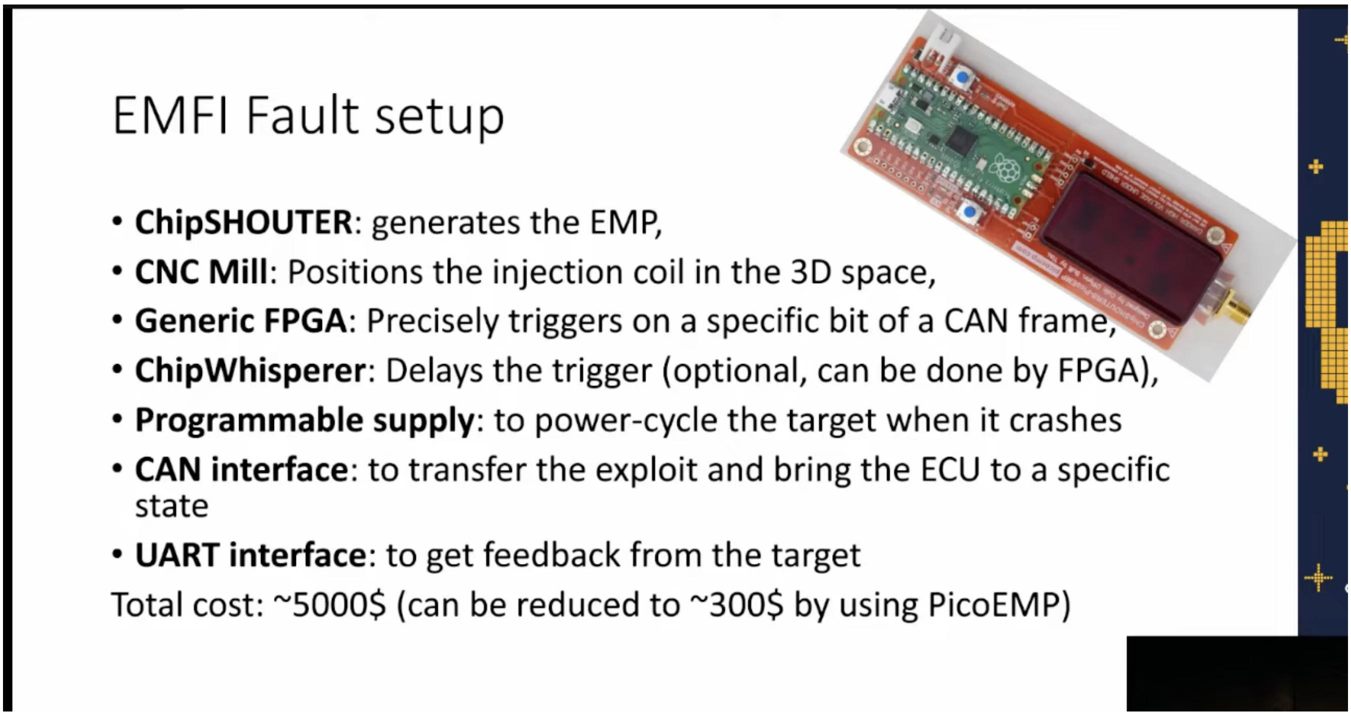
Biljeske 10.11. - 17.11.2023

Još analiza postojecih "napada"

TROOPERS23: Fault Injection Attacks on Secure Automotive Bootloaders



EMFI Fault setup

- **ChipSHOUTER**: generates the EMP,
- **CNC Mill**: Positions the injection coil in the 3D space,
- **Generic FPGA**: Precisely triggers on a specific bit of a CAN frame,
- **ChipWhisperer**: Delays the trigger (optional, can be done by FPGA),
- **Programmable supply**: to power-cycle the target when it crashes
- **CAN interface**: to transfer the exploit and bring the ECU to a specific state
- **UART interface**: to get feedback from the target

Total cost: ~5000$ (can be reduced to ~300$ by using PicoEMP)

Koristenje elektromagnetskog fault injection napada za zaobilazenje provjere potpisa firmwarea.

- moguci ishodi kod fault injectanja:
  - normalni CAN UDS odgovor
  - ECU Reset bez odgovora, exception stack dump preko UART-a
  - koruptirani CAN odgovor

Jos jedan rad od autora ovog talka, Dr Weißa, nazalost nije dostupan, prica o Virtual learning environmentu za kiberneticku sigurnost automobila

- https://library.iated.org/view/JAHN2021UND?re=downloadnotallowed
- poslati mail?

https://github.com/bri3d/sa2_seed_key/tree/master

- UDS seed and key rutina za volkswagen vozila

Nie, Sen, et al. "Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of Tesla cars." *Briefing, Black Hawt USA* (2018): 1-19.

Cai, Zhiqiang, et al. "0-days & mitigations: roadways to exploit and secure connected BMW cars." Black Hat USA 2019 (2019): 39.

https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/

Implemetacija virtualnih ECU-ova

SocketCAN

- https://www.kernel.org/doc/html/latest/networking/can.html

SocketCAN uses the Berkeley socket API, the Linux network stack and implements the CAN device drivers as network interfaces.