Read-Only Bus Access for ELDs and Other Connected Devices

Presented by Hayden Allen
Mechanical Engineering Undergraduate Student
Advisor: Dr. Jeremy Daily
Who Am I?

• Hayden Allen
  • University of Tulsa
  • Mechanical Engineering ’18
    • President of TU Auto Club
  • Automotive Enthusiast
    • Avid Weekend Racer, Weekend Mechanic
    • Currently Building: Miata Kart, 1973 BMW 2002, Duramax ‘52 3100
  • SAE Cyber Auto Challenge Participant
CAN bus

• What is a CAN bus?
  • CAN: Controller Area Network
  • The network that enables most of the electronic control units on the truck to communicate
    • Electronic Brake Controller
    • Engine Control Module
    • Instrument Cluster
    • Body Control Module
How does it work?

• In Heavy Trucks, CAN follows the J1939 Standard
  • Messages Have both ID and Data Field
  • Information is passed along the network from node to node
So what is connected?

- Engine Control Unit
- Diagnostic Connection
- Electronic Brake Controller
What else?
CAN Bus Downfall

- No authentication
- No permissions
- If you can connect, you can read and send messages
Wait, What Are Permissions?

- Tells the user what they are allowed to do within a file
  - Usually Read, Write, Execute
- What are some examples of these?
What is read only access?
Lorem Ipsum

"Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit..."

"There is no one who loves pain itself, who seeks after it and wants to have it, simply because it is pain..."


Lorem Ipsum

"Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit..."

"There is no one who loves pain itself, who seeks after it and wants to have it, simply because it is pain..."

What are permissions good for?

•Sharing Important Documents
•You do not want people to make changes to the documents you send them
•Dictates how the end user uses the shared file
•So what are the permissions in CAN?
<table>
<thead>
<tr>
<th>Actual Bus</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
</tr>
</thead>
</table>

**ELD**
<table>
<thead>
<tr>
<th>Actual Bus</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELD</td>
<td>Actual Bus</td>
<td>Ideal Bus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RW</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actual Bus</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>Ideal Bus</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>?</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>
What could go wrong?
What if you release a patch?
What Else Is Vulnerable?

• Electronic Logging Devices
  • Insurance Data Loggers
How?

• One simple web search tells you step by step what to do!
### Read-Only Bus Access for ELDs

<table>
<thead>
<tr>
<th>Actual Bus</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
<th>RW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ideal Bus</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

2/1/2018
CAN Bus

ECU

OBD

EBC

Radio

ELD

120 ohms

120 ohms
CAN Bus

Let’s look at this section

- ECU
- OBD
- EBC
- Radio
- ELD
How Do You Achieve Read Only?

- In order to achieve read only
  - Must allow messages in (READ) but not allow messages out (WRITE)
  - Must maintain functionality of the downstream device
Achieving Read Only

- Must have an additional device in place
  - Must be done through hardware
    - Software is vulnerable to attack and can be changed to allow for new functionality
    - Remember Miller and Valasek? Progressive?
Data Diode

Establishing a more secure CAN bus
What is a Data Diode?

• Removes full bus write access
  • Accomplished by wiring TX and RX pins together on two separate CAN transceivers
  • This removes full write ability

• Maintains functionality of downstream devices
  • The data diode contains an extra controller and transceiver to acknowledge the downstream unit
  • This maintains full functionality of the downstream (ELD)
Schematics and Prototype

Silent Low = Transmit Enable

CAN Transceivers as Data Diode
Assembly
Assembling the Backshell
PROOF of Concept
Testing Setup

- In order to test the data diode, two branches were created.
  - Unprotected (J1939) – Directly connected to a truck or test bed through the Deutsch 9-pin
  - Protected (ELD) – Connected to diagnostic but is protected by the Data Diode
Direct Diagnostic Connection

Plug into the OEM Diagnostic Connection

Data Diode

To Vehicle Spy 3 (unprotected)

To Oscilloscope (unprotected)

To Oscilloscope (protected) Downstream protected connection

To Vehicle Spy 3 (protected)
Adruino Teensy Tone Ring Frequency Generator

- Created to be able to display vehicle speed on a live bus
  - Offers a physical display of bus functionality
- A Teensy 3.2 Arduino that is emitting a frequency into the tone ring input on the test Cummins ECM
- A potentiometer is used to change the output frequency
Denial-of-Service

