CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

SAE Government Industry Meeting

January 24-26, 2018

DRAFT Version 1.0

NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Project Sponsor: **NHTSA**
Contractor: **University of Michigan Transportation Research Institute (UMTRI)**

DRAFT

- **What it is….**
  - Research MD/HD commercial vehicle landscape for cybersecurity items of interest/concern
  - Get a pulse on N.A. commercial vehicle industry (CMV) for organizational awareness of cybersecurity topics w/r/t product development process
  - Use light vehicle market (LD) insight as a foundation for MD/HD cyber research
  - Report findings to NHTSA
- **What it's not….**
  - Not intended to market, promote, rank, or discredit cybersecurity solutions, products, or network architectures for MD/HD industry
  - Not intended to address cybersecurity solutions for asset theft

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Introduction

- Research provides NHTSA with information regarding cybersecurity aspects currently related to the state of MD/HD commercial vehicle industry.

- Research highlights the vulnerable aspects of MD/HD security landscape and used as guidance to NHTSA for industry next steps.

- Develop framework to understand common/different features between passenger (LD) and MD/HD vehicle cybersecurity attributes:
  - Threat vector landscape, network architectures, risk assessment, lifecyle, control applications, countermeasures, etc.

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Introduction

- *Over past 5 years*, ethical whitehat hackers demonstrated to the public that modern passenger vehicles (LD) utilizing real-time ECUs w/private CAN architectures (Controller Area Network) do have cybersecurity vulnerabilities to a variety of exploits (attacks) - demonstrated negative impacts to safety/ convenience.

- Similarly, MD/HD commercial motor vehicles also utilize real-time ECUs w/communication network(s); primarily open-source CAN-based J1939, J1708, & private CAN networks providing both similar and unique functions relative to passenger vehicles.

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Research Examination

- Since MD/ HD vehicles share many similar functions & communiction attributes - leads one to the following questions:
  - Are MD/HD vehicles susceptible to cybersecurity attacks like passenger vehicles?
  - To what levels are they susceptible?
  - What is the MD/HD vehicle threat-surface landscape? (relative to LD)
  - Can an exploitation by an attacker lead to unintended vehicle kinematics (control) in the MD/HD domain?

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Research Strategy

- Design an investigative Framework to compare MD/HD commercial vehicle cybersecurity (CMV) landscape to passenger LD cybersecurity.
- Utlilize interested industry experts & stakeholders for data gathering.
- Framework consists of a list of technical areas to consider.
- Framework will provide a methodology to execute and investigate these areas.
- Identify threat landscape and fundamental risk assessment.
- Provide a final single comprehensive report to NHTSA ~ convey findings

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Project Tasks - Overview

- Task 1: Project Management
- Task 2: Develop a Comparison Framework
- Task 3: Compile a Body of Findings
- Task 4: Investigate Impacts
- Task 5: Study Demonstrated Cases of Hacking & Risk Assessment
- Task 6: Review Cybersecurity Section of NHTSA's RFC (NHTSA-2014-0108)
- Task 7: Study Cybersecurity Practices used by Heavy Duty Vehicle Segment
- Task 8: Final Report

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework

- Data Gathering Methodology – N.A. Market
  - Stakeholder Interviews:
    - How: Internal/ external MD/HD industry SME's ~ confidential
    - Who: Commercial vehicle OEMs, Tier-1 suppliers, associations, academia, industry consultants ~ total = 17 phone interviews.
  - Literature Reviews
    - Automotive cyber articles ~ numerous from 2010 - 2016
    - Heavy vehicle cyber articles ~ very few !!
  - Attend Workshops/Conf.
    - SAE ComVec, SAE Govt./Industry, NMFTA meetings, etc.

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework

- Data Gathering Methodology

Stakeholder Interviews - Caveat

Understandably, due to the protective nature of competitive organizations, interviews elicited limited information in the sense that it required stakeholders to provide very sensitive information concerning the research and development practices and policies as well as organizational commitment to the growing threat of vehicle security

KEEP????

