



Heavy Vehicle Cybersecurity Update

National Motor Freight Traffic
Association, Inc.



National Motor Freight Traffic Association, Inc. (NMFTA)

- Industry non-profit representing more than 600 companies operating in interstate, intrastate, and foreign commerce in both US and Canada representing over \$100 billion in freight revenue
- Our members operate close to 200,000 trucks on the road
- National Motor Freight Classification (NMFC)
- Standard Carrier Alpha Code (SCAC)
- Standard Point Location Code (SPLC)
- Other activities to the benefit of the transportation industry



NMFTA Heavy Vehicle Portfolio Survey 2017

- Of the 3.6 million class 7 and 8 vehicles in operation manufactured in or after the year 2000, 25% are from the years 2005-2007, and 34% are from the years 2012-2016. The popularity of vehicles from these model years makes them a high priority for cybersecurity research, potentially including analysis of common ECUs shared across OEMs
- This means **59% of all vehicles come from 7 model years**. Model year is noteworthy from a cybersecurity perspective because vehicles across brands manufactured during the same manufacturing cycle often share electronic components manufactured by the same supplier, or new industry standard technologies, such as wireless connectivity, which increase the cybersecurity risk regardless of manufacturer
- Our studies indicate that there may be as much as **60% commonality** in CAN network traffic between OEMs due to J1939 interoperability



Issues which present a unique risk profile

- J1939 Standard (interoperability)
- Supply chain risk
- Homogenous configurations
- 3rd Party Products (Diagnostic Port)
- Incident Response Plans
- Communication



The problem is

- Complex
- Distributed
- Extremely large in scale
- No single “fix”
- High probability
- High impact



Risk Identification, Mitigation and Reduction

- OEM and 3rd party industry awareness
- Fleet operator best practices
- Incident response plans
- Human resource development
- Joint open technology research and development
- Better tools and techniques



Heavy Vehicle Cyber Security (HVCS) Program

“Bringing together private industry, government, trade associations, and academia to work on the transportation cyber security problem on a shortened time table”



NMFTA HVCS Activities

- Sponsoring ongoing industry workshops
- Sponsoring industry research
- Student research programs
- Scholarship program
- NMFTA & DOT Volpe collaboration
 - Research
 - Information dissemination
 - Overlapping DOT/Volpe support for DHS
- An other industry activities



- **Industry Awareness Bulletin**
 - Available at www.nmfta.org website
- **DOT/Volpe Project - US fleet composition**
 - Determine transportation risk profile
 - Identify vulnerability/risk clusters
- **Project to collect CAN Data**
 - Statistical analysis
 - Development of better inline security

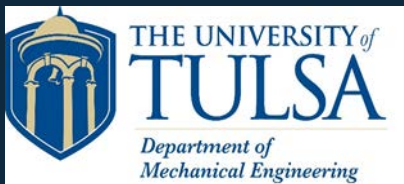
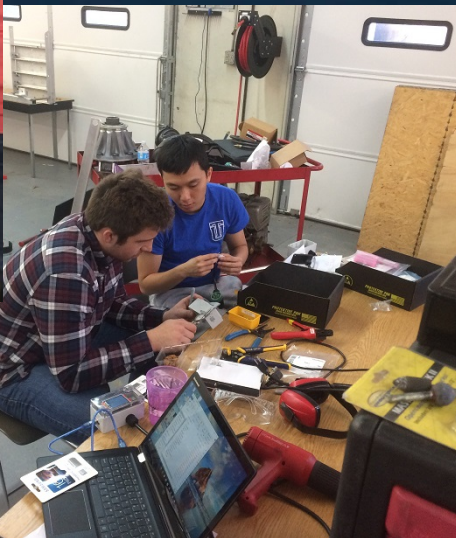
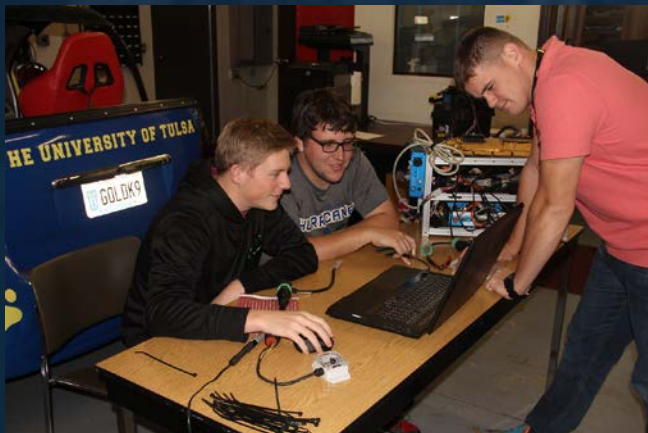


