

Forum:[Hack Forums](#)

Thread: [Relay attack passive keyless cars](#)

yyyyyyyyyy - November 20, 2018, 11:03 pm

Hi,

I am interested in finding out how to build, or how to get, the equipment to relay attack a car with passive keyless entry/start system. Does anyone know where to find information on this?

/Mike

jBloq - November 21, 2018, 12:55 am

A few "keyless" system operate through radio waves. Find the FCC ID of the car you are interested in and see what frequency it listens on. Afterwards, use a RTL SDR to capture the data transmitted over the frequency. Then create a simple board that uses RF to transmit data on the frequency and it should work.

ps: you have a long journey ahead

Nechifor - December 16, 2018, 7:21 pm

Send me a pm, i have some info about that.

FriendZone - December 18, 2018, 1:34 am

(Nov 21, 2018 01:55 AM)jBloq Wrote: [\[CITE\]](#) A few "keyless" system operate through radio waves. Find the FCC ID of the car you are interested in and see what frequency it listens on. Afterwards, use a RTL SDR to capture the data transmitted over the frequency. Then create a simple board that uses RF to transmit data on the frequency and it should work.

ps: you have a long journey ahead

He should also use the first captured signal to open the car for the owner after the first attempt capturing the second one and using it before a third generated signal.

Basically he needs something able to jam the signal and capture it, the car won't open, use it as soon the target car owner use a second signal to open the car, jam and capture it again, and simultaneously use the previous capture signal to open the car for the owner.

-Aspect- - December 19, 2018, 9:12 pm

https://www.youtube.com/watch?v=M2JY1_Xmokg&t

Just checking in.

I published this video a few days ago

[Video: https://www.youtube.com/watch?v=M2JY1_Xmokg&t]

It's possible, and it's cheap.

Although, rolling keys take a bit more effort, as jamming is necessary.

Nechifor - January 24, 2019, 3:25 pm

That's not what he's looking for. That's a device like Samy's RollJam, but he's looking for a passive keyless entry/ start device like those guys using in the Youtube "Relay attack Solihull" video

leoneldahma - September 4, 2019, 2:06 pm

Hi isn't it a radio signal booster you are wanting. I know English keyless cars are on 433.92mhz

cyberkun - September 4, 2019, 11:38 pm

(Nov 21, 2018 12:03 AM)yyyyyyyyyy Wrote: [\[CITE\]](#) Hi,

I am interested in finding out how to build, or how to get, the equipment to relay attack a car with passive keyless entry/start system. Does anyone know where to find information on this?

/Mike

Hi Mike. depending on your location you just buy them online. If you are good with electronics and coding, only then will you be able to reverse engineer or build similar devices from plans, books and other info available. Most of the parts are easily available but the programming of the chips and the pcb design will be tricky.

You have to relay 2 different frequency spectrums, if you want to go for maximum attack range LF (NFC for the wake up signal and the key challenge) and HF(UHF) to actually unlock and lock the vehicles (also works on some motor bikes). But by taking that route you will have to tweak the signal runtime, by using the right frequency and the right chips for fast processing. You only have few ms for the whole process to succeed. If you need more info hit me up.

(Nov 21, 2018 01:55 AM)jBloq Wrote: [\[CITE\]](#) A few "keyless" systems operate through radio waves. Find the FCC ID of the car you are interested in and see what frequency it listens on. Afterwards, use a RTL SDR to capture the data transmitted over the frequency. Then create a simple board that uses RF to transmit data on the frequency and it should work.

ps: you have a long journey ahead

A few? 99% of all PKES use radio waves and less than 1% uses biometrics as a "key". Capturing the system is not working on keyless systems for several reasons.

The wake up signal between keyfob and BCM are time restricted and can not be replayed...that's why it's called a relay attack. Your advice is useless for what the OP is asking.

(Dec 18, 2018 02:34 AM)FriendZone Wrote: [\[CITE\]](#) He should also use the first captured signal to open the car for the owner after the first attempt capturing the second one and using it before a third generated signal.

Basically he needs something able to jam the signal and capture it, the car won't open, use it as soon as the target car owner uses a second signal to open the car, jam and capture it again, and simultaneously use the previous capture signal to open the car for the owner.

Same as above...completely wrong attack... (Dec 19, 2018 10:12 PM)-Aspect- Wrote: [\[CITE\]](#) [Unlock Cars with a Raspberry Pi And SDR - Replay attack - YouTube](#)

Just checking in.

I published this video a few days ago

[Video: <http://Unlock Cars with a Raspberry Pi And SDR - Replay attack - YouTube>]

It's possible, and it's cheap.

