TEAM WHACK

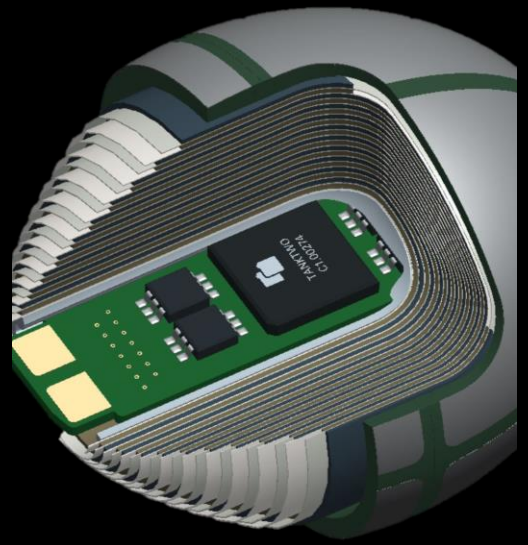
How we hacked the car

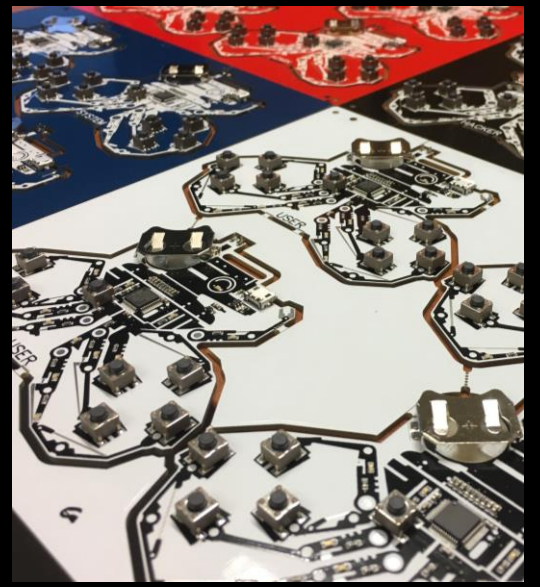
Heikki Juva

Hacker, GPL pilot, HAM operator

Head of System Security and SW dev @Tanktwo

Head of badge-team / HW engineer @Disobey



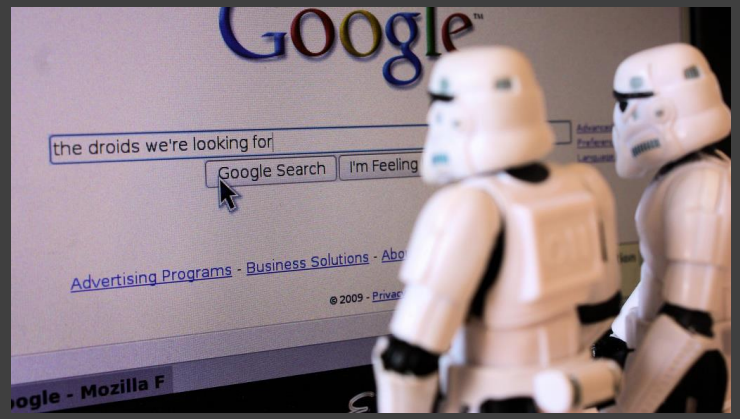


TASK 1. GET IN

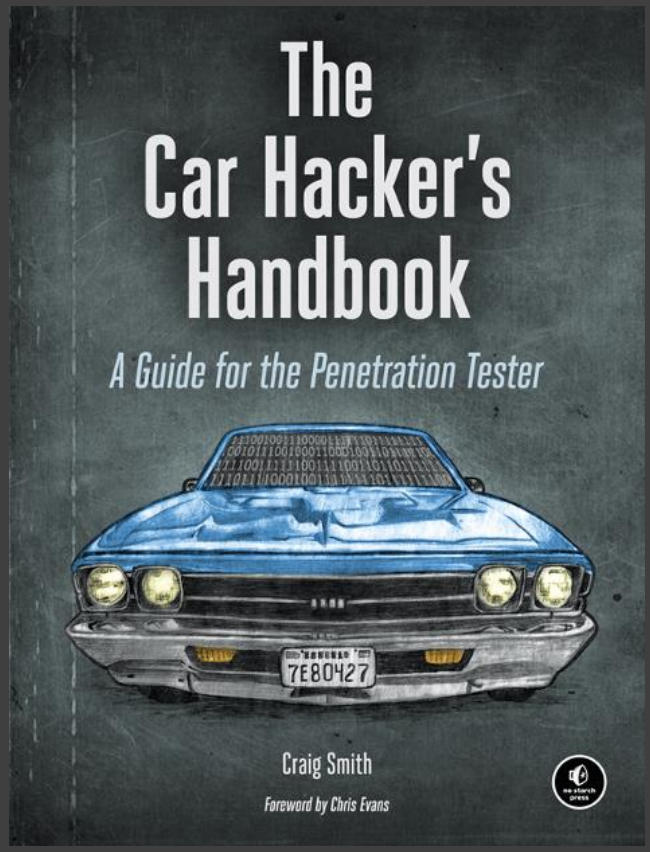
TASK 2. DRIVE AWAY

Multiple targets

- Few weeks time for R&D
- Attack has to work with popular & modern cars
- Attack needs to be repeatable and reliable
- Minimized risk of bricking the car


Google
the droids we're looking for
Google Search
I'm Feeling
Advertising Programs - Business Solutions - Abo
© 2009 - Privac
ogle - Mozilla F


Car hacking: This device can unlock your doors (CBC Marketplace)
"Cars are now, pretty much, just computers on wheels...

