

Forum:[Hack Forums](#)

Thread: [Keyless entry](#)

cyberghost101 - November 20, 2019, 3:42 pm

Hi there can anyone help me build a device that captures (recieve) a rolling code from a vehicle key fob and then transmits the code to another device allowing the vehicle to start and drive?

realsunjester - November 20, 2019, 4:35 pm

(Nov 20, 2019 04:42 PM)cyberghost101 Wrote: [\[CITE\]](#) Hi there can anyone help me build a device that captures (recieve) a rolling code from a vehicle key fob and then transmits the code to another device allowing the vehicle to start and drive?

youre going to need the key fob, its highly unlikely that youre going to get the data without using some kind of long range rfid gun. also, the data could be corrupted the further away you are when you try to transmit.

youre better off breaking the window and twisting the ignition lol.

but, if you can get specs on the keys or car model info on their design, sure, its quite possible.

cyberghost101 - November 21, 2019, 9:17 am

realsunjester do you know how to make this sort of device?

realsunjester - November 21, 2019, 10:51 am

(Nov 21, 2019 10:17 AM)cyberghost101 Wrote: [\[CITE\]](#) realsunjester do you know how to make this sort of device?

yes but the real problem is knowing the type of encryption (and breaking it) the fob/car uses.

GREN4DE! - November 21, 2019, 5:17 pm

(Nov 20, 2019 05:35 PM)realsunjester Wrote: [\[CITE\]](#) youre going to need the key fob, its highly unlikely that youre going to get the data without using some kind of long range rfid gun. also, the data could be corrupted the further away you are when you try to transmit.

youre better off breaking the window and twisting the ignition lol.

but, if you can get specs on the keys or car model info on their design, sure, its quite possible.

yes i agree the old brick and twist technique would be the best option :P

and unless its a neighbor and not someone you think "ill show you" depends on the effort you need to put as the RFID gun will only really work if you can capture the car being locked and unlocked so it has something to grab.

so unless you wanna wait in a car park bush i think getting the fob would be 10 time easier.

best practice is Hotel key cards.

Good luck

GREN4DE!

cyberghost101 - November 22, 2019, 11:16 am

Realsunjester & GREN4DE how do these fellas do it then? -> On YouTube called relay attack device .. they use a device to amplify the key fob ?

realsunjester - November 22, 2019, 11:46 am

(Nov 22, 2019 12:16 PM)cyberghost101 Wrote: [\[CITE\]](#) Realsunjester & GREN4DE how do these fellas do it then? -> On YouTube called relay attack device .. they use a device to amplify the key fob ?

i have no idea, i dont know what they are doing, never seen the video. its not a mysterious force, its RF. if its some youtube video, i can only assume they have it planned somehow and know all the internals of whatever rf they are targeting.

cyberghost101 - November 22, 2019, 12:31 pm

They scan the device untill it captures the code of the key and then the 1st device send the signal to the 2nd device and the vehicle thinks the 2nd device is the key opens and starts the vehicle. how do they do this hack realsunjester?

GREN4DE! - November 22, 2019, 6:14 pm

(Nov 22, 2019 01:31 PM)cyberghost101 Wrote: [\[CITE\]](#) They scan the device untill it captures the code of the key and then the 1st device send the signal to the 2nd device and the vehicle thinks the 2nd device is the key opens and starts the vehicle. how do they do this hack realsunjester? kind of :/

so you need something homemade not purchased which will listen and store what its captured in this case Car unlock... and then programs it to a button lets say button A you then listen to and wait for another signal in the case car lock... and then program this to button B BUT! with this you cannot start the car or drive it only to access it... you will need the fob itself to do that and if thats the case you have the keys and you wont need to do any of this :P

like i said i have made devices which do this and they work on garage doors and hotel room keys but fuck doing it with cars as they all have trackers in now :P

good luck

Gren4de!

Charger - November 22, 2019, 6:21 pm

The tool you're trying to make costs several thousand dollars. You can't hack it together.

realsunjester - November 22, 2019, 6:40 pm

(Nov 22, 2019 01:31 PM)cyberghost101 Wrote: [\[CITE\]](#) They scan the device untill it captures the code of the key and then the 1st device send the signal to the 2nd device and the vehicle thinks the 2nd device is the key opens and starts the vehicle. how do they do this hack realsunjester?

its really not that complicated. i have created several keyless entry systems using just my arduino and some proxy cards. like i said before, if you wan to do this at a distance you will need a nice antenna and you will also need to decode the information you get from the scanner. and it doesnt cost you thousands, not even hundreds to create something like this.

https://www.amazon.com/IZOKEE-RFID-RC522-13-56MHz-Arduino-Raspberry/dp/B076HTH56Q/ref=asc_df_B076HTH56Q/?tag=hyprod-20&linkCode=df0&hvadid=309750549985&hvpos=1o1&hvnetw=g&hvrnd=1574850876451404859&hvpone=&hvptwo=&hvmmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9030331&hvtargid=aud-801381245258;pla-564122493348&psc=1

cyberghost101 - *November 23, 2019, 7:36 am*

GRAN4DE or realsunjester how much would you charge to show me how to make this device?