# NMFTA Heavy Vehicle Cyber Security White Paper Executive Summary

In 2015 NMFTA conducted research regarding the status of heavy vehicle cyber security and developed a white paper outlining our findings. The initial research yielded a rather large amount of information, which -- in the end -- necessitated a larger document. The scope further expanded as we identified several topics and introductory concepts that we felt we needed to cover in order to present a logically complete survey of the current state of cyber security for heavy vehicles.

We have tried to summarize the basic overall findings of the paper in this memo. However, we would strongly recommend reading the entirety of the paper for a better understanding of the issues and current state of affairs. Furthermore, the reference section of the paper contains an annotated listing of many of the key resources identified in the course of developing the paper. Those key documents provide additional information for anyone who might wish to take a deep dive on any particular issue; but, for the general reader, these supporting materials may be safely set aside.

**Overview**

In 2013 there were approximately 10.6 million registered heavy vehicles in the US. It is estimated that the heaviest of vehicles, class 8 truck tractors, see a service life of 7-8 years, with approximately 150,000 new class 8 trucks on the road each year.

Heavy vehicles -- while having some potentially material differences -- are substantially similar in architecture to light vehicles. Therefore, there is no reason to believe that the heavy duty vehicles are less vulnerable than the average automobile. Indeed, while passenger vehicles are just now becoming “connected" through telematics systems such as OnStar, etc., heavy vehicles have been more pervasively “connected” through satellite and cellular communications connecting to telematics, fleet management, and engine management applications for quite some time.

The hardest part of hacking vehicles is really gaining access, ideally *remote* access. Inherently, heavy vehicles have more avenues for remote access than light vehicles. And, they also have a broader attack surface. Heavy vehicles are at least as computerized as light vehicles. And, with hundreds and sometimes thousands of virtually identically configured vehicles, commercial truck fleets have a high level of homogeneity that can enable an adversary to economically develop viable exploits for large numbers of vehicles simultaneously.

In the paper, we have endeavored to survey the available literature and knowledge on heavy vehicle engine system design, security vulnerabilities, the potential consequences of a breach and current hacking activities. We also consider the current state of affairs on *who is doing what*, if anything, to secure heavy vehicles from technical research and government policy perspectives.

Due the near absence of experimental data on heavy vehicles, we have had to research passenger vehicle security and analytically extrapolate how that information applies to heavy vehicles. The lack of heavy vehicle research is, arguably, due to a lack of funding for -- and the greater expense of -- experimenting on heavy vehicles. It is easier to get a Toyota Prius to experiment on than a recent model year Kenworth truck. A large amount of the research in this area is being funded by government agencies and most contracted to independent security researchers ('hackers'), universities and corporations. We cannot exclude the possibility that more data and information exists specifically for heavy vehicles. However, such data may be currently unpublished or otherwise not have been identified within the limited timeframe that we have had to prepare this paper.