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework

- Content Areas:
  - **Truck Classification:** LD/MD/HD
  - **Communication Networks:** SAE J1939/J1708 vs. CAN (ISO – 11898)
  - **Electronics Architecture/Topology:** MD/HD vs. LD
  - **Fleet Management:** OEM products & Integration with 3rd party electronics
  - **Private/commercial Sector:** Private vs. commercial aspects
  - **Customer Demands:** Electronics complexity
  - **Life Cycle:** MD/HD vs. LD
  - **Vehicle Development Process:** Security design in MD/HD vs. LD
  - **Supply Chain:** MD/HD customer requirements vs. LD
  - **Legal Limitations:** Do laws change threat vulnerabilities /types?
  - **Compliance:** Design requirements /impacts?
  - **National differences:** MD/HD vehicles vs. LD
  - **Organizational Structure:** Are MD/HD OEMs as prepared vs. LD?

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Comparison Framework

Content Areas	Light Vehicles		Heavy Vehicles	
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks
Communication Bus	Proprietary CAN FlexRay, ENet	Proprietary CAN	J1708, J1939, ENet, PLC, & Proprietary CAN	
Electronics Architecture Topology	Multi-CAN w/ Central Gateway		Multi-Flat CAN	
Communication Interfaces	Wired (diagnostics, USB, CD, etc.) and Wireless (Bluetooth, cellular, TPMS, OBD connector dongles, DSRC, etc.)			
Privacy	Protect personal data	Protect personal and/or business relevant data	Protect business relevant data	
Fleet Management	• Rental/company fleets • OBD-II dongles	• Rental/company fleets • OBD-II dongles • Logistics management • Remote health and tracking	• Logistics management • Driver “event” monitoring • Remote health and tracking • Electronic Logging Devices (ELD)	
Private vs. Commercial Sector	Private or Commercial		Commercial	
Customer demands	• Cost sensitive • Feature/Content driven • Multipurpose use-case		Cost driven Functional Demands	
Interoperability	No need		Interoperability between components (e.g. chassis from OEM, engine and transmission freely selected) and between tractor and trailer (to use same trailer with many tractors)	
Life cycle and Maintenance	10 years, 150,000 miles		10-20 years, 1.2 million miles	
Organizational structure	Dedicated cybersecurity groups (or individuals) are currently functioning with a preliminary scope defined for addressing current and future architectures		Wide spectrum of awareness (from little to organized) regarding cybersecurity aspects. Most companies appear to be “starting” to organize on this topic	
Development process	OEMs and suppliers target cybersecurity process, many OEMs and suppliers produce all vehicle categories			

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Comparison Framework (cont'd)

Content Areas	Light Vehicles		Heavy Vehicles	
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks
Legal limitations and organized compliance	• Automotive Information Sharing and Analysis Center [Auto -ISAC] is available • Future update to the Moving Ahead for Progress in the 21st Century Act (MAP-21) section 31402 to include cybersecurity aspects or spinoff regulation? • No mandated telematics/logging devices required: except on General Services Admin. (GSA) fleets		• Heavy Duty vehicle is now part of Auto-ISAC • Driver hours of service (HOS) are required to be monitored by federally mandated Electronic Logging Device (ELD) • Telematics/logging devices are required on GSA fleets	
National differences/ similarities	• U.S., European, Asian OEMs are members of the Alliance of Automobile Manufacturers • U.S. European, Asian OEMs, Tier-1 suppliers are members of AutoSAR • U.S. cyber security guidelines in progress: SAE J3061 • ISO collaborating with SAE to develop J3061 guidelines • European automotive cyber expert group (CaRSEC) in progress: European Union Agency for Network and Information Security (ENISA) • European E-Safety Vehicle Intrusion Protected Applications (EVITA) guidelines • Japan Information-Technology Promotion Agency (IPA) guidelines		• No heavy vehicle cybersecurity guidelines to date, potentially leverage SAE J3061 for heavy vehicle specific applications • U.S., European, and Asian OEMs utilize J1939 protocol • U.S. only: Implementation of federally mandated Electronic Logging Devices (ELD) • European: Many OEMs organized implementation of Fleet Management System (FMS) specifically defined message set for 3rd party telematics integrators	
Future applications	Advanced Driver Assist Systems (ADAS) and semi-autonomous systems. Eventual introduction of full autonomous systems.			

