Cybersecurity Implications of Modern Automobiles

Samuel C. Hollifield, Miki E. Verma

Electrical and Computer Engineering

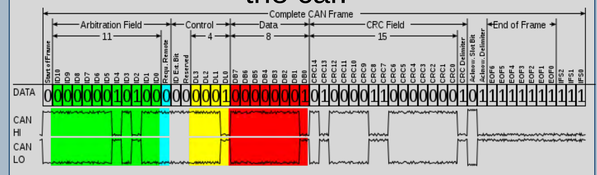
Mentors: Dr. Robert Bridges, Dr. Stacy Prowell, Dr. Sheikh Ghafoor

Controller Area Network (CAN)

What is CAN?

Controller **A**rea **N**etwork

The CAN Bus exists as the primary network in modern automobiles. It accounts for communication between electronic control units which operate the car.



Problem

- Vehicles are driven by many electronic control units which communicate via CAN.
- CAN has many inherent vulnerabilities. For instance, researchers can arbitrarily inject messages in order to influence vehicle operation.
- Previously demonstrated attacks have removed safety-critical functions from the vehicle, such as disabling the brakes on a moving vehicle [1].
- There is no reliable way to detect or prevent these attacks.

Research Goal

- Develop a solution which can detect cyberattacks in real-time regardless of vehicle make, model, or type.
- Establish a normal operating baseline on any CAN and subsequently detect anomalous messages.
- Deploy a pluggable device which has the ability to monitor a CAN and alert the driver in case of a cyberattack.
- Validate approach by detecting a real attack on a moving vehicle.

Contact Information

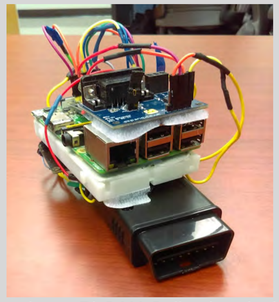
- Samuel C. Hollifield, schollifie42@students.tntech.edu
- Miki E. Verma, vermake@ornl.gov

Cyber and Applied Data Analytics Division
National Security Sciences Division
Oak Ridge National Laboratory

Progress

Data Generation & Collection

- Data from an assortment of vehicles is required. Therefore, we built numerous inexpensive collection devices using consumer electronics such as Raspberry Pi and Arduino boards.
- ORNL's Vehicle Security Lab has been instrumental in obtaining network traffic in a safe, controlled environment.
- Due to the cost and complexity of automobiles, an automotive electronics testbed has been incredibly valuable in rapid prototyping for experimental designs.



Raspberry Pi CAN Collection device

ORNL's Vehicle Security Lab

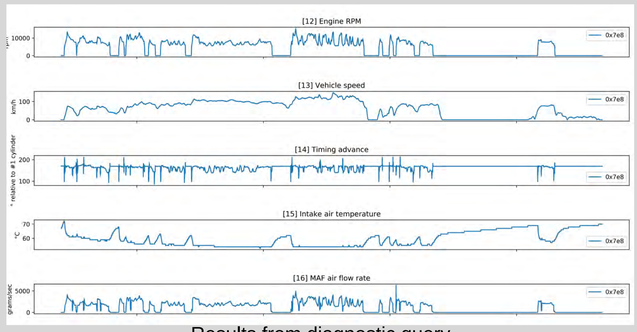
Automotive electronics testbed

Future Work

Data Analysis and Deployment

- Following the data collection phase, we will develop the algorithms necessary to deploy on a vehicle to detect cyberattacks.
- Using our automotive electronics testbed, we can rapidly prototype intrusion detectors which will next be used with a vehicle.
- We plan to expand on past work to understand and define unknown CAN message contents.

Although CAN is easily manipulated, manufacturers do not disclose the functional encoding of the traffic → We can map messages by translating diagnostic queries into raw CAN bits [2].



Results from diagnostic query

Acknowledgements

Special thanks to Michael Iannacone. Research sponsored by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory, managed by UT-Battelle, LLC, for the U. S. Department of Energy (DOE). This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Approach

1) Collect ambient CAN data and CAN data with emulated attacks.
2) Develop a vehicle-agnostic algorithm which profiles the standard network messages during normal operation.
3) Use a message-content-based detector to determine anomalies in order to prevent or detect cyberattacks.

Conclusions

- Automotive CANs present a massive attack vector within complex, expensive machines.
- Developing after-market protection which work regardless of vehicle make and model is difficult due to lack of standardization among CAN definitions.
- Mandated diagnostic protocols operate via CAN, this allows us to analyze network traffic during diagnostic requests to match patterns being transmitted elsewhere on the network.
- The use of consumer electronics (such as Raspberry Pis) have allowed for rapid prototyping and development of automotive applications.
- Vehicles are expensive and it can be dangerous to experiment on a moving car. A testbed has proven instrumental in completing our research.
- Current state-of-the-art intrusion detection methods do not reliably detect advanced attacks, so a modern solution is necessary to address this critical problem

References

[1]. Valasek, C., & Miller, C. (2015). *Remote Exploitation of an Unaltered Passenger Vehicle*. 91.

[2]. Verma, M.E., Bridges, R.A., & Hollifield, S.C. (2018). *ACTT: Automotive CAN Tokenization and Translation*. *CoRR, abs/1811.07897*.