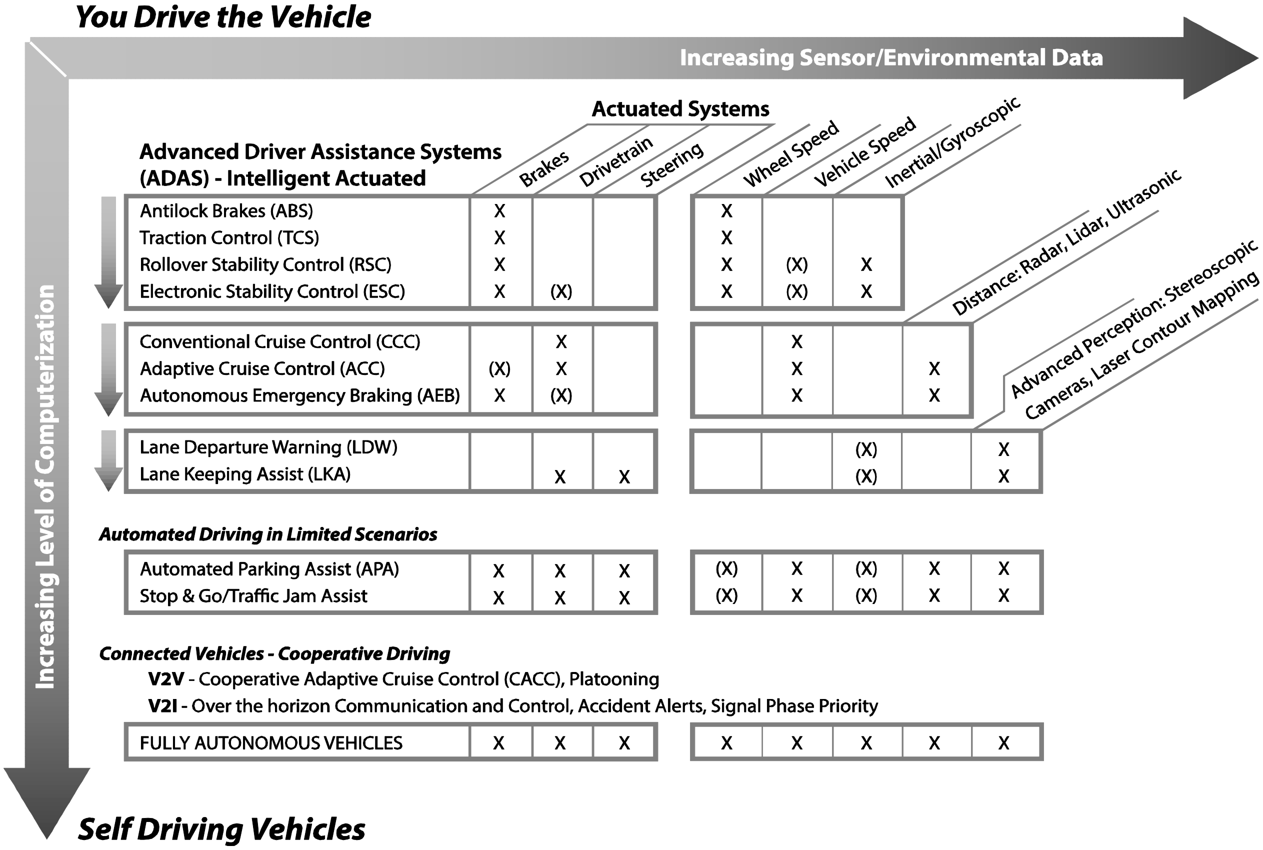
## Heavy Vehicle System Design

Today's vehicle is composed of a number of interconnected sensors, actuators and microprocessors called Electronic Control Units (ECUs). The local network that connects them all is called a control area network (CAN). When first implemented, the specifics of the network design and the way in which ECUs would communicate with each other on the network were specific to each Original Equipment Manufacturer (OEM). OEMs were able to leverage the ECUs in pre-production testing for design verification, testing, and quality control. Diagnostic routines helped verify assemblies on the production line. And, once on the road, the ECUs could monitor, log, and report operating data and analyze the results with respect to expected (and legislatively mandated) performance criteria.

All modern light vehicles have an OBD-II SAE J1962 (ISO 15031-3) connector within easy reach of the steering wheel. This connector is usually simply referred to as the OBD-II connector. Although the OBD-II standard initially allowed for multiple network standards, 2005 EPA regulations required model year 2008 cars (and thereafter) to all use a well define Controller Area Network (ISO 11898) for communication between the OBD-II diagnostic port and engine ECUs.

Heavy vehicle network communications are also based on the CAN (ISO 11898) standard. However, the manner in which CAN is fully implemented for these vehicles in the SAE J1939 standard differs from how it is implemented in lighter vehicles. SAE J1939 is, in fact, a much more complete and integrated set of standards than those governing lighter vehicles. However, SAE J1939 still reveals similar weakness in CAN bus communications and ECU design as found in light vehicles.

