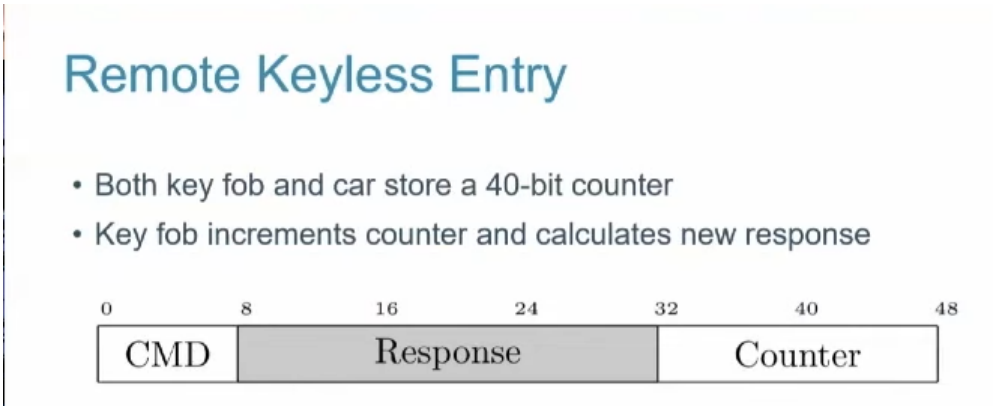
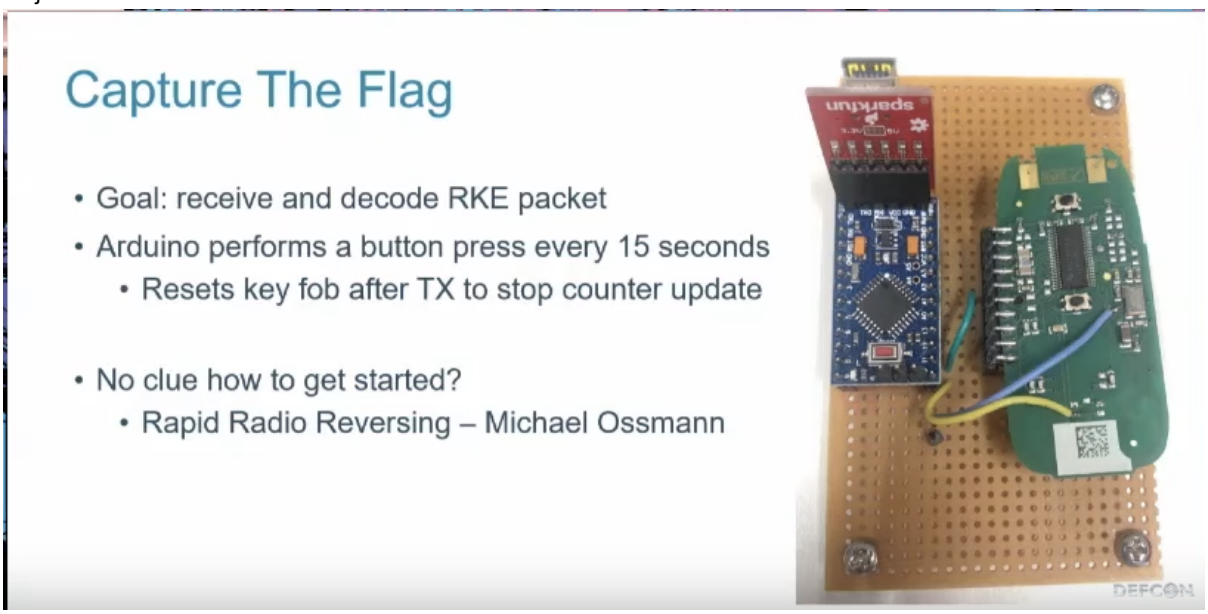
Biljeske 21.10. - 27.10.2023