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework (example)

Communication Bus Types:

- **LD Passenger Vehicles:** Controller Area Network (CAN) bus(s) based on ISO 11898 physical layer standard. Utilizes OEM specific, "proprietary" message sets/ databases. Multiple/ isolated CAN bus segments.

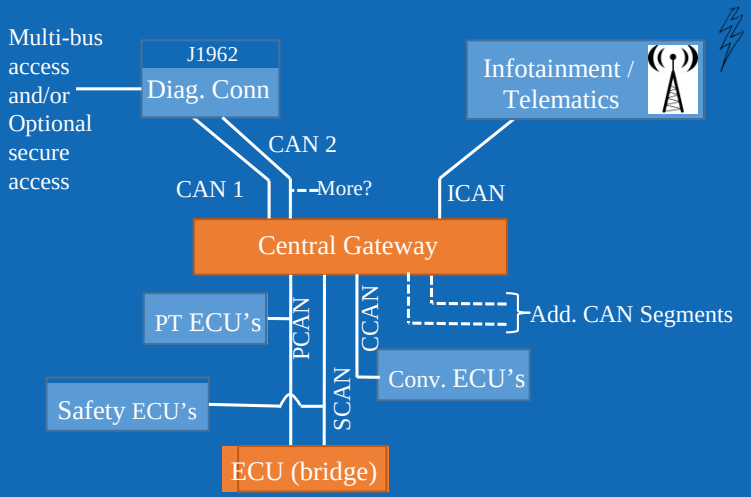
- **MD/HD Vehicles:** SAE J1939 utilizes same CAN physical lower layer interface, *BUT* incorporates a "published" open standards message set to allow for vehicle build flexibility/interoperability between suppliers (i.e. offers "plug and play" capability). Multiple/isolated J1939 bus segments. Continued use of legacy SAE J1708 protocol. Use of proprietary CAN buses.

Is open standard J1939 protocol more attractive to attackers?

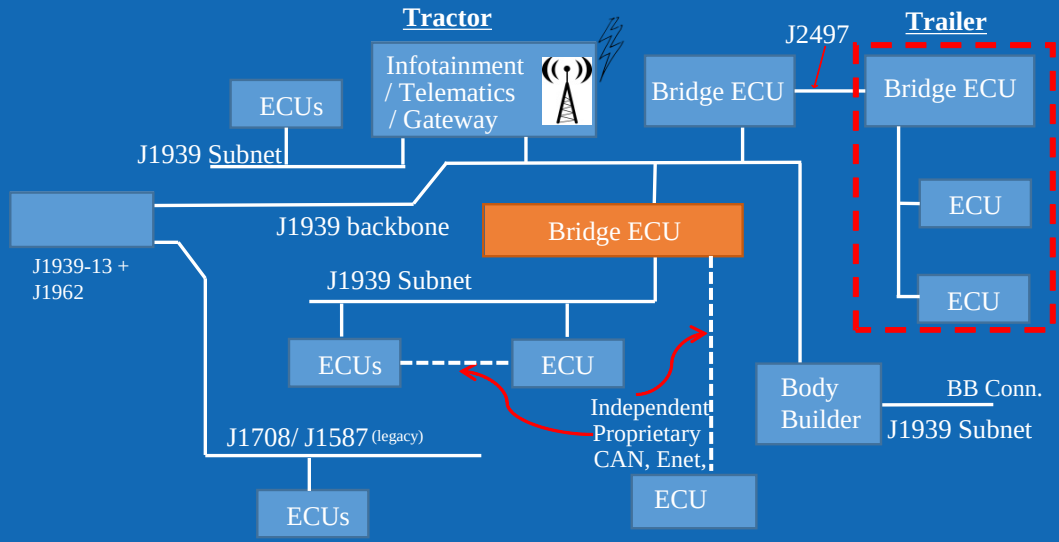
CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework (example)

Simplified LD Architecture



Simplified HD Architecture



NHTSA

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Develop Comparison Framework (example)

Communication Interfaces: Potential Threat Vectors on LD and MD/HD
Many commonalities and some differences…..