Computer and communication advancements continue to drive feature evolution in both passenger and heavy vehicles. Some ECUs now have processing capabilities rivaling that of many standalone PCs, complete with full operating systems. The costs of implementing communication technologies (both old and new) such as RFID, Bluetooth, Wi-Fi, DSRC, cellular and satellite continues to fall, enabling computer (ECU/ functionality) integration within the car, between vehicles (V2V), between vehicles and national infrastructure (V2I), and the world (the Internet). In the ongoing quest for fuel economy, traffic and cargo efficiency, driver safety and comfort, more safety critical features are being computerized; and, then interconnected with less carefully designed secondary systems. The most disconcerting part of our feature survey is the continued absence of evidence that cyber security is a true priority.


You Drive the Vehicle
Increasing Sensor/Environmental Data
Increasing Level of Computerization
Self Driving Vehicles

Actuated Systems

| Advanced Driver Assistance Systems (ADAS) - Intelligent Actuated | Brakes | Drivetrain | Steering | Wheel Speed | Vehicle Speed | Inertial/Gyroscopic | Distance: Radar, Lidar, Ultrasonic | Advanced Perception: Stereoscopic Cameras, Laser Contour Mapping |
|---|---|---|---|---|---|---|---|---|
| Antilock Brakes (ABS) | X | | | X | | | | |
| Traction Control (TCS) | X | | | X | | | | |
| Rollover Stability Control (RSC) | X | | | X | (X) | X | | |
| Electronic Stability Control (ESC) | X | (X) | | X | (X) | X | | |
| Conventional Cruise Control (CCC) | | X | | | X | | | |
| Adaptive Cruise Control (ACC) | (X) | X | | | X | | X | |
| Autonomous Emergency Braking (AEB) | X | (X) | | | X | | X | |
| Lane Departure Warning (LDW) | | | | | | (X) | | X |
| Lane Keeping Assist (LKA) | | X | X | | | (X) | | X |
| ***Automated Driving in Limited Scenarios*** | | | | | | | | |
| Automated Parking Assist (APA) | X | X | X | (X) | X | (X) | X | X |
| Stop & Go/Traffic Jam Assist | X | X | X | (X) | X | (X) | X | X |
| ***Connected Vehicles - Cooperative Driving*** | | | | | | | | |
| **V2V** - Cooperative Adaptive Cruise Control (CACC), Platooning | | | | | | | | |
| **V2I** - Over the horizon Communication and Control, Accident Alerts, Signal Phase Priority | | | | | | | | |
| FULLY AUTONOMOUS VEHICLES | X | X | X | X | X | X | X | X |

## Heavy Vehicle Cyber Security

There is a long list of known and documented vulnerabilities and hacks for passenger cars based primarily on the CAN bus design itself, and how CAN messages can in turn access, and compromise poorly protected ECUs.  Engineers seem to have assumed that the computerized vehicle would not have to operate in a hostile environment. While initial vehicle hacking required physical access, wireless attack surfaces are now ever present.

Researchers have had no trouble building a CAN network packet analyzer to deduce what the different messages were and then inject fake (spoofed) messages onto the CAN network which then caused ECUs to take actions based on the fake messages. There is no authentication or origination check built into the design, so an ECU originally designed to control windshield wipers could possibly be used to send a message regarding vehicle speed.

One does not really need to take over ECUs and take such dramatic action on a heavy vehicle to cause problems. It is possible to simply “tweak” a couple of sensors with bad data to cause problems. In certain extreme cases, it may even turn the engine off. While not catastrophic it would have significant economic consequences, especially if it impacted more than one vehicle simultaneously.

In one research paper we reviewed, a simple “self-destruct” was built for a 2009 vehicle which displayed a count down on the dashboard accompanied with more and more frequent honking of the horn. At the end of the countdown, the doors were locked (and rendered unable to open manually) thereby trapping the passenger in the vehicle as the engine was then killed. The attack was done using spoofed messages to functional components and required less than 200 lines of code.

Heavy vehicles suffer from the same vulnerabilities as discussed above but also have more external attack vectors and a certain homogenous nature which presents an even broader attack surface. Most modern truck engine manufacturers, such as Detroit Diesel and Cummins, are working to integrate connectivity almost directly into the engine for real time diagnostic and engine troubleshooting over regular cellular networks. This means that, as a matter of course, heavy vehicles have a higher percentage of integration with remote access telematics than automobiles. Since these telematics systems are used in trucks traveling across the country with varying degrees of cellular service, they most likely use the lowest common denominator (even 2G) in terms of protocol and service specification and equipment. Any time a communication system relies on older or outdated technology, there exists a security risk.

Additionally, fleet operators have added 3rd party communication systems such as QualComm and PeopleNet. These systems plug directly into the J1939 onboard diagnostic ports of the truck engines and connect them back directly to centralized servers, service centers and computer workstations. This is done either through 3G/4G cellular or satellite connectivity. This is problematic for a number of reasons. First, it adds another IP address to each vehicle, i.e. could possibly be seen/accessed from the Internet anywhere around the world; and, secondly, it centralizes access to whole fleets of trucks from a single server infrastructure located either at the service provider or the fleet operator. Truck fleets tend to be homogenous by operator as most companies have standardized on a single -- or small number of -- truck make(s)/model(s) and engine manufacturer(s) for more cost effective maintenance operations. While economically effective, this introduces a large systematic vulnerability for individual fleet operators by making it possible to leverage a single attack or design for self-replicating malware against an entire fleet.

Our research demonstrates that the issue of vehicle cyber security is not a topic that we must address sometime in the *future*, but is a serious problem upon us *today*. Real world hacks are being done against light vehicles. The attacker's capabilities have grown rapidly in sophistication and reach. Hackers have established tools for interfacing with vehicle network traffic, growing libraries of control command messages, and commercial tools to reverse engineer the OEM programming of most any ECUs and replace it with arbitrary malicious code. As reported just this summer, several vulnerabilities in the infotainment system on certain Chrysler & Jeep vehicles allowed security researchers ('white hat' hackers) to conclusively demonstrate that they could have taken arbitrary control of some 1.4 million vehicles -- driving them off the road at will -- from anywhere in the world using an Internet connection. All indications point to the likelihood that our industry will be targeted in short order, if it is not being targeted already.

Our review of academic literature on vehicle (cyber) security shows that research remains focused on what should or could be done in the *medium to long term future* to secure vehicles. Conspicuously absent is information on what has been done to harden vehicles *today*. Indeed, we find that the most promising near term protections (e.g. intrusion detection systems (IDS)) are still far from production.

And, in reviewing current ongoing legislative activity regarding vehicle cyber security we found that -- while recent news stories covering passenger vehicles have notably caught the interest of the House and Senate -- there is very little legislative work on heavy vehicle cyber security. It seems that current legislative activity is concentrated on preliminary information gathering, ambiguous consumer based legislation, all with a focus on automobiles.

## Conclusion

Based on our review of available literature, studies, and standards, as well as our discussions with experts -- we have concluded that significant cyber security vulnerabilities exist in heavy vehicles; vulnerabilities which can be most likely be exploited remotely and/or in large numbers. Previous studies and our own analysis conclude that there is the potential for significant impacts from even small, localized vehicle cyber security exploits. However, given the real potential for large scale exploitation of heavy vehicle cyber vulnerabilities, the consequence could be catastrophic. It is therefore advisable that we consider the cyber security of heavy vehicle transportation seriously and urgently.

Most organizations dramatically underestimate the costs they are likely to bear if their computers are compromised and under invest in protecting their assets. The same holds true of heavy vehicles. In the full paper, we have outlined a set of recommendations that we urge carriers to consider. These recommendations include short term actions which can be implement to better protect fleets and heavy vehicles by reducing vulnerabilities as well as strategies to react, mitigate and to recover from an attack. We would strongly advise that the members review and distribute this information within their company for consideration by appropriate officers, managers and staff. Additionally, the paper contains recommendations for medium and long term actions which can help our industry push for better product security and more effective responses to eventual attacks.