DEF CON 27 - Car hacking village talkovi

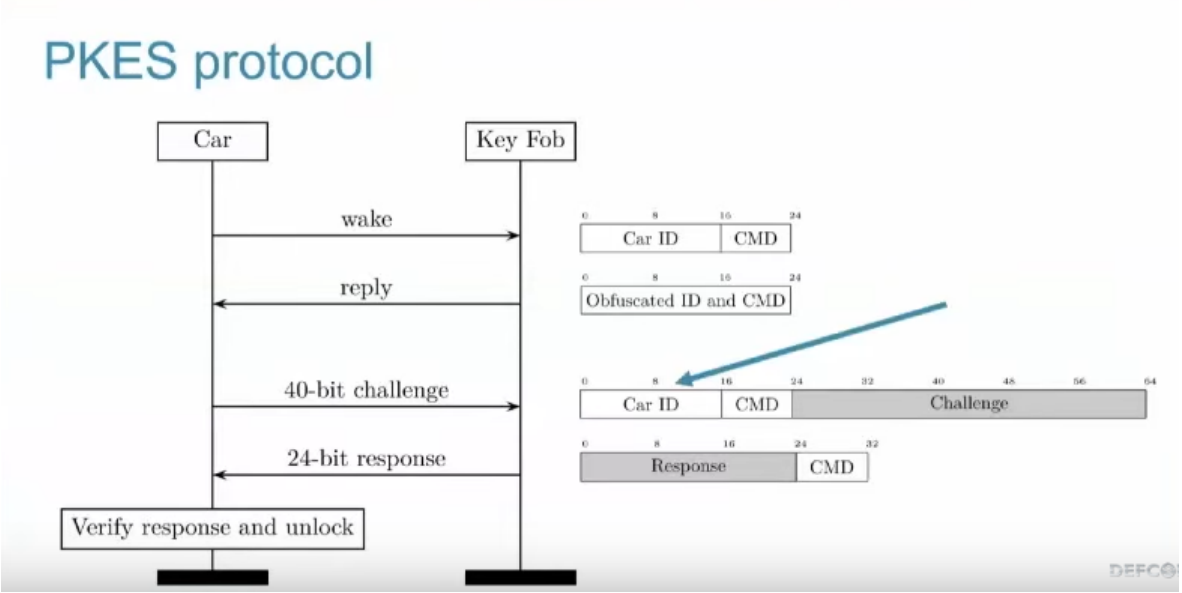
1. Lennert Wouters - Passive Keyless Entry and Start Systems - DEF CON 27 Car Hacking Village
    - Tesla kljuc nema onemogucen JTAG - dumpan firmware
    - ovakav tip kljuca bio je aktualan do 2018.
    - koristi zastarjelu DST40 šifru
        - https://en.wikipedia.org/wiki/Digital_signature_transponder
    - dva načina otključavanja, na pritisak gumba (RKE) i pasivno približavanjem automobilu(PRKE)
        - RKE - jednosmjerna komunikacija kljuc -> auto



        - ideja za RKE CTF izazov:



- PRKE



  - moguce je napraviti lookup tablicu za sve odgovore na odredjeni challenge prolazom kroz sve moguce kljuceve
  - slanjem challengea fizickom kljucu koji zelimo klonirati u lookup tablici pronalazimo DST40 kljuc koji je pohranjen u fizickom kljucu
  - Tesla vise ne koristi ovakve kljuceve, ali McLaren, Karma Automotive i Triumph koriste

2. Greg Hogan - Reverse Engineering and Flashing ECU Firmware Updates - DEF CON 27 Car Hacking Village
   - 3:30 - azuriranja honda i toyota firmwarea moguce nabaviti na https://techinfo.honda.com, https://techinfo.toyota.com
   - 6:23 - alat za reprogramiranje ECU-ova

Blockharbour

yt kanal - https://www.youtube.com/@blockharbor/videos
o platformi - https://blockharbor.io/vsec-platform/
VSEC - https://vsec.blockharbor.io/dashboard

