EE/CprE/SE 492

Weekly Report: 20 April 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's focus was on the final development of TweetNaCl. Issues were present regarding the number of bytes being encrypted, therefore, the messages passed could not be decrypted. Resolving these complications - how the message was being handled prior to encryption and the message's nonce - allowed for proper decryption. The accomplishment proved to be a strong milestone for the team. A note should be made regarding the speed of TweetNaCl, too. The encryption/decryption process was often hindered to better visualize its functionality during development; removing these delays will ensure the expected deliverable is met. Coupling this milestone, alongside the ability to send and receive messages between ECUs, will solidify the expected requirements. The time hereafter will be spent on further development to improve the system.

Past week accomplishments

· Aayush Chanda:

- Wrapped up integrating tweetnacl encryption/decryption of message with can_send and can_receive

· Baganesra Bhaskaran:

- Started working on the manifest list
- Synthesizing and improving readability of software with comments
- Separate Git repository allocated for code compilation

· Chau Wei Lim:

- Integration of TweetNaCl with the ability to Tx/Rx messages
- Helping with the development of a manifest list
- Assistance in the writing of the final report

· Michael Roling

- Code review for TweetNaCl and how messages are being handled
- Preparation for the final slide deck and poster to be presented
- Assistance with the final report writing

· Alexander Freiberg

- Debugging TweetNaCl and message encryption
- Integrating TweetNaCl and how overall messages are being Tx/Rx

· Brian Goode:

- Finalized conception of manifest list
- Will be assisting in the final report and presentation

Pending issues

- The only final task of the team is to create a manifest list. Development of the list will allow one primary ECU to have globally accessible message variables. The ECU will be permitted to transmit messages in CAN FD frames, or else stay on the receiving end of the communication. Implementation for this will ensure other controllers cannot be placed on the CAN Bus and possess the ability to Tx/Rx messages.

Individual contributions;

NAME	**Individual Contributions**	**Hours this week**	**HOURS cumulative**
Aayush Chanda	- Finished the complete can_send and can_receive tests - Encryption of message from transmitter and decryption from receiver.	6	13
Baganesra Bhaskaran	- Started working on the manifest for complete key distribution within - Separate Git repository allocated for code compilation - Review of final report and slides for presentation purposes	6	12
Chau Wei Lim	- Integration of TweetNaCl with other primary functionalities - Assisting in the manifest list	6	12
Michael Roling	- Drafting the final slide deck and poster for the team's presentation - Code review for TweetNaCl and its ability to handle messages; encrypt	6	12
Alexander Freiberg	- Development of TweetNaCl and message encryption to Tx - Will be merging TweetNaCl with the other primary functionalities; Tx/Rx	7	13
Brian Goode	- Development for the manifest list - Assistance with writing the final report and presentation	6	12

Plans for the upcoming week

· Aayush Chanda

- Convert the send and receive scripts into functions for a single ecu to be able to use.
- Integrate functions into ECU script (created by Baga and Chau)

· Baganesra Bhaskaran:

- Complete implementation for manifest on public/private key distribution
- Integration of working TweetNaCl encryption script into the ECU
- Testing and debugging of the ECU script with encryption in both sending and receiving mode

· Chau Wei Lim:

- Finalize integration between TweetNaCl and the ability to Tx/Rx between ECUs
- Help develop manifest list to prevent invalid ECUs to function on CAN Bus

· Michael Roling

- Finalize the final documents; report, slide deck, and presentation
- Code review of the integration between TweetNaCl and Tx/Rx functionality

· Alexander Freiberg

- Merge TweetNaCl with other files to ensure proper functionality
- Assist with the final report as the team prepares to present

· Brian Goode:

- Code review as manifest list begins to be integrated
- Assist in the final report writing and finalize other documents

Summary of weekly client meeting

Both meetings over the past two weeks proved to be of great benefit. The initial meeting was focused around the debugging of TweetNaCl; reviewing how messages were being generated, how they were handled in the encryption process, and how they were being decrypted. It was later found, outside the meeting, a bug was present in how the messages were generated. These issues were resolved and were a testament to TweetNaCl's effectiveness; the encryption/decryption process worked. The functionality was presented at the subsequent client meeting and final action items were discussed; integration of TweetNaCl into the master branch, alongside the creation of a manifest list, were the final steps of the project.