Flipper Zero

ASRG - Chicago Group

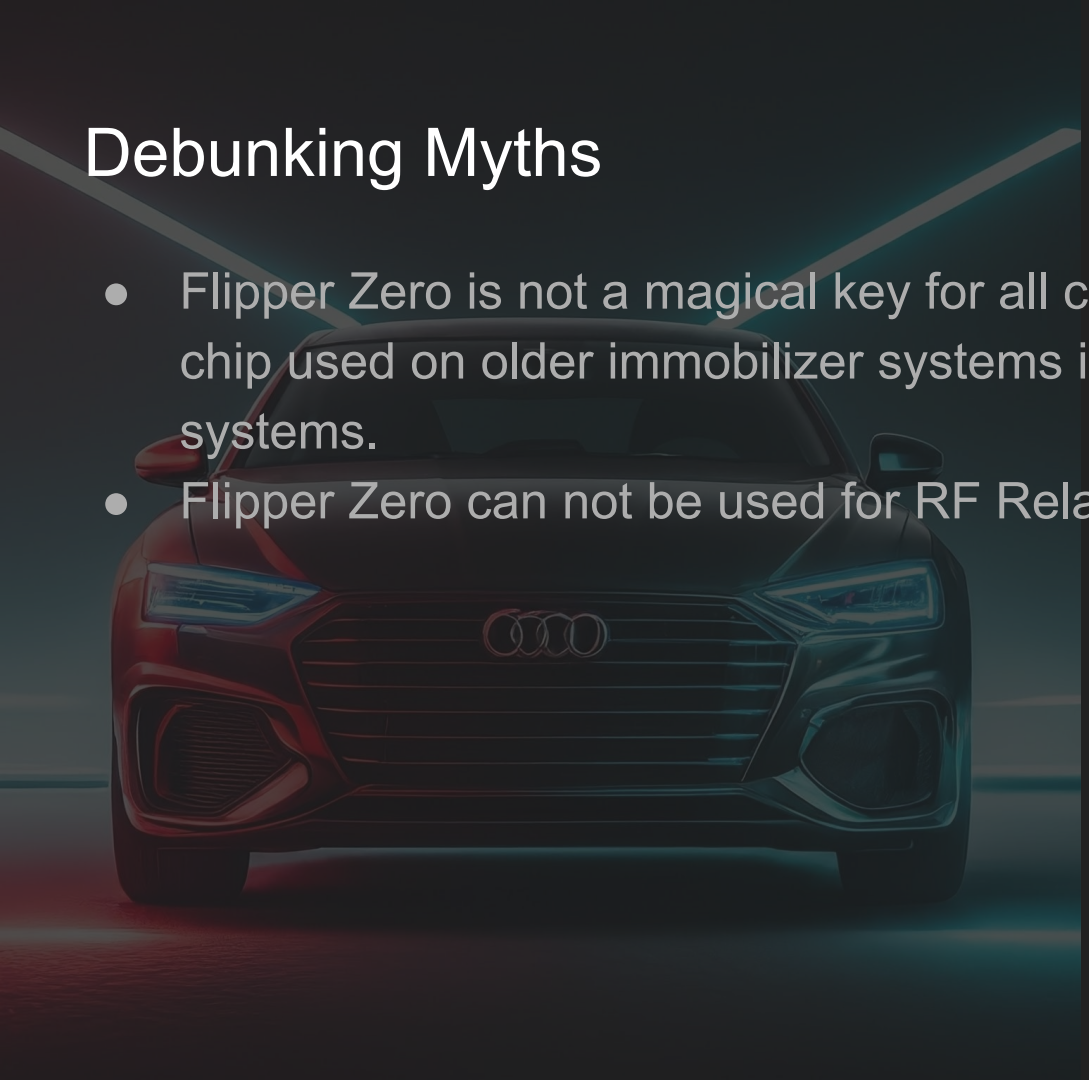
All the techniques and information we're going to discuss today are for educational purposes only. Please use this knowledge responsibly and ethically. Remember, you should only test or implement these techniques on systems where you have explicit authorization to do so.

Let's use our powers for good and ensure a safer digital world for everyone!