Uvod u CAN
Blockharbour - Automotive CAN, Sending & Receiving Data

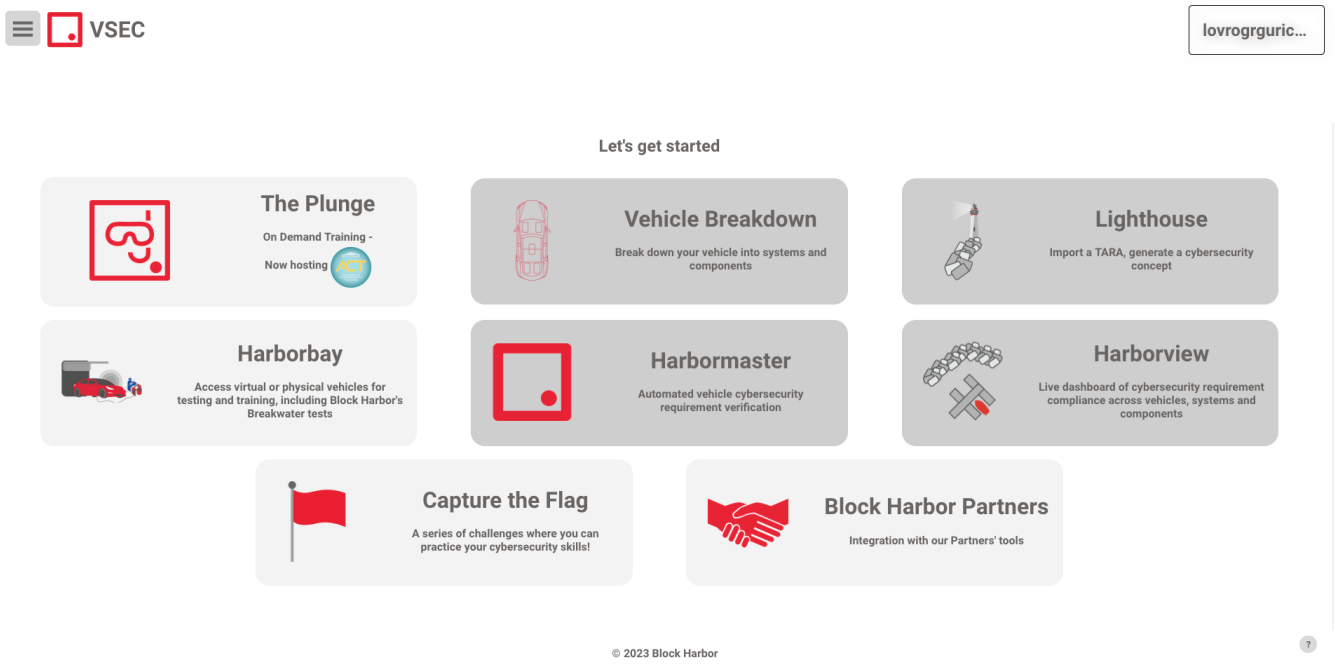
- najcesci CAN bitrateovi 500 000, 300 000, 250 000

Uvod u virtualni CAN i ICSim

- pogledat iduci tjedan skupa s ostalim simulatorima https://youtu.be/mQupRYb2c_Q?si=7QPT8LJbZ3KQfg13

platforma VSEC

Nakon prijave:



Funkcije dostupne "obicnim" korisnicima:

- The plunge - vodjena obuka kroz vise tema:
  1. Intro to Automotive Cybersecurity
  2. Block Harbor Hackathon 101
  3. BH Threat Analysis & Risk Assessment
  4. BH Vehicle Penetration Testing
  5. BH Vehicle Security Operation Center
- Harborbay
  - za tvrku koja kupi VSEC rjesenje ovdje bi bila virtualna ili fizicka vozila za testiranje i obuku
  - za obicne korisnike dva virtualna vozila kojima ne vidim razliku na prvu
- Capture The Flag
  - CTF odrzan prosle godine, neki izazovi se mogu jos uvijek rjesiti kroz Harborbay ili lokalno (primjerice reverzanje)

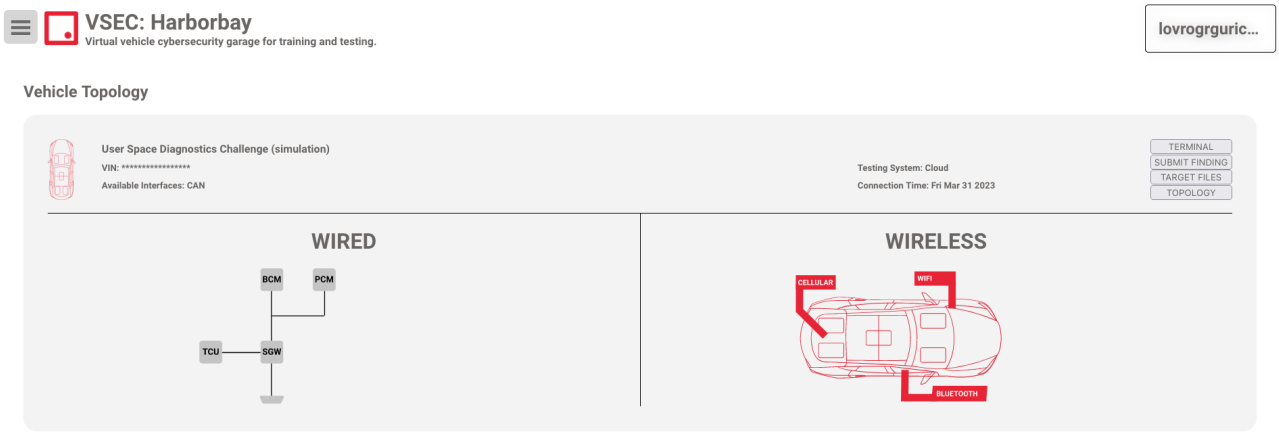
Funkcije dostupne zaposlenicima kompanija koje uzmu ovo rjesenje:

