SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Student CyberTruck Experience Manual

Jeremy Daily

May 20, 2020

A special thank you goes out to Urban Jonson at the National Motor Freight Traffic Association, Inc. (NMFTA) for being a champion of the program. His passion for cybersecurity and education was insiprational in creating the content and program called the Student CyberTruck Experience. The Executive Director the NMFTA, Paul Levine, deserves special thanks as he provided resources and guidance on bringing the Student CyberTruck Experience to life. Our initial sponsors at the University of Tulsa include the NMFTA, Geotab, and PeopleNet. The continued support from Geotab through Ryan Brander and Glenn Atkinson are gratefully appreciated.

Introduction to the Student CyberTruck Experience

In 2016, Urban Jonson of the National Motor Freight Traffic Association, Inc. () reached out to Dr. Jeremy Daily while he was teaching mechanical engineering at the Univeristy of Tulsa () to disuss some research findings related to heavy vehicle cybersecurity. In this conversation, Dr. Daily confirmed many of the hypotheses in the NNFTA whitepaper on the state of heavy vehicle cybersecurity. This converstation led to an invitation for Dr. Daily to attend the firs NMFTA Heavy Vehicle Cyber Security () meeting in Virginia. One of the results of the meeting was a recognition for the need to build the human talent needed to address the challenges assoicated with cybersecurity of heavy vehicles. This initiative is how the Student CyberTruck Experience came into being.

Learning Outcomes and Program Mission

To develop the talent necessary to improve the cybersecurity posture of the heavy vehicle.

Program Objectives

The Taxonomy of Educational Objectives (Bloom's Taxonomy)

Assessments and Exercises

Formative

Learning

Assessments are formative hands-on exercises where students

Summative

Research

Research is the top of the pyramid.