Capabilities

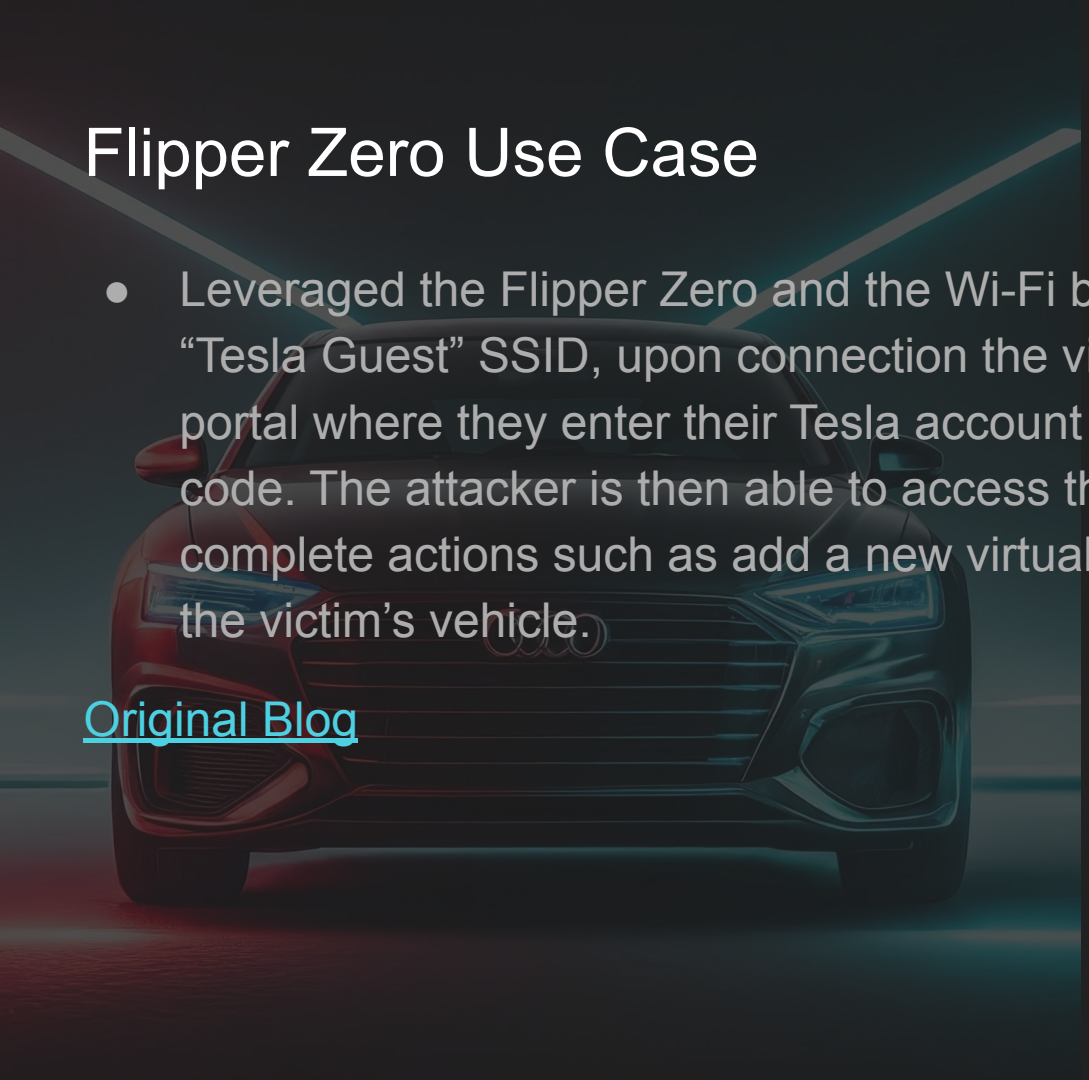
- Sub-1 GHz: Garage door remotes, boom barriers, IoT sensors and remote keyless systems.
- 125 kHz: Low-frequency proximity cards.
- NFC: High-frequency proximity cards.
- Bluetooth Low Energy (BLE).
- Infrared.
- GPIO for UART, SPI, I2C and others.

Debunking Myths



- Flipper Zero is not a magical key for all cars, while it can clone the RFID chip used on older immobilizer systems it does not work on modern systems.
- Flipper Zero can not be used for RF Relay attacks.