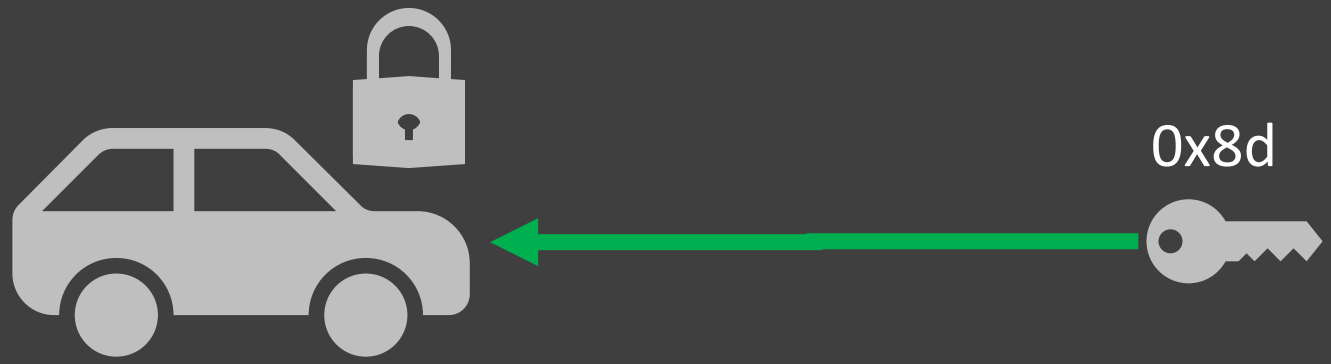

The
Car Hacker's
Handbook
A Guide for the Penetration Tester
7E80427
Craig Smith
Foreword by Chris Evans

Research

Rolling code

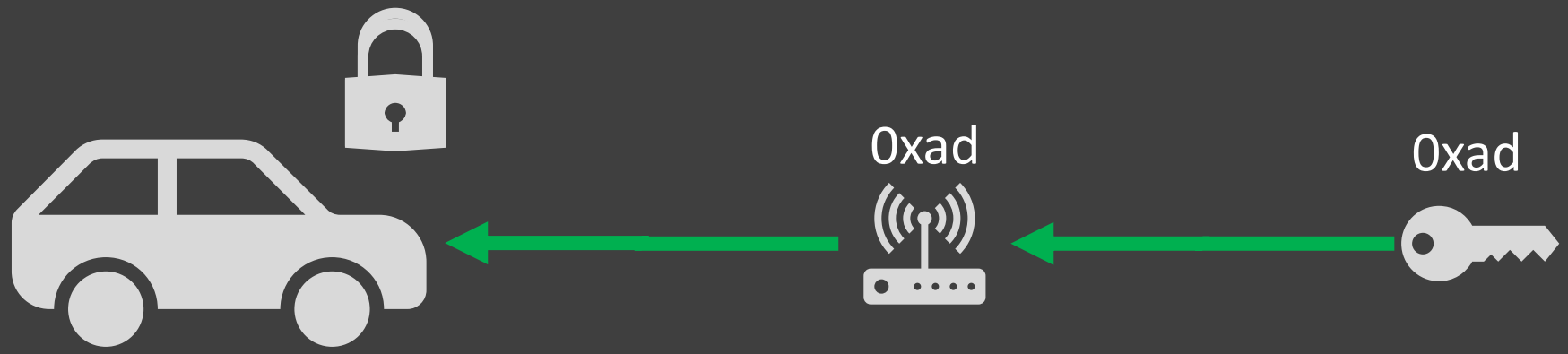
- PRNGs, sync with programmer or via galvanic/IR
- No time limits
- As a rule-of-thumb; car knows next 256 keys

~~0x69~~
~~0xa8~~
~~0x8d~~
0xad
0xb3
0xba
0x74
0xc2
0x64
0xb5

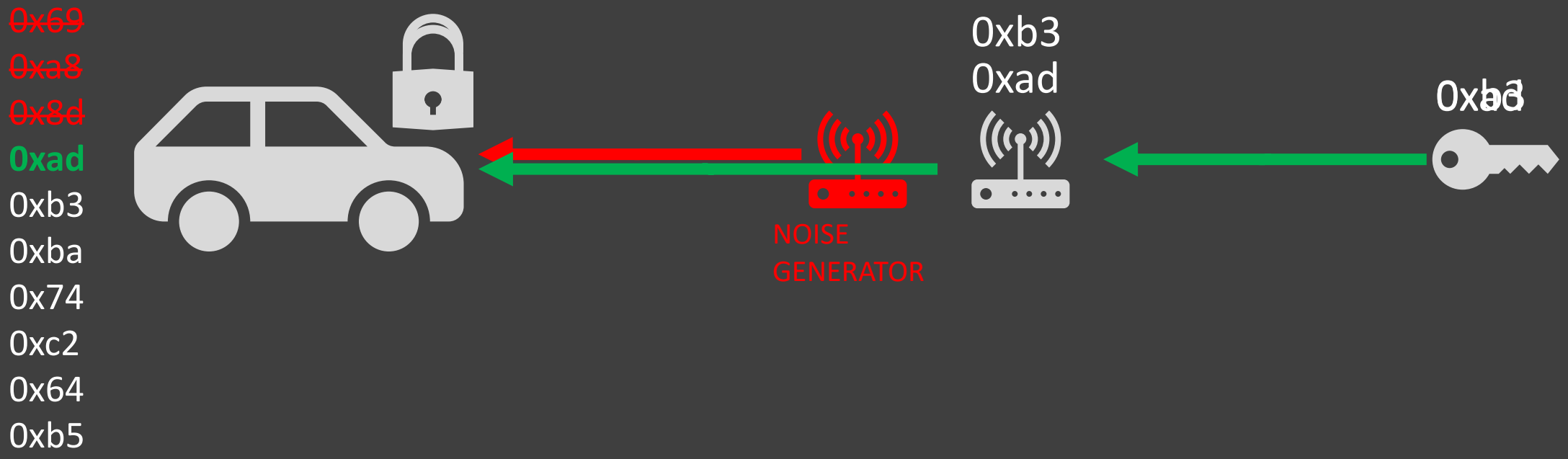


Attacking rolling code (Repeat)

