ENGINEERING AN AUTOMOTIVE OEM PROTOCOL OVER A CAN BUS

Gary Morrissey C00259786

MY AIM

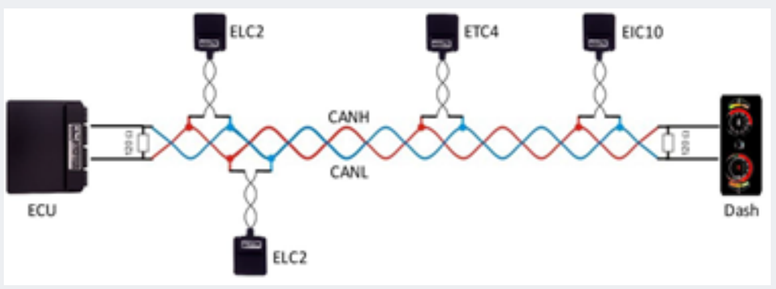
This project focuses on reverse engineering an OEM protocol over the Controller Area Network Bus. To reverse engineer and decode the communication protocol used by Mazda 6 OEM in their automotive systems.
For the purpose of this project, we will be focusing on the dashboard.

DELIVERABLE

This project will deliver an interface that can used to connect to a cars CAN Bus through the PEAK software. Once your laptop is connected to the car via USB to OBD2 port, you can use my application to brute force attack the dashboard. The software will interact with a camera pointed at the dashboard which will take a photo of the dashboard before sending a brute force attack, then send the attack and take another photo of the dashboard. The application will use OpenCV to detect which message sent affected the dashboard and would store it in a SQL database. The user then manually checks the stored messaged in the database and identifies the affects they had to the dashboard

CAN BUS

The CAN Bus (Control Area Network) is the communication protocol used in most cars. It is made up of a number of ECU's (Electronic Control Unit) that interact with different parts of the car. The CAN Bus has two different speeds, one at 125kbps and the other at 500kbps. Each speed consist of a High and Low bus for communication purposes.



TECHNOLOGY USED

Utilized the PEAK System softwares such as PCAN basic and PCAN View to establish connection to the CAN Bus and to send and receive messages. I also incorporated the Canon SDK to automatically take photos of changes during the attack.

BRUTE FORCE

This attack will occur by flipping each index on then off (from 00 to FF, then vice versa) and do that with each index position in the message. This will focus the user to which index affects the dashboard. Once narrowed down I can iterate through the binary digits of each index to focus on the dashboard