- **Wired:**
  - Diagnostic connectors (OBD J1962 and J1939-13), PLC, USB, CD/DVD, SD cards, vehicle charging ports, Aux input, Body Builder Conn.
- **Wireless (RF-based short range):**
  - FOB (keyless entry), Tire pressure monitors, Bluetooth, Wi-Fi, DSRC, RFID keys
- **Wireless (RF-based long range):**
  - Cellular (GSM/CDMA) & SAT. Telematics, GPS, Satellite radio, Digital radio

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Compile a Body of Findings

- Threat Vector Framework

	Light Vehicles		Heavy Vehicles		Research[3]		
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks	Attack Vector Translate to MD/HD (Y/N)?	Mitigation Translate to MD/HD (F/P/N)?	Research Gap? (Incremental/Unique/No)
Communication Bus	Proprietary CAN		J1708/J1587, J1939, & Proprietary CAN				
Electronics Architecture Topology	Multi-Flat CAN/ Central Gateway		Multi-Flat CAN				
Vehicle Threat Surfaces[4]							
Potential Threat Vector: Wired							
o Diagnostic connector	(J1962 – 16pin)		(J1962 – 16pin), (J1939/13– 9pin)		Y	F	N
▪ Network access	CAN – various HS/MS/LS channels		J1939, J1708/J1587		Y	P	I
▪ OBD dongles(aftermarket)	J1962 form factor		J1939 form factor		Y	P	I
▪ Diagnostic Standards	ISO 14229 (UDS) ISO 14230 (KWP)		J1939/73 ISO 14229 (UDS) Proprietary		Y	P	I
▪ Diagnostic Tools	Defined per OEM		Defined per OEM		Y	F	N
o USB	Available		Available		Y	F	N
o Compact Disc (CD)	Available		Available		Y	F	N
o Secure Digital Cards (SD)	Available		Available		Y	F	N
o Auxiliary input (radio Aux)	Available		Available		Y	F	N
o 12Volt Accessory Outlet	Available		Available		Y	-	U
o Body Builder Interface[5]	Not Available		Available		N	-	U
o Trailer PLC (bridge module) [5]	Not Available		Available		N	-	U
Potential Threat Vector: Wireless (Short Range <1km)							
o BlueTooth	Available		Available		Y	F	N
o Tire Pressure Monitor(direct)	Available		Available		Y	F	N
o Remote Keyless Entry(FOB)	Available		Available		Y	F	N
o Wi-Fi	Available		Available		Y	F	N
o RFID Keys	Available		Not Available		N	-	U
o DSRC (V2X)	Development phase		Development phase		Y	F	N

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Compile a Body of Findings

- Threat Vector Framework (cont'd)

	Light Vehicles		Heavy Vehicles		Research[3]		
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks	Attack Vector Translate to MD/HD?	Mitigation Translate to MD/HD?	Research Gap? Incremental/Unique
Potential Threat Vector: Wireless (Long Range >1km)							
o GSM/CDMA(telematics)	Available		Available		Y	F	N
o GPS(telematics)	Available		Available		Y	F	N
o Satellite Radio	Available		Available		Y	F	N
o Digital Radio (HD Radio)	Available		Available		Y	F	N
o Electronic Logging Device	Not Available		Available		N	-	U
Protocol Vulnerabilities on Select Vehicle Kinematics							
Unintended Vehicle Dynamics on Cyber-physical Systems	CAN Bus utilized		J1939 Bus utilized				
o Steering (Lateral)	Control		Control or Status??		N	-	U
o Braking (Longitudinal)	Control		Control or Status??		Y	N	U
o PowerTrain (Lat./Long.)	Control		Control or Status??		Y	N	U
Available Threat Countermeasures							
Mitigation Methods							
o Secure Architectures	In Process		In Process		Y	P	I
o Security Applications	In Process		In Process		Y	N	U
o Secure Development Process	In Process		In Process		Y	P	I
o Secure Development Tools	Available		Available		Y	F	N
o Security Hardware	Available		In Process		Y	F	N
o Sanity Checks	Available		Available		Y	P	I

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Compile a Body of Findings

- Threat Vector Framework

Research ??