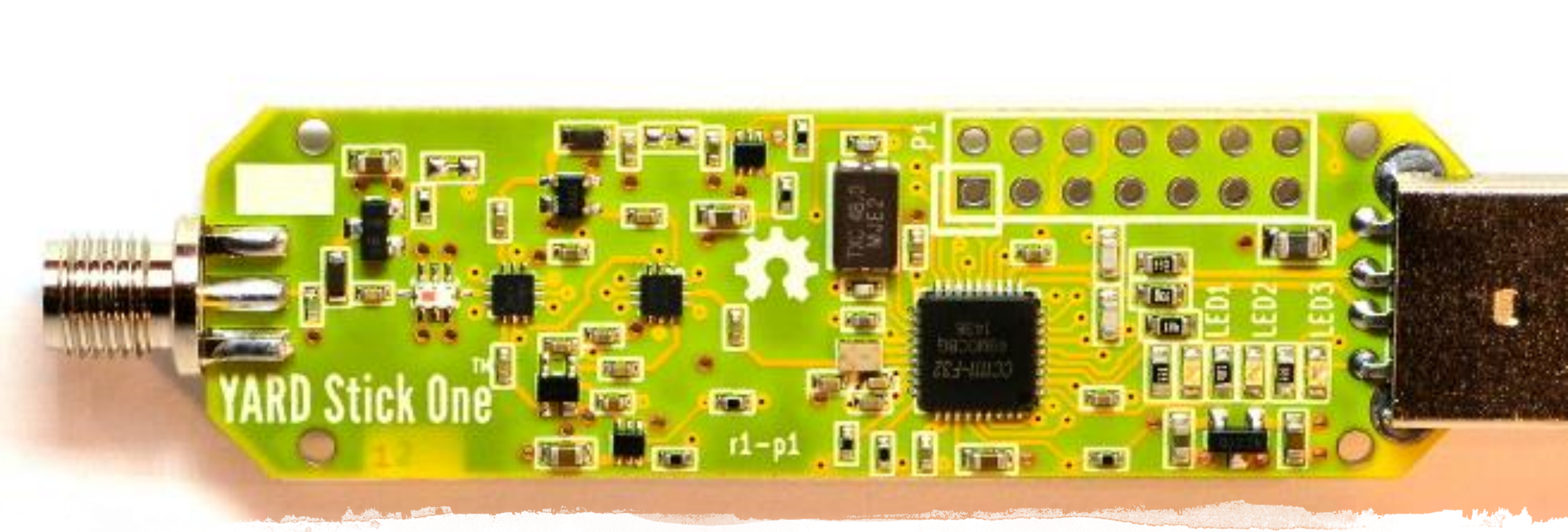
~~0x69~~
~~0xa8~~
~~0x8d~~
0xad
0xb3
0xba
0x74
0xc2
0x64
0xb5



Attacking rolling code (RollJam)