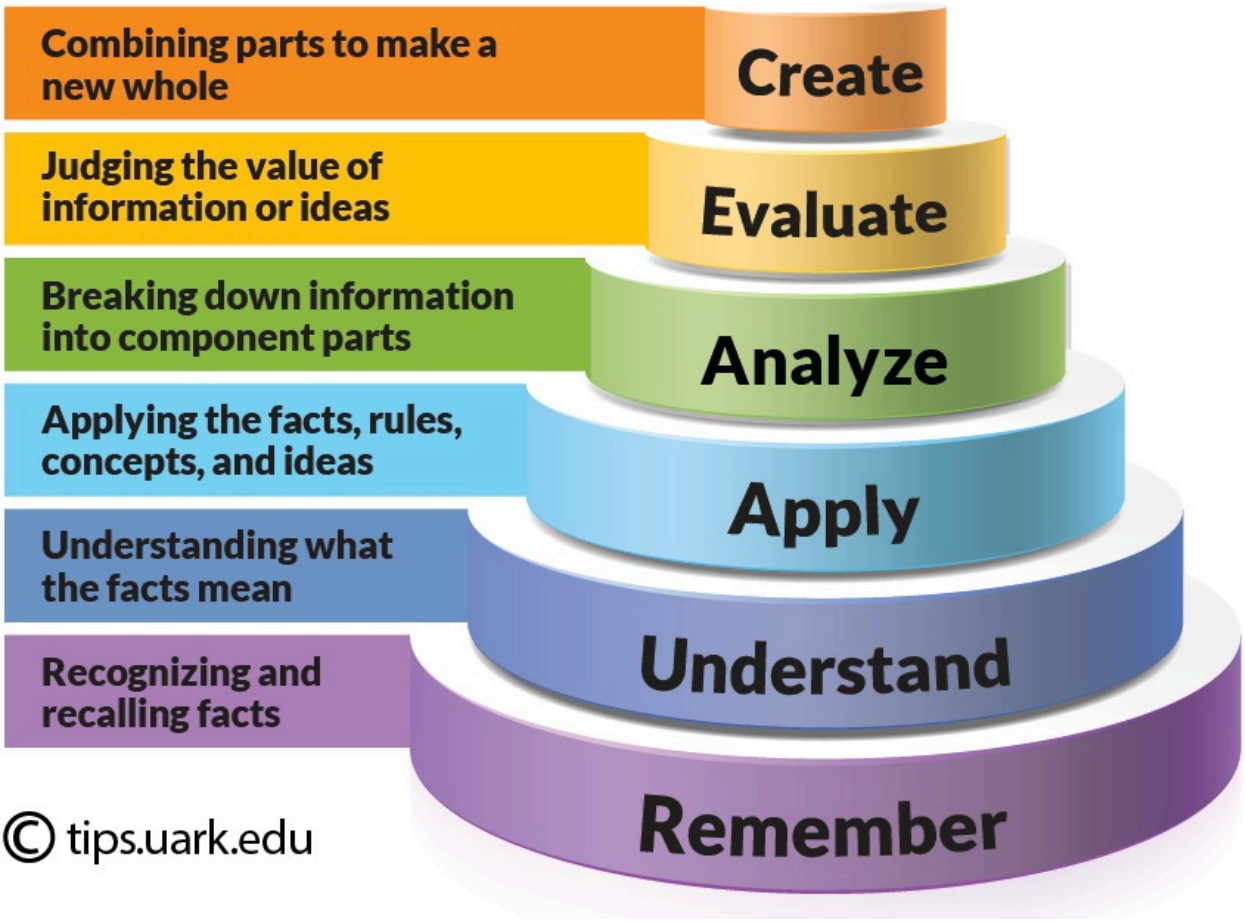

Figure 0.0.1.: Bloom's Taxonomy from Jessica Shabatura.

1. Introduction to Trucking

1.1. Objectives

What is the trucking industry?

What is a truck?

Who makes trucks?

Cybersecurity for Trucking

1.2. Assessments

2. Overview of Heavy Vehicles

Weight Classes

3. Building Hardware

The purpose of this chapter is to give students skills necessary to work with modern electronics and build their own hardware tools.

3.1. Recommended Hardware Kit

Each student should have access to the parts in the basic kit. These items are minimum to successfully accomplish the programming and learning exercises.

3.1.1. Basic Kit

Qty	Label	Description	Supplier	Supplier Part Number
1	A	Teensy 4.0 Development Board	PJRC	TEENSY40_PINS[1]
2	B	MPC2562 CAN Transceiver	Digi-Key	MCP2562FD-E/P-ND[2]
1	C	Solderless Breadboard	Digi-Key	BKGS-830-ND[3]
5	D	120 Ohm Axial Resistors	Digi-Key	
1	E	Wiz850IO Ethernet Expansion Board	Digi-Key	1278-1043-ND[4]
1	F	30 Pack of Male-Male Breadboard Wires	Sparkfun	PRT-14284[5]
1		20 Pack of Male-Female Breadboard Wires	Sparkfun	PRT-12794[6]
1	G	Ethernet Cat6 Cable, 3 ft.	Sparkfun	CAB-08915[7]
1	H	USB micro Cable, 6 inch	Sparkfun	CAB-13244[8]
1	K	ATECC608A Crypto Authentication Module	Digi-Key	ATECC608A-SSHDA-TCT-ND[9]
1	L	ATECC608 Crypto Co-Processor Breakout	Sparkfun	SPX-15838[10]
1	M	Trimpot 10K Ohm with Knob	Sparkfun	COM-09806[11]
1	N	SOIC8 to DIP Converter Board	Sparkfun	BOB-13655[12]
1	P	Break Away Headers - Straight	Sparkfun	PRT-00116[13]
1	Q	Ambient Temperature Sensor	Sparkfun	SEN-14049[14]
1	R	Conductive 18 Compartment Organizer	Flambeau	C618[15]

Table 3.1.1.: Basic Hardware Kit

Newer laptop computers may not have a physical Ethernet port, so a USB to Ethernet adapter may be necessary.

Exercise 3.1. []

3.1.2. Basic Tools

Multimeter Any modern digital multimeter is acceptable to get started. There are many on Amazon that are suitable.

Soldering Iron A

Tweezers

Wire Cutters

Wire Strippers

Carrying_Tote

30gauge Wire

Exercise 3.2. Write a program to send CAN messages from one node to another.

Hints:

1. Check the continuity of each hookup wire before using it. They can be fragile and break easily.

3.2. Advanced Hardware Kits

3.3. Build a Breadboad Arduino

Challenge: using the pieces below, send a CAN message.

[1] https://www.pjrc.com/store/teensy40_pins.html
[2] https://www.digikey.com/product-detail/en/microchip-technology/MCP2562FD-E-P/MCP2562FD-E-P-ND/4842807
[3] https://www.digikey.com/products/en?keywords=BKGS-830-ND
[4] https://www.digikey.com/products/en?keywords=Wiz%20850
[5] https://www.sparkfun.com/products/14284
[6] https://www.sparkfun.com/products/12795
[7] https://www.sparkfun.com/products/8915
[8] https://www.sparkfun.com/products/13244
[9] https://www.digikey.com/products/en?keywords=ATECC608A-SSHDA-TCT-ND
[10] https://www.sparkfun.com/products/15838
[11] https://www.sparkfun.com/products/9806
[12] https://www.sparkfun.com/products/13655
[13] https://www.sparkfun.com/products/116
[14] https://www.sparkfun.com/products/14049
[15] https://www.flambeaucases.com/18-compartment-box-1095.aspx
[16] https://www.pjrc.com/store/teensy41.html
[17] https://www.pjrc.com/store/teensy41.html