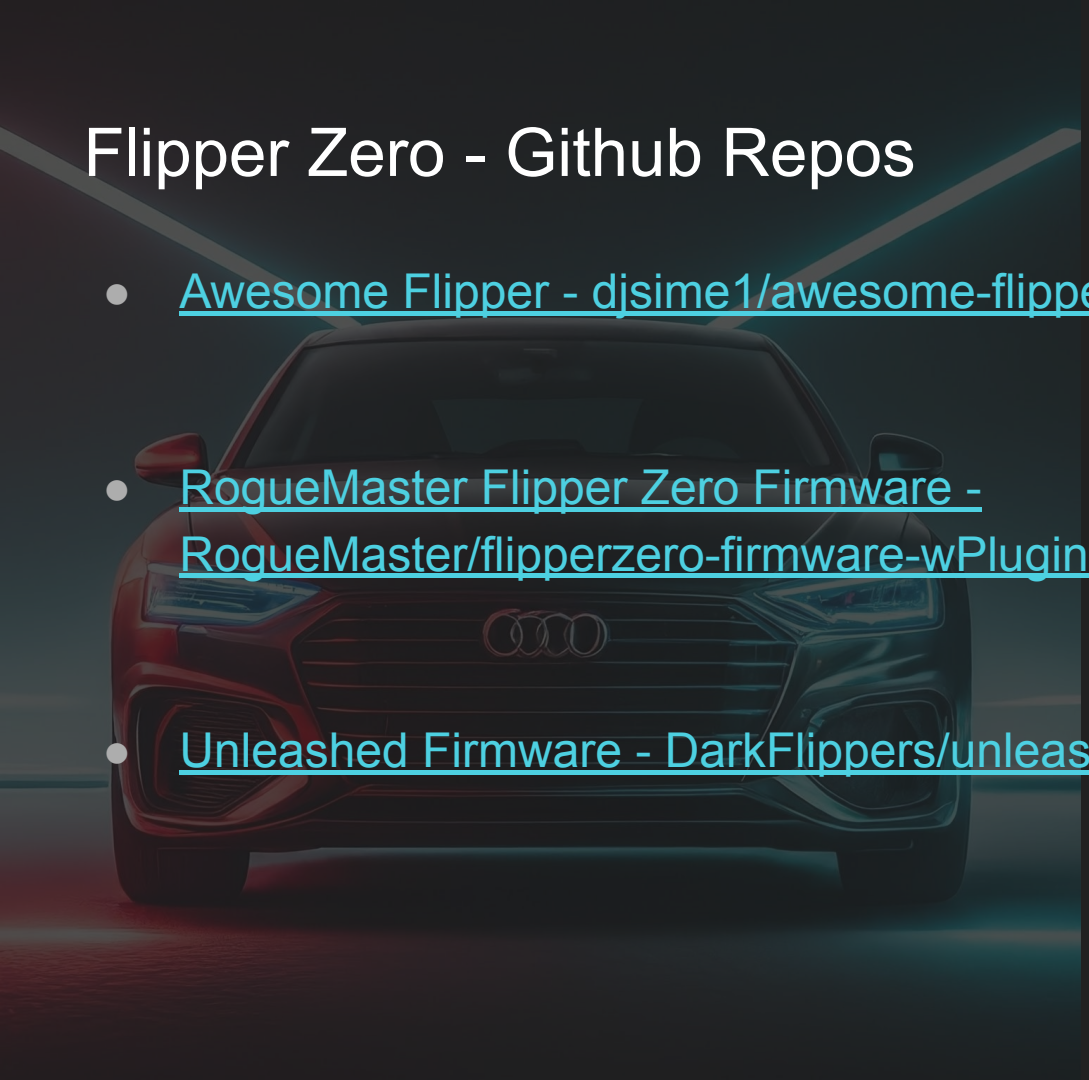
Flipper Zero Use Case



- Leveraged the Flipper Zero and the Wi-Fi board add-on the broadcast a fake “Tesla Guest” SSID, upon connection the victim is presented with a captive portal where they enter their Tesla account credentials including the 2FA code. The attacker is then able to access the victim’s Tesla account and complete actions such as add a new virtual key and use it to unlock and drive the victim’s vehicle.

