Final Lab: Cyber-Secure Vehicles in Modern Day

Riceli Foster, CIS 129

Introduction

- In this day and age, coding extends into everything we use, even some unexpected places… like vehicles.
- Wherever there is coding, there is the risk of the program being hacked, and this even affects the cars we drive today.
- There are millions of lines of codes encased in vehicle communication systems (commonly known as the Electrical Control Unit, or ECU)
- This interests me because I absolutely love cars; I love working on them, modifying them and am also equally concerned as vehicle software engineers about the safety of my own vehicles. This topic perfectly mixes my interest in cars and software, even adding cybersecurity in the mix.

Real World Applications

- Kevin Mahaffey and Marc Rogers, showed how they could take control of a Tesla Model S at the 2015 DEF CON hacking conference.
- Also in 2015, cyber researchers Charlie Miller and Chris Valasek hacked a Jeep Cherokee and took remote control of it from a house around 10 miles away, only using a laptop.
- These are incredibly dangerous situations; and, these are people who had no ill intentions of taking over these vehicles. Imagine as cars become more and more advanced, how much easier it will be for hackers to obtain control of these vehicles.
- One particular issue comes to mind: Teslas with autonomous driving.
- There was a recent update that extended to all Teslas (my father owns one and showed me the new program) that allowed Tesla owners to try the self-driving feature for free for a month. As we (well, the Tesla) were driving, I was thinking about the dangers of the car itself making mistakes; now imagine if that program was in the wrong hands.

Design Approach

- My design approach was heavily influenced by both what we learned in this class, and a particular website that explained how to code websites safely (referenced in last slide). I believe this could also be applied to vehicles, I just re-molded it to fit the design of vehicle communication systems:
  - Two-Step input validation
    - This allows the user to only input what the program deems as “correct” information. If not, you will get stuck in a loop.
    - If you allow the loop to happen three times, the vehicle will enter a lock mode, where the program cannot be accessed by anyone other than a dealership.
  - Sanitation of data
    - The stripping and processing of data that will be compared against the current contents of the program.
    - An
  - Authorized user access (last chapter we discussed with files)