

Forum:[Hack Forums](#)

Thread: [Flipper \[Bruteforce Car Signals \]](#)

Hephaestus - June 25, 2023, 3:04 pm

Is it possible to brute force car lock/unlock signals.

Looks like it should be possible, but is there any tool for it already created ?

pasnger57 - June 25, 2023, 3:15 pm

(Jun 25, 2023 03:04 PM)Hephaestus Wrote: [\[CITE\]](#) Is it possible to brute force car lock/unlock signals.

Looks like it should be possible, but is there any tool for it already created ?

yes no and its a bit complex but not breathable/copy/stall as the fobs have rolling keys that is/are based on the last sequence

Hephaestus - June 25, 2023, 3:19 pm

(Jun 25, 2023 03:15 PM)pasnger57 Wrote: [\[CITE\]](#) yes no and its a bit complex but not breathable/copy/stall as the fobs have rolling keys that is/are based on the last sequence

I understand that it have rolling keys, but its still should be possible to do it.

Lets say code is made from 100 digits. So if u spam it for long enough time it should pick one of 20 cars No ?

Rogers Communications - June 25, 2023, 3:32 pm

yes rolling keys and until you know the sequence iut aint happeniung

Hephaestus - June 25, 2023, 3:36 pm

(Jun 25, 2023 03:32 PM)Wpginterceptor Wrote: [\[CITE\]](#) yes rolling keys and until you know the sequence iut aint happeniung

Can u tell my how much values does rolling code have and tell my why its not happening.

Even if its 10000000000000 from this amount of numbers its still should be possible to brute force i don't say that its good way to unlock car or smth am just saying its still possible.

pasnger57 - June 25, 2023, 3:48 pm

(Jun 25, 2023 03:32 PM)Wpginterceptor Wrote: [\[CITE\]](#) yes rolling keys and until you know the sequence iut aint happeniung

not quite you can Stall the sequence copy the last Unused key and pass it as new

you dealing whit the FOB as the transmitter and its some most older just init a key sequence easy to creak 1995-2003 (low band 800mhz - 80Kh)

Others uses a rolling you an copy last unused key
some can be just a Vale key and not Owner key

Rogers Communications - June 25, 2023, 4:37 pm

yeah you can do that but just a 1 time use

pasnger57 - June 25, 2023, 4:55 pm

(Jun 25, 2023 04:37 PM)Wpginterceptor Wrote: [\[CITE\]](#) yeah you can do that but just a 1 time use

True that but Once is More then enough entry for theft you may not be able to hit one target but you

can Hit a hole parking lot and get a few number of entry's along with starts and more a lot varying on signification of atk

Hephaestus - June 27, 2023, 10:57 am

(Jun 25, 2023 04:55 PM)pasnger57 Wrote: [\[CITE\]](#) True that but Once is More then enough entry for theft you may not be able to hit one target but you can Hit a hole parking lot and get a few number of entry's along with starts and more a lot varying on signification of atk Exactly.

sub0day - July 21, 2023, 6:46 am

(Jun 25, 2023 03:04 PM)Hephaestus Wrote: [\[CITE\]](#) Is it possible to bruteforce car lock/unlock signals.

Looks like it should be possible, but is there any tool for it already created ?

In theory, yes, the Flipper Zero's ability to transmit and receive radio signals in the 300-928 MHz range could potentially be used to program new key fobs for cars. However, doing this in practice can be quite complex for several reasons:

Proprietary Protocols: Many car manufacturers use proprietary protocols for their key fobs that are not publicly documented. Without knowledge of these protocols, it would be very difficult to program a new key fob.

Security Measures: Modern key fobs often use rolling codes or other security measures to prevent unauthorized copying or programming. These measures would need to be circumvented in order to program a new key fob.

So while the Flipper Zero has the technical capabilities that could be used to program new key fobs, doing so in practice would likely be difficult, potentially illegal, and possibly unethical. If a mechanic or car owner needs to program a new key fob, the best course of action is generally to go through the car's manufacturer or a qualified professional who has the proper equipment and authorization to do so.

I am also working on some exploits for this specifically Audi.