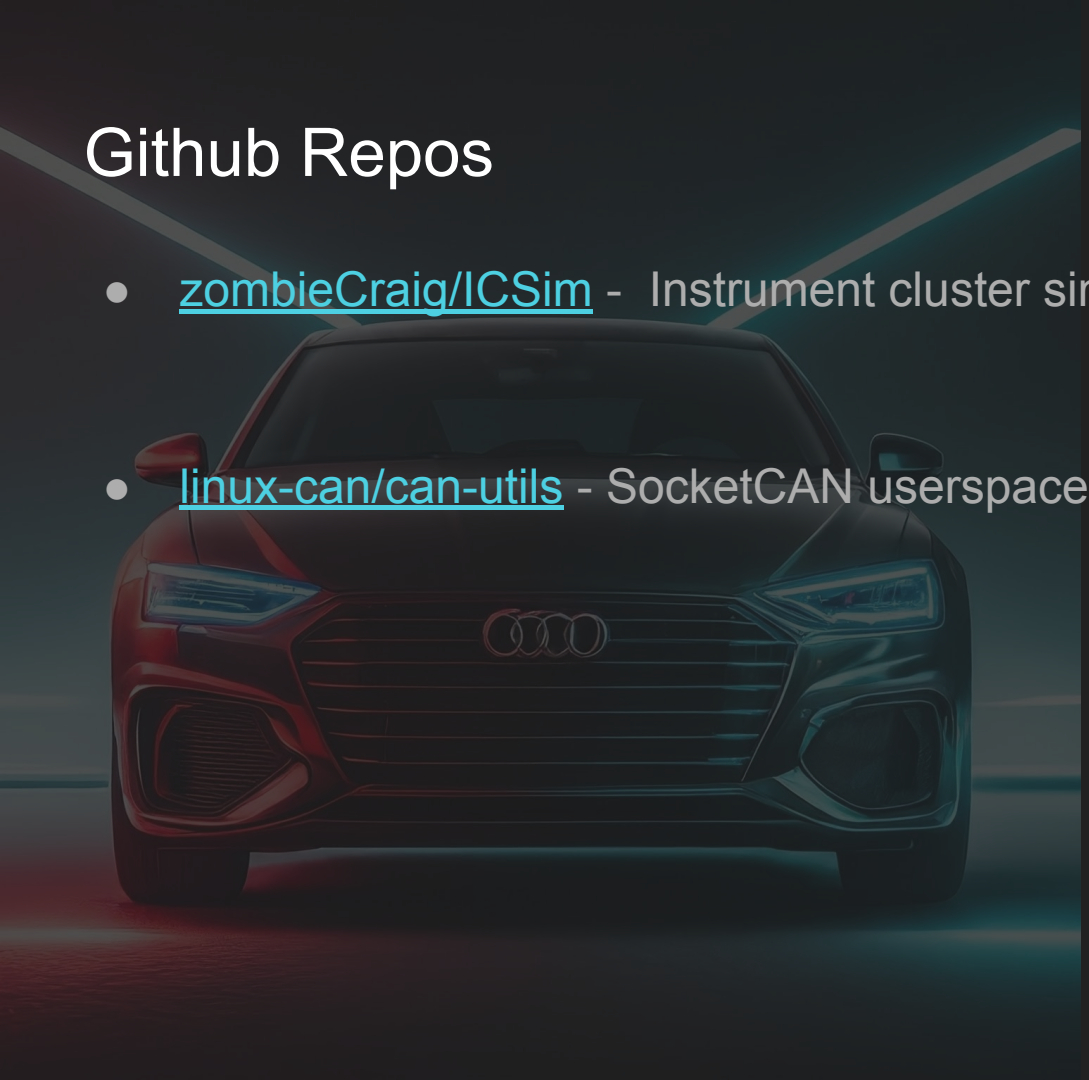
Original Blog

Flipper Zero - Github Repos



- Awesome Flipper - djsime1/awesome-flipperzero
- RogueMaster Flipper Zero Firmware - RogueMaster/flipperzero-firmware-wPlugins
- Unleashed Firmware - DarkFlippers/unleashed-firmware

