BRUTE FORCE ATTACK ON AN AUTOMOTIVE CAN BUS

Project Specification

Gary Morrissey C00259786

Table of Contents

Purpose

The intention behind this project is to reverse engineer a cars dashboard through the cars CAN Bus by implementing brute force attacks. A cars CAN bus (Controller Area Network) is the communication system used for the car to operate. This CAN bus is made up of electronic control units (ECU's) that have a specific purpose for different parts of the car. The purpose behind my project will be to communicate with the car through these ECU's and will send and receive the information through this channel to successfully reverse engineer the dashboard. Once the user has reverse engineered the dashboard, they can then determine how to change the dashboard switches. For the purpose of this project, the objective of your Brute Force Attack is to reverse engineer the Original Equipment Manufacturers (OEM) protocol, in this case on a Mazda 6.

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 an Open API to compare the images and point out the differences in them. The software will take this comparison of the two images and take note of what attack created the change. These will be added to a table of all attacks that were successful. Once a full collection is made of all changes, a library will be created, and the user will obtain all information needed to make their own changes to the dashboard. Meaning with a click of a button they can turn on and off the switch for the check engine light on the dashboard.

Deliverable Users

The purpose behind this project is not to create an application for general use, but to show the weakness in a cars CAN Bus system and expose its vulnerabilities through reverse engineering the OEM protocols. The people using this would be penetration testers to test their cars vulnerabilities but may also be used by a person with no technological background for an educational purpose.

Metrics

There are many different metrics available to judge this project off. Some include:

Attack Success Rate

We can measure the percentage of attacks that were successful and compare them to the number of overall attacks.

Rate of Attacks Attempted

Take the number of attacks attempted and calculate the amount of time it took for the attack to succeed or fail. It can show individual, average, and overall time taken.

User Experience

The users of the software can leave feedback on its functionality and usability, which can be used for future updates.

False Positives

We can calculate the number of false positives relayed back to the system which can lead to a slower run time to complete the attacks. If there is a high false positive rate, then the system will lead to the software using up resources that could be used to proceed with other attacks.

Camera Quality

The quality of the photos taken may affect the results of what attacks relate to what function. This could lead to the software making false operations on the dashboard. The camera quality should be clear as so the application can compare and contrast them.

FURPS

FURPS is a metrics model that will show the different variables that affect the production of this software.

Functionality:

My software will be a user-friendly interface. It will open with an empty table display. You then click a button to begin the brute force attack once connected to the car through the PEAK software. In the background the software will take pictures before and after each attack to determine what change it made. It will then populate the table with what attack caused what change and integrate it into a window where you can turn on and off the different lights and switches on the dashboard.

Usability:

The interface will display a clear and concise table showing the user exactly what changes occur after what attack. It will then add this to a display containing easy to read button that will indicate on or off. Once clicked it will change the status of the switch it correlates to on the dashboard. There will also be an option for to print the page of vulnerabilities that were exposed during the attack.

Reliability:

It may take time to gather all the information as some of the brute force attacks may not be successful. This will slow down the overall performance and cause the second display to load much slower.

Performance:

After initial testing and code fixes, the software will be able to perform the brute force attack efficiently. Once the attacks are successful, then the table will populate at an efficient rate. Once the connection through the CAN network is secured, the second display with the control buttons will be able to communicate with the dashboard quick and efficiently.

Supportability:

Updates to the software will be available through its release with upgrades to the display and the tables available. As well as updates to the brute force attacks and any bug fixes if necessary. Updates will have to be made if compatibility with the PEAK software is lost which may take time but overall won’t be necessary.

Deliverable Precent

While there are many brute force attack applications available for use, there is not one specific for a cars CAN Bus system. I gained inspiration from seeing different ethical hackers using wireless connections to gain access to locked cars as well as wired connection to change the cars default manufacturers settings. Many of these ethical hackers created their own Arduino unit to connect to the car, but I will be using a PEAK USB to OBD2 connection along with the PEAK software's API. My software will be unique due to its necessary connection through the PEAK software. The PEAK software allows the user to connect to the cars OBD2 port making an ease of access connection.

References

1. What is FURPS+? :https://businessanalysttraininghyderabad.wordpress.com/2014/08/05/what-is-furps/
2. Cybersecurity KPIs to Track + Examples: https://reciprocity.com/blog/cybersecurity-kpis-to-track-examples/