Qty	Description	Supplier	Supplier Part Number	URL
1	Teensy 4.1	PJRC	TEENSY41	[16]
1	Beagle Bone Black			
1	Quadrature Encoder with breakout board. Bournes PEC09			

Table 3.2.1.: Advanced Hardware Kit

Qty	Description	Supplier	Supplier Part Number	URL
1	Smart Sensor Simulator 2	DG Technologies	TEENSY41	[17]
1	Beagle Bone Black			
1	Quadrature Encoder with breakout board. Bournes PEC09			

Table 3.2.2.: Vehicle ECU Testing Kit

Materials:

Breadboard Prototyping Wire ATmega328P MCP2551/MCP2562/MCP2558 MCP2515/MCP25625 LED 120ohm (2) or 60 ohm (1) resistor a 16MHz crystal 6 pin straight header a 10k resistor 18-22 pF capacitor (2)

Resources:

Use Datasheets to determine how to connect everything To find datasheets use google, digikey, and mouser Learning how to push code to the arduino: https://www.arduino.cc/en/Tutorial/ArduinoISP For help with SPI communication to MCP2515: http://avrbeginners.net/architecture/spi/spi.html

Challenge:

Send a CAN Message (Verify with oscilloscope) Decode the message from the oscilloscope to ensure that it is the mesage you told your arduino to send This can be done with Python Create an Altium Schematic of the layout that you created

4. Networking Fundamentals

4.1. Problems of Networking

4.1.1. Encoding

4.1.2. Framing

4.1.3. Data Transmission

Link Access

Media Access Control

Collision Avoidance

4.1.4. Flow Control

4.1.5. Routing

switching

4.1.6. Reliable Delivery

4.1.7. Fault Tolerance

error detection

error correction - Hamming Codes

4.2. OSI Layered Model

4.3. Ethernet

4.3.1. TCP/IP

4.3.2. UDP

4.3.3. Automotive Ethernet

4.4. Wireless Protocols

4.4.1. Wifi

Krack

4.4.2. Cellular

4.4.3. Bluetooth

Blueman

Blueborne

4.4.4. Zigbee

4.4.5. Iridium Satelite

4.4.6. Other Communications

4.5. In-vehicle Networking

4.5.1. Contoller Area Networks

4.5.2. J1708 Serial Communications

Figure 4.5.1.: Title

5. Truck Systems for Computer Scientists

6. Computer Programming for Engineers

7. Initial Heavy Vehicle Serial Protocols

8. High speed communication with SAE J1939 and CAN Bus

Exercise 8.1. CAN Frame Decoding

Capture a CAN Frame using an oscilloscpope on a J1939 network and decode it according to SAE J1939.

Exercise 8.2. Read Live Engine RPM Challenge

Using a BeagleBone Black and a Truck Cape, connect to an engine contoller that is broadcasting non-zero engine RPM. Gather this data using candump. Interpret the raw CAN frames and extract information for Engine RPM, or J1939 SPN 190. Plot 20 seconds of changing RPM with matplotlib. Print the properly labeled plot to PDF and show it to your instructor. Objectives

Learn how to interface with Linux SocketCAN and can-utils Be able to look up a signal definition in the J1939 Digital Annex (spreadsheet) Use grep to search for specific strings from a candump Have a reliable CAN datalogger for use in future projects Plot data using matplotlib in Python.

Suggested Materials

This exercise can be run with any Linux device with CAN hardware. An example of a commercial product with these features is the DG Technologies' Beacon device. An example of a hand built project is the BeagleBone Black with a TU TruckCape. Resources

J1939DA Internet Access (you may want to share your PC's connection sharing)

Exercise 8.3. Man in the Middle

Build a man-in-the middle board and box that takes CAN signals into one can channel and sends them out on another. Start a diagnostics session with a PC and RP1210 device to perform maintenance. Create a forwarding system that inspects and forwards network traffic in both directions. Attempt to hijack a a diagnostic session and affect a parameter change started with the PC diagnostics software.

Using DDEC Reports, try to prevent resetting the CPC clock during a data extraction on a CPC.

9. Princples of Cybersecurity

9.1. Introduction to Cryptography

9.2. Message Authentication

9.3. Encryption on CAN

10. Heavy Vehicle Digital Forensics

A. Data Sheet Snippets