EE/CprE/SE 491 Bi-WEEKLY REPORT 4

2/24/2024 –

3/30/2024

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***

- **Weekly Summary**

  This period was spent making progress towards the IDS rule development by completing ways to send the CAN messages through Snort IDS. The process was preceded by the completion of our Raspberry Pi testbed, as well as significant progress in the functionality of the car testbed.

- **Past week accomplishments**

  - Cole: Created video presentation and stitched all team member videos together for peer review assignment. Research possible solutions to the current error in car testbed. Research issues the usb2can device.
  - Trace: Created video presentation and demo for peer review assignment. Gave and received feedback in person with group 41. Completed Pi testbed to have 4 sensors be able to send consistent data. Integrated snort to the Pi to look at a tcp socket, and began creating rules to view offline CAN traffic loaded onto the Pi.
  - Tiffanie: Created video presentation and demo for peer review assignment. Helped Cole come up with different theories of what is causing the error CAN messages and potential solutions to try and troubleshoot.
  - Alec: Completed feedback for our partner team after reviewing their project and

demo video. Completed final steps in Raspberry Pi testbed by fixing potentiometer outputs that are sent by the Arduino. Wrote python code to send packets to the Raspberry Pi so that Snort can read the CAN data being sent in each packet. Simple testing was done with basic Snort rules to get a better understanding of how they can be used in our packet format.

- **Pending issues** *(If applicable: Were there any unexpected complications? Please elaborate.)*
    - Cole: Fix the usb2can monitoring device
    - Trace: Issue with online loading of snort, need to figure out how to integrate it correctly
    - Tiffanie: Need Snort configured and test attack detection. We don't have a vehicle diagnostic tool to run error codes on the car testbed.
    - Alec: Small issue in the fact that Snort may not be able to be used online with our CAN channel and may be limited to just viewing log files instead.

- **Individual contributions**

NAME	Individual Contributions *(Quick list of contributions. This should be short.)*	Hours these 2 weeks	HOURS cumulative
Cole		50	22
Trace	Completed Pi testbed, added initial rules for snort	15	45
Tiffanie	Virtual CAN interface working, able to sniff the interface using Wireshark, able to simulate an attack.	36	16
Alec	Completed Pi testbed. Initial setup of Snort with log file. Feedback	14	46

- **Plans for the upcoming week**
  - Cole: Find a fix to the usb2can then research the issues with the car testbed.
  - Trace: Began to add more snort rules for other potential attacks. Begin working on an online version of IDS on the Pi testbed.
  - Tiffanie:
  - Alec: Do more research and testing with what CAN attacks can be run through Snort and how the rules can work to detect intrusions in the CAN message.

- **Summary of weekly advisor meeting**

  Advisor was absent for this period due to personal reasons. The team met with each other and a graduate student to update everyone on our current progress and receive a demonstration on the basics of Snort and how we can apply it to our current strategy of collecting CAN messages.

  Summarize the feedback you received (both written and verbal).

  The feedback that we received was less technical feedback and more regarding our presentation. Our project is more niche compared to others, and we need to ensure that we fully explain the problem and exactly what we want our final product/IDS to do based on that problem. Therefore, most of our time was spent explaining our project and the scope of it, which should have been portrayed through the presentation.

  Describe any new insights your team generated based on this feedback.

  We learned that we need to discuss more within our team to see which aspect of the project we will each be explaining. Since we have 2-3 different avenues we are taking, we need to make sure that the general idea that connects all of the aspects is properly communicated to the viewer/reviewer.

  What steps are you taking based on the feedback?

We plan to focus on improving communicating our project to the audience by streamlining ideas so that the project goals and deliverables are clear and concise. Given the complexity and layers to our project it would be best to provide background such as the significance of each of our testbeds and the overall impact it has to the automotive industry.