Group number: SDMay24-39

Project title: Intrusion Detection System on Automotive CAN Bus

Client &/Advisor: Manimaran Govindarasu

Team Members/Role:
1. *Cole Burkle - Lead Vulnerability Tester/Car Testbed Lead*
2. *Trace Haage - Client Liaison/Pi Testbed Lead*
3. *Tiffanie Fix - Vulnerability Research and Development Lead*
4. *Alec Cose - Testbed Design/IDS Rule Development*

o **Weekly Summary**

Our team continued efforts in configuring our test beds (car and pi) to have a working model. We have begun a new phase in the project that introduces IDS development and testing before implementing it to the test beds. Moreover, each team curated a presentation on their progress and impending obstacles to our client.

o **Past week accomplishments**

- Cole: Meet with ETG to obtain power cable, met with Sourdeep for teensy connectors

- Trace: Scaled up Pi network. Added 3 new potentiometers onto the Arduino network to emulate 3 more PID's. Added message arbitration to the arduino to send CAN frames based on the lowest ID

- Tiffanie: Set up virtual machine for Snort as well as researched application in which Matlab could be used to simulate traffic

- Alec: Researched possible attacks for CAN environment. Created code to make potentiometer readings emulate CAN messages. Created logs for both clean CAN messages and attacks to be used in IDS.

o **Pending issues** *(If applicable: Were there any unexpected complications? Please elaborate.)*
- Cole: Awaiting missing parts
- Trace: Need to add a logging function to the Raspberry Pi receiver.
- Tiffanie: Needs to become more versed in Matlab Vehicle Network Toolbox and get virtual CAN working
- Alec: Learn more about Snort to begin IDS rule development.

○ **Individual contributions**

NAME	Individual Contributions *(Quick list of contributions. This should be short.)*	Hours these 2 weeks	HOURS cumulative
Cole	Worked to power the network	3	22
Trace	Scaled up network, added message arbitration	10	25
Tiffanie	Virtual machine set up for Snort and CAN	8	16
Alec	Created CAN messages into logs.	12	32

○ **Plans for the upcoming week**
- Cole: Powering network, collecting traffic through OBD2
- Trace: Add a logging function to start analyzing CAN traffic.
- Tiffanie: Continue setting up CAN config for virtual machines
- Alec: Plug CAN logs into Snort IDS and develop simple rules to detect current attacks.

○ **Summary of weekly advisor meeting**

Discussed week long milestones, all of which were accomplished and documented above.

Individually review Section 4.4. Consider the following questions:

Area	Description	Examples
Public health, safety, and welfare	Our project works towards ensuring the safe usage of passenger vehicles by detecting and alerting operators of potential intrusions occurring. Problems that result from not secure CAN Bus channels could cause harm to passenger vehicle users.	Detecting possible hacks into the CAN channels of passenger vehicles causing the vehicle to not function correctly. Denial of Service attack.
Global, cultural, and social	Globally, most individuals commute to their workplace or school using an automotive vehicle whether that is passenger vehicle, or bus transit many rely on cars to live. An IDS would assure malicious actors would not leave people without reliable transportation.	In 2021, kia challenge trend caused an uptick of 19% in car theft where on average of 17 Kias and Hyundais were stolen every day in Columbus due to an exploit where malicious actors use a usb cable to start the vehicle
Environmental	Testing the IDS may result in damage to the test bed or cause faulty parts in which replacement parts would be required that would have had a negative impact on the environment. We lead a carbon neutral footprint in utilizing recycled material	Replacement parts require the processing of raw materials, usage of fossil fuels for shipment so we thought it is our best interest to utilize parts from salvaged vehicle in the area or borrowed from the ETG

Economic	IDS would enact a positive measure in assuring their product's reliability as well as the customer's privacy and safety.	Companies are greatly impacted by the financial losses experienced in recalls and security breaches so there would be a huge selling market to manufacturers in being the only of its kind on the market

Have we identified or become aware of new effects?

We have not become aware of new effects, but we have realized that the Environmental effect is lower than we initially expected. Mostly all the parts needed for the car testbed were required secondhand from a junkyard, which would have all gone to waste if not used in our testbed.

How can we argue for or provide evidence of positive effects?

It is a positive effect on the environment because we are putting use to parts that would have been scrapped. We can instead use these parts to get a better understanding of a car's control system security and look to improve the general safety of CAN bus channels.

How can we address or justify negative effects?

Keep a running list of parts that we acquired secondhand versus parts that we needed to purchase. Ensure that we are not producing more waste than we are avoiding by going to the junkyard.