- Lighthouse za TARA
- Harborview - pregled compliancea za vozila i povezane sustave
- Harbormaster - automatizirana verifikacija sigurnosnih zahtjeva?
- Vehicle Breakdown - pregled komponenti i sustava vozila

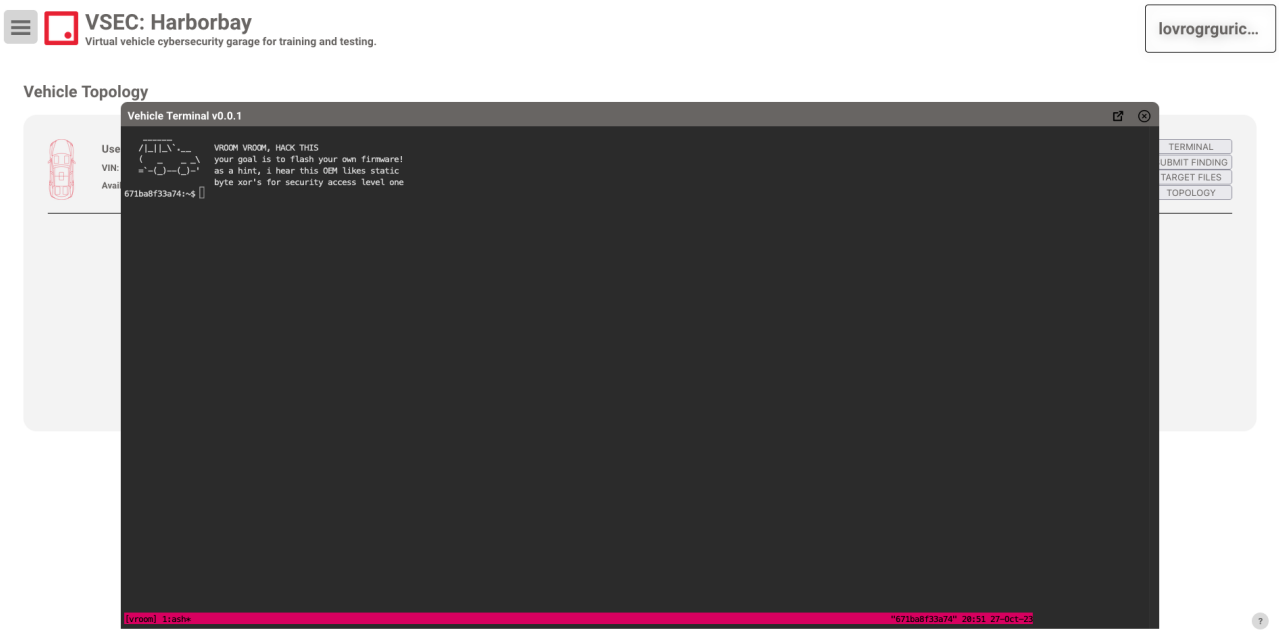
Harborbay

Primjer jednog od dva virtualna vozila:

- topologija:



- pristup preko terminala



  - koristi se za pristup virtualnom can sucelju vcan0 za rjesavanje CTF izazova:

```
671ba8f33a74:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:11:00:02
          inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18791 (18.3 KiB)  TX bytes:186835 (182.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

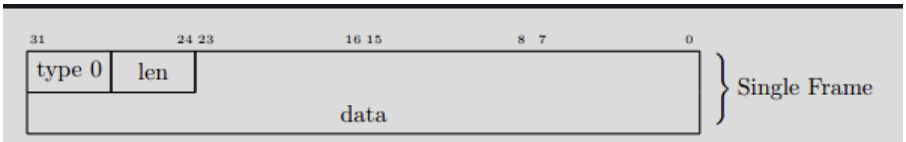
```
vcan0     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:72  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Blockharbour CTF

- rjesenje jednog od kompleksnijih UDS izazova "Security Access Level 3" : CTF - Automotive Reverse Engineering
  - citanje firmware-a iz memorije ECU-a preko UDS-a
  - reverzanje funkcije za firmwarea u ghidri
  - tijekom analize firmware da se zakljuciti da su za potrebe CTF-a emulirani samo odgovori na odredjene poruke te da se ne radi o pravom firmwareu
- rjesenje drugog UDS izazova
  - https://youtu.be/AwKT3oZuPWI?si=moTrPhYjnT8j3G9u

Read data by identifier izazov (UDS)

