# *EE/CprE/SE 492*

***Weekly Report: 02 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 found success in utilizing TweetNaCl; a protocol used to encrypt and decrypt messages sent on the CAN Bus. The protocol uses two primary functions: Box and Box Open. These functions - which meet the project's requirements in terms of efficiency and language - are capable of being integrated into the team's developed code. In addition to TweetNaCl, the team furthered its development by writing software to send and receive data. The ability was extended across multiple 'users' which simulate nodes on the CAN Bus. Discussing these developments with the team's client provided additional action items. Meetings will continue to be held as the software development progresses in simulating the CAN Bus with added security.*

**Past week accomplishments**

· Aayush Chanda:

- Software development to bring functionality to CAN socket communication
- Looked into J1939 protocols and existing security measures
- Assessed TweetNaCl and its ability to be integrated

· Baganesra Bhaskaran:

- Reviewed the code for CAN socket communication
- Worked on formatting and optimizing the encrypt and decrypt script for TweetNaCl
- Planned on task division and git repository management

· Chau Wei Lim:

- Debugged and reviewed TweetNaCl and CAN socket communication implementation
- Researched on implementation of multiple nodes with SocketCan
- Managed the team website to make sure it is up to date

· Michael Roling

- Reviewed software regarding TweetNaCl and the ability to encrypt/decrypt messages
- Assessed CAN Socket software and conformity to J1939 standards
- Setting next action items for coming week(s) and documenting progress

· Alexander Freiberg

- Implemented NaCl encryption demo for the client
- Troubleshooted vcan socket programming
- Began transitioning current vcan socket programming to J1939 protocol

· Brian Goode:

- Researching socketCAN functionalities and implementation examples.
- Working on team socketCAN code and reviewing code

**Pending issues**

· All team members

- Need to complete splitting encryption and decryption into separation scripts with header files associated to ease the use in the socket communication as function calls
- Bringing encryption/decryption protocols into CAN socket communication
- Integrating J1939 standards to increase readability of developed software; will assist for applicable use on CAN Bus hardware regarding controller's identification and length of message being Tx/Rx

**Individual contributions ("should be between 6-8 hours/week")**

| **NAME** | **Individual Contributions** | **Hours this week** | **HOURS cumulative** |
|---|---|---|---|
| Aayush Chanda | - Implemented test for CAN FD communication | 7 | 13 |
| Baganesra Bhaskaran | - Git repository management<br>- Code review and optimisation for TweetNaCl scripts | 6 | 12 |
| Chau Wei Lim | - Code review for TweetNaCl and CAN socket communication implementation<br>- Team website management | 6 | 12 |
| Michael Roling | - Reviewing CAN Socket software and conformity to J1939 standards<br>- Assessing TweetNaCl encryption and decryption of messages being sent | 6 | 12 |
| Alexander Freiberg | - Implemented NaCl encryption demo for the client<br>- Troubleshooted vcan socket programming<br>- Began transitioning current vcan socket programming to J1939 protocol | 6 | 15 |
| Brian Goode | - Researching socketCAN functionalities and implementation examples.<br>- Working on team socketCAN code and reviewing code | 5 | 13 |

**Plans for the upcoming week**

· Aayush Chanda

- Further work on CAN communication scripts
    - Look into 29-bit identifiers
    - Read length of message and check for validity

· Baganesra Bhaskaran:

- Integration of TweetNaCl into CAN socket communication
- Code review and optimization

· Chau Wei Lim:

- Help out with implementing a encrypted CAN socket communication using TweetNaCl
- Configure a stable virtual environment to run our final design implementation

· Michael Roling

- Developing software to be more inline with J1939 standards
- Code review for integrating CAN socket communication with TweetNaCl

· Alexander Freiberg

- Finish transitioning vcan socket program to J1939 protocol
- Integrate NaCl demo code into current socket communication protocol

· Brian Goode:

- Working with bringing tweetNACL encryption into our current working implementation of socketCAN
- Bringing our current socketCAN implementation to J1939

**Summary of weekly client meeting**

Discussions with the client revolved around introducing TweetNaCl and CAN socket communication. The former action item was deemed to be a success in week one's meeting; a *n*-byte message was encrypted and decrypted within the project's requirement time constraints. Communication between multiple terminals - sending and receiving messages - was achieved during the second week. Verifying these capabilities across several nodes was a strong lead-in for the coming week's action items: integrating TweetNaCl with current CAN socket communication abilities and improving CAN socket communication by introducing J1939 standards. These achievements met the past week's goals and were strong steps towards the overall development of securing the CAN Bus.