Although, rolling keys take a bit more effort, as jamming is necessary. Still the wrong attack but nice video though

(Sep 4, 2019 02:06 PM)leoneldahma Wrote: [\[CITE\]](#) Hi isn't it a radio signal booster you are wanting.

I know English keyless cars are on 433.92mhz

Yes, but just boosting the signals is not enough as i wrote previously. In most cases the frequencies used are according to international standards or the assigned/available frequency spectrum plus all unmodified keyless vehicles use 125 / 130 kHz (Audi: 20 kHz) in the LF spectrum and with small deviations Europe: 433 MHz/868 MHz and Japan and the USA: 315 MHz in the HF spectrum.

Jinxter - September 7, 2019, 9:50 am

(Sep 4, 2019 11:38 PM)cyberkun Wrote: [\[CITE\]](#) Hi Mike.depending on your location you just buy them online.If you are good with electronics and coding, only the will you be able to reverse engineer or build similar devices from plans , books and other info available. most of the parts are easily available but the programming of the chips and the pcb design will be tricky.

You have to relay 2 different frequency spectrums,if you want to go for maximum attack range LF (NFC for the wake up signal and the key challenge) and HF(UHF) to actually unlock and lock the vehicles(also works on some motor bikes) . but by taking that route you will have to tweak the signal runtime, by using the righ frequency and the right chips for fast processing..you only have few ms for the whole process to succeed.if you need more info hit me up.

A few? 99% of all PKES use radio waves and less than 1% uses biometrics as a "key". capturing the system is not working on keyless systems for several reasons.

The wake up signal between keyfob and BCM are time restricted and can not be replayed...thats why it's called a relay attack .your advice is useless for what the OP is asking.

Same as above...completely wrong attack...
still the wrong attack but nice video though

Yes, but just boosting the signals is not enough as i wrote previously. In most cases the frequencies used are according to international standards or the assigned/available frequency spectrum plus all unmodified keyless vehicles use 125 / 130 kHz (Audi: 20 kHz) in the LF spectrum and with small deviations Europe: 433 MHz/868 MHz and Japan and the USA: 315 MHz in the HF spectrum.

Listen to this man, great advice right there.

(Sep 4, 2019 02:06 PM)leoneldahma Wrote: [\[CITE\]](#) Hi isn't it a radio signal booster you are wanting. I know English keyless cars are on 433.92mhz

Boosting can work over a limited range but it is the 125khz signal that needs to be 'boosted' or relayed and without relaying the 433Mhz signal back you are limited to it's normal range.

This is what's happening in many of the videos or news articles you see, the 433Mhz remote in the house is in range of the car already.

gasvo99 - October 7, 2019, 1:10 am

hi,

i want to make a keyless go amplifier.

It may be for short distances for testing purposes.

Anyone have any interesting information? what is best to use what works?

Thanks

cyrusdavirus - October 31, 2023, 5:05 pm

@cyberkun please contact me as soon as possible

bisla002J - November 4, 2023, 12:15 pm

A guy literally uploaded a video on the same topic on youtube

BigEzA - January 9, 2024, 8:11 pm

Anyone have a link to a cheap relay set up? I have spent hours looking for just the right system but I don't have thousands of dollars right now.

Anyone have a link to a cheap relay set up? I have spent hours looking for just the right system but I don't have thousands of dollars right now.

SIM-5186353 - January 10, 2024, 7:34 am

(Jan 9, 2024 09:11 PM)BigEzA Wrote: [\[CITE\]](#) Anyone have a link to a cheap relay set up? I have spent hours looking for just the right system but I don't have thousands of dollars right now.

Anyone have a link to a cheap relay set up? I have spent hours looking for just the right system but I don't have thousands of dollars right now.

Try buying a rtl sdr and a hackrf, for roll jam attacks. The clone hackrf it's pretty good, and it's better if you buy the portapack.

BigEzA - January 13, 2024, 6:01 pm

I'm looking to copy the fob and send the signal

SUSSTIQUE - January 14, 2024, 9:02 pm

Google This:

#HITB2017AMS D2T2 - Chasing Cars: Keyless Entry System Attacks - Yingtao Zeng, Qing Yang and Jun Li

Custom devices online use cheap SDR units, but are purpose built, with Hacker, you need 4x hackrf's AND 2x WIFI to make it work.

Both 315Mhz and 125Khz need to be boosted, and both devices need a fast connection between them.

i think owning one is illegal but i keep seeing this Hack Key unicorn pop up, it is not sold anywhere