Diplomski projekt - Edukacijski materijali / CTF platforma za kibernetičku sigurnost u automobilskoj industriji

Biljeske 13.10. - 20.10.2023

Postojeci "dostupniji" edukacijski materijali

Value PASTA

https://www.youtube.com/watch?v=MSk9KEwDcCc
https://github.com/mintynet/value-pasta-auto

Jeftinija verzija Toyota PASTA-e s 4 ECU-a baziranima na Teensy 4.0 mikrokontrolerima. Teensy ima 3 interna CAN kontrolera od kojih se u powertrain, chassis i body ECU-ovima koristi samo jedan. Gateway ECU koji filtrira promet izmedju ECU-ova koristi sva tri i jedan dodatan vanjski CAN kontroler MCP2515.

An Arduino based remote car can be controlled using #Value-Pasta-Auto . Minor changes for the lights were made to the code to control the lights from Value-Pasta-Auto. Arduino Sketch is in the Software folder.
Link to Amazon Freenove 4WD Car Kit
Original software for the car is Here

Car Hacking for Poories

https://illmatics.com/car_hacking_poories.pdf

- Charlie Miller i Chris Valasek, autori rada u kojem opisuju hakiranje Jeep-a
  - Remote Exploitation of an Unaltered Passenger Vehicle
- rad opisuje kako napraviti vlastiti test bench s prozivoljnim ECU-ovima za njihovo testiranje
- pokriva ozicenje, alate, reverzno inzenjerstvo, moguce probleme te spajanje tog test bencha na go kart

Primjerice ogranicenja test bencha:
"Working on a CAN network on a workbench certainly has its advantages, such as cost and convenience. However, there are some significant drawbacks. No matter how

accurate you try to make your artificial bench environment, you'll be missing some ECUs, sensors/actuators, or some traffic or something (unless you're a manufacturer who has a professional bench setup).
It won't be a perfect copy. For these reasons, some ECUs may not act exactly as they would in the vehicle. This can work both ways. You may send traffic to the ECU that won't affect it on the bench but would have done something interesting in the car, since perhaps the ECU is not in the right state to receive these messages. Likewise, you may think you found a great attack against an ECU when in the car it fails to work, perhaps because of a safety feature around speed or gear of the vehicle.
A great example of this is steering using the Toyota's Lane Keep Assist (LKA) feature on the bench. Without the steering angle ECU reporting the angle (and a simulated angle of 'straight ahead'), the LKA messages could be used to turn the wheel without the angle limitations adhered to in the car. The LKA scenario is interesting for two reasons. First, you might have thought you had a great attack that worked on the bench, but would not work properly in the car, due to angle turning limitations. Secondly, you could alter your attack in the car to always report 'straight ahead' as the steering angle in addition to the LKA messages."

Cloudcar

- CAN bus izazovi izvedeni preko virtualnih socketCAN sucelja
- writeup s DEFCON-a 2022
  - https://github.com/camercu/chv-ctf-2022-writeup/blob/main/CloudCar.md
  - https://www.youtube.com/watch?v=0CjFu-K3gNY&t=1619s
  - vecinom snimanje prometa i replay napadi
  - koristenje UDS servisa (primjerice za dohvacanje VIN-a)

BlockHarbor VSEC

https://www.youtube.com/watch?v=cG4O8_nueUY
https://vsec.blockharbor.io/login

Cheap Car Hacking for Everyone - A Prototype for Learning about Car Security

https://opus4.kobv.de/opus4-oth-regensburg/frontdoor/deliver/index/docId/641/file/RARC+2020+Proceedings.pdf

- opis
  - potencijalnog CTF sustava gdje raspberry pi-evi simuliraju ECU-ove spojene CAN sabirnicom i Etherent switchom
  - softvera koji bi se mogao koristiti
  - vrsta izazova
- jako osnovno
- "...another major change could
  also be to follow a similar approach as the picoCTF and to im-
  plement challenges inside a virtualized environment, therefor
  cutting the cost factor even more and nearly completely cutting
  the hardware part"

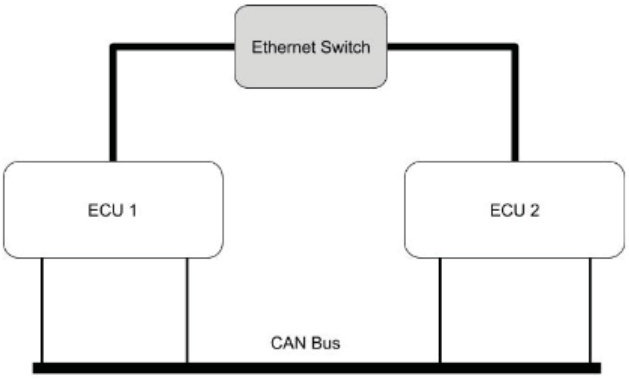

Fig. 1. Abstract graphical overview of the hardware architecture of the platform, with two ECUs replacements and two bus systems

Izazovi s reverzanjem

DEFCON 2023
https://github.com/camercu/chv-ctf-2022-writeup

UDS izazov
https://www.linkedin.com/posts/dbstephan_dash-activity-7118521976347930624-T0QT?utm_source=share&utm_medium=member_desktop