHRADER
DODGE	CARAVAN	2004	2005	315MHZ	04727392AB	SIEMENS
DODGE	CARAVAN	2006	2006	315MHZ	56053030AB	SIEMENS
DODGE	CARAVAN	2007	2007	315MHZ	56053030AB	SIEMENS
DODGE	CHALLENGER	2008	2008	433MHZ	56029400AD	SCHRADER
DODGE	CHALLENGER	2009	2019	433MHZ	56029398AA	SCHRADER
DODGE	CHALLENGER SR/T	2017	2019	433MHZ	68241067AB	SCHRADER

https://itmtpms.com/wp-content/uploads/2019/04/ITM_APPCHART_040519.pdf

Final Kismet Goal:

Get alerts when certain makes enter my hood



What to do once car is unlocked?

Some cars still don't use transponders/immobilizers in their ignitions (e.g. Kia and Hyundais)

TikTok Hack-Led Car Thefts Now Make Kia And Hyundai Models Uninsurable

Insurance companies are refusing to cover the vehicles stolen by Kia Boyz. But the latest Hyundai anti-theft software update seems to be working.

BY SOURAV BANIK UPDATED APR 21, 2023

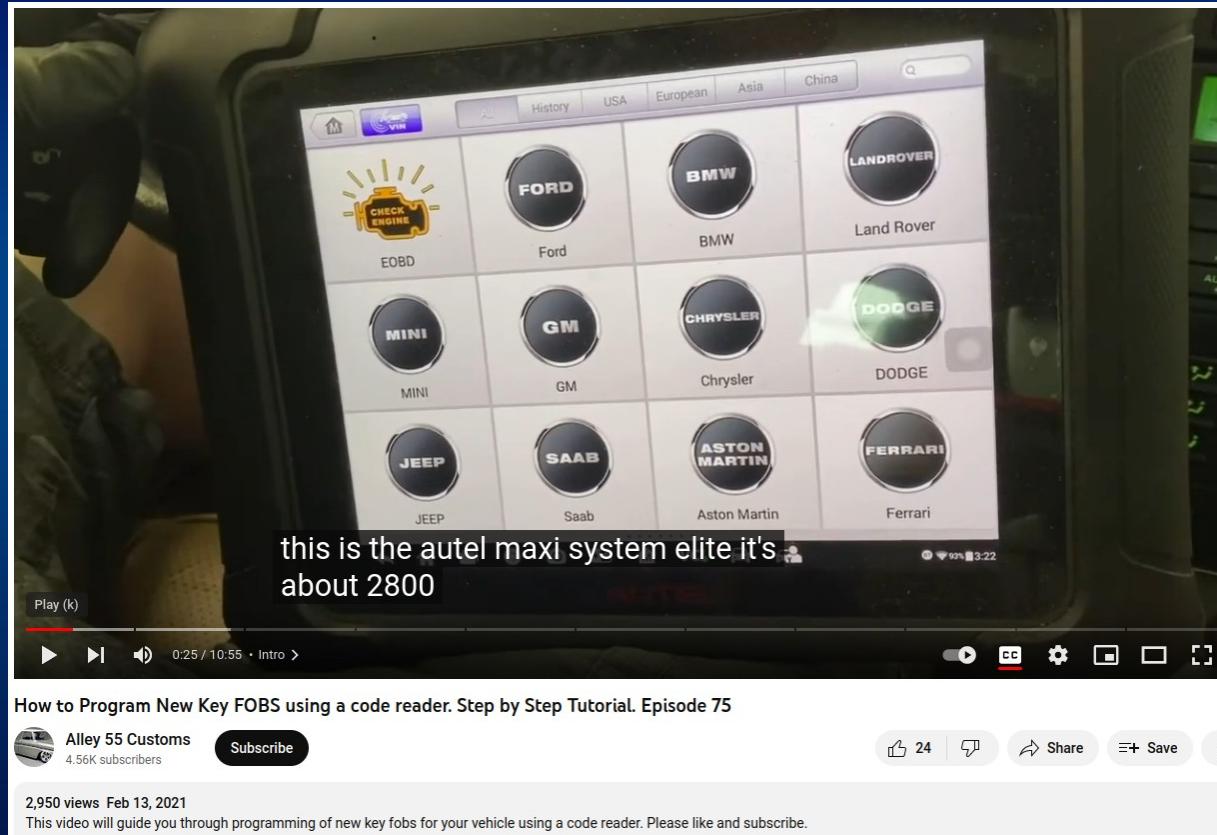


It can be argued that social media can be blamed for a lot of issues in the world today. Now, you can add not being able to insure your car to that list. If you own a 2012-2021 [Kia](#) or a 2015-2021 [Hyundai](#), that is. Late last year, a group of teens calling themselves the "Kia Boyz" identified a security loophole in these Kia and Hyundai models that weren't equipped with an engine immobilizer.