	Light Vehicles		Heavy Vehicles		Research[3]		
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks	Attack Vector Translate to MD/HD (Y/N)?	Mitigation Translate to MD/HD (F/P/N)?	Research Gap? (Incremental/Unique/No)
Communication Bus	Proprietary CAN		J1708/J1587, J1939, & Proprietary CAN				
Electronics Architecture Topology	Multi-Flat CAN/ Central Gateway		Multi-Flat CAN				
Vehicle Threat Surfaces[4]							
Potential Threat Vector: Wired							
o Diagnostic connector	(J1962 – 16pin)		(J1962 – 16pin), (J1939/13– 9pin)		Y	F	N
▪ Network access	CAN – various HS/MS/LS channels		J1939, J1708/J1587		Y	P	I
▪ OBD dongles(aftermarket)	J1962 form factor		J1939 form factor		Y	P	I
▪ Diagnostic Standards	ISO 14229 (UDS) ISO 14230 (KWP)		J1939-73 ISO 14229 (UDS) Proprietary		Y	P	I
▪ Diagnostic Tools	Defined per OEM		Defined per OEM		Y	F	N
o USB	Available		Available		Y	F	N
o Compact Disc (CD)	Available		Available		Y	F	N
o Secure Digital Cards (SD)	Available		Available		Y	F	N
o Auxiliary input (radio Aux)	Available		Available		Y	F	N
o 12Volt Accessory Outlet	Available		Available		Y	-	U
o Body Builder Interface[5]	Not Available		Available		N	-	U
o Trailer PLC (Bridge module) [5]	Not Available		Available		N	-	U
Potential Threat Vector: Wireless (Short Range <1km)							
o BlueTooth	Available		Available		Y	F	N
o Tire Pressure Monitor(direct)	Available		Available		Y	F	N
o Remote Keyless Entry(FOB)	Available		Available		Y	F	N
o Wi-Fi	Available		Available		Y	F	N
o RFID Keys	Available		Not Available		N	-	U
o DSRC (V2X)	Development phase		Development phase		Y	F	N

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Gap definitions created to categorize "uniqueness" of threat vectors between passenger and heavy vehicle domains

Translation Conditions

Proposed Gap-Types

	Attack Vector Translates to HD/MD?	Mitigation Translates to HD/MD?	Research Gap	Description
1	Y	(F) Full	(N) No perceivable gap	The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger vehicle domain directly or nearly directly (i.e., fully) translate to the heavy vehicle domain. No unique strategy should be necessary.
2	Y	(P) Partial	(I) Incremental gap	The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger domain require some non-fundamental (i.e., incremental) modification for translation to the heavy vehicle domain.
3	Y	(N) No	(U) Unique gap	The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger vehicle domain either do not apply or require some fundamental (i.e., unique) modification for translation to the heavy vehicle domain. Unique strategies should be developed for heavy vehicles.
4	N	-	(U) Unique gap	An attack vector in heavy vehicles has no analogue in passenger vehicles (or vice versa). Unique strategies must be developed for heavy vehicles.