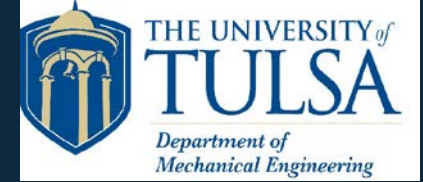
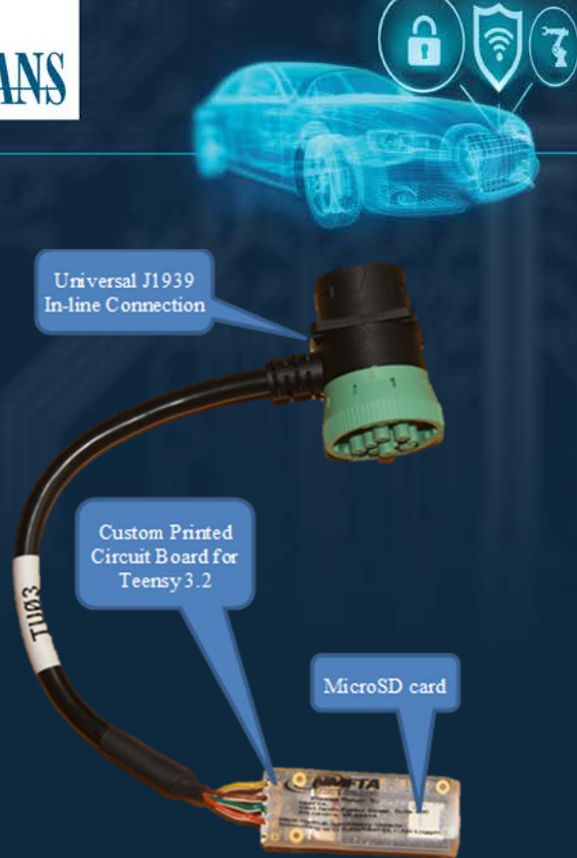
Automotive ISAC

- Washington, DC, January 25, 2017 – The Automotive Information Sharing and Analysis Center (AutoISAC) today announced the inclusion of the commercial vehicle segment in its membership.
- Auto-ISAC was formed by light-duty vehicle OEMs in late 2015, and extended membership to light-duty vehicle suppliers in early 2016. Building upon the success of this collaboration, the beginning of 2017 marks another valuable expansion — the inclusion of the commercial vehicle segment, including heavy-duty vehicle OEMs, their tier 1 suppliers, telematics providers, and freight carriers.



University of Tulsa Student Research Experience Program





A 32 GB SD card could hold about 189 hours or just under 8 days' worth of 100% bus load data. Since a truck is not always on and is not at 100% busload, it is likely a truck could go for 2 weeks with a 32GB card

<https://github.com/heavy-Vehicle-Networking-at-U-Tulsa/NMFTA-CAN-Logger>



CAN Data Collection Project

- Complete bus data collection from diagnostic port via motor freight carrier members of NMFTA and other researchers
- Not sample data but complete data sets from normal commercial operations
- Examples include short runs, deliveries, long haul as well as attack data
- 3rd party analysis environment for research and product development

$$P(A) = \frac{F(A)}{T} \quad \text{and} \quad P(B) = \frac{F(B)}{T}$$

also

$$P(A|B) = \frac{F(A|B)}{F(B)} \quad \text{and} \quad P(B|A) = \frac{F(B|A)}{F(A)}$$

Now

$$F(A|B) = F(B|A)$$

Hence

$$\begin{aligned} P(A|B) P(B) &= \frac{F(A|B)}{F(B)} \frac{F(B)}{T} \\ &= \frac{F(B|A)}{T} \\ &= \frac{F(B|A)}{F(A)} \frac{F(A)}{T} = P(B|A) P(A) \end{aligned}$$

That is

$$P(A|B) P(B) = P(B|A) P(A)$$



Next Steps

- Keep working the issue from all possible angles
- Improve coordination and communication
- Process for coordinated responsible disclosure
- Work on common “language” to discuss cyber security
- Continue to work with Automotive ISAC & SAE
- Improve stakeholder awareness



Get involved...

- Develop an incident response plan
- Start a cyber security program in your organization
- Work with and support your industry associations
 - SAE, MEMA, NMFTA, ATA, IEEE, NIST, etc.
- Support ongoing research and development
- Join the Automotive ISAC



The Clarence “Kelly” Johnson Challenge – What can we do in the next 6 and 12 months to improve heavy vehicle cyber security?



DARPA ... “borrow” stuff from the smart kids

- High-Assurance Cyber Military Systems (HACMS)
 - Dr. Ray Richards – Program Manager
 - Secure Micro Kernel (seL4)
 - Programming Tools & Techniques (Ivory)
- Cyber Grand Challenge (CGC)
 - Mr. Mike Walker – Program Manager
 - Autonomous Network Defense
 - Fuzz the ***** out of it!



<https://hvcslistservice.nmfta.org>

- Updates on heavy vehicle cyber security
 - Updates on NMFTA HVCS meetings
- Access to previously distributed documents
 - Hosted and supported by NMFTA
- Official Use Only – NMFTA Approval Required To Join



Questions?



Thank You

Urban Jonson
Chief Technology Officer
National Motor Freight Traffic Association, Inc.
www.nmfta.org

Urban.Jonson@nmfta.org

