Expanding Talent Development

Students: LAUREN HERRINGTON, KELLY HOWELL, RYAN CORLEY
Advisor: DR. JEREMY DAILY

NMFTA National Motor Freight Traffic Association, Inc.

THE UNIVERSITY of TULSA
Student CyberTruck Experience

Objectives

Develop a curriculum to:

1. Generate interest in heavy vehicle cyber security
2. Build a foundation in engineering, computer science, cyber security, and the trucking industry
3. Prepare student participants to have a future impact on the industry regarding heavy vehicle cyber security

Curriculum

Computer Knowledge Development

A Computer Science (CS) student researcher may be familiar with basic programming and computer operations. This is a skill that the Mechanical Engineering (ME) students will have to acquire during the research experience.

Vehicle Networking

Vehicle Networking involves both reading and hands-on learning. Although both researchers will have to finish the readings to be knowledgeable about the industry. The hands-on data acquisition will generally be easier for the engineering student researcher in comparison to the computer science researcher.

Cyber Security Overview

CS researchers may have previous knowledge of cyber security but for the researcher new to this topic, cybrary.it provides a free platform to take training courses regarding different operating systems and programs with a cyber security emphasis

Trips and Experiences

The Cyber Auto and Cyber Truck Challenges provide good hands-on experience for any researcher. The challenges allow the students to strengthen their vehicle knowledge, cyber security and reverse-engineering skills.

Instagram Photo of Laruen and Maya during the Student CyberTruck Research Experience.

PEOPLENET
A TRIMBLE COMPANY

GEOTAB
management by measurement

Computer Knowledge

- Multiple Operating Systems
- Low Level Bit and Byte Operations
- Programming in Different Languages
  - Python in Linux
  - C in Arduino

Vehicle Networking

- CAN Knowledge
- Diagnostic Software
- Embedded Hardware
- SAE J1939
- ISO 15765

Cyber Security Overview

- Seed-Key Exchange
- Symmetric vs Asymmetric Encryption
- Secure Hash Algorithms
- Security in Depth

Trips and Experiences

- Cyber Auto Challenge
- Cyber Truck Challenge
- Sponsor Site Visits
- OEM / Supplier Factory Tours
- Fleet Carrier Operations

Bibliography

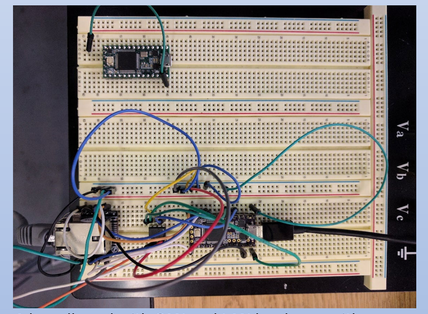
The following references are recommended for new student researchers:

[1] Schleissheimer, Hans-Joachim. “CAN-Bus Basics.” *CanEasy, www.schleissheimer.de/caneasyhelp/index.html*
[2] “Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications,” SAE J1708-2008-10, PA: Society of Automotive Engineers, 1986
[3] “Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications,” SAE J1587-2008-07, PA: Society of Automotive Engineers, 1988
[4] "Recommended Practice for a Serial Control and Communications Vehicle Network," SAE J1939-2009-03, PA: Society of Automotive Engineers, 2004
[5] “Online Cyber Security Training, Free, Forever.” Cybrary, www.cybrary.it/.
[6] Smith, Craig. *The Car Hacker’s Handbook.* No Starch Press, 2016.
[7] Codecademy.com

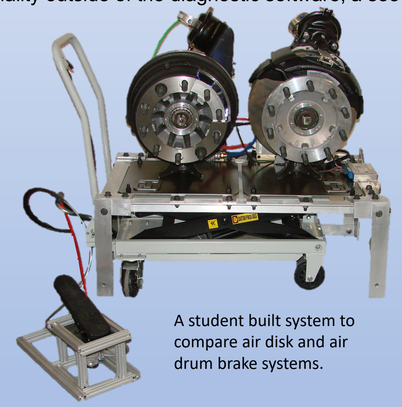
Truck Air Brake Demonstrator

The objective of this project is to illustrate differences between drum brakes and disc brakes and to create the physical system demonstrator to show physical actions from vehicle network commands. Students worked with mechanical hardware, electronics, networking and computer software on this project.

A potential cyber security exploit would require learning how the ABS brake modulator functioned. Student researchers sought to understand the vehicle messages between the Electronic Brake Controller (EBC) and the diagnostic software. To start, the brake controller is put into diagnostic mode so preprogrammed diagnostic tests can be performed. To duplicate this functionality outside of the diagnostic software, a seed-key map was needed to activate these specific tests at will.



A breadboard with CAN and LAN hardware with an Arduino compatible Teensy 3.2 as the microprocessor.



A student built system to compare air disk and air drum brake systems.

CAN to LAN

This project is to send and receive CAN messages across a Local Area Network connected with Ethernet. Students learned about sending messages across multiple networks as they gained knowledge about computer programming across multiple platforms.

Cyber Truck Challenge

The CyberTruck Challenge provided beneficial knowledge to fill knowledge gaps in cyber security. The CyberTruck Challenge was broken into two halves: the first half being classroom style sessions with guided lectures and the second half was time dedicated solely on looking for exploits on the vehicles and hardware at the challenge.
This inaugural event in June of 2017 brought together industry, students, professional cybersecurity researchers, and government to build a network of stakeholders and develop talent.

University of Tulsa students getting deep into learning at the CyberTruck Challenge

Cyber Auto Challenge

The SAE Cyber auto challenge gives students the opportunity to start with the basics of vehicle networks and build up a comfortable foundation for working with vehicle systems as a team.

Professionals from every facet of the vehicle industry are present and looking to expand education in vehicle cyber security. The participants range from high school students to Masters Degree seeking students, most with little to no background in vehicle network systems. The challenge gives them the introduction they would have never had into the industry. By the end of the experience, the participants have the fundamental knowledge to explore further on their own.