Mobile Vehicle Cybersecurity with Onboard Key Management

Iowa State University: ECpE sdmay23-15

Aayush Chanda, Alexander Freiberg, Baganesra Bhaskaran, Brian Goode, Chau Wei Lim, Michael Roling

Overview

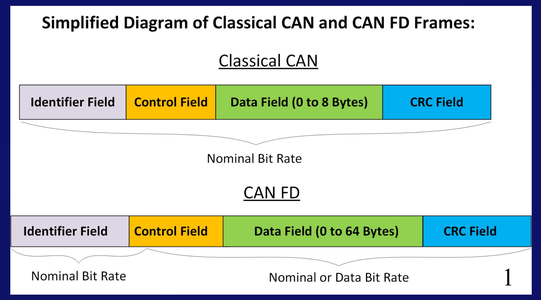
The controllers used within a vehicle - the computers which interpret sensor data, operate a number of drive systems, and yield reliable performance - all communicate via the controller area network (CAN) bus. It is a two-line system which reduces complex wiring and allows controller communication without a host computer. The data sent on the CAN bus, therefore, will be received by each controller. It is in the interest of all parties involved - the manufacturers, operators, and third-party producers - the data is genuine. Security and safety issues arise when illegitimate controllers are placed on the vehicle's CAN bus; specifically, devices which can read and manipulate data. Similar threats can be implemented through software attacks, for example, the vehicles which communicate via cellular towers. Providing a novel solution to secure the data sent on a vehicle's CAN bus and render falsified information purposeless is the primary goal of sdmay23-15's project.

Introduction

- Project deliverables
  - Handle entire CAN frames
  - Ability to generate keys to encrypt/decrypt data
    - Functionality should be achieved without OEMs injection of confidential information; implications extend to 3rd parties
  - Communication operations are to meet recognized standards within the automotive industry
    - ISO and SAE
- Other project objectives
  - Encryption/decryption and Tx/Rx must be handled in an efficient manner (5mS)
    - E.g.near immediate acceleration and deceleration
  - Familiarity with other encryption/decryption methods within the automotive industry

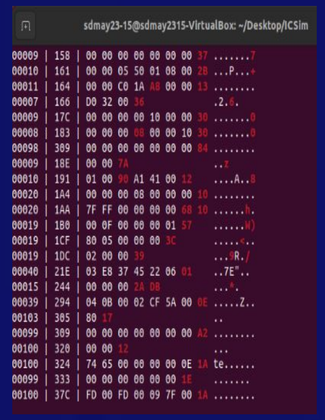
Methodology

- Preliminary research
  - CAN functionality, J1939 Protocols, and pertinent ISO Standards
- Design proposals
  - Using of existing CRC bit field to hold encrypted data being transmitted
- Revision of design to increase scalability
- Implementation of CAN and encryption tools



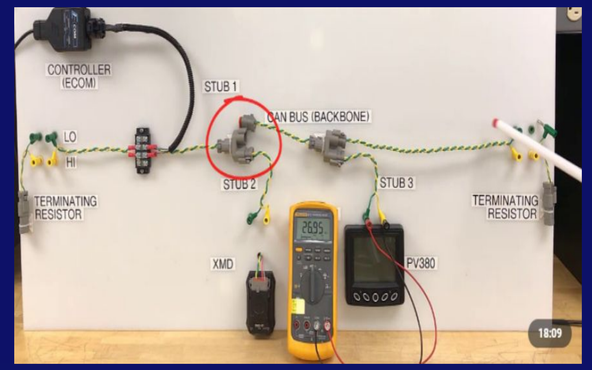
Implementation

- Virtual simulation environment
  - Ubuntu; multiseat operation
- CAN Socket in C
  - CAN Tx/Rx
  - Multiple nodes on the CAN Bus
- CAN FD and J1939
  - Extension of CAN Frames
  - Increased bits/second
- TweetNaCl encryption
  - Efficiency
  - Box Function; nonce and MAC
  - Functionality ensures security



Results

- Effectively met project requirements
  - Technical ability to handle CAN-FD segments
    - Sequential Tx/Rx CAN messages (<5 mS)
  - Implementation of key management protocols (J1939)
  - Generated key to handle encryption/decryption of messages; specifically, not OEM generated.
    - TweetNaCl



Impact

- Strong safety applications to the vehicle industry
  - OEM and 3rd party manufacturers
    - Controllers can be used across vehicle platforms
    - Encourages business and innovation
  - Vehicle owners; improved safety

Conclusion

- Brings awareness to importance of digital security
- Novel approaches to encryption/decryption
- Abilities to transfer large amounts of data in little time

All images were created by researchers unless otherwise specified. Image 1 (KVaser).
Additional resources are featured on sdmay23-15's website: sdmay23-15.sd.ece.iastate.edu