EE/CprE/SE 492

Weekly Report: 18 Feb. 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 focused on integrating TweetNaCl, a compressed version of NaCl, to encrypt/decrypt messages sent on the CAN bus. Reviewing TweetNaCl's C code allowed the group to gain a stronger understanding of how Box and Box-Open operate; the encryption methods to be used. These functions met the requirements of the project with respect to its language, efficiency, and integration. Recognizing where these functions fit within our CAN Socket software was the subsequent step. Questions were raised whether the CAN Socket software should be translated to Python, but C was the decision made as the translation would be at the expense of efficiency. These decisions were reviewed among our team and then our client.

Past week accomplishments

· Aayush Chanda:

- Worked on compiling a document to assess TweetNaCl
- Reviewed software to better understand how TweetNaCl will be implemented
- Having discussions on how TweetNaCl should be used in development

· Baganesra Bhaskaran:

- Worked on implementation of PyNacl for demonstration of encryption and decryption key plus the secret messages
- Proper establishment of key derivation function and digestion of string of any size to a 32 byte input to be stored in a box (crypto secret box)
- Organized and uploaded code to the git repository for code sharing and version control
- Research about CAN key exchange protocols and how PyNacl facilitates it

· Chau Wei Lim:

- Did research on the Python libraries related to CAN to utilize them in implementation
- Worked on implementing a simple CAN bus communication in Python to compare its efficiency with existing C code
- Helped Baganesera with debugging the implementation of PyNacl

· Michael Roling

- Researched key exchange protocols applicable to CAN Bus
- Assessed current VCAN software to recognize where NaCl encryption should occur
- Began looking into TweetNaCl and its encryption protocols

· Alexander Freiberg

- Reviewed current VCan implementation C code to identify where NaCl encryption should be implemented
- Researched C libraries with lightweight TweetNaCl implementation
- Began rudimentary implementation of TweetNaCl demo

· Brian Goode:

- Reviewed existing CAN socket software to analyze where encryption should occur
- Becoming more familiar with TweetNaCl and its functionality
- Studied key exchange protocols to see which best fit CAN bus

Pending issues

· All team members

- Conversion of PyNaCl into TweetNacl
- The encryption and decryption code was written in Python with the integration of PyNacl. Proceeding with TweetNacl, which is a C implementation, will streamline development as the working software is written in C. The existing issue was discussed with the client and the team was advised to implement TweetNaCl. The client also suggested simplifying the Python implementation as TweetNacl could facilitate it as it offers adequate tools.
- Implementation of key server for key generation and management for ECUs on the CAN bus

Individual contributions

NAME	Individual Contributions	Hours this week	HOURS cumulative
Aayush Chanda	- Reviewed TweetNaCl encryption protocols for the CAN bus - Studied software to better understand where the encryption protocols will be most effective	3	6
Baganesra Bhaskaran	- Implementation of working code of PyNacl for encryption and decryption of key and secret messages - Organization of code repository - Addressing issue of converting the current implementation into a different language for the ease of project	4	7
Chau Wei Lim	- Implementation of Python script to demonstrate the CAN communication by utilizing Python libraries - Research on the potential concerns of having two programming languages running on a small storage component	4	6
Michael Roling	- Researched key exchange protocols which are applicable to the CAN bus	4	7

	- Reviewed existing C code on to locate where NaCl encryption can occur - Looked into TweetNaCl encryption		
Alexander Freiberg	- Presented previous findings to client - Researched C libraries with TweetNaCl implementation - Studied current simulation code to identify where NaCl encryption should be implemented - Began rudimentary TweetNaCl implementation in C	5	8
Brian Goode	- Reviewed TweetNaCl and its encryption protocols - Reviewed existing software to see where encryption best fits	3	6

Plans for the upcoming week

· Aayush Chanda

- Will be looking to implementing TweetNaCl into existing software
- Cutting out redundant code, if applicable, to increase efficiency

· Baganesra Bhaskaran:

- Will be working on converting the working implementation into C language and make TweetNacl as the tool for key exchange in the project
- Research on integration of TweetNacl into the project based on the requirements
- Work on code sharing and version control with the team members

· Chau Wei Lim:

- Work on implementing a demonstration code of public and private key exchange using TweetNacl to meet client's requirement

· Michael Roling

- Will be starting to integrate TweetNaCl into the project
- Looking to build existing knowledge of public/private key exchange on CAN bus

· Alexander Freiberg

- Finish rudimentary TweetNaCl demo implementation to determine if this library is adequate

· Brian Goode:

- Integrating encryption protocols into existing software
- If applicable, removing unnecessary code to make software more succinct.

Summary of weekly client meeting

Integrating TweetNaCl with the existing CAN socket software was the primary focus of the weekly meeting. Reviewing what needs to be passed into TweetNaCl's Box and Box Open functions led into a stronger understanding for the team's next action items. Discussing the need for each controller's unique address and a manifest list to keep track of each verified controller was brought up as well. These action items will assist in identifying invalid controllers on the CAN bus. The weekly meeting proved to be beneficial as each member was brought up to speed on the project's development and where it will be going.