CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

SAE Government Industry Meeting

January 24, 2018

NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Project Sponsor: **NHTSA**

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

- Identify cybersecurity items of interest or concern
- Assess CMV industry organizational awareness
- MD/HD versus light vehicles:
  - Develop framework to compare MD/HD and light vehicle cybersecurity attributes
  - Threat vector landscape, network architectures, risk assessment, lifecyle, control applications, countermeasures, etc.

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Research Questions

- White-hat hackers have demonstrated publicly that modern CAN-based vehicles can be attacked (i.e. Miller/Valasek) with limited successes.
- For MD/HDs:
  - Is there potential vulnerability to attacks like passenger vehicles?
  - To what levels are they susceptible?
  - What is the MD/HD threat-surface landscape, relative to light vehicles?
  - Can unintended vehicle control occur in the MD/HD domain?
- HD Examples: NMFTA/UMTRI (2016), U. Tulsa (2016), U. Tulsa/NSF (2018)

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Project Overview

- Internal/ External MD/HD Stakeholder Interviews
- Independent Literature Review (Passenger/MD/HD)

- Create Comparison Framework
- Identify Industry Content Areas on Security Landscape (Passenger/MD/HD)

- Create Threat Vector Framework
- Identify All Possible Threat Areas (Passenger/MD/HD)

- Discover Difference/ Similarities between Passenger and LD/MD/HD vehicles.
- Identify "Unique & Incremental" MD/HD Threat Vector Gaps

- Deep Dive into Threat Vector Impacts and other CMV Industry Attributes

- Provide Simplified Risk Assessment, Mitigation Methods, and HV Hacking insight

- Provide Comprehensive Report to NHTSA

COMPARISON FRAMEWORK

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. passenger
  - **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. passenger
  - **Vehicle Development Process:** Security design in MD/HD vs. passenger
  - **Supply Chain:** MD/HD customer requirements vs. passenger
  - **Legal Limitations:** Do laws change threat vulnerabilities /types?
  - **Compliance:** Design requirements /impacts?
  - **National differences:** MD/HD vehicles vs. passenger
  - **Organizational Structure:** Are MD/HD OEMs as prepared vs. passenger?

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

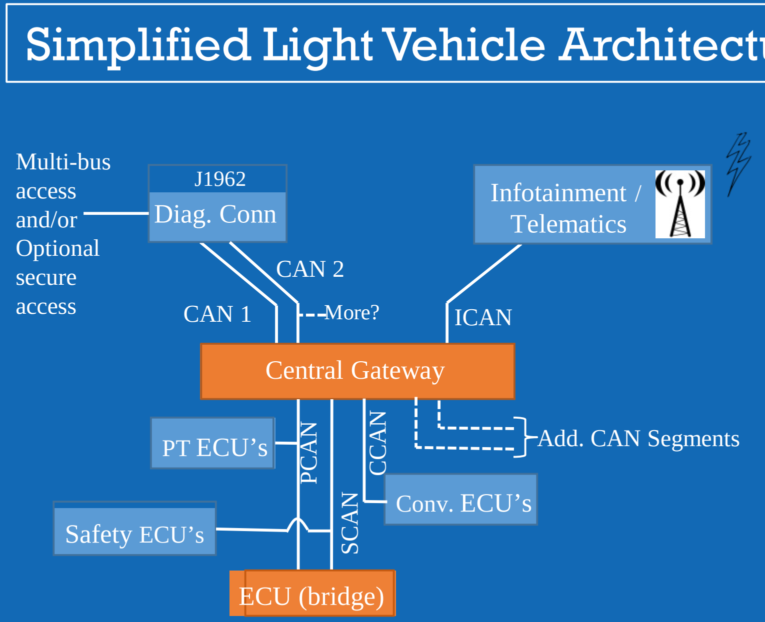
Comparison Framework

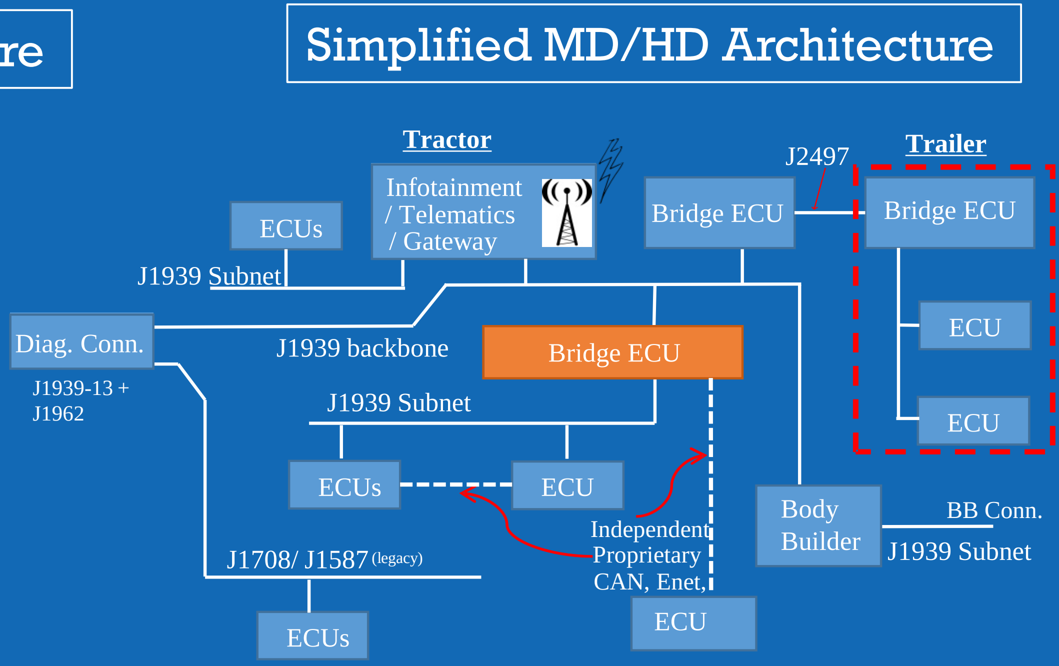
	Light Vehicles		Heavy Vehicles	
	Passenger Vehicles	Light Duty Trucks	Medium Duty Trucks	Heavy Duty Trucks
Communication Bus(s)	Proprietary CAN, MOST, Ethernet, FlexRay, VAN, LIN		J1708/J1587, J1939, & Proprietary CAN	Power Line Communication (PLC) J2497
Electronics Architecture Topology (common arch.)	• Multi-Flat CAN w/gateway(s) • OBD-II /Telematics segmented CANs w/central" gateway		Multi-Flat J1939 w/gateway(s)	
Communication Interfaces	Wired (OBD-II, USB, CD, etc.) and Wireless (Bluetooth, cellular, Wi-Fi, TPMS, OBD-II dongles, DSRC, etc.)			
Control Systems Impacting Vehicle Dynamics	• Steering: hydraulic, electro-hydraulic power assist (EHPAS), full electric power assist (EPAS) • Braking: hydraulic with electronic braking systems (EBS) (e.g. ABS, ESC, TC, RSC) • Vehicle/ trailer braking with trailer braking control (TBC) (e.g. ABS, SRW) o disc/drum brakes • Powertrain: o Engine: gas/diesel/CNG/hybrid/full electric o Transmission: auto/manual (majority automatic)		• Steering: hydraulic/manual EHPAS • Braking: Tractor/trailer hydraulic/pneumatic • Tractor/trailer coupled braking w/ trailer braking control (TBC) (e.g. ABS, SRW, ESC) o disc/drum • Powertrain: o Engine: gas/diesel/CNG/hybrid o Transmission: auto/manual	• Steering: hydraulic/manual/ EHPAS • Braking: o Tractor/trailer pneumatic EBS (e.g. ABS, ESC, RSC), (N.A.), CFC (Europe) o disc/drum • Powertrain: o Engine: diesel o Transmission: auto/manual (majority manual)
Privacy	Protect personal data	Protect personal and/or business relevant data	Protect business relevant data	
Fleet Management Systems (FMS)	• Wide-spread use of voluntary telematics for rental/ company fleets o Logistics management o Driver "event" monitoring o Remote health and tracking • Voluntary use of 3rd party OBD-II dongles for insurance benefits/ vehicle performance tracking		• Wide-spread use of voluntary telematics for rental/carrier company fleets o Logistics management o Driver "event" monitoring o Remote health and tracking o May include electronics logging of drivers' hours of service records	
Private vs. Commercial Sector	Private or Commercial		Commercial	
Customer demands	• Cost sensitive • Feature/Content driven • Multipurpose use-case		• Cost Sensitive • Specific Functional use-cases • Fleet efficiencies	
Hardware Interoperability	Interoperability variations between vehicle model components are very limited, requiring minimized supplier base (e.g. chassis, engine, and transmission options pre-defined by OEM and offer very limited customer selection flexibility)		• Interoperability variations between vehicle components are significant, integrating multiple supplier systems (e.g. chassis, engine, and transmission options are largely customer selectable) • Interoperability between tractor and trailer (tractor may interface with many trailers)	

	Light Vehicles	Heavy Vehicles
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	• Many OEMs and suppliers investigating and designing cybersecurity elements into their product development cycle • OEMs and suppliers are in process of evaluating in-vehicle anomaly detection systems • Independent evaluation of in-vehicle anomaly detection systems currently in progress at UMTRI	• Some OEMs and suppliers investigating cybersecurity elements into their product development cycle • OEMs and suppliers have not indicated use of anomaly detection systems for HV applications. • Independent evaluation of in-vehicle anomaly detection systems unknown.
Legal limitations and organized compliance	• Automotive Information Sharing and Analysis Center [ISAC] is available • No federally regulated telematics/ logging devices required for general vehicle ownership • Telematics/logging devices required on U.S. General Services Admin. (GSA) fleets[1]	• Automotive ISAC allows membership to HV OEMs and suppliers • N. American commercial drivers subject to Hours of Service regulations are required to use compliant technology to electronically record duty status - per FMCSA mandate (start Dec 2017) • Telematics/logging devices required on U.S. GSA fleets
National differences/ similarities	• U.S. European, Asian OEMs, Tier-1 suppliers are members of AutoSAR • U.S. cyber security guidelines in progress: NHTSA's draft "Cybersecurity Best Practices for Modern Vehicles" guidelines, SAE J3061 • ISO collaborating with SAE to convert J3061 guidelines into a global standard • 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 "explicit" heavy vehicle cybersecurity guidelines to date, can leverage SAE J3061 or NHTSA's draft "Cybersecurity Best Practices for Modern Vehicles" guidelines • U.S., European, and Asian OEMs utilize J1939 protocol as main vehicle backbone bus; EU also uses the KWP2000 protocol • European: Many OEMs organized implementation of Fleet Management System (FMS) specifically defined message set for 3rd party telematics integrators. Standard CAN communication between tractor and trailers which does not exist in NA. Coupling Force Control (CFC) requirement in EU. Primarily ECBS use in EU as opposed to ABS architecture in the US.
Future applications	Advanced Driver Assist Systems (ADAS) and semi-autonomous systems. Eventual introduction of fully automated driving systems.	

[1] EO 13693 subparagraphs (3 g) and (3 g iii)

Develop Comparison Framework (example)





CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Threat Vector Framework

WIRED ACCESS	DIFFERENCE	Does attack &/or mitigation translate?		Research Gap?
USB, CD, SD, Auxiliary inputs		YES	YES	NO
Diagnostic connector	Connector	YES	YES	NO
▪ Diagnostic Tools	Per OEM	YES	YES	NO
▪ Network access	CAN difference	YES	PARTIAL=>	INCREMENTAL
▪ OBD dongles (aftermarket)	Form factor	YES	PARTIAL=>	INCREMENTAL
▪ Diagnostic Standards	Standards	YES	PARTIAL=>	INCREMENTAL
12-Volt Accessory Outlet		NO	-	**UNIQUE**
Body Builder Interface[6]	Unique to CMV	NO	-	**UNIQUE**
Trailer PLC (bridge module)[6]	Unique to CMV	NO	-	**UNIQUE**
WIRELESS				
GSM/CDMA, GPS, Satellite, Digital Radio (HD)		YES	YES	NO
Bluetooth, TPM, Remote keyless entry, WiFi, DSRC		YES	YES	NO
RFID Keys	CMV: Not avail			
MITIGATION METHODS				
Secure Architectures	In Process	YES	PARTIAL=>	INCREMENTAL
Security Applications	"	YES	NO	**UNIQUE**
Secure Development Process	"	YES	PARTIAL=>	INCREMENTAL
Secure Development Tools	Available	YES	YES	NO
Security Hardware	"	YES	YES	NO
Sanity Checks	"	YES	PARTIAL=>	INCREMENTAL

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts

Deeper dive into unique cyber aspects of heavy vehicle identified in Tasks 2 and 3.