	Light Vehicles		Heavy Vehicles		Research[3]		
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks	Attack Vector Translate to MD/HD (Y/N)?	Mitigation Translate to MD/HD (F/P/N)?	Research Gap? (Incremental/Unique/No)
Communication Bus	Proprietary CAN		J1708/J1587, J1939, & Proprietary CAN				
Electronics Architecture Topology	Multi-Flat CAN/ Central Gateway		Multi-Flat CAN				
Vehicle Threat Surfaces[4]							
Potential Threat Vector: Wired							
o Diagnostic connector	(J1962 – 16pin)		(J1962 – 16pin) (J1939/13– 9pin)		Y	F	N
▪ Network access	CAN – various HS/MS/LS channels		J1939, J1708/J1587		Y	P	I
▪ OBD dongles(aftermarket)	J1962 form factor		J1939 form factor		Y	P	I
▪ Diagnostic Standards	ISO 14229 (UDS) ISO 14230 (KWP)		J1939/73 ISO 14229 (UDS) Proprietary		Y	P	I
▪ Diagnostic Tools	Defined per OEM		Defined per OEM		Y	F	N
o USB	Available		Available		Y	F	N
o Compact Disc (CD)	Available		Available		Y	F	N
o Secure Digital Cards (SD)	Available		Available		Y	F	N
o Auxiliary input (radio Aux)	Available		Available		Y	F	N
o 12Volt Accessory Outlet	Available		Available		Y	-	U
o Body Builder Interface[5]	Not Available		Available		N	-	U
o Trailer PLC (bridge module)[5]	Not Available		Available		N	-	U
Potential Threat Vector: Wireless (Short Range <1km)							
o BlueTooth	Available		Available		Y	F	N
o Tire Pressure Monitor(direct)	Available		Available		Y	F	N
o Remote Keyless Entry(FOB)	Available		Available		Y	F	N
o Wi-Fi	Available		Available		Y	F	N
o RFID Keys	Available		Not Available		N	-	U
o DSRC (V2X)	Development phase		Development phase		Y	F	N

NHTSA

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts

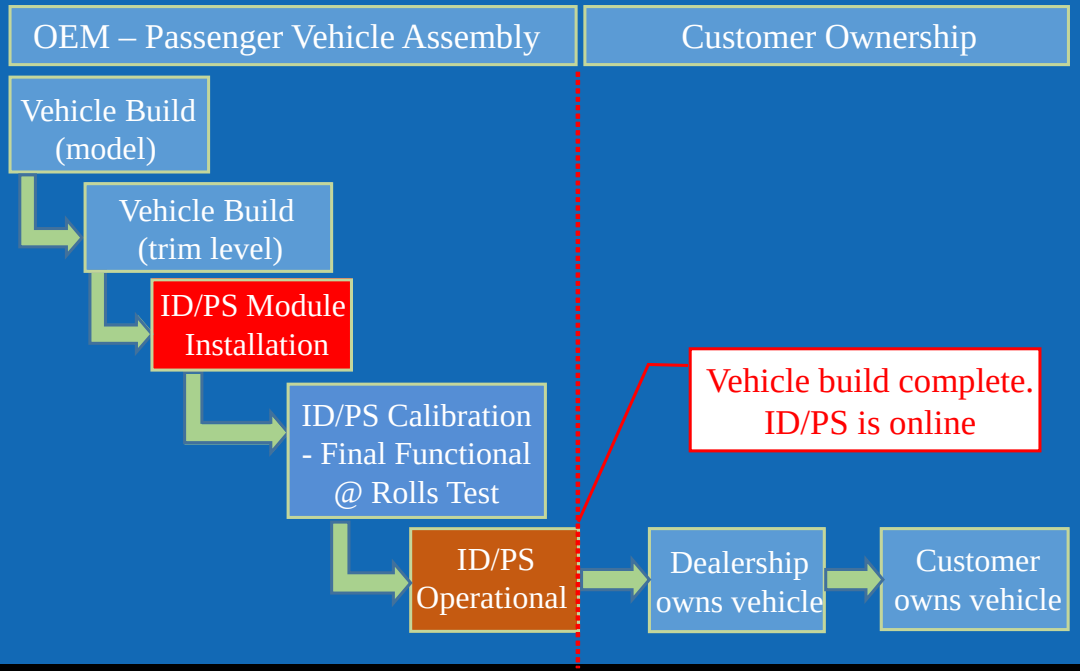
Deeper dive incremental/unique HD research gaps identified in Threat Vector Framework