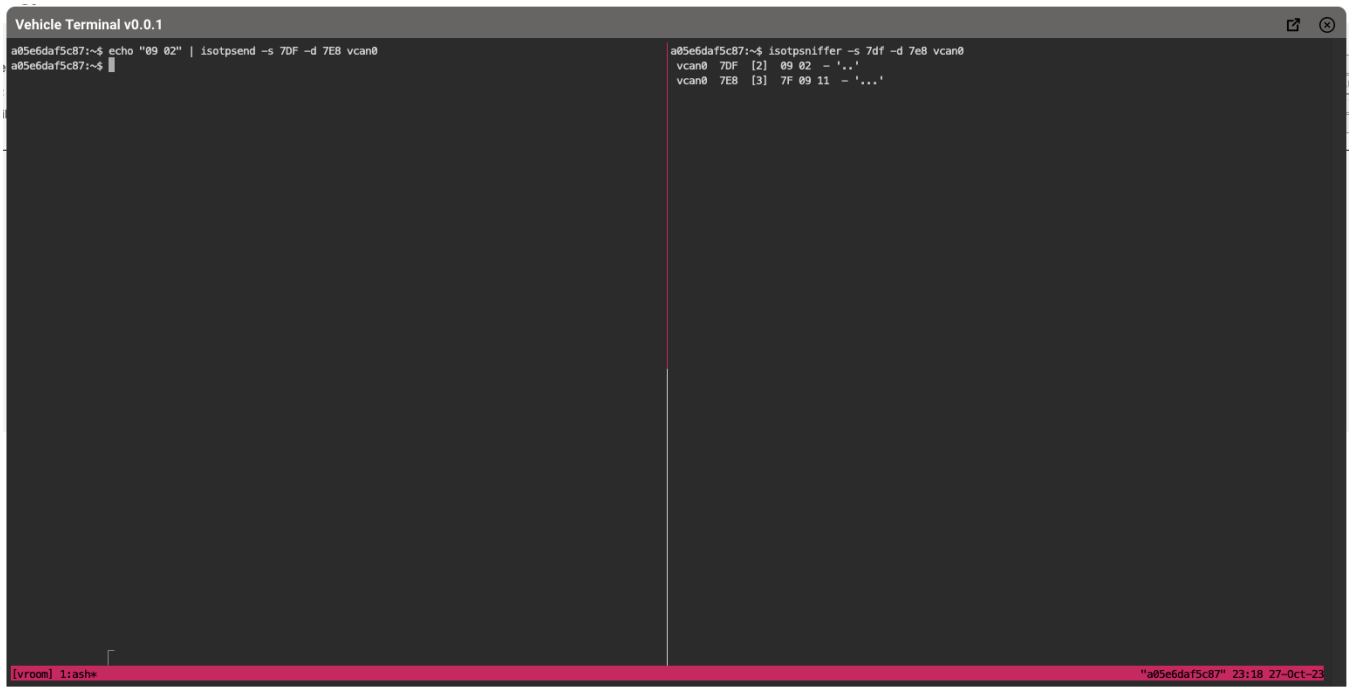
ISO-TP okvir tip 0 (pojedinacni okvir)



- isotpsend - alat za komunikaciju preko CAN transportnog protokola ISO-TP (koristi ga UDS)

```
APLIKACIJSKI    UDS
------------    ------
TRANSPORTNI     ISO-TP
------------    ------
FIZICKI + PP    CAN

primjerice dohvacanje VIN-a:
goli paket: 7df 02 09 02

7df  - CAN ID za OBD-II dijagnostiku                          [CAN]
02   - duljina podataka                                       [ISO-TP]
09   - mod "Requests vehicle information" (Definiran UDS-om) [UDS]
02   - PID zahtjeva za VIN u modu 0x09                        [UDS]

po ISO-TP protokolu paket s odgovorom imat ce ID uvecan za 0x08, odnosno 0x7e8

niz naredbi za poslati ovakav paket:

$ echo "09 02" | isotpsend -s 7DF -d 7E8 can0

a za snimati promet u oba smjera:

$ isotpsniffer -s 7df -d 7e8 vcan0
```

U terminalu na VSEC-u to izgleda ovako:



Medjutim nisam dobio potpuni VIN niti ocekivanu vrijednost UDS moda (umjesto 7F, vraceni UDS mod trebao je biti originalnih 0x09 + 0x40). Ovo je mozda tako zamisljeno u CTF-u medjutim to ne mogu potvrditi obzirom da CTF vise nije aktivan (s terminalom je moguce interaktirati neovisno o CTF-u).