• DOS attack
  • Works by sending the inherent highest priority message
    • ID = 0x00;
  • Simple attack to execute
  • When implemented, all bus communication ceases
    • Visually evident by gauge cluster no longer displaying the speed from the tone ring frequency generator

```c
#include <FlexCAN.h>
#include <kinetis_flexcan.h>

FlexCAN J1939bus(250000);
static CAN_message_t txmsg,txmsg;

void setup()
{
    J1939bus.begin();
    txmsg.id = 0x00000000;
    txmsg.len = 0;
    txmsg.ext = 1;
    txmsg.buf[0] = 0x00;
    txmsg.buf[1] = 0x00;
    txmsg.buf[2] = 0x00;
    txmsg.buf[3] = 0x00;
    txmsg.buf[4] = 0x00;
    txmsg.buf[5] = 0x00;
    txmsg.buf[6] = 0x00;
    txmsg.buf[7] = 0x00;
}

void loop()
{
    J1939bus.write(txmsg);
}
```
DOS at Diagnostic Port Video

• Placeholder

2/1/2018

Read-Only Bus Access for ELDs

42

Diode Bus

J1939 Bus
Read-Only Bus Access for ELDs

J1939 Bus

Diode Bus
Potential Implementations

- Direct In-Line Connection
  - As displayed in testing
- Dsub 15 Connection
- Delphi 14 pin Connection
- J1962 OBD-II Connection
Data Diodes w/ Requests
Some Requests Handled by Other Nodes

• However, with the Data Diode, an ELD will be unable to request any additional information
  • For Example:
    • VIN Number
    • Engine Hours

• The ELD is not the only node that may need to know this information
  • For example, an instrument cluster may request Engine Hours from the ECM
Requesting Enabled Diodes

• A potential solution:
  • Implementing a requestor that sends out timely request messages
  • Operates parallel to the ELD
  • Connected to J1939 network
  • Not directly connected to the ELD network
  • Would send out request messages so that the responses are logged by the ELD

• Design is done, but boards have to be built.
Why Is This Important?
2015 ELD Mandate

• Mandates that all trucks 2000 or newer will be required to have an Electronic Logging Device installed on all trucks.

• Why?
  • Taken from the first sentence within the mandate:
    “This rule improves commercial motor vehicle (CMV) safety and reduces the overall paperwork burden for both motor carriers and drivers by increasing the use of ELDs within the motor carrier industry” – FMSCA 2015
Downfalls of the Mandate

- Mandate adds additional attack vectors to Heavy Vehicles
  - Attack Vector: A path or means by which a hacker (or cracker) can gain access to a network.
How are they doing this?

- Adding Internet Connectivity
- Adding Bluetooth and USB 2.0

In consideration of the comments, FMCSA revised the data transfer options, by establishing two options for electronic data transfer (option one is a telematics-type ELD with a minimum capability of electronically transferring data via wireless Web service, and email; option two is a “local connectivity” type ELD with a minimum capability of electronically transferring data via USB 2.0 and Bluetooth). Additionally, both types of ELDs must be capable of displaying a
How Much Does It Cost?
Adding an ELD

- The FMSCA projects that adding a web supported ELD will cost $419 annually, with an initial purchase price of $500/unit.
- USB 2.0 or Bluetooth ELDs will cost $166 annually.
- How much would adding a diode cost?
Data Diode Prototyping Costs

- Amphenol/Deutsch 9-pin Connector: $9.22
- 4 Deutsch PCB pins: $8.00
- M/F J1939 Type II Pigtail Cable: $11.84
- CAN Data Diode Assembled Printed Circuit Board: $72.49
- Backshell and Compression Nut: $7.05
- 0.25 Hours Assembly: $5.00
- Total: $113.60
Understanding the Current Design

• Cost would drop if production scales.
• Over the Air Updates are incompatible
  • No write access prevents the telematics device from being able to write to the bus.
• If data needs requested (i.e. VIN), a separate node must do the job.
• Patent Pending
  • University of Tulsa filed for a utility patent
Acknowledgements

This material is based upon work supported by National Motor Freight Traffic Association, Inc (NMFTA), PeopleNet, and Geotab. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of NMFTA, PeopleNet, and Geotab.
Questions?

Name: Hayden Allen
Email: hayden-allen@utulsa.edu
Phone: (918) 645-4938
Requesting CAN Controller and Transceiver

Protected CAN Controller and Transceiver

External Connections

CAN Transceivers as Data Diode

Power Input, Protection, and Regulation

Only Bus Access for ELDs

Notes according to TMC’s RP1226 for 14 Way Apen 2.8 Apen Signal Color Part Pin
1 SW-BATT PINK 5
2 CAN_1_R YEL 3
3 IGN ORN 6
4 GND BLK 1
5 CAN_1_L GRN 2
6 BATD RED 4

Use Delphi Part Number 54304136 (14-way male connector) for the CAN_IN Male Unused terminals are Delphi/FCA Part 1075277

Use Delphi Part Number 54304142 (14-way female connector) for the CAN_OUT Female Unused terminals are Delphi/FCA Part 10753090

Output CAN Filter and Termination

2/1/2018