- **Gap Exposition in Heavy Vehicles**
  - Tractor/Trailer – Power Line Communications (PLC) – SAE J2497
  - Tractor/Trailer – CAN Communication (Europe) – ISO 11992
  - Heavy Vehicle – J1939 Physical Packaging – easy access
  - OBD Segmentation/ Firewalling – utilized but not as centralized as light vehicle designs
  - Installation of 3rd Party Telematics – management of homogenous fleets
  - Body Builder Modules – interface to allow powertrain control by vocational integrator systems
  - CMV Electronic Logging Devices (ELD) – FMCSA mandate for digital RODS
  - Use/ Installation of Intrusion Detection Systems (IDS) – layered approach, not yet ready, but solutions available by "Argus" for CMV domain

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts (example)

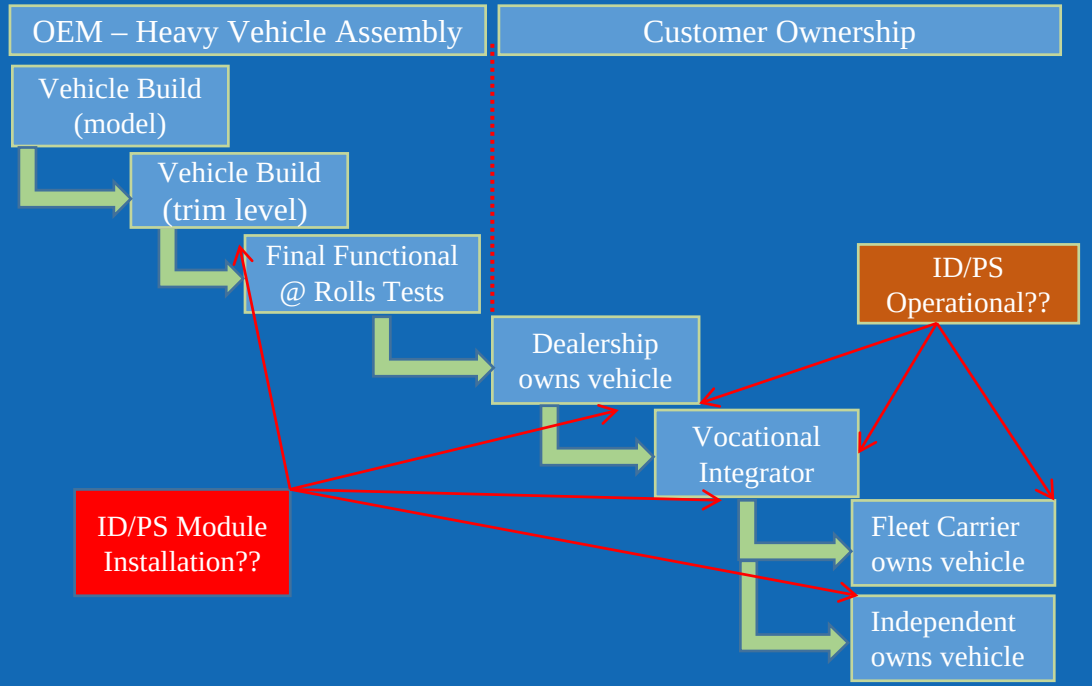
- **Intrusion Detection System: LD Vehicle**



CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts (example)

- **Intrusion Detection System: HD Vehicle**



CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Demonstrated Cases of HV Hacking

- **Public exploitation of MD/HD not as popular as passenger vehicle hacking**
  - Passenger vehicles easily accessible for DIY hacker – in your driveway
  - MD/HD vehicle access limited and $$$$ - not in everyone's driveway

- **Published HD ethical hacking projects:**
  - Univ. of Tulsa
    - "Truck Duck" diagnostic tool via "Truck in-a-box" simulator (2016)
    - NSF project: Test bed for HV cyber security experimentation (2018)
  - Univ. of Michigan (w/UMTRI support)
    - J1939 security analysis on HD via on-site Class 8 tractor (2016)