CAR RENDERS

What to do once car is unlocked?

- Steal the car by adding a new key. Requires OBD/CANBUS commands, keyfob button press combo



What to do once car is unlocked?

Hack the Infotainment system



Forbes
FORBES > INNOVATION > CYBERSECURITY
EDITORS' PICK

Cops Can Extract Data From 10,000 Different Car Models' Infotainment Systems

- Phone data (Contacts list)
- GPS data, traveled locations
- Wifi networks
- DEFCON talks and guides are published

What to do once car is unlocked?

Add GPS tracker and wiretap

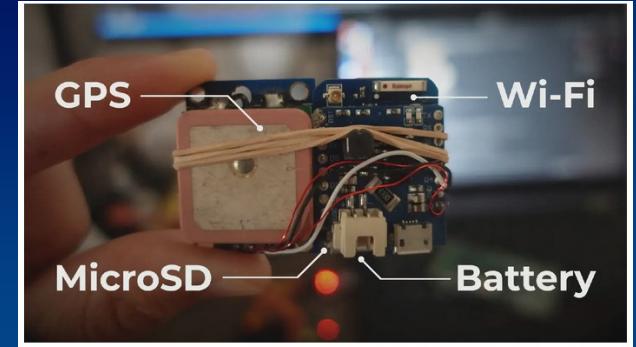
Stealthy GPS Tracker & Drive-by Telemetry Using Open Wi-Fi

Posted on October 14, 2022 by Alex Lynd - 10 min read



<https://alexlynd.com/Stealthy-Drive-by-GPS-Tracker-ESP8266/>

<https://www.hackster.io/mvtdesign/wifi-spy-microphone-with-esp8266-and-nodemcu-e783bb>



Uses D1 mini (ESP8266)
Can also use ESP8266 for wiretap



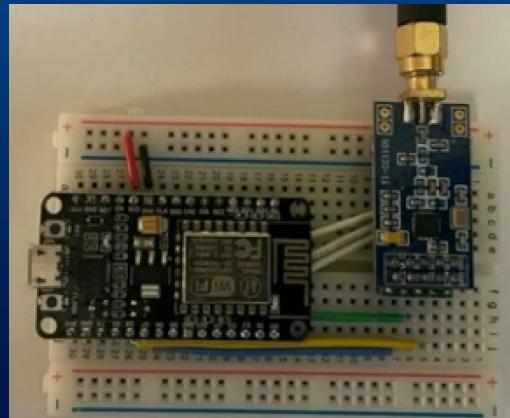
Can't afford Flipper Zero or HackRF?

- Use CC1101 with ESP8266 (\$10-\$20). FlipperZero uses CC1101
<https://github.com/LSatan/SmartRC-CC1101-Driver-Lib>

- RC-Switch library captures and replays raw radio signals
<https://github.com/sui77/rc-switch>

- LittleFS to save signals for later replays (rollback)
<https://randomnerdtutorials.com/install-esp8266-nodemcu-littlefs-arduino/>

- Build your own patch antenna with copper tape
<https://youtu.be/7mciNPmT1KE>



Copper Tape

Use the printout as a template to help cut the tape

```
dollarhyde@ops:~/VCU/AntennaCalculator$ python3 antenna_calculator.py rectangular_patch --type microstrip -f 1.5e9 -er 4.4 -h 1.6e-3 --pngoutput 1.5_FR4_
[*] W = 68.06 millimeter
[*] L = 47.41 millimeter
[*] Ws = 3.06 millimeter
[*] y0 = 30.43 millimeter
[*] x0 = 18.25 millimeter
```

Questions?

Demo (if time):
Telegram Bot
Narrowband Jammer
Wideband jammer
URH

Find me in the dc402 slack #wireless