source: https://samy.pl/defcon2015/2015-defcon.pdf



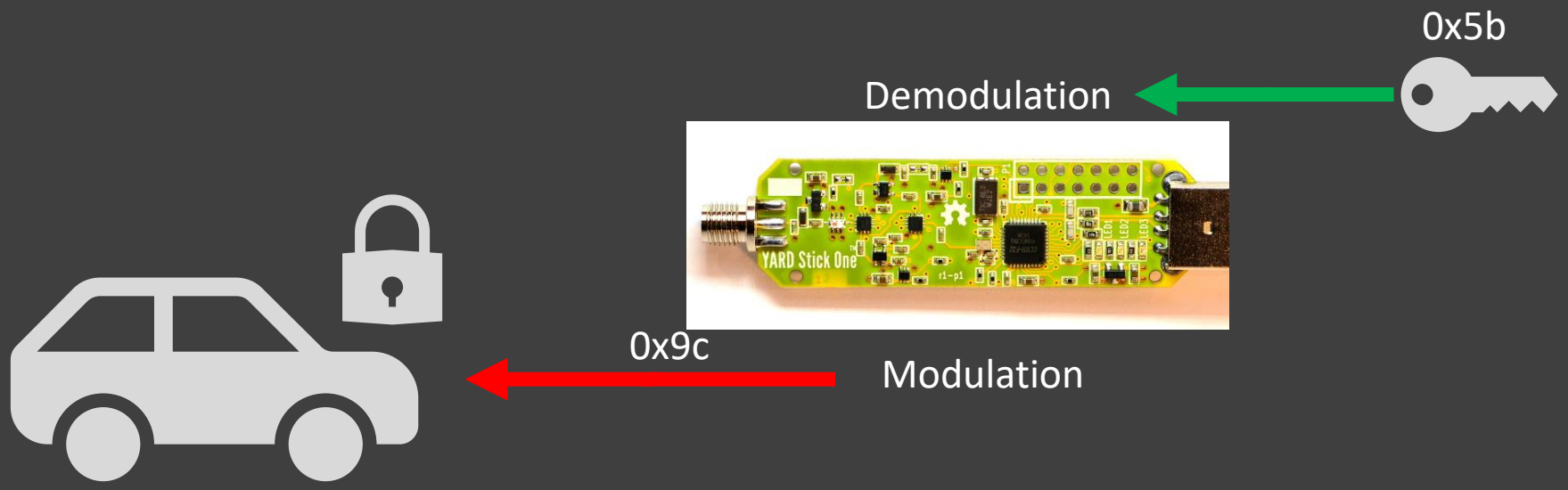
YARD Stick One

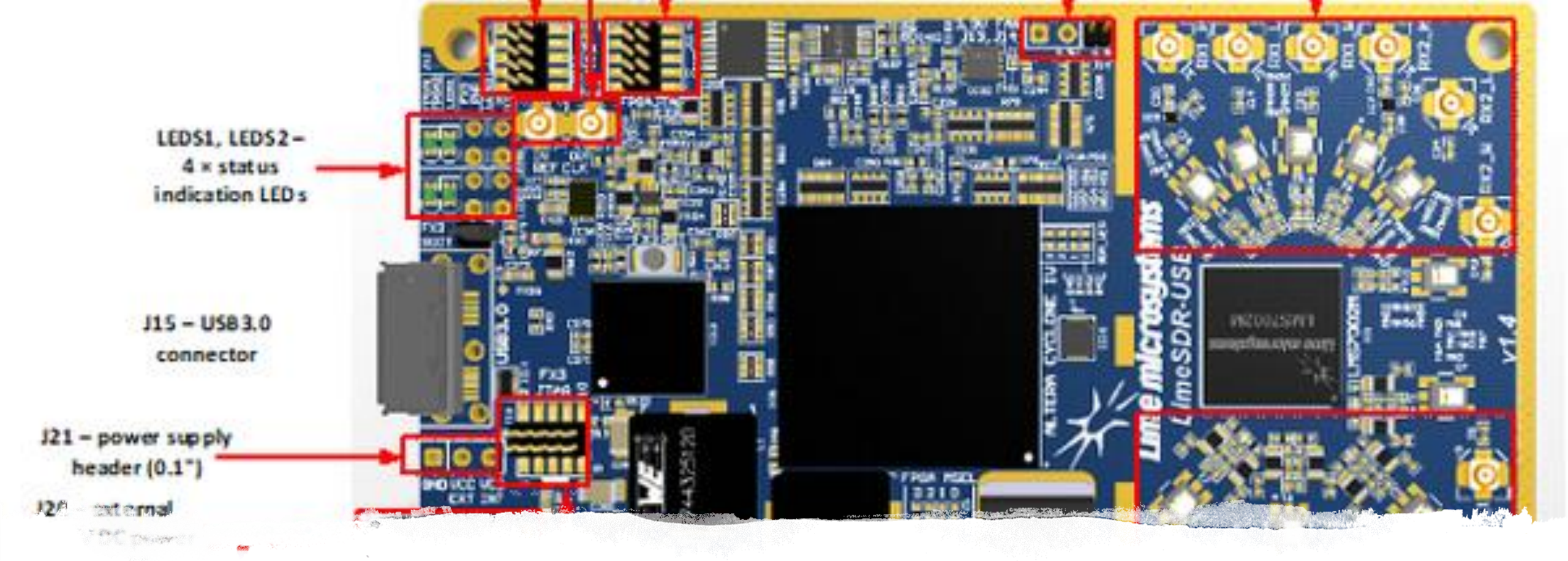
+ Cheap

+ Easy to use

- Forces demodulation (you have to know correct modulation- & baudrate-settings)