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Risk Assessment

- **Consist of UMTRI's methodology previously used on:**
  - Security of firmware and software updates in passenger vehicles
  - Utilizes aspects of NHTSA and EVITA methodologies

- **Methodology**
  - Define Threat Actors – resources/motivation
  - Define Impact Score – Aggregate of safety/financial
  - Identify Abuse Cases – w/ impact score
  - Identify Heavy Vehicle Risks

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Risk Assessment

- Threat Actors

Threat Actor	Resources	Motivation
Nation states	Well-to-very-well-funded Backed by military force	Self-defense Control Ideological
Terrorist groups	Moderately-to-well-funded Backed by militia	Control Ideological
Organized crime (OC)	Moderately-to-well-funded Backed by violence	Financial Control
Activist/ideologues/terrorists or small groups	Minimally-funded	Ideological Attention
For-profit blackhat hackers or small groups	Minimally-to-well-funded	Financial Attention
Thieves or small groups	Minimally-to-moderately-funded	Financial
Competitors	Well-Funded	Financial
Aftermarket tuners (owners or third-party).	Minimally-to-moderately-funded	Financial Sport
Owners	Minimally-funded	Financial Sport

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Risk Assessment

- Abuse Cases:
  - Attacker's end goal
  - Impact=2*safety + financial

Abuse Case	Impact Score
Coordinated, Intentional Vehicle Collisions	12
Denial of Service (DoS) of Essential Services	11
Intentional, Single-Vehicle Collision	8
Intentional Vehicle Performance Degradation	5
Remote Control of Auxiliary Functionality	4
Performance Tuning	3
Surreptitious Tracking	3
Vehicle or Contents Theft	2
Trade Secret Theft	2
Unauthorized Feature or Content Activation	2
Ransomware	1

Example:

Abuse Case	**Denial of Service (DoS) of Essential Services**			
Threat Actor	Nation state	Terrorist	Organized crime	Activist/ideologue
Probability of Success	4	3	3	2
Motivation	4	4	3	2
Safety Violation	4			
Financial Violation	3			
Impact Score	11			

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Risk Assessment

- **Heavy Vehicle Risks**
  - Malware
    - Attacker installs malware on vehicle system components (ECUs, aftermarket devices, trailer, diagnostic tools, ELD, etc.)
  - Spoofing
    - Attacker mimics/manipulates data to/from vehicle (via telematics, sensors, etc.)
  - Man-in-the-middle
    - Attacker passively siphons data
    - Attacker aggressively breaches message transport security tunnel
  - Clandestine equipment installation
    - Attacker installs rogue device

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Study Cybersecurity Practices in Heavy Vehicle Segment

- **OEM/Supplier Stakeholder "Generalized" Feedback**
  - Segmentation of J1939 bus/ use of central gateway for isolation
  - Enhanced levels of encryption
  - Integration of intrusion detection systems
  - Integration of active mitigation systems
  - Endpoint authentication/ Endpoint security management
  - Embedded hardware security modules

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Summary – So where are we at???

- HD network architectures are complex / trend towards segmented /multi-backbone design.
- HD J1939 vehicle physical interface is directly accessible and unsecured.
- Open-source J1939 communication protocol is flexible for interoperability and ease of use (plug and play) ~ there is no obscurity.
- HD interoperability allows for increased vulnerabilities due to incremental supply chain risks.
- CMV vulnerabilities offer a broad threat to homogeneous fleets ~ connected fleet management systems and electronic logging devices.
- Potential HD cyber attacks on connected fleets could yield a large socio-economic impact to the economy.
- HD threat vector landscape expands beyond what currently exists in LD domain.
- Intrusion detection systems POC in HD domain lags the LD market ~ 3-4 years.

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Thank you !

Stephen Stachowski, P.E.
smstacho@umich.edu

David LeBlanc, PhD.
leblanc@umich.edu

University of Michigan Transportation Research Institute
2901 Baxter Rd, Ann Arbor, MI

NHTSA

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES