CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

SAE Government Industry Meeting
January 24, 2018
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, lifecycle, control applications, countermeasures, etc.
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?

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
- Provide Comprehensive Report to NHTSA
- Provide Simplified Risk Assessment, Mitigation Methods, and HV Hacking insight
- Deep Dive into Threat Vector Impacts and other CMV Industry Attributes
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

<table>
<thead>
<tr>
<th>Light Vehicles</th>
<th>Light Duty Trucks</th>
<th>Medium Duty Trucks</th>
<th>Heavy Vehicles</th>
<th>Proprietary CAN, MOST, Ethernet, FlexRay, VAN, LIN</th>
<th>J1-861/2107, J1939, &amp; Proprietary CAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication Bus(es)</strong></td>
<td></td>
<td></td>
<td></td>
<td>Proprietary CAN</td>
<td></td>
</tr>
<tr>
<td><strong>Electronics Architecture</strong></td>
<td>Multi Flat CAN w/ gateway(s)</td>
<td>OBD-II</td>
<td>Multi Flat CAN w/ gateway(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Communication Interfaces</strong></td>
<td>Wired (OBD-II, USB, CD, etc.) and Wireless (bluetooth, cellular, Wi-Fi, TPMS, OBD-II, dsrc, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Control Systems Integration Dynamics</strong></td>
<td>Steering, hydraulic/elec hydro-pwr assist (EPAS), full electric power assist (EPAS)</td>
<td>Braking hydraulic with electronic braking systems (EBS) (e.g. ABS, ESC, TC, ESC)</td>
<td>Tractor/trailer hydraulic/pneumatic braking (TCB) (e.g. ABS, SRW, ESC)</td>
<td>Tractor trailer coupled braking system (TCB) (e.g. ABS, SRW, ESC)</td>
<td></td>
</tr>
<tr>
<td><strong>National Differences/Similarities</strong></td>
<td>U.S. European, Asian OEMs, Tier-1 suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Future Applications</strong></td>
<td>Advanced Driver Assist Systems (ADAS) and semi-autonomous systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Life Cycle and Maintenance
- **19 years, 150,000 miles**
- **19-36 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
- Some OEMs and suppliers investigating cybersecurity elements into their product development cycle
- Some OEMs and suppliers have not indicated use of any automated driving systems for HV applications
- Independent evaluation of vehicle anomaly detection systems unknown
- SAE allows membership to HV OEMs and suppliers
- Non-American commercial vehicles subject to hours of service regulations require use complaint technology to electronically record duty status - per FMCSA mandate (start Dec 2017)
- Telematics logging devices required on U.S. GSA fleets

### Privacy

#### Fleet Management Systems (FMS)
- Protect personal data
- Protect personal and business relevant data
- Wide spread of voluntary telemetry for rental company fleets
- Logistics management
- Driver “even” monitoring
- Remote health and tracking
- Voluntary use of 3rd party and IIoT for insurance benefits vehicle performance tracking

#### Future Applications
- Advanced Driver Assist Systems (ADAS) and semi-autonomous systems
- Eventual introduction of fully automated driving systems

### Hardware Interoperability

#### Interoperability
- Interoperability variations between vehicle and component models are very limited, requiring minimized supplier base (e.g. chassis, engine, and transmission options pre-defined by OEMs and interoperability variations between vehicle components are significant, integrating multiple suppliers systems (e.g. chassis, engine, and transmission options are largely customer selectable)
- Interoperability between tractor and trailer (hitches may interfere with many trailers)
Develop Comparison Framework (example)

Simplified Light Vehicle Architecture

Central Gateway
- J1962 Diag. Conn
- CAN 1
- CAN 2
- CAN 1
- CAN 2
- More?
- ICAN
- PCAN
- CCAN
- Add. CAN Segments
- PT ECU's
- Safety ECU's
- ECU (bridge)

Infotainment / Telematics

Simplified MD/HD Architecture

Tractor
- Bridge ECU
- J1939 backbone
- J1939 Subnet
- ECU
- ECU
- ECU
- ECU
- ECU
- J1939 Subnet
- J1962
- J1939-13 + J1962
- J1708/ J1587 (legacy)
- Independent Proprietary CAN, Enet

Trailer
- Bridge ECU
- J2497
- ECU
- ECU
- BB Conn. J1939 Subnet

Body Builder
- J1939 Subnet
- Gateway

Develop Comparison Framework (example)
# Cybersecurity Research Considerations for Heavy Vehicles

## Threat Vector Framework

<table>
<thead>
<tr>
<th>Wired Access</th>
<th>Difference</th>
<th>Does attack &amp;/or mitigation translate?</th>
<th>Research Gap?</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB, CD, SD, Auxiliary inputs</td>
<td></td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Diagnostic connector</td>
<td>Connector</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>• Diagnostic Tools</td>
<td>Per OEM</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>• Network access</td>
<td></td>
<td>YES</td>
<td>PARTIAL⇒</td>
</tr>
<tr>
<td>• OBD dongles (aftermarket)</td>
<td>Form factor</td>
<td>YES</td>
<td>PARTIAL⇒</td>
</tr>
<tr>
<td>• Diagnostic Standards</td>
<td>Standards</td>
<td>YES</td>
<td>PARTIAL⇒</td>
</tr>
<tr>
<td>12-Volt Accessory Outlet</td>
<td></td>
<td>NO</td>
<td>-</td>
</tr>
<tr>
<td>Body Builder Interface</td>
<td></td>
<td>NO</td>
<td>-</td>
</tr>
<tr>
<td>Trailer PLC (bridge module)</td>
<td></td>
<td>NO</td>
<td>-</td>
</tr>
</tbody>
</table>

## 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 |
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
Investigate Impacts (example)

MD/HD Vehicle Intrusion Detection System:

• Production Integration?
CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES

Risk Assessment

- Threat Actors

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Resources</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation states</td>
<td>Well-to-very-well-funded</td>
<td>Self-defense</td>
</tr>
<tr>
<td></td>
<td>Backed by military force</td>
<td>Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ideological</td>
</tr>
<tr>
<td>Terrorist groups</td>
<td>Moderately-to-well-funded</td>
<td>Control</td>
</tr>
<tr>
<td></td>
<td>Backed by militia</td>
<td>Ideological</td>
</tr>
<tr>
<td>Organized crime (OC)</td>
<td>Moderately-to-well-funded</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td>Backed by violence</td>
<td>Control</td>
</tr>
<tr>
<td>Activist/ideologues/terrorists or small groups</td>
<td>Minimally-funded</td>
<td>Ideological</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attention</td>
</tr>
<tr>
<td>For-profit blackhat hackers or small groups</td>
<td>Minimally-to-well-funded</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attention</td>
</tr>
<tr>
<td>Thieves or small groups</td>
<td>Minimally-to-modernly-funded</td>
<td>Financial</td>
</tr>
<tr>
<td>Competitors</td>
<td>Well-Funded</td>
<td></td>
</tr>
<tr>
<td>Aftermarket tuners (owners or third-party).</td>
<td>Minimally-to-modernly-funded</td>
<td>Financial</td>
</tr>
<tr>
<td>Owners</td>
<td>Minimally-funded</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sport</td>
</tr>
</tbody>
</table>
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
CYBERSECURITY RESEARCH CONSIDERATIONS FOR HEAVY VEHICLES