Fail





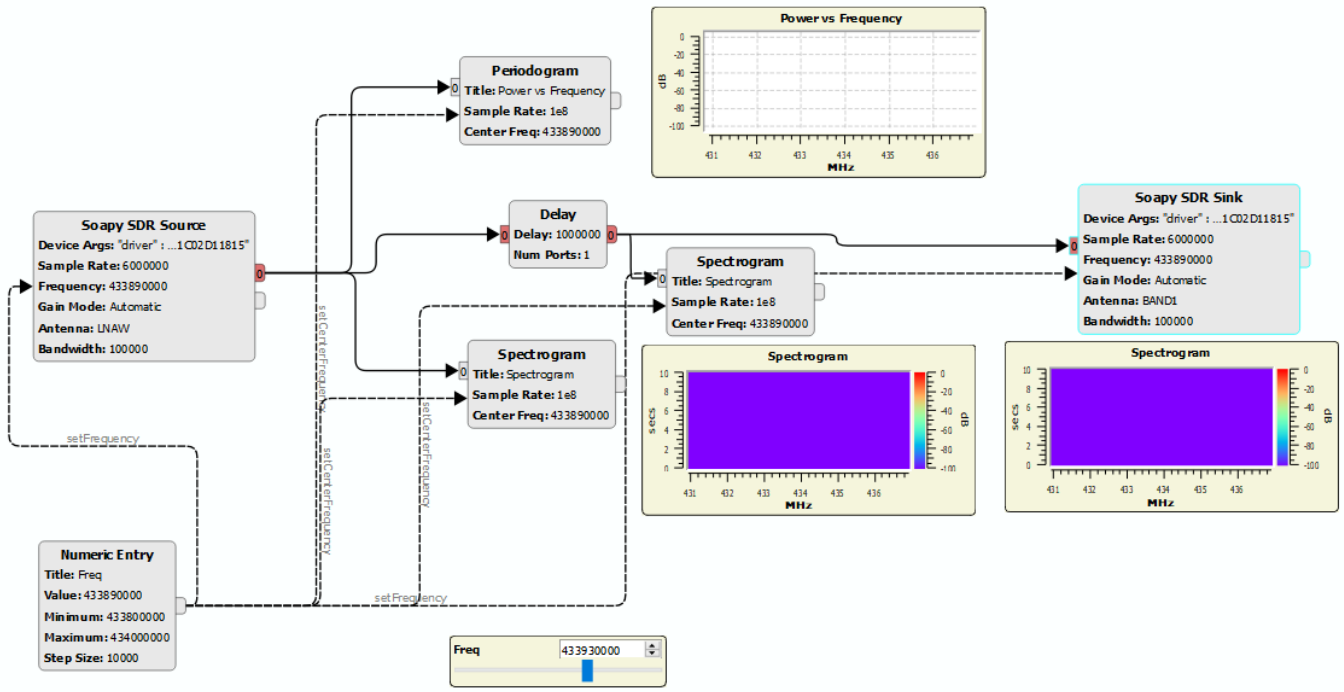
LimeSDR

+ Offers raw access to RF data

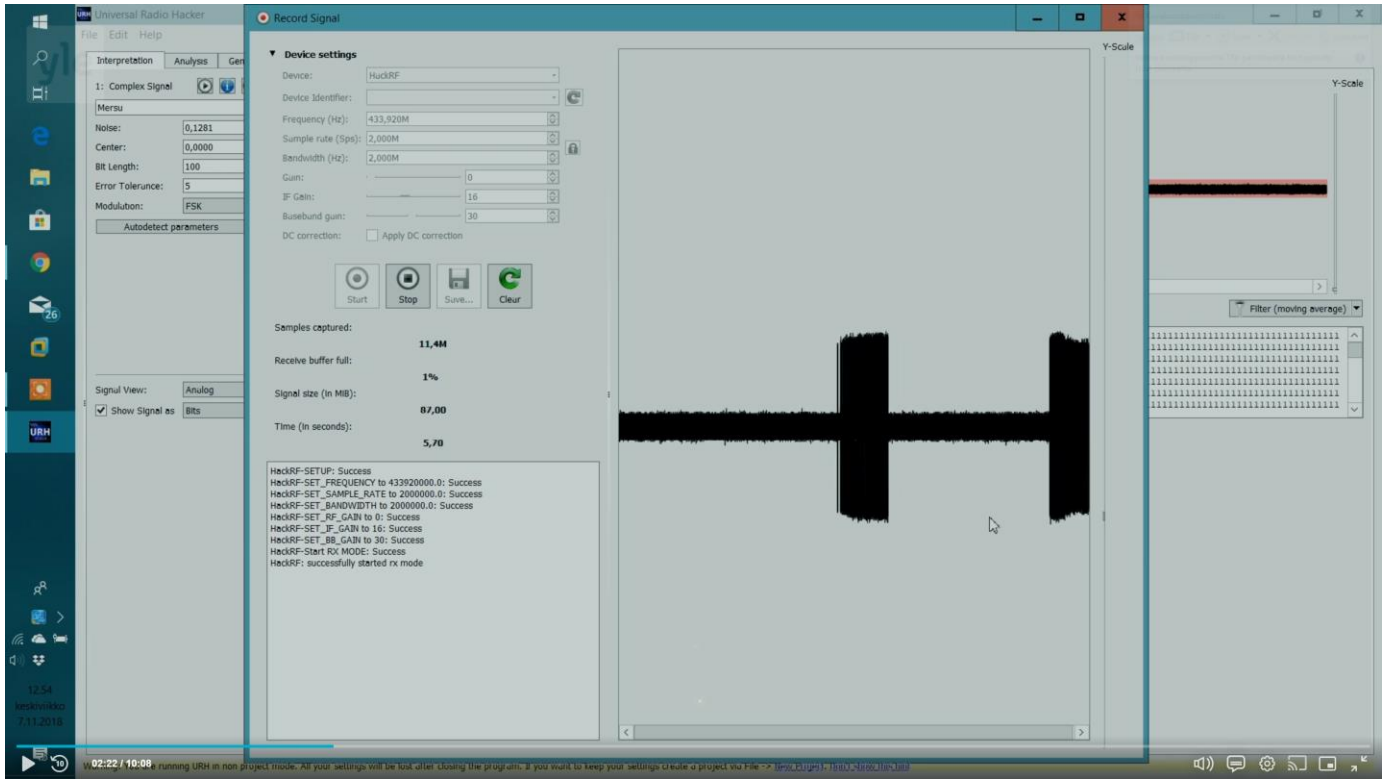
- Some studying required

- Relatively expensive

PothosSDR / GnuRadio

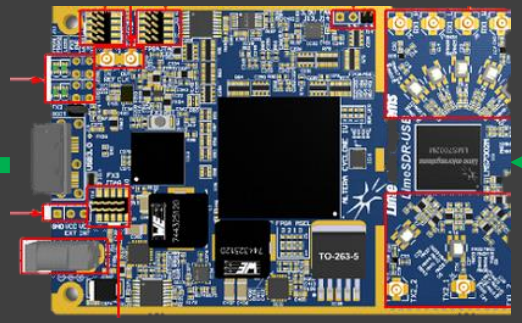


Universal Hacker Radio



Success

RAW I/Q transmit



RAW I/Q capture

0x5b

We are in, what’s next?

