EE/CprE/SE 492

Weekly Report: 24 March 2023

Group number: sdmay23-15

Project title: Mobile Vehicle Cybersecurity with Onboard Key Management

Client &/Advisor: John Potter and Joseph Zambreno

Team Members/Role:

- ***Aayush Chanda - Advisor Liaison***
- ***Baganesra Bhaskaran - Gitlab Administrator***
- ***Chau Wei Lim - Strategist***
- ***Michael Roling - Documentor***
- ***Alexander Freiberg - Client Liaison***
- ***Brian Goode - Team Organizer***

Weekly Summary

The team made progress on developing its existing software. Gaining confirmation of communication between two nodes allowed for additional nodes to be generated; these simulate several devices on the CAN Bus. Extending the amount of data being transferred between these nodes was achieved as well. Initial messages being sent were only 12 bytes; progression has been made to allow for up to 64 bytes (CAN-FD). Merging development branches to include TweetNaCl - the project's means to encrypting and decrypting data - has begun as well. These past successes (multiple nodes, CAN-FD, and TweetNaCl) will pave the way for integration of many branches; communication is more closely mirroring that of the CAN Bus.

Past week accomplishments

· Aayush Chanda:

- Furthered progress on sending CAN FD frames through J1939 protocol
- Started integrating TweetNaCl into project to encrypt data before sending and decrypt data after receiving

· Baganesra Bhaskaran:

- Worked on identifying the need of encryption/decryption function splitting for the usage of CAN communication
- Tested splitted function for decryption and ruled out the need of those as header files in the can send/receive communication

· Chau Wei Lim:

- Reviewed and tested the updated CAN communication with J1939 protocol
- Researched on how to set up a remote desktop that share with other team members

· Michael Roling

- Reviewed the integration of TweetNaCl to encrypt/decrypt messages being sent
- Tested CAN communication in conjunction with J1939 protocols

· Alexander Freiberg

- Developed code to bring TweetNaCl into the main branch
- Code review to handle box and box open functions within the main branch

· Brian Goode:

- Looked into practicality of manifest list and its value added to project
- Implementing a nonce to prevent replay attacks

Pending issues

· All team members

- Need to identify the ways of integrating and implementing the manifest into the scripts to hold public-private key pairs of each ECU connection.
- Continued development on bringing the software to align with pertinent J1939 protocols; discussions surrounding the necessity of the matter are being held.
- Integrating box/box open functions with handling a nonce

Individual contributions

NAME	**Individual Contributions**	**Hours this week**	**HOURS cumulative**
Aayush Chanda	- Furthered progress on sending CAN FD frames through J1939 protocol - Started integrating TweetNaCl into project to encrypt data before sending and decrypt data after receiving	7	14
Baganesra Bhaskaran	- Identification of need of encryption/decryption function splitting - Ruled out the necessity of header files inclusion in can send/receive scripts - Code review and Git repository management	6.5	13
Chau Wei Lim	- Code review on the updated CAN communication with J1939 protocol - Researched on setting up shared remote desktop - Team website management	6	12
Michael Roling	- Code review on passing CAN FD frames through J1939 protocol - Integration of TweetNaCl to handle encryption/decryption - Documentation of weekly meetings,	6	12
Alexander Freiberg	- Integrating TweetNaCl with main branch to encrypt/decrypt - Integrating Box/Box Open functions with main script to handle data	6.5	13.5
Brian Goode	- Analyzed possible means of a manifest list and its practicality - Development surrounding the nonce	6	12

Plans for the upcoming week

· Aayush Chanda

- Encrypt data being sent, then decrypt the encrypted data when it is being received

· Baganesra Bhaskaran:

- Work with the team to get the scripts and project on progress
- Implementation and testing of how manifest can be integrated within the CAN socket communication

· Chau Wei Lim:

- Integrate the encryption and decryption functionalities into the CAN communication with J1939
- Implement a fully functional shared remote desktop

· Michael Roling

- Integrating TweetNaCl with main branch; encrypting and decrypting data
- Code review for other segments of the project; Box/Box Open and manifest list

· Alexander Freiberg

- Merging development branches of Box/Box Open and encryption/decryption
- Software development regarding manifest list and its place in the project

· Brian Goode:

- Work on implementation of the nonce within our project and research/testing of different manifest implementations.

Summary of weekly client meeting

Integrating the development branches for CAN-FD, J1939 protocols, a manifest list, TweetNaCl, and Box/Box Open functions will be the upcoming action items. It was well-received that individual testing for each of these functions was being conducted; the separation increases the probability of overall success when they are merged. A point of particular interest was J1939. Implementation of the entire protocol list is outside the scope of the project, but using items such as PGNs will assist in the identification of messages; these characteristics will be amplified as a manifest list will verify a sender's validity.