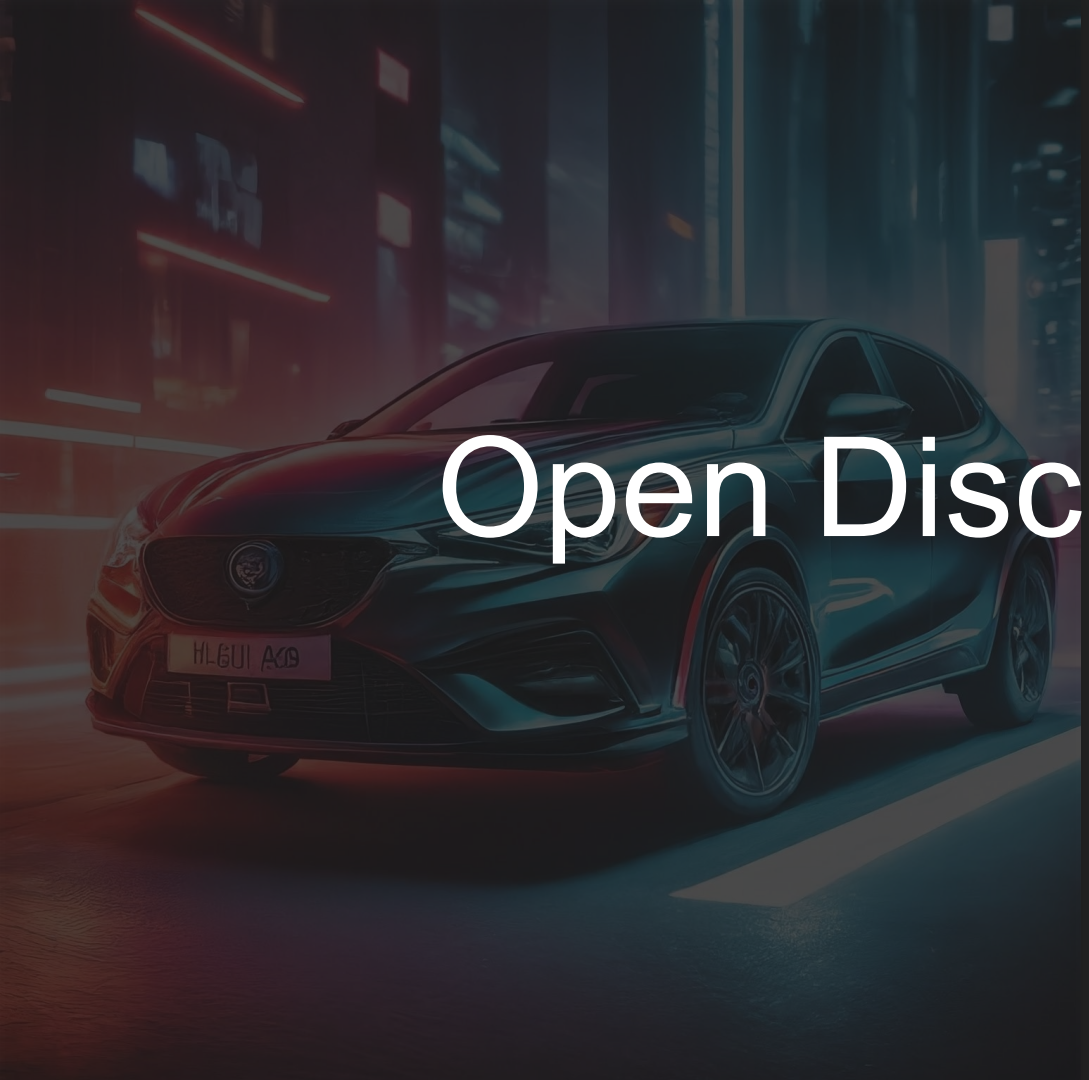
Github Repos



- zombieCraig/ICSim - Instrument cluster simulator for SocketCAN
- linux-can/can-utils - SocketCAN userspace utilities and tools

Other Available Tools

- Wi-Fi Pineapple Mark VII
- USB Rubber Ducky
- Shark Jack
- Bash Bunny
- Key Crock
- Packet Squirrel
- Screen Crab
- LAN Turtle



Open Discussion

KEY CYBER ATTACK VECTORS IN AUTOMOTIVE