Plan A

- Bypassing ignition
- Disabling immobilizer
- Drive away

Plan B

- Add remote control
- Have fun

CANbus

- CAN protocol was developed in late 80s
- No support for message authentication
- No way to prevent malicious node from communicating

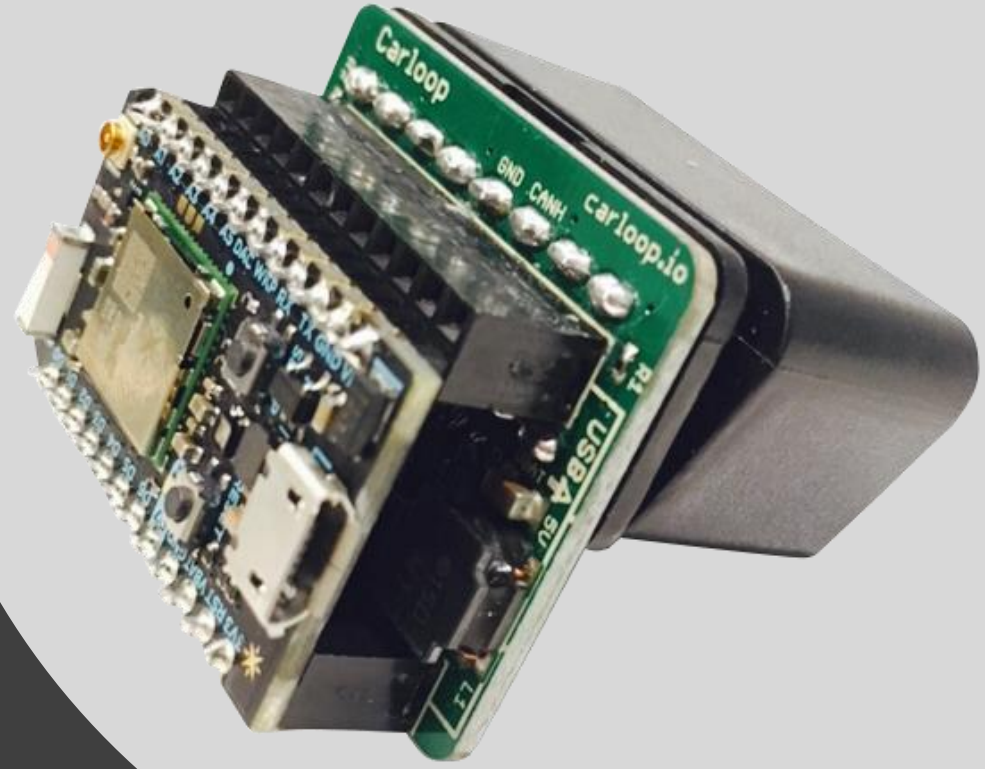
→ Trivial to flood bus and stop all comms

Remote CAN

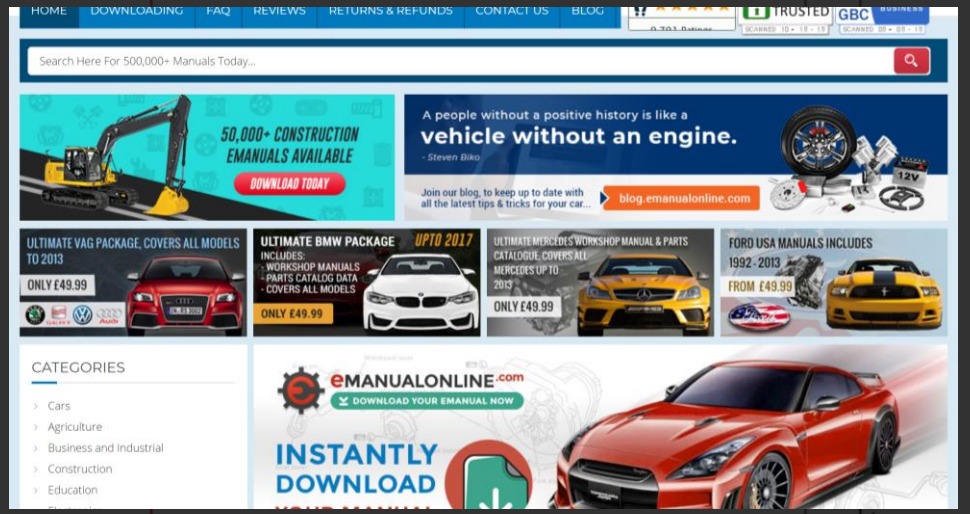
- Carloop OBD / Carloop CanHitch
  - No safety features -> allows TX into busy bus
- Particle Photon

- Canbus-lib by Carloop
- Remote control via Particle cloud

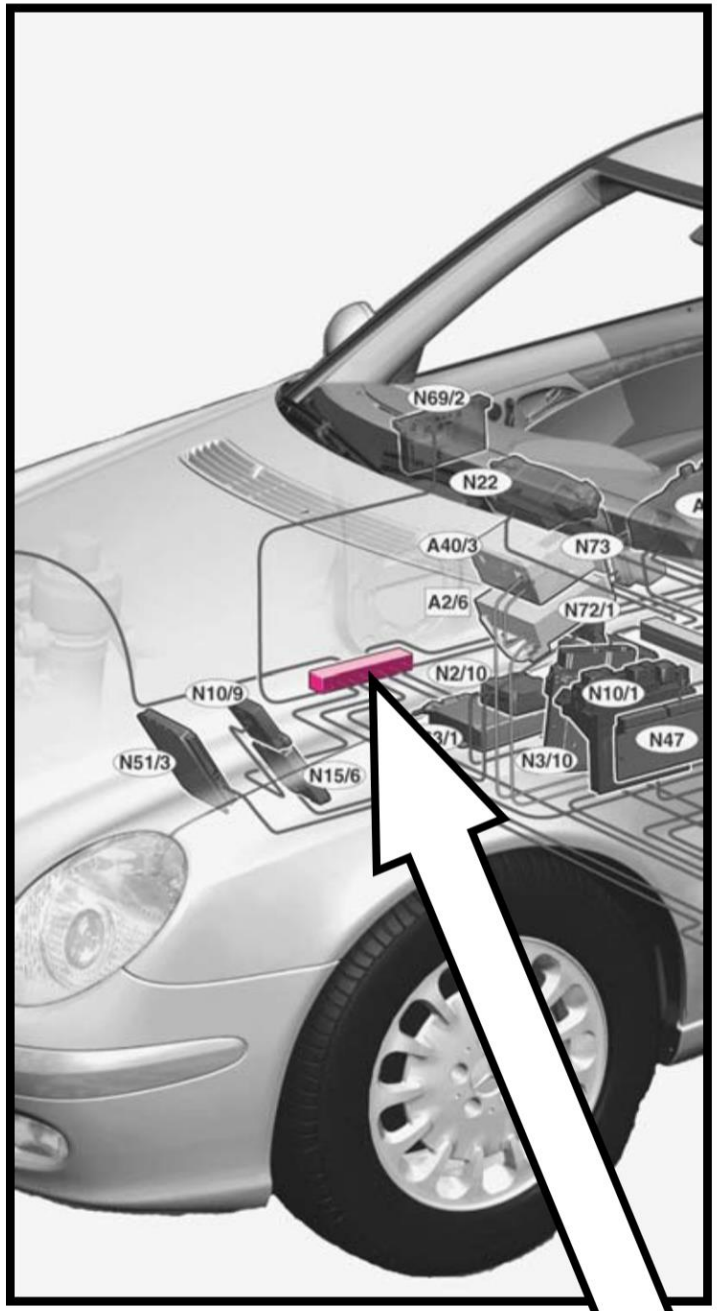
- OBD2 usually isolated from critical communication

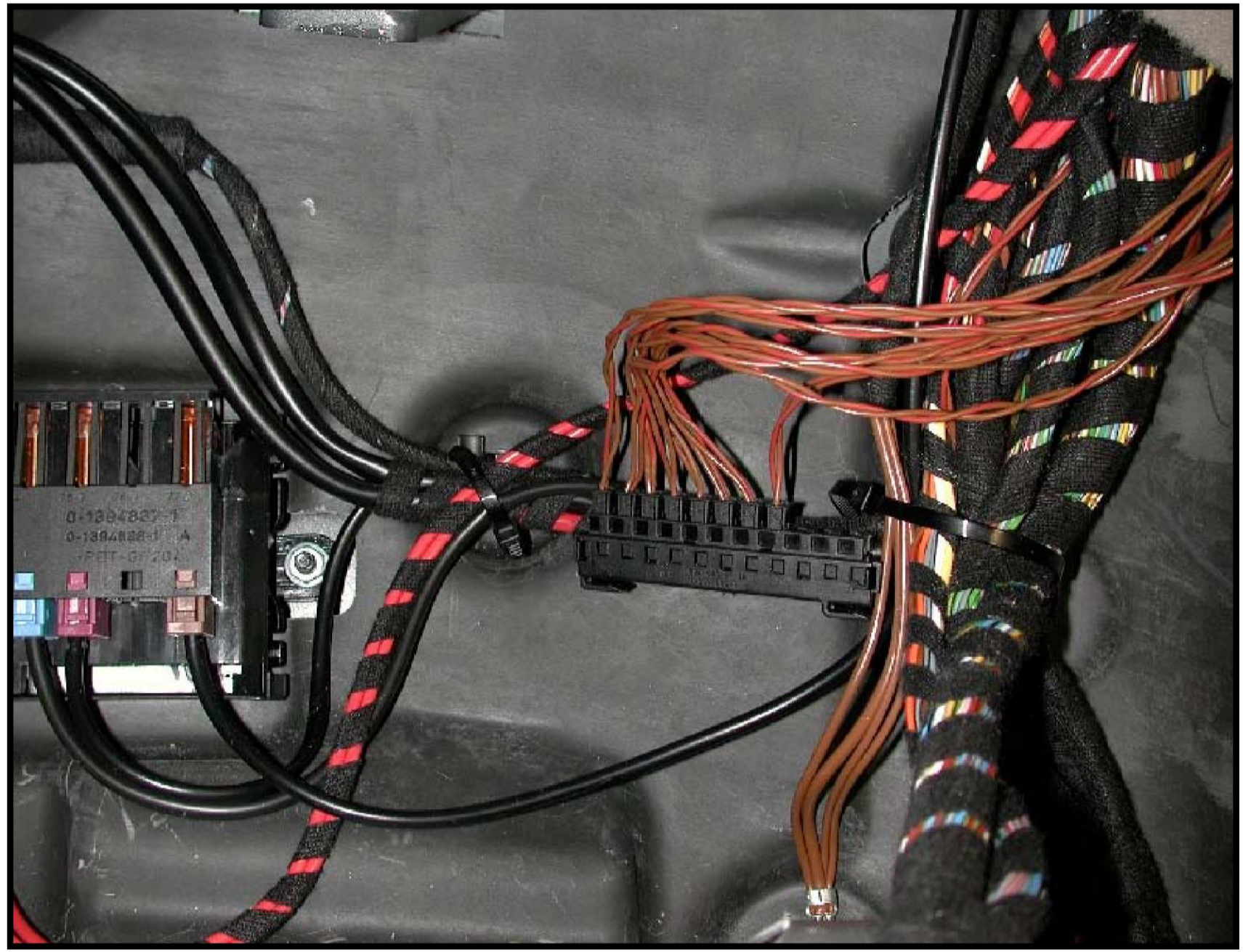


Schematics



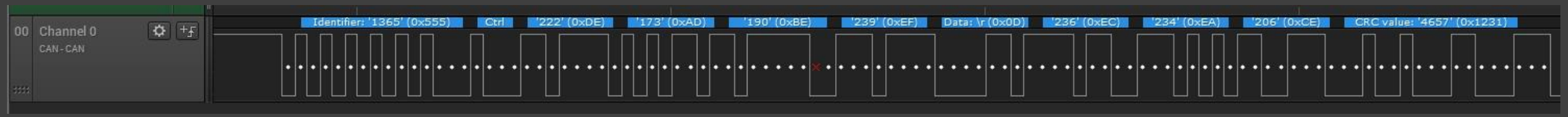
Buy service manual or use Google Image search

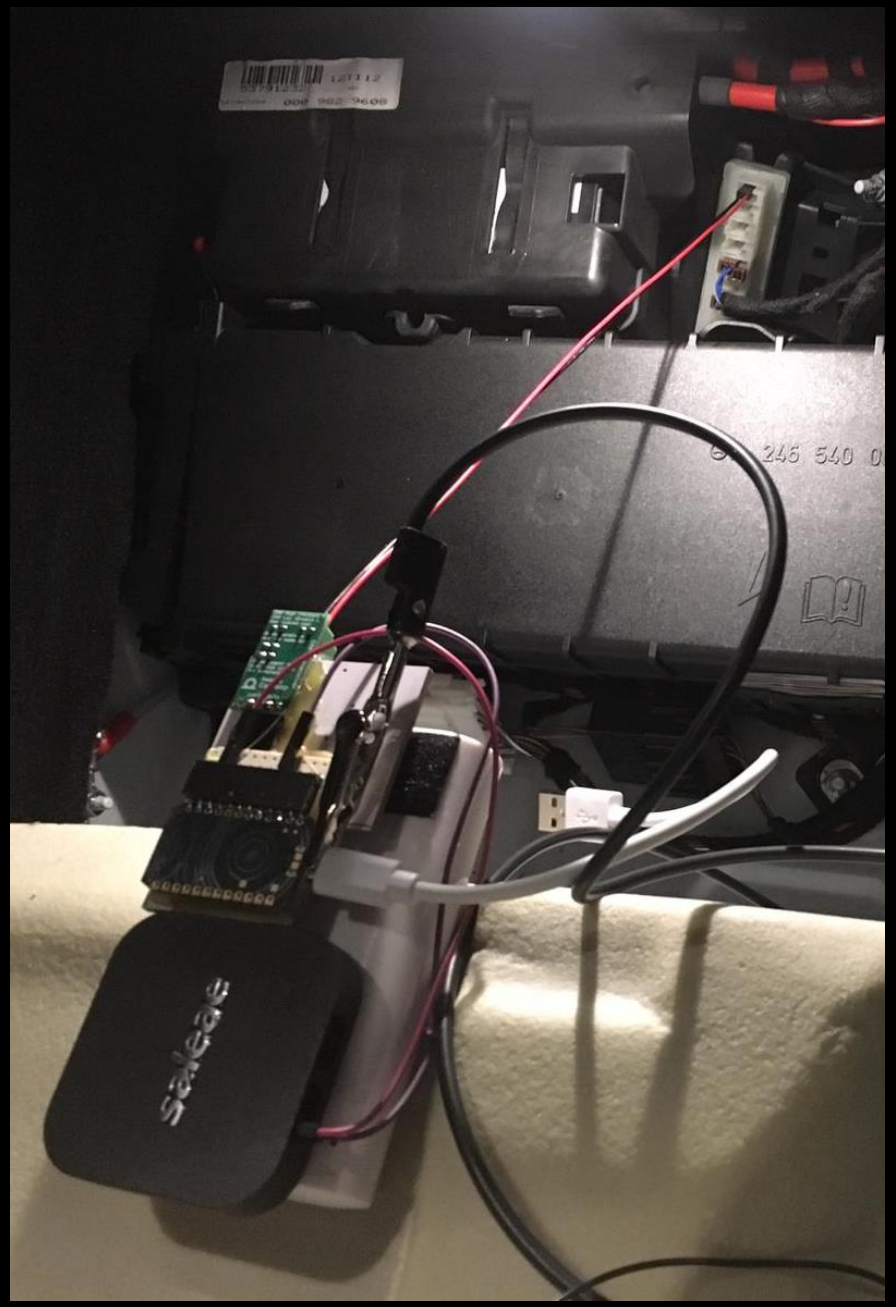

N69/2
N22
A40/3
N73
A2/6
N72/1
N2/10
N10/1
N10/9
N47
N51/3
N15/6
N3/10



Code

```
24
25  int disableCAN(String input) {
26      carloop.disableCAN();
27      return 1;
28  }
29
30  int sendObdRequest(String input) {
31      carloop.enableCAN();
32      CANMessage message;
33      message.id = 0x555;
34      message.len = 8;
35      message.data[0] = 0xDE;
36      message.data[1] = 0xAD;
37      message.data[2] = 0xBE;
38      message.data[3] = 0xEF;
39      message.data[4] = 0x0D;
40      message.data[5] = 0xEC;
41      message.data[6] = 0xEA;
42      message.data[7] = 0xCE;
43      carloop.can().transmit(message);
44      return 0;
45  }
```





Test setup

Conclusion

- Successfully cloned keys to three cars
- Managed to create system that can be theoretically used in any modern car to disable it remotely (your milage may vary)

Lessons learned

- Plan systems to fail well
- Store your car keys safely
- Hacking cars is fun

Thank you

Questions?

Contact me:
@hjuva
heikki@juva.lu