CAR HACKING

INTRODUCTION

As we all well know, today's cars all have keys that can remotely unlock your car with the push of a button. No more pesky key insertions and twisting and manual locking/unlocking. Technology!

Yeah, about that…

RKS uses radio to send an unlock or lock signal to the car, to unlock it. Have you ever wondered what would happen if someone had the ability to record that signal and just replay it once you've left your car in the parking lot?

Let's find out.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.

FCC ID

All devices or remote devices have an FCC ID, that help to transmit on radio frequency

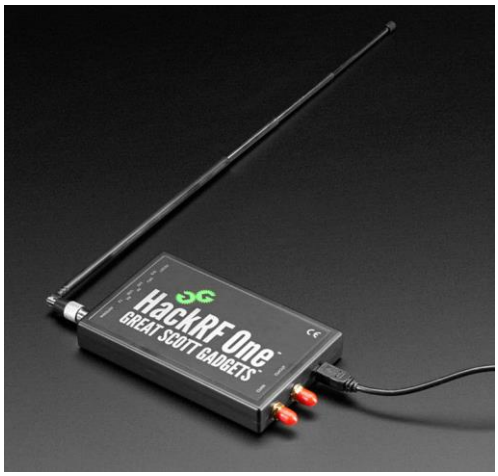
You can find any devices infos just by typing their id on the official website : fcc id . io and by that you can gather infos that can help you to attack a device like wich band or frequency is working on .

LET'S GET INTO THE HOT STUFF

Gear: HackRF One

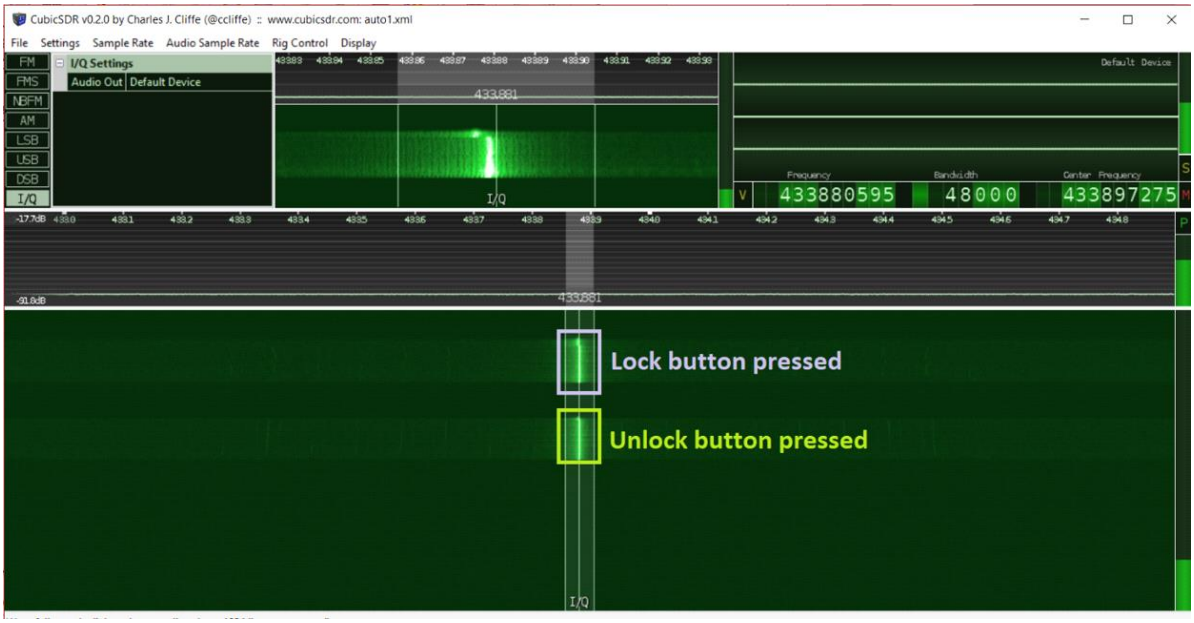
HackRF One is a Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

Hackrf one is mostly used for replay attack for exemple capturing car keys signal freqency while their owners open them and later lanch the saved signal to reopen them by the attacker



CAPTURING THE SIGNAL

Installing some programs that can allow you to record the signal the program using here is **CbicSDR** we plug in the hackrf one and by connecting them we can start capturing near signals



nd their you are having the both sifgnal of locking and unlocking tha can be used by replaying them with the hackrf one .