- **Extended 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

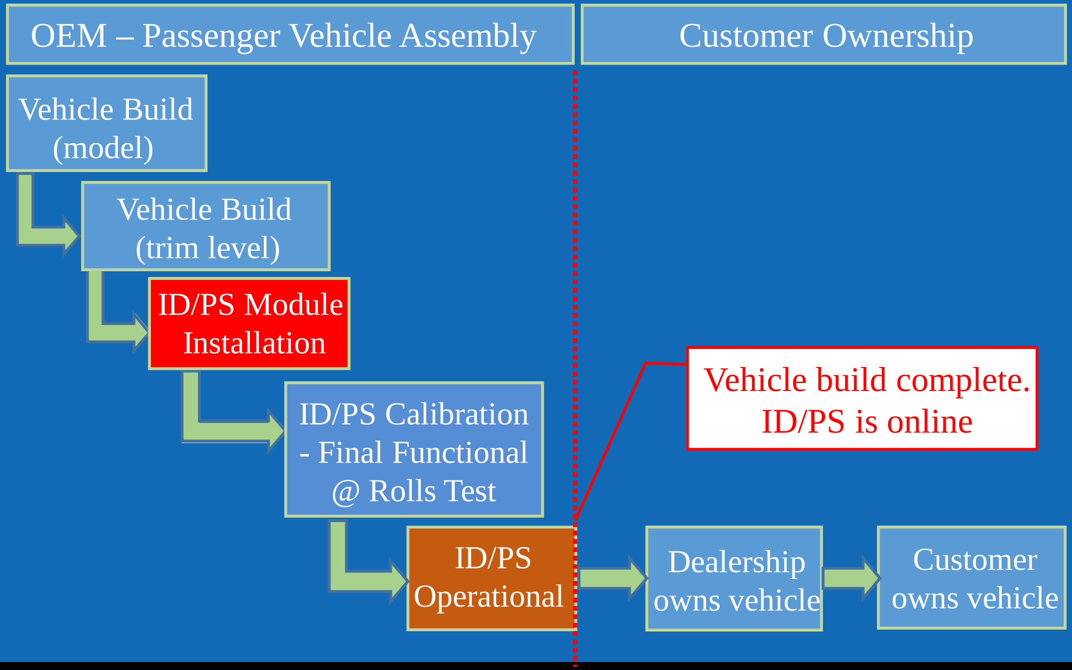
CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts (example)

Passenger Vehicle

Intrusion Detection System:

- Production Integration



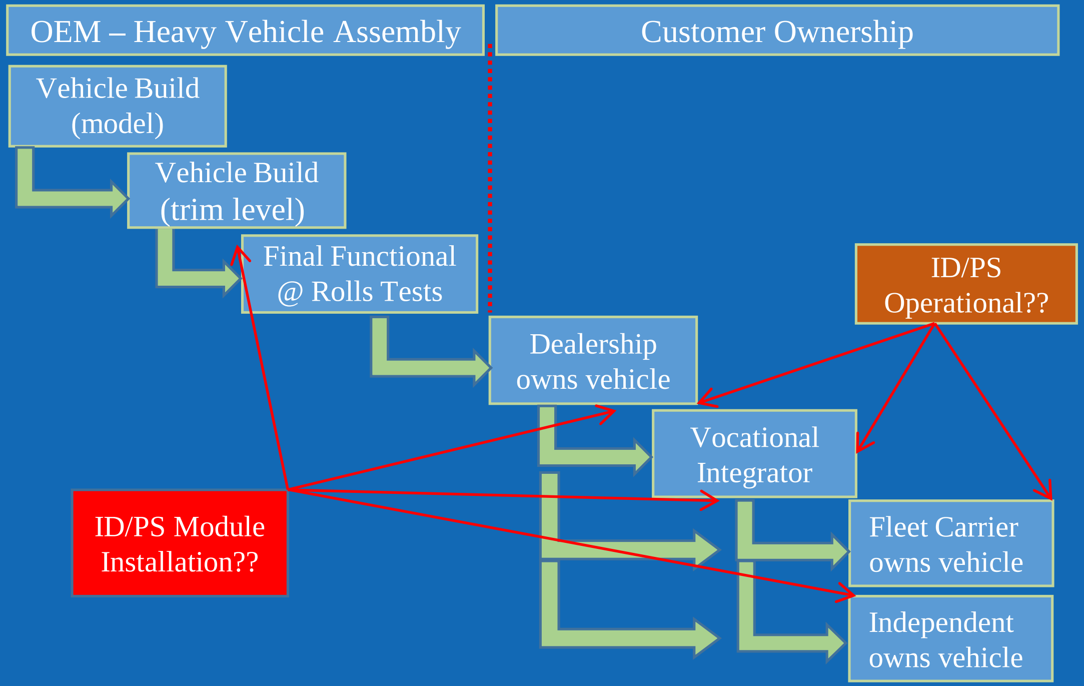
CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Investigate Impacts (example)

MD/HD Vehicle

Intrusion Detection System:

- Production Integration?



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

- **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, replay attacks, injects anomalous messages, 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 for “Next Steps”**
  - 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-standard 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 P.O.C. in HD domain lags the passenger market ~ 3-4 years.

Thank you !

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

David LeBlanc, PhD., UMTRI
leblanc@umich.edu

Arthur Carter, NHTSA
Arthur.Carter@dot.gov

NHTSA

CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES