Hackers and Hardware

Obinna Okonkwo (EE, Sr)
Isaac Mbappe (CpE, Sr)

Hakeem Thomas(EE, Jr) | Stephen Young(EE, Jr) | Azeezah Muhammad(CS, Fr) | Rahmana Muhammad(CS, Fr) | Faith Adegbenro(EE, Fr) | Cameron Lewis(CPE, Jr) | Olaide Afolabi(EE, Fr) | Olaoluwakitan Ajani(EE, Fr),

Faculty Advisor: Dr. Michaela Amoo

Background

FPGA Slam?

- A Field - Programmable Gate Array (FPGA) is an integrated circuit that be configured within the field by the designer to perform certain operations, but also be reprogrammed when necessary.
- SLAM (Simultaneous Localization and Mapping) would allow an Autonomous robot to localize itself within the environment while building a map of its surrounding.

What the General Public can look forward to

- Autonomous Electric Vehicles owned by Transport companies will make up 60% of vehicles on US roads by 2030.
- While 3 out of 4 vehicles will be autonomous by 2040.
- Global sales of fully autonomous vehicles are projected to by 600,000 vehicles in 2025.

- Lacking Charging Stations
- Expensive Impact on Buyers (whether garage charging systems or actual car)
- Physical Safety and Security
- Cyber Security Concerns
- Car Design
- Regulatory Standards, Insurance Liability and other legal issues

Problem Statement

- To address SLAM problem in autonomous navigation. In this case, the SLAM problem is how to do real time processing and control, given limited processing power.
- How to combat security issues whether with Hardware or Software solution.

Constraints

- The processing power available with a Pic 32 microprocessor.
- Financially, this project is well in means compared to other projects.

Design Requirement

Safety - The hardware security must adhere to the component safety standard.

Compliance - The device should be able to obtain the CE certificate, so it will various tests for its compatibility and efficiency.

Intellectual Property - Shouldn’t disrupt the software security protocol or any other security protocols.

Energy, Power, and Environment - Should not require too much power from the device and bring any danger toward the environment if damaged.

Size and Weight - The microprocessor can be 10mm long by 7mm wide, and approximately 0.5lb.

Pic 32 microprocessor with a Cansports, Ethernet and TCP/IP ports.


06/23/20
vocativ

Current Status of Art

- Tesla Manufacturing Issues

Solution Approach (Ideas)

- Use a lot of microcontrollers to create several encryptions.
- Connect the device on a specific network.
- Create firewalls.

Design Solution

- Software approach (standard approach)

  . Needs more microcontrollers(firewalls, antivirus)

  . Needs more power

- Hardware approach, requires us to build a convenient hardware-based security (reverse Engineering).

Various Sources to Hack our Autonomous Platform

- Serial Port
- CAN bus
- TCP/IP network

Controller Area Network (CAN) Bus

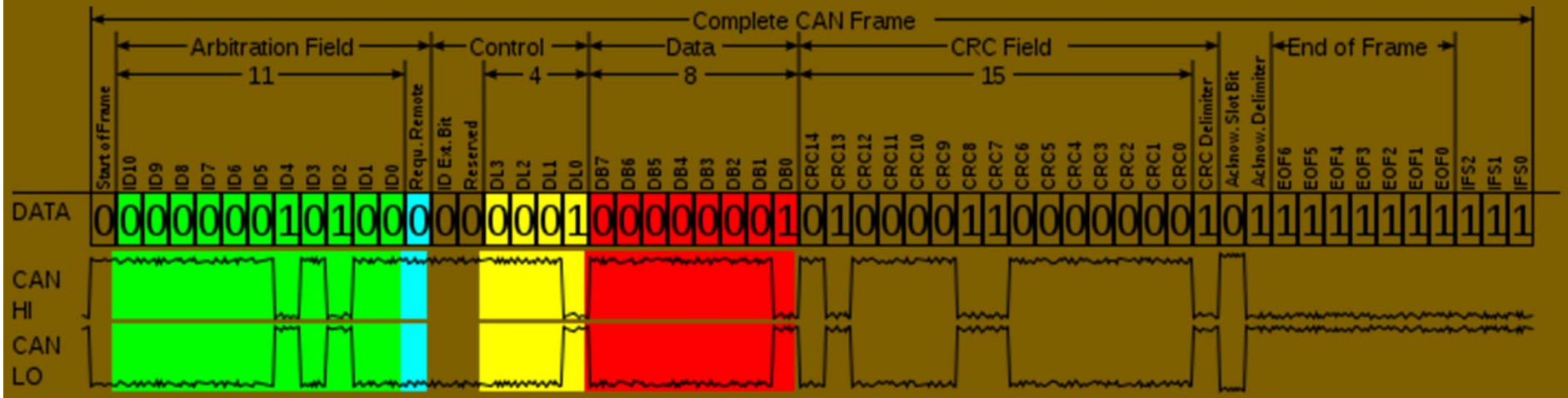
. Standard bus for vehicles.

. Connects devices to microcontrollers.

. Reduces wires used in a vehicle.

CAN Bus (Cont'd)

A hacker can infiltrate our system through the CAN by understanding the CAN frame.



CAN Bus (Cont'd)

The identifier ID and Data are the main important attributes for a hacker.

Identifier ID: - Sniff the CAN ID of devices

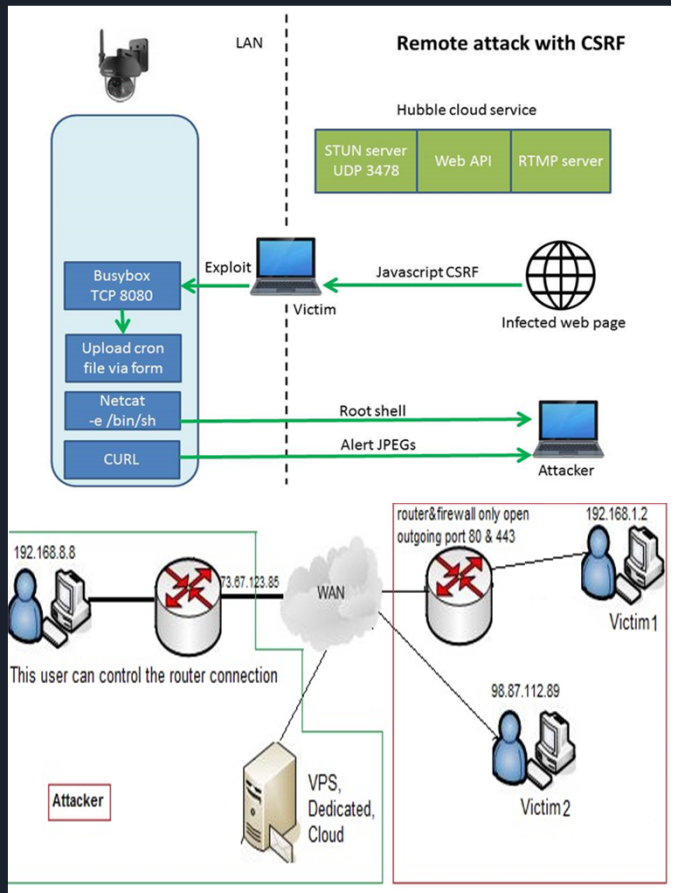
- Use them to spoof legitimate devices.

Data: - Sniff the legitimate traffic

- Decipher the vehicle CAN message data.

Transmission Control Protocol/Internet Protocol (TCP/IP) Network.

- Scanning for open ports is one common way a Hacker gaining entrance into one's system.
- Fault Injection , Bait and Switch, Virus/Trojan, etc



Conclusion

We can help the community safety related to autonomous vehicles, in creating well-developed procedure to keep intruders away from our system by figuring out all possible ways they can hack our system.