EE/CprE/SE 492

Weekly Report: 7 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

Integrating CAN send/receive functionality was one of the team's primary advancements. The current design programs each ECU to be in a continuous search until it receives its intended message; the provided loop offers succinct software and scalability. Additional observations should be made as these features are integrating CAN-FD protocols, an extension of CAN which handles more data at a quicker rate. Further development is being made on the encrypted payload using TweetNaCl. Decryption issues recently arose which highlighted the initial encryption process. Debugging the software - analyzing the data being sent, how it is handled, and the reception process - are the current practices being employed. Integrating these functions will help ensure the overall success of the encryption/decryption process on the CAN bus to secure the data being sent.

Past week accomplishments

· Aayush Chanda:

- Worked on encrypting the message before adding it to the nonce and sending it as the can fd frame payload

· Baganesra Bhaskaran:

- Combined the can frame sending and receiving script into one ECU script
- Have single C file to have receiving can_fd frame and able to send message (12 bytes size)
- Helped teammate with debugging the send and receive integration script

· Chau Wei Lim:

- Debugged the ECU script for simultaneously receiving and it only get interrupt when there is data for it to send
- Created a demo script to show the functionality of ECU script
- Discussed with teammates on the pseudocode for the implementation of main ECU script (manifest)

· Michael Roling

- Code review of CAN send/receive functionality and its conciseness
- Analyzed TweetNaCl and its ability to encrypt messages with necessary payload
- Upkeep of team documentation and further software development

· Alexander Freiberg

- Integrating encrypt/decrypt functionality for CAN messages
- Debugging the encrypt portion of TweetNaCl; issues present with nonce

· Brian Goode:

- Researching most efficient way to integrate nonce
- Assisting in the development of a manifest list to identify invalid users

Pending issues

- Have globally accessible message variables to be set and read by the main ECU. This enables a single ECU to send messages in CAN FD frames if there is any passed from the main ECU, or else stay on the receiving end of the communication.
- Running into issues with encrypting the message correctly so that the receiver can decrypt it; running into several “Numerical result out of range” errors.

Individual contributions;

NAME	Individual Contributions	Hours this week	HOURS cumulative
Aayush Chanda	- Worked on encrypting the message before adding it to the nonce and sending it as the can fd frame payload	6	13
Baganesra Bhaskaran	- Integrated send and receive can fd frame script into one ECU script - Helped in debugging the ECU script to have in function on both ends of the CAN communication.	6	12
Chau Wei Lim	- Completed the receiving function in ECU script - Created a demo script to show the functionality of ECU script - Discussed ideas for the implementation of main ECU script (manifest) - Team website management	6	12
Michael Roling	- Code reviewed the CAN send/receive functionality to be integrated - Team documentation regarding notes, updates, and further development. - Researched TweetNaCl integration	6	12
Alexander Freiberg	- Encrypting messages correctly with a nonce to prevent replay attacks - Integrating TweetNaCl into the main development branch	7	13
Brian Goode	- Research and development on the most effective way to integrate a nonce - Analyzing the creation of a manifest list to ensure ECUs are aware of invalid users on the CAN Bus	6	12

Plans for the upcoming week

· Aayush Chanda

- Work on the errors with encryption and then be able to decrypt the message from the receiver ECU side.

· Baganesra Bhaskaran:

- Have the send and receive integration work efficiently in detecting if any instruction/data to be sent with the globally accessible message variable.
- Debug the script
- Git repository management

· Chau Wei Lim:

- Work together with Baga on the ECU script for debugging send functionality
- Implement the code for main ECU (manifest)

· Michael Roling

- Code reviewing the integration of TweetNaCl and how messages are handled
- Nonce implementation to ensure it is encrypted correctly with CAN FD frame
- Continue with documentation upkeep; notes, updates, and development.

· Alexander Freiberg

- Debugging the encrypt portion of TweetNaCl; decryption appears to have the proper functionality.
- Integrating TweetNaCl into the main development branch
- Implementing a nonce into the encryption of TweetNaCl

· Brian Goode:

- Integration of a manifest list which recognizes valid users in a timely manner
- Code review and development of TweetNaCl which handles the nonce

Summary of weekly client meeting

Discussions revolved around the integration of TweetNaCl; a demonstration was offered to the client as issues were present during decryption. It was determined encryption must be the root of the complication as the number of bytes being transmitted did not align with TweetNaCl's protocol. These observations were solidified by the use of Valgrind; a tool which monitors memory in real-time. Plans were made for the near future to debug the complication as it is the primary functionality of the project. Further discussions focused on the integration of the current CAN send/receive functionality; operations worked as anticipated and confirmed the project's current standing.